Issued by: Nexi SPA Version: 20.4 Issued on: 20/06/2024

Technical Specifications for Integration with the XPay Payment Gateway

TABLE OF CONTENTS

Table of Contents **2**
Revisions **10**
XPay payment gateway **15**
Configuration **17**
Easy Payment **19**
Base code 21
Initiation Message 21
Cancellation 27
Result Message 28
One Click Payment 34
Oneclick payment via merchant site 34
Oneclick Payment via checkout page 39
Recurring Payment 58
Activation and/or first payment 58
Management of Recurring Payments/Subsequent Payments 62
Multi-Currency Payment (DCC) 64
Payment via Link 66
Pay-by-Link Link Request 66
Regenerate Pay-by-Link link 73
Pay-by-Link Report 77
Payment Methods **81**
Google Pay 86
API Integration 89
Apple Pay 96
API Integration 100
American Express 103
JCB 104
UnionPay 105
Bancomat Pay 106
MyBank 108
AliPay 111
WeChat Pay 113
Giropay 115
iDEAL 117
Bancontact 120

EPS - Electronic Payment Services 122
Przelewy24 124
Skrill 127
Skrill 1tap 129
PayU 131
Blik 133
Multibanco 135
Satispay 137
Amazon Pay 139
Integrated Payments 141
Management change amount based on shipping address 146
Paypal 149
Paypal - Pay in 3 installments 152
Oney 155
PagoDIL 163
Pagolight 172
Deposit Methods 173
XPay Build 174
Card data collection form 176
Basic payment 189
Recurring Payment 193
First payment 193
Subsequent Payment 200
OneClick Payment 207
First payment 207
Subsequent payment 215
Card Renewal 217
Card Verification 222
3D Secure Management 226
Alternative payment methods 228
Lightbox 232
Payment Management 233
Recurring Payment 238
First Payment 239
Recurring Subsequent Payment 240
OneClick Payment 241
First Payment 242

Recurring Subsequent Payment 242
IFRAME 243
Server to Server 244
3D Secure Payments 245
MOTO Payments 253
Payments with External 3D Secure MPI 257
MIT-CIT-ASI 261
Recurring Payment - One Click Payment 267
3D Secure Card Verification 268
3D Secure First Payment 275
OneClick 3D Secure Subsequent Payment 285
Recurring Payment 296
Card Renewal 3D Secure 301
Contract Update 312
Recurring MOTO Subsequent Payment 322
First Payment 322
Recurring Subsequent Payment 327
Multi-Currency Payment 331
Verification 332
Generate XpayNonce 334
Payment 339
Plugin CMS 343
Storeden 344
Setup 344
Support 344
Italiaonline 345
Setup 345
Support 345
Shopify 346
Setup 346
Support 346
Wordpress 347
XPay 347
XPay Build 354
Prestashop 362

XPay ... 362
XPay Build ... 368
Magento ... 376
Magento 2 ... 376
Magento 2 Build ... 383
BigCommerce ... 391
Installation ... 391
Configuration ... 391
Payment methods ... 392
Opencart ... 394
Installation ... 394
Configuration ... 394
Test and production ... 395
Payment methods ... 395
Payment flow ... 397
Farmakom ... 399
Setup ... 399
Support ... 399
Zencart ... 400
Installation ... 400
Configuration ... 400
Test and production ... 401
Payment methods ... 401
Payment flow ... 403
Salesforce ... 405
Setup ... 405
Support ... 405
OsCommerce ... 406
Installation ... 406
Configuration ... 406
Test and production ... 407
Payment methods ... 408
Payment flow ... 409
SmallPay ... 411
Setup ... 411
Support ... 411

Virtuemart 412
Installation 412
Configuration 412
Test and production 414
Payment methods 414
Payment flow 415
MigliorShop 417
Setup 417
Support 417
ReStore 418
Setup 418
Support 418
eDock 419
Setup 419
Support 419
LifePay 420
Installation 420
Support 420
Pcommerce 421
Installation 421
Support 421
Ecwid 422
Installation 422
Support 422
SAP Commerce Cloud 423
Installation 423
Support 423
Scontrino 423
SDK for app 424
Introduzione 424
IOS SDK 425
Getting Started 425
Easy Payment 429
One tap Payment 433
Recurring Payment 434

Native Form 436
Apple Pay 442
Jailbreak Control 445
ANDROID SDK 446
Getting Started 446
Easy Payment 450
One tap Payment 453
Recurring Payment 455
Native Form 456
Payment Chrome Custom Tabs 462
Google Pay 466
Root Control 468
SERVICES AVAILABLE ON ANDROID AND IOS SDKS 469
Back office Deposit 469
Contract Management 490
Hosted Payments 499
Subsequential First Payment 508
Recurring/OneClick 524
Varie 532
3D Secure 2.2 536
3D Secure 2.2 management via API 537
3D Secure 2.2 management through redirection 543
Back Office API 549
Deposit 550
Reversal/Refund 552
Order Details Query 555
Order List 561
Report 565
Warning 569
Active payment methods 572
Incasso senza Pensieri 576
Payment 577
Guaranteed booking 577
Guaranteed booking with penalty 589
Prepaid Refundable 601
Prepaid Not Refundable 615
Bundle 626

API 641
Structure insertion 641
Inserting terms and conditions 648
Modification of terms and conditions 651
Delayed Charge 653
Incremental 657
Payment No Show 662
Extension Report 666
Loading of booking data 670
Bundle 726
Deferred and Extended Collection 742
Deferred collection 742
Extended collection 743
Evolved Tokenization 748
Notifications 748
Tokenization details 751
Additional services 755
Contract Management 755
Loading Contracts from POS Transactions 756
Contract Cancellation 759
Contract Disabling 761
Contract Enabling 763
Contract Query 765
Contract Details 768
Contract Status 771
Control Management 776
Adding to Blacklist 777
Cancellation from Blacklist 779
Checking Existence in Blacklist 782
Blacklists 785
Verification of Tax Code/PAN Pairing 787
Removing Tax Code/PAN Pairing 790
List of Associated Tax Codes/PANs 793
TABLES AND CODING 796
Restful API Error Codes Table 796
Coding: resultCode 798
Coding: message 800

Coding: languageId 802
Coding of DCCcurrency codes for DCC 803
Transaction Type Coding 804
Card Type Coding 806
ECI, XID and CAVV Coding 807
VAT Codes 808
Invoice Status Code 808
SDK iOS Version 809
MIT framework parameters 810
HTTP/XML API 813
Server to Server Payments 813
Payment 813
Codebase 815
Payment for CardOnFile/Recurring/OneClick Registration 827
Payment on Registered Contracts 829
Payment with External 3D Secure MPI 830
Generating Pay-by-Link Links 836
Codebase 837
Recurring/Card on File Payment 846
Back Office API 850
Deposit/Cancellation/Refund 850
Order Query 855
Order List 862

REVISIONS

Version	Date	Author	Description
10.8	09/02/2017	Nexi	Drafting
10.9	04/04/2017	Nexi	Addition of PayPal deferred deposit management and PayPal recurring/CardOnFile payments management
11.0	09/05/2017	Nexi	Revision
11.1	01/09/2017	Nexi	Fixed Payment error on S2S/ addition enrolled card on file contract on hosted fields
11.2 11.3 11.4	18/09/2017 24/10/2017 08/03/2018	Nexi Nexi Nexi	Addition link of GitHub example Rebranding Added Apple Pay Paragraph / Typo Error fixed
12.0	24/5/2018	Nexi	Added XPay Build, Klarna, Paypal Paragraph Updated SDK description. Updated disposition description . Further Typo Error fixed.
13.0	24/05/2018	Nexi	Added Amazon Pay section
13.1	30/06/2018	Nexi	Fixed minor errors
13.2	30/06/2018	Nexi	Removed Hosted Fileds section
13.3	11/07/2018	Nexi	Updated Amazon Pay Section
14.0	02/10/2018	Nexi	Added Google Pay section Added Lightbox section Added Personalization section Fixed minor errors
14.2	24/10/2018	Nexi	Added Oneclick new payment method
15.0	04/12/2018	Nexi	Added API download report Added API Google Pay Added API 3DS subsequent payment Added APM WeChat e Alipay Updated SDK section

			Fixed minor errors
15.2	28/03/2019	Nexi	Electronic Billing section added Added 3D Secure 2.0 section Added ReportPay-by-Link API and Contract Status Fixed minor errors
16.0	01/04/2020	Nexi	Added recurring payments with Apple Pay, Google Pay, Amazon Pay, Masterpass Subsequent payments for OneClick transactions changed New mode selectedcard New Lightbox mode with XPay Build New alternative payment methods: GiroPay, iDEAL, Bancontact, EPS, Przelewy24. New American Express and Diners sections. New section "Payment methods" Added OneClick payments with XPay Build
16.2	28/07/2020	Nexi	Added Bancomat Pay and MyBank sections Added card renewal API Added Warning API Added timeout field to define payment timeouts for individual transactions Fixed 3D Secure 2.1 fields format Added new esito_informazioniSicurezza parameter Fixed minor errors
17.0	16/09/2020	Nexi	Added section dedicated to XPay plugins Added separate fields in XPay Build IOS SDK Useful information about supported WebView Fixed minor errors
18.0	17/05/2021	Nexi	New alternative payment methods: Skrill, Skrill 1tap, PayU, Blik, Multibanco, PoLi New section JCP, UPI

			New file batch v 3.7 New 3dsDinamico parameter
18.6	30/07/2021	Nexi	New alternative payment methods PagoinConto, Oney New 3DSDinamico parameter New "soft decline" outcome in the outcome encoding table and among optional parameters S2S services Updated "Transaction type coding" table New "Rigenera link Pay-by-Link" API New "Update contract" API New "Circuit Tokenization" service Moved dedicated APM parameters from Simple Payment sections under each individual APM, Added more information about scheduled/unscheduled payments, Fixed minor errors
18.7	10/09/2021	Nexi	New plugin CMS Lifepay
19.0	16/12/2021	Nexi	New types of deferred and delayed collection in the Incasso Senza Pensieri section Removed pre-authorization from "Incasso senza pensieri" New Extension Report API Added New BigCommerce CMS plugin Removed APM Masterpass Added list of banks supported with Klarna Fixed minor errors
19.4	31/03/2022	Nexi	Added VPay and Visa Electron in payment methods UPI/JCB/Bancomat Pay: added oneclick payments Build/Lightbox Improved Information Privacy Satispay alternative payment method added Diners circuit removed PagoinConto specific outcome additions MyBank added incompatibility with iFrame XPay Build added section dedicated to alternative payment methods Minor fixes

19.6	30/06/2022	Nexi	Added new PCommerce plugin PagoinConto: startup parameters modified Improved results coding sections Added dedicated Batch File section Added API for retrieving active payment methods on a terminal New Nexi SDK version for Android and iOS Minor fixes
20.0	19/01/2023	Nexi	Google Pay: added new native integration API Google Pay: updated compatibility Bancomat Pay: reversals entered Removed POLI payment method Easy Payment: added more details in notification section Added recurrences with Apple Pay and Google Pay Satispay: reversal notes added Minor fixes
20.1	01/03/2023	Nexi	Fixed GPay compatibility notes
20.2	26/05/2023	Nexi	PayPal: updated activation guide Incasso Senza Pensieri: Added new reservation mode dedicated to tour operators New Ecwid plugin added Updated APM PPRO activation guide Added new payment method 'PayPal Pay in 3 installments' Updated PagaMPI API Added new Scontrino plugin

20.3	20/12/2023	Nexi	Removed Electronic Invoicing section (get your bill). Removed payment method PagoinConto. Removed alternative payment method Klarna. Added new section dedicated to payment via link. iOS SDK: improved handling of outcome on Apple Pay payments. Nexi XPay Plugin: added compatibility with Prestashop 8. API "pagaMPI": added new parameter "dataStanza." Order List API: added record limit of 15000. BigCommerce: new integration mode. Modified links for APM PPRO and Paypal guides. Improved description of the "urlpost" parameter and added indication of compatibility only with TLS 1.2. Minor corrections. Changed contact number for support with XPay payment gateway integration.
20.4	20/06/2024	Nexi	Evolved Tokenization: examples of notification inserted Reporting API: information on accounting status inserted XPay Build: information on SCA iframe inserted Incasso senza pensieri: instructions for installment cancellation inserted MyBank: specified usable characters Batch File: instructions for updating expiration inserted Minor fixes

XPAY PAYMENT GATEWAY

This section is designed to give you all the information and tools you need for integrating Nexi XPay gateway quickly and easily.

What will be covered?

- Step-by-step technical guides for implementation
- “Turnkey” solutions (Easy Payment) and additional features (OneClickPay, Recurring Payments)
- Advanced solutions, S2S, XPay Build etc.
- Sample codes, ready to use
- Materials to download: APIs, SDKs, Brand Repository, Information Documents

Are there any prerequisites?

The integration does not have any specific requirements. XPay is compatible with any programming language and with any type of e-commerce. It is also available for use in all environments (web/mobile and app) and is optimised for all devices.

Do I need to register?

All technical documentation and sample codes are freely available.
Registration (which does not need personal data - email address and password only) is required to access the Test Area, where you can test your solution and obtain support from the Nexi Technical Support team.

NB *You do not have to implement your solution from scratch if you already use an e-commerce platform, which makes integration even easier. Just download the related plugin and integrate it with the CMS.* Here *you can find modules for a wide range of platforms.*

Easy Payment

Integrating the Nexi “Easy Payment” module is the fastest way to begin receiving online payments on your website. The process is quite simple. It manages the transfer of the customer from the merchant’s e-commerce site to the secure Nexi environment, and back

again.

Additional customisations

Nexi also makes other types of more structured solutions available to merchants: I-Frame and XPay Build provide for greater customisation of the payment experience, with sensitive data handled by Nexi at all times. Server to Server requires the merchant to achieve PCI DSS certification.
In any case, integrating any of the solutions is simple and straightforward.

Back office integration API

Nexi makes available a control panel for the merchant, where transactions can be viewed and advanced reporting tools managed. Access is available by using web credentials, or by integrating the back office directly into the merchant's management system.

Further information and support

Whatever your needs may be, Nexi makes additional resources available for your use:

- Test Area
- Technical and commercial FAQs
- DEV COMMUNITY
- Download Section (documents, specifications and brand repository)

Not to mention that our technical support team is always at your disposal.

CONFIGURATION

Nexi offers merchants the possibility to customize the XPay service according to a series of characteristics, according to their needs, both in the test environment and in production. It is possible to proceed with the configuration of your terminal by connecting to the XPay back office or by contacting technical support.

What should I do before activating XPay on my site?

- Display your logo on the checkout page by uploading it through the "Configuration" section of the Nexi back office.
- Via the configuration section of the back office, Nexi sets up one or more emails to which Payment notifications will be sent.

WARNING: once the test back office has been configured and the testing phase is completed, it is necessary to access the production back office in order to make changes and align the configurations of the two environments. If you do not complete the "Configuration" section in the production back office, behaviors can differ from those obtained in the test area.

What other configuration options does XPay offer?

Below you can find the list of the additional features XPay makes available to its customers.

Description
You may choose either immediate or deferred deposit. It is typically set for immediate deposit. If you elect to defer deposits, the maximum guarantee period is 3 days. Once the number of deferral days has elapsed, you can set it so that the deposit is executed or the order is cancelled automatically.
XPay carries out the transaction and sends the result to the merchant at the url indicated in the "urlpost" field. If sending fails: • XPay can consider the transaction successful in any case, and the merchant will be responsible for recovering the result via the Back office, email or API • XPay cancels the authorisation without charging anything to the customer It is therefore necessary to advise technical support whether the transaction should be cancelled or not if the POST notification fails.
For recurring or OneClick Payments, there is an option to prevent previously registered credit cards from being used to activate additional registrations. If activated, this restriction returns the pan hash used for the Payment to the merchant.
Activating Payment session duration: if active, the merchant may set a validity period for the session so as to have certainty over the maximum amount of time a user may take to complete a Payment.

Setting additional fields: merchants can request one or more additional fields that they would like to occur on the check-out page. These can be viewed, or just saved to the detail of the transaction and made available for back office and reporting.

Viewing additional data: if merchants request the activation of additional fields, they can choose whether these will be visible on the check-out page and in notification emails. Otherwise, they are only available via the back office and reporting.

Viewing the result page: at the end of the transaction, the user is automatically directed to the merchant site and will be shown the Payment result. However, it is also possible to activate viewing of the result page via Nexi.

EASY PAYMENT

The easiest way to enable an e-commerce site to receive payments, without having to worry about handling sensitive customer data. The customer remains on the merchant's e-commerce site until the point of checkout. The customer is then redirected to the secure Nexi environment to make payment. The merchant does not need to handle any sensitive data.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-semplice

At a technical level, the implementation requires three stages:

1. Redirecting the user to the Nexi payment environment

IN PRACTICE

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL

https://ecommerce.nexi.it/ecomm/ecomm/DispatcherServlet

TEST ENVIRONMENT URL

https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherServlet

All communications to and from services hosted by Nexi must meet MAC security parameters. In this case too, the related calculation is displayed in the relevant section for each service.

2. Managing notification of the transaction result

IN PRACTICE

Collect the parameters sent by Nexi in server-to-server mode at the moment when the transaction is completed. In this way, merchants are confident of receiving the transaction result, even if the end customer closes the browser session before returning to the launch site.

3. Planning for the user’s return to the merchant site

IN PRACTICE

Manage the customer’s return to the merchant site, and display a positive or negative message based on the parameters received from the Nexi check-out page.

Base code

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-semplice

Initiation Message

Payment Initiation Message: required fields

This table shows required fields that have to be entered through a POST, into a redirect URL, with ISO-8859-1 coding, and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents, i.e. 5000 represents € 50.00.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CHAR.
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the special characters accepted are: +, -.
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative	AN MAX 500 CHAR.

		outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	
✓	url_back	Recall url, in case the user decides to abandon the transaction during the payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500 CHAR.
	mail	Buyer's email address to which the payment result will be sent.	AN MAX 150 CHAR.
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will	AN MAX 7 CHAR.

		be in the default language defined during the service configuration process.	
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
	Note2	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
	Note3	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
	additional parameters	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values. The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.	AN MAX 4000 CHAR.
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN 16 CHAR.
	selectedcard	If present, the payment page that is shown only allows the user to	AN

		make payment using the networks or payment methods indicated. This feature is useful for merchants who wish to enter the choice of payment method on their own check-out page. The possible values are shown in the Card Type Coding. It is necessary to separate the values with a comma ",".	
	TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to C (immediate), when the transaction is authorised the payment is deposited without any further intervention on the part of the merchant and without considering the default profile set for the terminal. If set to D (deferred) or if the field is empty, when the transaction is authorised it will be handled as defined by the terminal profile.	AN 20 CHAR.
	infoc	Additional information about the individual payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.
	infob	Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20 CHAR.
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	AN
	tipo_richiesta	"VC" (Card Verification) is used to perform a card verification, amount	AN MAX 2 CHAR.

		field is required to be “0”. With this type of call XPay only checks the card’s validity, no tokenization or other operations are involved in this process.	
	xpayTimeout	Payment timeout, valued with the seconds of validity of the payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.	
	cellulare	The mobile number with which the user has registered on the Bancomat Pay circuit. This way the customer does not have to enter it manually on the XPay gateway.	
	nome	Name of the person who made the payment.	AN MAX 150 CHAR.
	cognome	Surname of the person who made the payment.	AN MAX 150 CHAR.

3D Secure 2.2

To use this service see **3D Secure 2.2**

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications)
- By contacting Nexi customer support, you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request for all payments.
- The XPay checkout page is set to use the ISO-8859-1 character encoding.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans

- divisa
- importo
- secretKey

SAMPLE STRING

MAC = HASH SHA1(codeTrans=<val>divisa=<val>importo=<val><secretKey>)

Cancellation

If a customer decides to cancel the payment from the Nexi check-out page by using the appropriate cancellation button, or if an error occurs during the payment process, the customer will be redirected to the url indicated in the "url_back" parameter during the payment initiation process, along with the additional parameters as shown in the following table.

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
importo	Transaction amount retrieved from the payment initiation message.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed (EUR = Euro).	AN 3 CHAR.
codTrans	Code associated with the payment retrieved from the payment initiation message.	AN MIN 2 - MAX 30 CHAR.
Esito	Possible values: CANCELLED or ERROR	AN MIN 6 - MAX 7 CHAR.

If result = ANNULLO, the merchant may choose to return the user to the payment page with the same transaction code.

Result Message

The result of the payment will be sent in the following ways:

- Server to server notification > A notification is sent to the address indicated in the payment initiation parameter "urlpost".
- Redirect to merchant result page > The user, once the payment has been completed, is redirected directly to the merchant site at the address indicated in the payment initiation parameter "url". The user then returns to the merchant's site carrying with him the parameters confirming the completion of the transaction.

Result/Notification Message

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents, i.e. 5000 represents € 50.00.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CHAR.
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the

		merchant may choose to decrease this to less than 3 attempts.	special characters accepted are: +, -.
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
✓	esito	Operation result. Possible values: Valori possibili: - OK - KO - ANNULLO - ERRORE - PEN: (Pending): This state is returned only with some alternative payment methods: MyBank, AliPay, WeChat Pay, Giropay, iDEAL, Bancontact, EPS, Przelewy24, Skrill, Skrill 1tap, PayU, Blik, Multibanco, Satispay, Oney, PagoDIL.	AN MAX 7 CHAR.
✓	data	Transaction date	yyyymmdd
✓	orario	Transaction time	HHmmss
✓	codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods.	N MAX 3 CHAR.

✓	codAut	Authorisation code assigned by the credit card issuer, only present when authorisation is granted.	AN MIN 2 - MAX 6 CHAR.
✓	pan	Masked credit card number with only the first 6 and/or the last 4 digits showing.	AN MAX 100 CHAR.
✓	scadenza_pan	Credit card expiry date	yyyymm
✓	nazionalita	Shows the country of the card used for making payment.	AN 3 CHAR. ISO 3166-1 alpha-3 code
✓	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7 CHAR.
✓	TipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
✓	messaggio	Shows a brief description of the payment result. The possible values are shown in the table here.	AN MAX 300 CHAR.
	Parametri aggiuntivi	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit	AN MAX 4000 CHAR.

		to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values.	
	regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR.
	descrizione	If this information is provided during INPUT from the merchant, it will also be returned as OUTPUT, otherwise the field will be null.	AN MAX 2000 CHAR.
	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
	nome	Name of the person who made the payment.	AN MAX 150 CHAR.
	cognome	Surname of the person who made the payment.	AN MAX 150 CHAR.
	mail	Email address of the person who made the payment.	AN MAX 150 CHAR.
	hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for payment.	AN 28 CHAR.
	infoc	Additional information about the individual payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.

	infob	Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20 CHAR.
	codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
	esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- secretKey

SAMPLE STRING
MAC = HASH SHA1 (codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><SecretKey>)

NOTES:

- The merchant will receive a message with transaction details to the email address provided during configuration.
- By contacting technical support it is possible to configure up to 3 payment attempts for the same transaction code.

- If you have a terminal set to allow multiple payment attempts for the same transaction code, you will receive multiple notifications for the same order. There may be cases of a negative outcome for which non-final notifications are not sent: for a terminal set up with 3 attempts, one could receive only one negative outcome notification for a transaction code (final notification), even though the customer actually attempted the payment 3 times.The POST notification has the format 'application/x-www-form-urlencoded'.
- To confirm receipt of the notification, the message returned by the call must be an 'HTTP 200'. No action may be taken on the transaction until the result (HTTP 200) has been returned in response to the notification.
- The outcome redirect on the parameter 'url' occurs after the response to the url 'urlpost' only in the case where the cancellation of the order in the event of a POST notification failure is configured on the merchant terminal.

One Click Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
You can implement this solution in different ways:
• Via the merchant site
• Via cash page
The two solutions are distinguished for the management of subsequent payments: in the first case the subsequent payments will have to be managed by the merchant site, while in the second case it will be the gateway XPay to deal with it.

Oneclick payment via merchant site

Integrating One Click Payment allows end customers to store details of their credit card or PayPal account, and use them to make subsequent purchases with just one click.
At a technical level, this service consists of two stages:

- Activation and/or first payment
- Management of subsequent payments

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-oneclick/su-sito-merchant

Activation and/or first payment

During the first transaction, an identifying code must be generated for use in subsequent purchases. This identifying code (parameter: num_contratto) allows Nexi to save a paired link between the user and the payment card used.
The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

IN PRACTICE

The “Codebase” module must be integrated and the following specific required parameters added.

"First Payment" Initiation Message

Name	Description	Format
num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_oc3d”. ‘paga_multi’ to have the option of also making pagamenti ricorrenti	AN MAX 30 CHAR.
tipo_richiesta	- PP (first payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (contract update) to be used to update a contract on the same card.	AN 2 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

NOTES:

- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first payment status KO. Therefore not usable for new recurrences.
- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- By contacting Nexi customer support, you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request for all payments.
- The XPay checkout page is set to use the ISO-8859-1 character encoding.

"First Payment" Notification Message: required fields

The same information found in the "Codebase" module is received in response, along with the following specific parameters.

Name	Description	Format
num_contratto	Contract number retrieved from the initiation message.	AN MIN 5 - MAX 30 CHAR Except the “+” character and the quotes

tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Notification Message: optional fields

The same optional information found in the "Codebase" module can be received in response, along with the following specific parameter.

Name	Description	Format
Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.

Payment Notification Message: additional fields for PayPal

This table indicates the fields provided in response to PayPal payments.

Name	Description	Format
PAYERID	Unique identifier of the user's PayPal account.	AN 13 CHAR.
PAYMENTINFO_0_TRANSACTIONID	Unique identifier of the payment transaction.	AN.
PAYMENTREQUEST_0_SHIPTONAME	Name and surname attached to the shipping address.	AN 128 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET	First shipping address field	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET2	Second shipping address field. Optional.	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOCITY	Shipping address city	AN 40 CHAR.
PAYMENTREQUEST_0_SHIPTOSTATE	Shipping address country or province. The PayPal	AN 40 CHAR.

	country code list can be found here.	
PAYMENTREQUEST_0_SHIPTOZIP	Postal Code	AN 20 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYCODE	Country Code	AN 2 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYNAME	Country	AN 20 CHAR.
BILLINGAGREEMENTACCEPTEDSTATUS	Indicates whether the customer accepts recurring payments (valued with "1" if he accepts otherwise with "0")	N
BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

3D Secure 2.2

To use this service see **3D Secure 2.2**

Management of subsequent payments in one click mode

Each time registered users make subsequent purchases, the e-commerce provider must send a call to Nexi with the registered contract details.

IN PRACTICE

There are two ways to make a charge on a previously registered contract:

- Through a 3D Secure call in server-to-server mode
- By redirecting the customer to the Nexi payment environment as in the first payment

3D Secure call

In server-to-server mode, the services displayed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and responses are JSON objects. Alternatively, Non-Rest APIs are available where communication is handled synchronously (using https calls accompanied by a series of parameters and values). The result message is an XML handled on the same connection.

See the 3D Secure Subsequent Payment section for detailed information on the call and the response to handle.

NOTES:

- OneClick payments can be performed using contract numbers created from scheduled and unscheduled MIT transactions.

Redirection

As an alternative to synchronous calls, users can be redirected in the same way as they were for the first payment by integrating the call with the following specific parameters.

Name	Description	Format
num_contratto	Unique code assigned at the time of first payment for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_oc3d”.	AN MAX 30 CHAR.
tipo_richiesta	PR. This field indicates the Subsequent Payment of an already registered user.	AN 2 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

NOTES:

- OneClick payments can be performed using contract numbers created from scheduled and unscheduled MIT transactions.
- By contacting Nexi customer support, you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request for all payments.
- The XPay checkout page is set to use the ISO-8859-1 character encoding.

Oneclick Payment via checkout page

In this mode the call to the gateway will be identical for both the first and subsequent payments: XPay will manage them. In case of first payment, XPay will show the form for entering the card data, while in the case of subsequent payments, it will show the previously inserted card data or the possibility to enter the data of a new card.

In case of first payment on the XPay checkout page, the cardholder will be given the option to save his card details to make Oneclick payments.

The only data that must be managed by the operator is the "num_contratto" parameter which will be evaluated with a unique identifier for each customer (for example, the customer id of their site).

To activate this service you need to contact Nexi technical assistance, which will proceed with the creation of a unique alias to be used for the initiation of payments.

The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-oneclick/su-pagina-di-cassa

"First Payment" initiation Message

This table shows required fields that have to be entered through a POST into a redirect URL and their features.

Mandatory	Name	Description	Format
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	tipo_servizio	The field must be set to: “paga_1click”.	AN
✓	gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30

✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents, i.e. 5000 represents € 50.00.	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the request with the same codTrans for another 2 times, during configuration the operator can choose to decrease the 3 attempts	AN MIN 2 MAX 30 (character # is forbitten). In case of MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500
✓	url_back	Recall url, in case the user decides to abandon the transaction during the payment phase on the check-out page (result = CANCELLED) or if the	AN MAX 200

		call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of	AN MAX 2000

		service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field where the merchant can show information relating to the order.	AN MAX 200
	Note2	Field where the merchant can show information relating to the order.	AN MAX 200
	Note3	Field where the merchant can show information relating to the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	selectedcard	If present, the payment page that is shown only allows the user to make payment using the networks or payment methods indicated. This feature is useful for merchants who wish to enter the choice of payment method on their own check-out page. The possible values are shown in the Card Type Coding. It is necessary to separate the values with a comma ",".	AN
	TCONTAB	This field identifies the merchant’s chosen deposit method for each transaction. If set to C (immediate), when the transaction is authorised the payment is deposited without any	AN MAX 20

		further intervention on the part of the merchant and without considering the default profile set for the terminal. If set to D (deferred) or if the field is empty, when the transaction is authorised it will be handled as defined by the terminal profile.	
	infoc	Additional information about the individual payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	AN
	xpayTimeout	Payment timeout, valued with the seconds of validity of the payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.	
	3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is	AN

		enabled, Nexi will automatically send the request for 3DS exemption in all OneClick payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with: - "SCA": the 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.
	tipo_richiesta	- AC (contract update) to be used to update a contract on the same card. If the contract does not exist, for example the user has not previously accepted the tokenization, a normal first payment request will be made. In the event of a contract update, it will not be allowed to change the card.

NOTES:

- N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL
- By contacting Nexi customer support, you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request for all payments.
- The XPay checkout page is set to use the ISO-8859-1 character encoding.

3D Secure 2.2

To use this service see **3D Secure 2.2**

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiave segreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>gruppo=<val> num_contratto=<val><chiaveSegreta>)

NOTES:

- field values “url”, “urlpost” e “url_back” must start with “http://” o “https://”
- The address indicated in “urlpost” must have a pubblic certificate and it must not be protected by authenticationDevono essere utilizzate le porte standard 80 o 443
- For a correct management of calls you have to comply standard RFC 2396 e RFC 3986
- Parameters related to the working framework must not be sent (es.: i VIEWSTATE for ASP.NET applications)
- OneClick payments can be performed using contract numbers created from scheduled and unscheduled MIT transactions.
- By contacting Nexi support you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick payments.

Cancellation

In the event that the customer decides to cancel the payment once landed on the Nexi cash page through the appropriate cancel button, or if an error occurs during the payment process, it will be redirected to the URL indicated in the "url_back" parameter in payment start phase with addition of the parameters indicated in the following table.

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi	AN MIN 2 MAX 30 (character # is forbitten). In case of MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.
✓	esito	Result of the operation. Possible values: Valori possibili: - OK - KO - ANNULLO	AN MAX 7

	- ERRORE - PEN: (Pending): This state is returned only with some alternative payment methods: MyBank, AliPay, WeChat Pay, Giropay, iDEAL, Bancontact, EPS, Przelewy24, Skrill, Skrill 1tap, PayU, Blik, Multibanco, Satispay, Oney, PagoDIL.

In case of reply=ANNULLO the merchant can decide to send user to checkout page with the same transaction code.

Payment Result

Merchants receives payment result through:

- Via mail > Merchant receives a message via email (the one comunicated in configuration phase) with transaction details.
- Online > User, once payment ends, is sent directly to merchant site, to the url indicated in initiation message. User will be redirect to merchant site with all the parameters that certify transaction end.

Payment Result message: required fields

Mandatory	Name	Description	Format
✓	aliasEffettivo	Alias with which the transaction is actually executed.	AN MAX 30
✓	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	messaggio	Shows a brief description of the payment result. The possible values are shown in the table here.	AN
✓	tipo_servizio	The field will be valorized with: "paga_1click".	AN MAX 30

✓	tipo_richiesta	Possible values: - PP (first payment) in first payments - PR in subsequent payments - PA If the customer does not click the option to save the card data, a simple payment is then made	
✓	gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi	AN MIN 2 MAX 30 (character # is forbitten). In case of MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the special characters

			accepted are only : +, -.
✓	brand	Credit card network.	AN MAX 100
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
✓	esito	Result of the operation (Possible Values OK, KO, ANNULLO, ERRORE)	AN MAX 7
✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	orario	Hour of transaction	AN MAX 6 hhmmss
✓	codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods.	N MAX 3
✓	codAut	Authorisation code assigned by the credit card issuer, only present when authorisation is granted.	AN MIN 2 MAX 6
✓	pan	Masked credit card number with only the first 6 and/or the last 4 digits showing.	N MIN 16 MAX 19
✓	scadenza_pan	Credit card expiry date	DATA aaaamm
✓	nazionalita	Shows the country of the card used for making payment.	AN 3 CHAR. ISO 3166-1

			alpha-3 code
✓	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
✓	tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20
	Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.
	hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for payment.	AN MAX 28
	infoc	Additional information about the individual payment. This information can be transmitted to the company on the basis of prior	AN MAX 35

		agreement with the same company.	
	Infob	Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15
	Nome	Name of the person who made the payment.	AN MAX 150
	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
	Regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30
	Descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instrucrizione della disposizione SCT ma viene troncato al 140mo carattere	AN MAX 2000 for MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL:

		AN MAX 127 CHAR
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

Notification

The merchant receives payment notification directly from the Nexi server through a POST call. The notification contains the same parameters as the result and is performed towards the address indicated in the "urlpost" parameter of the payment initiation message.

ATTENTION: to confirm the receipt of the notification the message returned by the call must be an "http 200"

Payment notification message

Mandatory	Name	Description	Format
✓	aliasEffettivo	Alias with which the transaction is actually executed.	AN MAX 30
✓	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	messaggio	Shows a brief description of the payment result. The possible values are shown in the table here.	AN
✓	tipo_servizio	The field must be set to: “paga_1click”.	AN MAX 30
✓	tipo_richiesta	Possible values: - PP (first payment) in first payments - PR in subsequent payments - PA If the customer does not click the option to save the card data, a simple payment is then made	
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation	AN MIN 2 MAX 30 (character # is forbitten). In case of

		request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the richiesta con medesimo codTrans per altre 2 volte, in fase di configurazione l'esercente può scegliere di diminuire i 3 tentativi	MyBank you can only use: / - : ( ) . , + With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
✓	esito	Result of the operation (Possible Values OK, KO, ANNULLO, ERRORE)	AN MAX 7
✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	orario	Hour of transaction	AN MAX 6 hhmmss
✓	codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods.	N MAX 3
✓	codAut	Authorisation code assigned by the credit card issuer, only present when authorisation is granted.	AN MIN 2 MAX 6
✓	pan	Masked credit card number with only the first 6 and/or the last 4 digits showing.	N MIN 16 MAX 19

✓	scadenza_pan	Credit card expiry date	DATA aaaamm
✓	regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30
✓	nazionalita	Shows the country of the card used for making payment.	AN 3 CHAR. ISO 3166-1 alpha-3 code
✓	timeStamp	Timestamp in milliseconds	N 13 CHAR
✓	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instrucrizione della disposizione SCT ma viene troncato al 140mo carattere	AN MAX 2000 for MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
✓	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
✓	tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below:	AN MAX 200

		product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	
✓	Nome	Name of the person who made the payment.	AN MAX 150
	Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.
	Hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for payment.	AN MAX 28
	Infoc	Additional information about the individual payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	Infob	Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20

	codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15
	esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Mac Calculation

For the notification message, the string to sign must contain the following fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.

If you are instead interested in a solution that allows the end customer to store their credit card data, and use it later to make purchases more quickly, refer to the OneClick solution.

Recurring Payments are also identified with the term “MIT” (Merchant Initiated Transaction). MITs are broken down into:

- Scheduled: debited with defined frequency (e.g. first of each month).
- Unscheduled: debited with undefined frequency.

It is necessary to notify XPay support of the type of debits that will be made by your store, as it is necessary to properly configure the assigned Nexi profile.

It is not permitted to use contract numbers created through MIT Scheduled payments to carry out MIT Unscheduled transactions, and vice versa.

At a technical level, this service consists of two stages:

- Activation and/or first payment
- Management of recurring payments/subsequent payments

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-ricorrente

Activation and/or first payment

During the first transaction, an identifying code must be generated for use in subsequent purchases. This identifying code (parameter: num_contratto) allows Nexi to save a paired link between the user and the payment card used.

The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

IN PRACTICE

The “Codebase” module must be integrated and the following specific parameters added.

"First Payment" Initiation Message

Mandatory	Name	Description	Format
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
✓	tipo_richiesta	- PP (first payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (aggiorna contratto) da utilizzare quando si vuole aggiornare un contratto sulla medesima carta.	AN 2 CHAR.
	gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment It is necessary to pass this parameter inside the MAC calculation as a parameter after the “importo“ parameter.	

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first payment status KO. Therefore not usable for new recurrences.
- The XPay checkout page is set to use the ISO-8859-1 character encoding. Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action in order to keep these

contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

"First Payment" Notification Message: required fields

The same information found in the "Codebase" module is received in response, along with the following specific parameters.

Name	Description	Format
num_contratto	Contract number retrieved from the initiation message.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Notification Message: optional fields

The same optional information found in the "Codebase" module can be received in response, along with the following specific parameter.

Name	Description	Format
Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.

Payment Notification Message: additional fields for PayPal

This table indicates the fields provided in response to PayPal payments.

Name	Description	Format
PAYERID	Unique identifier of the user's PayPal account.	AN 13 CHAR.
PAYMENTINFO_0_TRANSACTIONID	Unique identifier of the payment transaction.	AN
PAYMENTREQUEST_0_SHIPTONAME	Name and surname attached to the shipping address.	AN 128 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET	First shipping address field	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET2	Second shipping address field. Optional.	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOCITY	Shipping address city	AN 40 CHAR.
PAYMENTREQUEST_0_SHIPTOSTATE	Shipping address country or province. The PayPal country code list can be found here.	AN 40 CHAR.
PAYMENTREQUEST_0_SHIPTOZIP	Postal Code	AN 20 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYCODE	Country Code	AN 2 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYNAME	Country	AN 20 CHAR.
BILLINGAGREEMENTACCEPTEDSTATUS	Indicates whether the customer accepts recurring payments (valued with "1" if he accepts otherwise with "0")	N
BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

3D Secure 2.2

To use this service see **3D Secure 2.2**

Management of Recurring Payments/Subsequent Payments

Each time registered users make subsequent purchases, the e-commerce provider must send a call to Nexi with the registered contract details.

IN PRACTICE

There are two ways to make a charge on a previously registered contract:

- Through a synchronous call in server-to-server mode
- Through batch file

Synchronous call

When you need to debit a contract previously registered, your system must send Nexi a call with the data of the contract previously registered during the first payment phase.
For the server to server mode, the services exposed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and responses are a formatted JSON object. Alternatively, non-Rest APIs are available where communication is managed synchronously (with https call + a series of parameters and values). The result message is an xml managed on the same connection.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/pagamento-ricorrente

The environment endpoints are as follows:

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it
URI
ecomm/api/recurring/pagamentoRicorrente

METHOD
POST

ACCEPT
application/json

See the Subsequent Payment section for detailed information on the call and the response to handle.

Batch file

The batch file is a tool dedicated to merchants who perform a large number of recurrences periodically.
This solution allows you to upload via SFTP, in a remote Nexi folder, a file containing a list of recurrences to be executed. The file will then be processed by the XPay gateway, which will execute the recurring payments present in the document and return a similar file containing the results of the transactions performed.
More information on the composition of the files is shown in the layout below:

The trace for managing recurring payments through batch files can be found here.

Download trace

To activate this service it is necessary to contact Nexi technical assistance, providing:

- The calling IP address
- The RSASSH public key

The SFTP user and two remote folders will then be made available to the merchant:

- OUT: where the input files should be placed
- IN: where the output files will be deposited once processed by XPay

NOTES:

- The IN folder should not be considered an "archiving folder", therefore it is requested to withdraw and delete the outcome files.
- It is important that the input file extension is set to uppercase ".TXT", if set to lowercase ".txt" the file will not be processed.
- The batch file processing procedure runs every 15 minutes, but the outcome is not immediate: it depends on the amount of files that the gateway is processing at that moment. The best practice is to poll for the presence of the output file.
- If a pan deadline associated with the contract number is entered in the file, the associated card will be updated with the new deadline.

Multi-Currency Payment (DCC)

The Dynamic Currency Conversion (DCC) service makes it possible to make multi-currency payments starting from transactions in euro.

The service is available for Visa and MasterCard cards issued in currencies other than euro (39 currencies).

Cardholders may carry out transactions in their card's currency with a guaranteed exchange rate by selecting the currency directly at the time of payment.
The DCC service is provided in collaboration with the partner Global Blue, and is available for customers that have activated the XPay Pro Gateway.

DCC is compatible with the following solutions:

- Simple Payment
- OneClick Payment: First Payments
- I-Frame
- Lightbox: simple payments and first OneClick payments
- Server to server

IN PRACTICE

The "Codebase" module must be integrated. The only difference is that the result message is enriched with additional information regarding:

- Whether or not the user accepts the exchange rate
- Exchange rate applied
- Equivalent value in the user's currency

3D Secure 2.2

To use this service see **3D Secure 2.2**

Github sample code: https://github.com/NexiPayments/XPay/tree/master/pagamento-multivaluta

Payment Result Message: additional fields for DCC

Name	Description	Format
dccRate	Exchange rate applied on the basis of exchange rates issued by Global Blue. Only present for the DCC service.	AN MAX 15 CHAR.
dccAmount	Shows the value of the amount converted into the currency chosen by the payer for the transaction. The currency used is shown in the dccCurrency field. Blank space characters are added on the left until 20 characters are reached.	AN 20 CHAR.

dccCurrency	Code of the currency in which the dccAmount is expressed (e.g. 840=USD). Only present for the DCC service. For allowed values, see the table here.	AN 3 CHAR.
dccState	Shows if the transaction took place using DCC. The possible values are: 00 No DCC provided for the card used 02 DCC not accepted by cardholder 03 DCC accepted by cardholder	AN 2 CHAR.

Payment via Link

The implementation of this solution allows the merchant to send payment links and collect online without the need for an e-commerce site.
This functionality can be utilized in the following ways:

- Integrated via API
- Using the advanced Back Office to generate payment links

In the latter mode, access to the XPay Back Office is available, and the following simple steps can be followed:

1. Enter the amount, description, payment method, and create the link in real-time.
2. Share the link with the customer via SMS, email, or chat.
3. The customer receives the link, chooses the payment method, confirms the details, and receives real-time confirmation.

It will be possible to accept One Click and recurring payments.

Integration via API
The following APIs are provided to integrate the Pay-By-Link service into your website or management system:

- Pay-by-Link request
- Regenerate Pay-by-Link
- Pay-by-Link report

Pay-by-Link Link Request

This service allows to obtain a Payment link which can be sent to customers for example by email, enabling them to be redirected to the XPay Payment pages to complete their transaction securely.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/api-back office/richiesta-link-pay-by-link

URI
ecomm/api/bo/richiestaPayMail

METHOD
POST

ACCEPT
application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.

✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
	timeout	Number of hours the generated Payment link will remain valid.	N MAX 4 CHAR.
	url	Merchant url where the Virtual POS will direct the user upon completion of the transaction, transferring, using the GET method, the response parameters which show the transaction result.	AN MAX 500 CHAR.
	timeoutPagamento	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office.. It is necessary to include this parameter within the "parametriAggiuntivi" object.	
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the	AN MAX 500

		notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	
	url_back	Recall url, in case the user decides to abandon the transaction during the payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	nome	Customer name	AN MAX 150
	cognome	Customer surname	AN MAX 150
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR

	Note1	Field in which the merchant can report information about the order. This data	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	TCONTAB	The field identifies the collection mode that the merchant wants to apply to the individual transaction, if populated with: - C (immediate) the transaction if authorised is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - D (deferred) or the field is not entered, the transaction if authorised is managed according to what is defined by the terminal profile. Immediate collection is established as standard by Nexi. If you want to manage deferred collections, ask technical support for this feature to be enabled. Once enabled, in the event of deferred collection, the collection is under the responsibility of the merchant, which may manage it from the back office, via API or at the automatic deadline communicated during the profile configuration phase	AN MAX 20
	timeoutPayment	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office..	N
	selectedcard	If present, the Payment page is displayed, enabling the user to make the Payment only with the	AN MAX 25

		circuits or Payment methods specified. This function is useful for those who want to include Payment method selection on their checkout page. The possible values are specified in the Card type coding table. It is necessary to separate the individual values with a comma “,”.	

First Payment

For the first recurring Payment, it is necessary to add the following parameters to the “parametriAggiuntivi” item.

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
✓	tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 MAX 30 Except the “+” character and the quotes
	gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized.	AN MIN 4 MAX 10

Pagamenti successivi

Vai alla sezione **Payment successivo** per il dettaglio della chiamata e della risposta.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey

- codiceTransazione
- importo
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val> timeStamp=<val><chiaveSegreta>)

Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, the possible values are shown in the table here messaggio -> error details	AN
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR
✓	payMailUrl	Contains the link to be used to make the Payment	Pay-by-LinkUrl

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
This calculates and returns a URL for invoking a Payment on XPay check-out pages.

If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. " parametriAggiuntivi ": {}

The "timeout" field is expressed in hours.

Regenerate Pay-by-Link link

The API makes it possible to regenerate, with the same parameters as the original link, a link that has previously expired or which was paid with a negative result. The API may also be used to extend the period of an unused link that is still active. The new expiry of the link generated will be the date of the request plus the specific timeout.

If the link associated with the transaction code has not yet been used, the API updates only the link expiry. In this case, the paymail link returned will be identical to the previous one.

If the link has already been used with a negative Payment result, a new link will be created with only a different transaction code. The other parameters are unchanged with respect to the original link.

The new transaction code will be the value of the nuovoCodiceTransazione field, if not specified XPay will generate a code by appending a counter to the original one. (In order not to exceed the 30 character maximum size of the transaction code, the last two characters may be replaced). The transaction code associated with the new link will be returned in response to the API and will need to be reused for any new regenerations.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/rigenera-link-pay-by-link**

URI
ecomm/api/bo/rigeneraPayMail

METHOD
POST

ACCEPT
application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	timeout	Number of hours the generated Payment link will remain valid	N MAX 4
	nuovoCodiceTransazione	New transaction identifier assigned by the merchant	AN

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	payMailUrl	Contains the link to be used to make the Payment	AN
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	codiceTransazione	Transaction code associated to the link. In the event that the link has already been used with a negative payment outcome, a different transaction code will be returned than the one passed in the start-up message. In this case the transaction code returned will be incremental: original transaction code + _n	AN MIN 2 MAX 30

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Esito dell'operazione	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Pay-by-Link Report

This api invoked by a common POST, searches for Pay-by-Link links and returns the Payment status. Each search will return a maximum of 1000 links.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/report-pay-by-link**

URI
ecomm/api/bo/ReportPayMail

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	linkCreatiDal	Start date of search for created links	dd/mm/yyyy hh:mm:ss
	linkCreatiAl	End date of search for created links	dd/mm/yyyy hh:mm:ss

NOTES:

- If the search parameters are not passed, the search is carried out on the previous week.
- If the time is not passed, Nexi will return the results of the day indicated (24h).
- It is not possible to search for an individual link by means of an identifying parameter such as the “codiceTransazione”.

MAC Calculation

For the startup message, the string to be signed must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey<val> timeStamp=<val>chiaveSegreta>)

Positive Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	paymail	Array whose structure is described in the following table	Array
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Paymail Object

Mandatory	Name	Description	Format
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
✓	divisa	978 for Euro	AN MAX 3
✓	stato	Pay-by-Link link status Values: "0", "1", "2", “3”	N
✓	statoEsteso	Status description. Possible values: - "Link P@ymail non utilizzato", - "Payment Effettuato Correttamente", - "Payment Non Riuscito", - "Link Pay-by-Link scaduto"	AN
✓	dataTransazione	Transaction Date	DATE dd/mm/yyyy hh:mm:ss
✓	circuito	Circuit used for Payment	AN
✓	destinatarioLink	Link receiver	AN
✓	dataCreazioneLink	Link creation dare	dd/mm/yyyy hh:mm:ss
✓	Pay-by-LinkId	Id Pay-by-Link	N
✓	Pay-by-LinkToken	Token Pay-by-Link	AN
✓	descrizione	Iterm description	AN MAX 500

✓	dataScadenzaLink	Link expire date	dd/mm/yyyy hh:mm:ss
✓	operatore	Operator who generated the payment link	AN

Negative result message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	JSON
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the result message, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

PAYMENT METHODS

XPay allows the merchant to offer to his e-commerce customers the possibility to pay by credit card and alternative payment methods.

Payment methods	Description	Activation mode
Visa - Easy Payment - OneClick Payment - Recurring Payment - Multi-Currency Payment DCC - XPay Build - LightBox - Server to server - I-Frame	Visa is a payment card circuit recognized worldwide. It is currently one of the most popular.	Automatically activated with Nexi contract.
VPay - Easy Payment - OneClick Payment - Recurring Payment - Multi-Currency Payment DCC - XPay Build - LightBox - Server to server - I-Frame	V Pay is a debit card circuit of the VISA Group.	Automatically activated with Nexi contract.
MasterCard - Easy Payment - OneClick Payment - Recurring Payment - Multi-Currency Payment DCC - XPay Build - LightBox - Server to server - I-Frame	Mastercard is a payment card circuit recognized worldwide. It is currently one of the most popular.	Automatically activated with Nexi contract.
Maestro - Easy Payment - OneClick Payment - Recurring Payment - Multi-Currency Payment DCC	Maestro is the debit card circuit of Mastercard’s group.	Automatically activated with Nexi contract.

- XPay Build - LightBox - Server to server - I-Frame		
Google Pay - Easy payment - Recurring payment - XPay Build: basic and recurring payment - I-Frame	Google Pay allows you to pay quickly and easily using the credentials of your Google account.	Automatically activated with Nexi contract.
Apple Pay - Easy Payment - Recurring payment - XPay Build: basic and recurring payment - I-Frame	Linked to Apple devices, it allows you to pay quickly and securely.	Automatically activated with Nexi contract.
JCB - Easy Payment - XPay Build: basic payment and OneClick - LightBox: basic payment and OneClick - I-Frame - Server to server: 3D Secure Payment and OneClick	JCB is one of the largest payment circuits on the world stage, and a leader in the issuing and acquiring sector in Japan.	Can be activated on request with Nexi contract
UPI - Easy Payment - XPay Build: basic payment and OneClick - LightBox: basic payment and OneClick - I-Frame - Server to server: 3D Secure Payment and OneClick	International payment card circuit based in China.	Can be activated on request with Nexi contract
American Express - Easy Payment - OneClick Payment - Recurring	American Express is an international credit card circuit.	Can be activated by contract with American Express.

Payment - XPay Build - LightBox - I-Frame - Server to server		
Bancomat Pay - Easy Payment - OneClick Payment - XPay Build: basic payment - I-Frame	The digital service of BANCOMAT S.p.A. to pay easily, quickly and securely via smartphone.	Can be activated by contract with BancomatPay inside the XPay back office.
MyBank - Easy Payment - XPay Build: basic payment	MyBank allows you to make secure payments by bank transfer.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office*.
Alipay - Easy Payment - XPay Build: basic payment - I-Frame	AliPay is the most popular online payment system in China that allows you to pay quickly and easily using your account credentials.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
WeChat Pay - Easy Payment - XPay Build: basic payment - I-Frame	WeChat Pay is a wallet that allows you to pay via mobile in an innovative way using the WeChat system.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Giropay - Easy Payment - XPay Build: basic payment - I-Frame	It is an online payment service popular in Germany. Customers are redirected to their banking environment and the amount is immediately settled.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
iDEAL - Easy Payment - XPay Build: basic payment - I-Frame	It is a very popular payment method in the Netherlands: it allows consumers to pay online through their bank account.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Bancontact - Easy Payment - XPay Build: basic payment - I-Frame	It is an online payment method, based on debit card, widely used in Belgium.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
EPS - Easy Payment - XPay Build: basic	It is an Austrian payment method based on bank transfers, in which transactions are processed in real time.	Can be activated by contract with Nexi's partner PPRO

payment - I-Frame		inside the XPay back office.
Przelewy24 - Easy Payment - XPay Build: basic payment - I-Frame	It is an online payment system based on bank account, widely used in Poland.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Skrill - Easy Payment - XPay Build: basic payment - I-Frame	It allows you to pay through Skrill wallet by simply entering your email address and password.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Skrill 1tap Easy payments and oneclick	It allows you to use Skrill to pay with a tap, without having to enter credentials with every payment anymore.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
PayU - Easy Payment - I-Frame	This is a very popular bank transfer payment service in Poland and the Czech Republic.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Blik - Easy Payment - I-Frame	This is a popular service in Poland that allows a payment to be made by bank transfer thanks to a Blik code generated in the client's home banking system.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Multibanco - Easy Payment - XPay Build: basic payment - I-Frame	It is the most widely used payment method in Portugal, allowing customers to pay via online banking.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Satispay - Easy Payment - XPay Build: basic payment - I-Frame	Satispay is an Italian payment system that allows the consumer to manage payments via a mobile APP.	Can be activated by contract with Nexi's partner PPRO inside the XPay back office.
Amazon Pay - Easy Payment - Recurring Payment - XPay Build: basic payment and	Simplify the purchase process by making use of the information stored in existing Amazon accounts.	Can be activated by contract with Amazon Pay directly from back office XPay.

recurring - I-Frame		
PayPal - Easy Payment - Recurring Payment - XPay Build: basic payment and recurring - I-Frame	Among the most popular payment systems, it does not transmit sensitive card data linked to the account. Registration is free.	Can be activated by contract with PayPal directly from back office XPay.
Klarna - Easy Payment - I-Frame	It allows you to receive online transfers easily and safely and eliminates the risk for the buyer and seller.	Can be activated by contract with Klarna directly from back office XPay.
Oney Easy payment	Allows you to finance your purchases in 3 or 4 instalments by Credit/Debit Card and Postepay, simply, quickly and without risk.	Can be activated by contract with Oney Bank S.A directly from back office XPay.
PagoDIL Easy payments	PagoDIL makes it possible to offer deferred payments to its customers.	Activated by contract with Cofidis directly from the XPay back office.

Note: In order to activate the MyBank service, merchants who are customers of Monte dei Paschi di Siena, Banca Popolare di Sondrio and Banca del Piemonte will have to apply directly at their reference branch.

Google Pay

Google Pay is wallet by Google to memorize your own credit cards in a smart and safe way.

Activation

The payment method is activated automatically on the merchant's terminal. No back office activation is required to make Google Pay visible on the XPay cash page.

The GPay section of the back office, present in the "Alternative payments" menu, allows you to change the name of the store sent to Google and visible to the customer during the payment phase. By default, the store name is set with the name of the brand associated with the XPay terminal.

Payment

It is possible to redirect users directly to GooglePay using the parameter “selectedcard” enhanced “GOOGLEPAY” during initiation payment phase.

Payment with Google Pay is compatible and follows the specifications of the following solutions:

- Simple Payment
- Recurring Payment
- XPay Build: basic and recurring payment
- I-Frame

Payment with Google Pay follows the specifications of Simple Payment, however it undergoes the following changes in the Initiation Message, Result Message and Notification Message:

Mandatory	Name	Description	Format
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	AN

Payment Result and Notification Message

The following parameters are included in the result message if you use Google Pay and enhance the shipping parameter in the initiation phase of the payment

Mandatory	Name	Description	Format
✓	shipping_name	The full name of the adressee	AN
✓	shipping_address1	First line of the address	AN
✓	shipping_address2	Second line of the address	AN
✓	shipping_address3	Third line of the address	AN
✓	shipping_postalCode	Postal code	AN
✓	shipping_countryCode	Country code	AN
✓	shipping_locality	City, town, neighbourhood, or suburb	AN
✓	shipping_administrativeArea	A country subdivision (e.g. state or province)	AN
✓	shipping_sortingCode	The sorting code	AN

Shipment

You can request the shipping data, provided by the Google Pay wallet, valuing the "shipping" parameter during the start of the payment process.

Alternative integration methods

WEB

To integrate Google Pay into a web page via frame or XPay Build it is only necessary to enable the Payment METHOD as indicated in the previous "Activation" section.

APP

To integrate Google Pay into an app without using the SDKs made available by XPay, it is required to perform the following operations depending on the implementation method:

- full redirect, webview, frame in webview: a browser compatible with Google Pay must be used.
- native: direct integration with Google Pay is required. The payment API is presented on the API integration page.

In this mode, Nexi will only take care of the authorisation part of the payment, the data concerning Google Pay will be collected by the Merchant's site or app, which will forward the JSON received from Google to Nexi via the API described below.
The integration varies in its use depending on how Google Pay returns the payload with the payment data:

- Payload with tokenized pan: the API below will execute the payment by completing the transaction.
- Payload with clear pan (real PAN): the API below will not directly execute the payment, but will return the data required to perform 3D Secure authentication.

Example on GitHub: https://github.com/NexiPayments/XPay/tree/master/metodi-di-pagamento-alternativi/googlepay

URI
ecomm/api/paga/v2/pagaGooglePay

METHODO
Post

ACCEPT
Application/json

Payment Initiation Message

Mandatory	Name	Descrizione	Format
✓	apikey	Alias assigned to the merchant by Nexi	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	AN MIN 2 - MAX 30 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN 3 CRT

✓	googlePay	JSON ottenuto dalla chiamata a Google	JSON
✓	urlRisposta	Parameter used by the gateway in the case of a Google payload with clear pan. Url to which XPay will redirect and return the result in GET via the following parameters: esito idOperazione xpayNonce timestamp mac and in case of error also codice and messaggio	
✓	timeStamp	Timestamp in milliseconds	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	parametriAggiuntivi	N additional parameters can be specified that will be returned in the result messages. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their total value should not exceed 4000 characters. In the following table an example of parameters	AN MAX 4000 Avoid the following names, they are used by Xpay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

MAC Calculation

For the transaction start message, the string to be signed must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val> timeStamp=<val><chiaveSegreta>)

TOKENIZED PAN

If the Google payload contains a tokenized pan, the PayGooglePay API executes the payment by completing the transaction. No further steps are necessary

Payment Result Message

Mandatory	Name	Descrizione	Format
✓	esito	Result of the request (possible values OK, KO, ANNULLO and ERRORE)	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CRT
✓	codiceConvenzione	Merchant code assigned by the acquirer (where expected)	AN MAX 15 CRT
✓	data	Transaction date	aaaa/mm/gg
✓	ora	Transaction time	hh:mm:ss
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30 CRT
✓	brand	Type of card used by the user to make paymen	AN MAX 100 CRT
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below:	AN MAX 200 CRT

		product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	
✓	tipoTransazione	Indicates the payment method. See the table Transaction Type Coding for possible values. In case of payment with negative result an empty string will be sent	AN MAX 20 CRT
✓	timestamp	Timestamp in millisecond format	
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the result message, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<*val*>*idOperazione=*<*val*>*timeStamp=*<*val*><*chiaveSegreta*>*)*

CLEAR PAN

With real pan 'payGooglePay API responds with a JSON containing the HTML code provided by the card issuer for the input of data useful for 3D Secure, it is up to the receiver to print the received HTML to the user's browser.
Subsequently, after authentication by the user, the result is returned to the address indicated in the request parameter 'urlResponse'.
With the data received, it is necessary to proceed with the payment via the paga3DS API.

Payment Result Message with HTML

Mandatory	Name	Descrizione	Format
✓	esito	Result of the request (possible values OK, KO, ANNULLO and ERRORE)	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	html		
✓	timeStamp	Timestamp in millisecond format	
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Payment Result Message with nonce

Mandatory	Name	Descrizione	Format
✓	esito	Result of the request (possible values OK, KO, ANNULLO and ERRORE)	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	xpayNonce	Code assigned by XPay for use in the payment request	
✓	timeStamp	Timestamp in millisecond format	
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	warning	HTML code to be printed on the user's browser for 3D Secure authentication	Object

Object Warning

Mandatory	Name	Descrizione	Format
✓	esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the sent 3D Secure 2.2 parameters. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the specific Warning API or consult the order details in the XPay back office.	

MAC calculation if you receive the html or in case of error

For the result message, if you receive the html or in case of error, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH *SHA1(esito*=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

MAC calculation if you receive the nonce

For the result message, if you receive the nonce, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<*val*>*idOperazione*=<*val*>*xpayNonce*=<*val*>*timeStamp*=<*val*><*chiaveSegreta*>*)*

The outcome parameter "xpayNonce" is the parameter necessary to proceed with the payment through the API paga3DS.

NOTES:

Google's 'tokenizationSpecification' object, which contains information about the payment gateway, must be valorised as follows:

const tokenizationSpecification = {
type: 'PAYMENT_GATEWAY',
parameters: {
'gateway': 'nexi',
'gatewayMerchantId': 'numeroterminalenexi'
}
};

The terminal number corresponds by default to the numeric code contained in the alias (apiKey), example:

- alias: ALIAS_WEB_0001234
- gatewayMerchantId: 0001234

Apple Pay

Apple Pay is a mobile payments service that allows users to make payments in person, in iOS apps, and on the web. It digitizes and can replace a credit or debit card chip and PIN or magnetic stripe transaction at a contactless-capable point-of-sale terminal. It is very similar to contactless payments already used in many countries, with the addition of twofactor authentication via Touch ID, Face ID, PIN or passcode. The service lets Apple devices wirelessly communicate with point of sale systems by using a near field communication (NFC) antenna, a "dedicated chip that stores encrypted payment information" (known as the Secure Element), and Apple's Touch ID and Wallet.[For the complete list of device support check https://support.apple.com/it-it/KM207105

Activation

The payment method is activated automatically on the merchant's terminal and activations from the back office are not required with the use of solutions that use the XPay cash page.

With the "XPay Build" mode and with the API integration it is necessary to configure the service by accessing the Apple Pay section of the XPay back office, within the "Alternative Payments" menu.

The Apple Pay section of the back office allows you to change the store name sent to Apple and visible to the customer during payment. By default, the store name is set with the name of the brand associated with the XPay terminal.

Simple Payment

Once the payment method has been activated from the Nexi back office, the Apple Pay payment button will appear on the XPay page.

It is possible to redirect users directly to GooglePay using the parameter “selectedcard” enhanced “APPLEPAY” during initiation payment phase.

Payment with Apple Pay is compatible and follows the specifications of the following solutions:

- Simple Payment
- Recurring payment
- XPay Build: basic and recurring payment
- I-Frame

However, it undergoes the following changes at the start of payment:

Mandatory	Name	Description	Format

	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	AN

Alternative integration methods

WEB

To integrate Apple Pay into a web page via frame or XPay Build, it is necessary:

- Enter your domain from the XPay back office in the section dedicated to Apple Pay and follow the instructions.
- Send the parameter "frame = S" during payment and include the following javascript on the page depending on the environment:

TEST

```
<script
    src="https://int-ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

PRODUCTION

```
<script
    src="https://ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

APP

To integrate Apple Pay into an app without using the SDKs made available by XPay, it is necessary to perform the following operations depending on the implementation mode:

- full redirect: Safari must be used.
- webview: the SafariViewController or WKWebView controller must be used.
- frame in webview: you need to register your domain from the XPay back office in the section dedicated to Apple Pay and follow the instructions; use the SafariViewController controller; send the "frame = S" parameter during payment and include the javascript presented in the previous WEB section on the page.
- nativo: direct integration with Apple Pay is required, also in the XPay back office it is necessary to complete the "Apple Pay S2S Management" section. The payment API is presented on the API integration page.

API Integration

Nexi will manage only the authorization of the payment , Apple Pay revelevant and needed data will be retrieved by the web site or by the App of Merchant, these parameters will be sent with JSON received by Apple towards Nexi using the API described below

There is a specific guide available for developer that explan ApplePayJS at this link: https://developer.apple.com/apple-pay/.

Once receive the JSON from Apple, you should sent it to Nexi API following these instruction in order to make the payment.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/metodi-di-pagamento-alternativi/applepay

URI
ecomm/api/paga/applePay

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Descprition	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR
codiceTransazione	Transaction identifier assigned by the merchant.	
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. It must be equal to the amount that was sent to Apple for the token generation	AN MIN 2 - MAX 30 CHAR
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN 3 CHAR
applePay	JSON receive from the Apple call	JSON
timeStamp	Timestamp in milliseconds	N 13 CHAR
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

Payment Initiation Message: optional fields

Nome	Descrizione	Format
parametriAggiuntivi	N additional parameters can be specified that will be returned in the result messages. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their total value should not exceed 4000 characters. In the following table an example of parameters	AN MAX 4000 Avoid the following names, they are used by Xpay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- timeStamp
- chiaveSegreta (secretKey that was received by Nexi)

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val>timeStamp=<val><chiaveSegreta>)

Payment Notification Message

Name	Description	Format
esito	Result of the operation (Possible Values OK, KO, ANNULLO e ERRORE)	AN MAX 7 CHAR
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR
data	Transaction date	aaaa/mm/gg
ora	Operation date	hh:mm:ss
nazione	Credit card country	AN ISO 3166-1 alpha-3

regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR
brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100 CHAR
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR
tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR
shippingContact	JSON with info received about Shipping (received by Apple)	JSON
billingContact	JSON with info received about Billing (received by Apple)	JSON
timestamp	Timestamp in milliseconds	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- results
- idOperazione
- timeStamp
- chiaveSegreta (secretkey received by Nexi)

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

When you execute a payment authorization through Apple Pay the results is a JSON object that contains all the answer parameters.

If you do not want to add optional parameter you can:

- do not add the element "parametriAggiuntivi" in the JSON
- or add "parametriAggiuntivi" and leave empty /"null"

You can use this 'API only if the merchant has been enable to use Apple Pay : the PCCS12 has been correctly loaded in the back office of Nexi.

American Express

Activation

To make this card circuit available on the checkout page, you must contact American Express for both the eCommerce and MOTO profiles, providing your XPay terminal code (the terminal code is the numeric code in the alias provided by Nexi). For the agreement, it is necessary to call the American Express Commercial Service on 800 919 019 (from Monday to Friday from 09.00 to 20.00).
Once American Express tells you the activation code, forward it by email by contacting support.ecommerce@nexi.it.
It is possible to integrate American Express through the "Single Payment" method or through “Recurring Payment”.

Simple Payment

Payment initiation does not change with respect to BaseCode.

It is possible to redirect users directly to American Express using the parameter “selectedcard” enhanced “Amex” during initiation payment phase.

Payment by American Express is compatible with and follows the specifications of the following solutions:

- Simple Payment
- OneClick Payment
- Recurring Payment
- XPay Build
- LightBox
- I-Frame
- Server to server

JCB

Activation

To make this card circuit available on the checkout page, it is necessary to request it when signing the contract with Nexi.

It is possible to integrate JCB through the "Simple Payment" method.

Simple Payment

Payment by JCB is compatible with and follows the specifications of the following solutions:

- Easy Payment
- OneClick Payment
- XPay Build: Easy Payment and OneClick
- LightBox: Easy Payment and OneClick
- I-Frame
- Server to server: 3D Secure Payment and OneClick

Payment initiation does not change with respect to BaseCode.

It is possible to redirect users directly to JCB using the parameter “selectedcard” enhanced “jcb” during initiation payment phase.

UnionPay

Activation

To make this card circuit available on the checkout page, it is necessary to request it when signing the contract with Nexi.

It is possible to integrate UnionPay through the "Simple Payment" method.

Simple Payment

Payment by UnionPay is compatible with and follows the specifications of the following solutions:

- Easy Payment
- OneClick Payment
- XPay Build: Easy Payment and OneClick
- LightBox: Easy Payment and OneClick
- I-Frame
- Server to server: 3D Secure Payment and OneClick

Payment initiation does not change with respect to BaseCode.

It is possible to redirect users directly to UnionPay using the parameter “selectedcard” enhanced “UPI” during initiation payment phase.

Bancomat Pay

The digital service of BANCOMAT S.p.A. to pay easily, quickly and securely via smartphone.

Activation

To make this payment method available on the till page, you must configure and activate the service by accessing the Bancomat Pay page of the XPay back office, , in the menu "Pagamenti alternativi"

It’s possible to integrate Bancomat Pay through the "Simple Payment" method.

Simple Payment

The merchant will be able to redirect its customers to the Bancomat Pay cash page by valuing the "selectedcard" parameter with "BANCOMATPAY" in the payment initiation phase.

Payment by Bancomat Pay is compatible with and follows the specifications of the following solutions:

- Simple Payment
- OneClick Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at the start of payment:

Initiation Message

Mandatory	Name	Description	Format
	cellulare	The mobile number with which the user has registered on the Bancomat Pay circuit. This way the customer does not have to enter it manually on the XPay gateway. Prefix is required (e.g. '+39')	AN AN ^(\\+)([0-9]{10,15})$

OneClick Payment

It is possible to manage OneClick payments via Bancomat Pay, the solution involves associating the mobile number to the contract number, in this way the customer will not have to enter it manually in subsequent payments, he will still have the possibility to confirm or change with another number.

The OneClick payment with Bancomat Pay follows the specifications of the OneClick payment via the merchant's website and the specifications of the OneClick payment via the cash page, with the following variations in the payment initiation phase:

Mandatory	Name	Description	Format
	cellulare	The mobile number with which the user has registered on the Bancomat Pay circuit. This way the customer does not have to enter it manually on the XPay gateway. Prefix is required (e.g. '+39')	AN AN ^(\\+)([0-9]{10,15})$

It will not be possible to manage OneClick payments using 3D Secure server-to-server payment.

Notification

Post notification can arrive in a-synchronous mode: if the user closes the browser while XPay is awaiting authentication on the Bancomat Pay app, XPay will send the post notification upon receipt of the result from the Bancomat.
The option to cancel transaction in case of failed notification is not available.
The notification also shows the "IdTransazioneBPay" field which uniquely identifies the ATM cash transaction.

Back office operations

With the Bancomat Pay payment method it is possible to carry out total/partial accounting operations, deferred collections and reversals.

NOTES

- While the XPay gateway is awaiting confirmation, cancellation or time out of customer authentication on the Bancomat Pay app, the transaction will be in the "in progress" state.
- In the event of a positive result, the "codAut" parameter is always valued with "BPAY".

MyBank

MyBank allows you to make secure payments by bank transfer.

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

In order to activate the MyBank service, merchants who are customers of Monte dei Paschi di Siena, Banca Popolare di Sondrio and Banca del Piemonte will have to apply directly at their reference branch.

Payment

It is possible to redirect users directly to MyBank using the parameter “selectedcard” enhanced “MY_BANK” (for requests via PPRO) or “SCT” (for requests via bank) during initiation payment phase.

Payment with MyBank is compatible with and follows the specifications of the following solutions:

- Simple Payment
- XPay Build: basic payment

However, it undergoes the following changes at the start of payment:

Iniziation Message

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For MyBank, the only special characters that can be used are: "a" to "z", "A" to "Z", 0-9 e - ? : ( ) . , + Space**

Payment Result and Notification Message

This table shows the fields provided in response for MyBank payments.

Mandatory	Name	Description	Format
	SRCACCOUNTHOLDER	Account holder of the consumer's account	AN
	SRCIBAN	IBAN of the consumer's account	AN
	SRCBIC	BIC of the consumer's account	AN
	SRCCOUNTRY	The 2-letter ISO code of the country from where the consumer makes the payment. It is extracted from the IBAN.	AN 2
	PAYMENTPURPOSE	This parameter reflects what the consumer will see on the proof of payment (e.g. bank statement record and similar).	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

NOTES:

- It is not possible to use the MyBank payment method with the iFrame solution.

AliPay

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to AliPay using the parameter “selectedcard” enhanced “ALIPAY” during initiation payment phase.

Payment with AliPay is compatible with and follows the specifications of the following solutions:

- Simple Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at the start of payment:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For AliPay, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

WeChat Pay

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to WeChat Pay using the parameter “selectedcard” enhanced “WECHATPAY” during initiation payment phase.

Payment with WeChat Pay is compatible and follows the specifications of the following solutions:

- Simple Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For WeChat Pay, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
	locale	Language of payment page	Only allowed values: zh-CN,zh-TW,en-US

Payment Result and Notification Message

This table shows the fields provided in response for wechatPay payments.

Mandatory	Name	Description	Format

	SRCAMOUNT	The total amount in the minor unit of the consumer wallet currency.	N
	SRCCURRENCY	The currency of the consumer's WeChat wallet.	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Giropay

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to Giropay using the parameter “selectedcard” enhanced “GIROPAY” during initiation payment phase.

Payment with Giropay is compatible and follows the specifications of the following solutions:

- Simple Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Giropay, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €. **Minimum value that can be used with Giropay: "10" (10 cents).**	N MAX 8 CRT

	bic	BIC of the consumer’s account	AN allowed values: ^(?=[0-9a-zA-Z]*$)(?:.{8}|.{11})$

Payment Result and Notification Message

This table shows the fields provided in response for Giropay payments.

Mandatory	Name	Description	Format
	PAYMENTPURPOSE	This parameter reflects what the consumer will see on the proof of payment (e.g. bank statement record and similar).	AN

Payment notification and outcome: Pending status

With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to iDEAL using the parameter “selectedcard” enhanced “IDEAL” during initiation payment phase.

Payment with iDEAL is compatible and follows the specifications of the following solutions:

- Simple Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For iDeal, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €. **Minimum value that can be used with iDEAL: "10" (10 cents).**	N MAX 8 CRT

	bic	BIC of the consumer's account	AN allowed values: RABONL2U, ABNANL2A,FVLBNL22, TRIONL2U,INGBNL2A, SNSBNL2A,ASNBNL21, RBRBNL21,KNABNL2H, BUNQNL2A,MOYONL21, HANDNL2A

Payment Result and Notification Message

This table shows the fields provided in response for iDEAL payments.

Mandatory	Name	Description	Format
	PAYMENTPURPOSE	This parameter reflects what the consumer will see on the proof of payment (e.g. bank statement record and similar).	AN
	SRCBANKNAME	Bank name of the consumer's account	AN
	SRCACCOUNTHOLDER	The account holder	AN
	SRCACCOUNTNUMBER	Account number of the consumer's account	AN
	SRCBANKCODE	Bank code of the consumer's account	AN
	SRCBIC	BIC of the consumer's account	AN
	SRCIBAN	IBAN of the consumer's account	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to Bancontact using the parameter “selectedcard” enhanced “Bancontact” during initiation payment phase.

Payment with Bancontact is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Bancontact, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**

Payment Notification Message

This table shows the fields provided in response for Bancontact payments.

Mandatory	Name	Description	Format

	CARDBIN	BIN of the Bancontact card used (first six digits of the Bancontact card)	N
	CARDLAST4DIGITS	Last four digits of the Bancontact card used	N
	CARDTOKEN	Unique token representing the Bancontact card	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

EPS - Electronic Payment Services

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner

Payment

It is possible to redirect users directly to EPS using the parameter “selectedcard” enhanced “EPS” during initiation payment phase.

Payment with EPS is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For EPS, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €. **Minimum value that can be used with EPS: "100" (1 Euro).**	N MAX 8 CRT

Payment Result and Notification Message

This table shows the fields provided in response for EPS payments.

Mandatory	Name	Description	Format
	PAYMENTPURPOSE	This parameter reflects what the consumer will see on the proof of payment (e.g. bank statement record and similar).	AN
	SCHEMERETURNCODE	The reason for a failed transaction call	AN
	SRCBIC	BIC of the consumer's account	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Przelewy24

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Przelewy24 using the parameter “selectedcard” enhanced “P24” during initiation payment phase.

Payment with Przelewy24 is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Przelewy24, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	mail	Buyer’s email address to which the payment result will be sent.	AN MAX 150 CHAR

Payment Result and Notification Message

This table shows the fields provided in response for Przelewy24 payments.

Mandatory	Name	Description	Format
	P24DESCRIPTOR	Przelewy24 generated payment descriptor.	AN
	P24METHOD	Numeric identifier of the payment scheme or bank used for the payment. This number is assigned by Przelewy24 once the transaction succeeded.	N
	P24METHODNAME	Friendly name of the payment scheme or bank used for the payment. Assigned together with the above output parameter if current information of available payment methods could be retrieved from the scheme.	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Skrill

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Skrill using the parameter “selectedcard” enhanced “SKRILL” during initiation payment phase.

Payment with Skrill is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Skrill, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	nome	Customer name.	AN
✓	cognome	Customer surname.	AN
	mail	Buyer’s email address to which the payment result will be sent.	AN MAX 150 CHAR

Payment Result and Notification Message

This table shows the fields provided in response for Skrill ans Skrill 1tap payments.

Mandatory	Name	Description	Format
	SRCEMAIL	The email address that was actually used by the consumer	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Skrill 1tap

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Skrill 1tap using the parameter “selectedcard” enhanced “SKRILL1TAP” during initiation payment phase.
Payment with Skrill 1tap follows the specifications of Simple Payment, however it undergoes the following changes in the Initiation Message, Result Message and Notification Message:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Skrill 1tap, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	nome	Customer name.	AN
✓	cognome	Customer surname.	AN
✓	mail	Buyer’s email address to which the payment result will be sent.	AN MAX 150 CHAR
	Buyer_account	Buyer account on merchant site	AN MAX 64
	skrill_onetapamount	Maximum amount that may be debited. If a 1-Tap maximum amount is specified or the transaction amount exceeds a maximum amount specified previously, an “Initial 1-Tap Payment” is carried out. Customers will be redirected to	

		a Skrill access module before making the actual Payment. Otherwise, the access module will not be displayed. The 1-Tap maximum amount is specified in the smallest unit of the currency (e.g., Cents)

Payment Result and Notification Message

This table shows the fields provided in response for Skrill ans Skrill 1tap payments.

Mandatory	Name	Description	Format
	SRCEMAIL	The email address that was actually used by the consumer	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

PayU

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to PayU using the parameter “selectedcard” enhanced “PAYU” during initiation payment phase.

Payment with PayU is compatible and follows the specifications of the following solutions:

- Single Payment
- I-Frame

However, it undergoes the following changes at the start of payment:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For PayU, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	importo	Amount to be authorised, expressed cents with no separator. The first 2 numbers to the right represent the cents. es.: 5000 is 50,00. **Minimum value that can be used with PayU: "300" (3 Euro).**	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, the	

	only acceptable value being: CZK (Czech crown), PLN (Zloty)

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Blik

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Blik using the parameter “selectedcard” enhanced “BLIK” during initiation payment phase.

Payment with Blik is compatible and follows the specifications of the following solutions:

- Simple Payment
- I-Frame

However, it undergoes the following changes at the start of payment:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Blik, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**
✓	importo	Amount to be authorised, expressed in cents with no separator. The first 2 numbers to the right represent the cents. es.: 5000 is 50,00. **Minimum value that can be used with Blik: "100" (1 Euro).**	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, the **only acceptable value being: PLN (Zloty)**	

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Multibanco

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Multibanco using the parameter “selectedcard” enhanced “MULTIBANCO” during initiation payment phase.

Payment with Multibanco is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. **For Multibanco, the only special characters that can be used are: ^[a-zA-Z0-9.,_-]*$**

Payment Result and Notification Message

This table shows the fields provided in response for Multibanco payments.

Mandatory	Name	Description	Format
	MULTIBANCOSERVICESUPPLIERID	The entity reference of the transaction.	AN
	MULTIBANCOPAYMENTREFERENCE	The payment reference of the transaction.	AN
	TERMINALADDRESSLOCATION	Location of the terminal where the consumer paid.	AN
	TERMINALIDENTIFICATION	The ID of the terminal where the consumer paid.	N
	TERMINALTYPE	Type of terminal where the consumer paid.	AN

Payment notification and outcome: Pending status
With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations
Ppro allows only the bookkeeping operation of starling of transactions for which the funds have been received therefore it will be possible just to effect starlings of transactions in state "Contabilizzato."

Satispay

Activation

To make this payment method available on the cash page, you must activate it in the Nexi back office, in the menu "Pagamenti alternativi", entering the ID received by nexi partner.

Payment

It is possible to redirect users directly to Multibanco using the parameter “selectedcard” enhanced “SATISPAY” during initiation payment phase.

Payment with Multibanco is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Payment notification and outcome: Pending status

With this payment method it will be necessary to manage a further possible "Pending" notification before the final positive or negative outcome notification sent by XPay.

Once the payment has been completed by the user, the new pending outcome can be received. While managing the outcome, XPay will update the order and, if requested in the payment call, the notification will be sent to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.

In this phase, in the event of immediate collection, the order is not accounted for as the order is in a non-final state.

Furthermore, since the payment is in a non-final state, it is necessary not to process the order.

The notification message (and outcome) in the event of a pending outcome, in addition to the standard parameters and any additional parameters of the alternative payment method, will have some additional features:

- The "outcome" parameter will be valued with "PEN".
- The "codAuth" parameter will not be present.

Back office operations

With this payment method it will be necessary to wait for the status "Contabilizzato Rimborsabile" before being able to proceed with the reversal/cancellation function provided by the XPay Backoffice. The technical times for the change of status of a Satispay order from "Contabilizzato" to "Contabilizzato Rimborsabile" can reach a maximum of 3 days.

Only the reversal operation is allowed through Satispay.

Amazon Pay

Activation

To set Amazon Pay service you have to select the “Amazon Pay” option into the back office, in the menu "Pagamenti alternativi".
Into this section it must be entered your merchant ID, client ID and the MWS token obtained from the registration trough Amazon Pay web portal.
Also you can choose to enable or disable the use of the payment method from the checkout page and choose if immediately record the payment otherwise perform independently the accounting form the back office.

For the correct setup of the payment method you must apply some changes in your profile of the PayPal account: how to change your profile.

Payment

The start of payment does not undergo variations compared to the base code.
In case of a valid call XPay will show the “Amazon Pay” logo (if is set and enabled) within the page of choice in the section “Wallet”.

You will be able to redirect your own customers directly to the Amazon Pay checkout page setting the parameter “selectedcard” with “AMAZONPAY” in the start up payment phase. If the checks described above carried out fails, with the use of the option “selectedcard” will be returned an error.

Esempi su GitHub: https://github.com/NexiPayments/XPay/tree/master/metodi-di-pagamento-alternativi/amazonpay

Payment with Amazon Pay is compatible and follows the specifications of the following solutions:

- Single Payment
- Recurring Payment
- XPay Build: basic and recurring payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	XML coded

Payment Result and Notification Message

This table indicates the fields provided in response to Amazon Pay payments

Mandatory	Name	Description	Format
	amazonpay	Contains the response XML file provided by Amazon through the authorization API. For more information on the XML file see the Amazon technical specifications	XML coded

Recurring Payments

To manage recurring payments, follow the instructions in the Recurring Payments section

NOTES:

- It is possible to make subsequent payments only via API.

Operations from back office

From back office you will be able to carry out the standard operations carried out for the cards.

Merchants can choose to integrate Amazon Pay, leaving the payment phase at XPay. In this case, it has to be created the dispay and management of amazonpay's widgets and at his point must be called XPay, through an api rest, to make the payment.

URI
ecomm/api/paga/amazonpay

METHODO
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi	AN MAX 30
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	N MAX 3
timeStamp	Timestamp in milliseconds	N 13 CHAR
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used (only for Recurring Payments)	AN MIN 5 MAX 30
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
amazonpay	Object whose structure is shown in the following table	JSON

Initiation Message: optional fields

Name	Description	Format
urlRisposta	Url where the outcome of the payment will be received at the end of the SCA procedure (Strong Customer Authentication).	AN

Object amazonpay

Name	Description	Format
amazonReferenceId	In case of simple payment use the amazonOrderReferenceId field while in case of the first payment indicated with the presence of the field createContratto = 'S' use the amazonBillingAgreementId field	AN
accessToken	Access token obtained by Amazon login	AN
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN
creaContratto	In case of creation of a new contract valorise ‘S’	AN
scaReady	This parameter, if valued with 'S', indicates that the merchant has adapted the javascript code to manage the SCA procedure (Strong Customer Authentication). (Optional field)	AN

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- apikey
- codiceTransazione
- importo
- divisa
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val> divisa=<val>timeStamp=<val><chiaveSegreta>)

Payment Notification Message

Name	Description	Format
amazonReferenceId	In case of simple payment use the amazonOrderReferenceId field while in case of the first payment indicated with the presence of the field createContratto = 'S' use the amazonBillingAgreementId field	AN
esito	Result of the operation (Possible Values OK, KO)	AN MAX 2
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15
data	Transaction date	DATA dd/mm/yyyy
ora	Operation date	DATA hh:mm:ss
ppo	Payment with wallet (Apple Pay, ecc...)	AN MIN 2 MAX 30
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30

brand	Type of card used by the user to make payment. The possible values are shown in the table here	AN MAX 100
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20
amazonpay	Contains the response XML file provided by Amazon through the authorization API. For more information on the XML file see the Amazon technical specifications	XML codificato
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table Restful API Error Codes Table messaggio -> error details	JSON
timeStamp	Timestamp in milliseconds	N 13 CHAR
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

The error code 96 indicates that the payment to Amazon has failed due to a soft declined, so the merchant will have to re-propose the wallet widget as indicated by Amazon in the documentation. In this case the message field will contain the name of the error obtained: InvalidPaymentMethod or PaymentMethodNotAllowed.
Do not show the widgets again with the JS "OnOrderReferenceCreate" method, otherwise a new Amazon side order will be created. The OnOrderReferenceCreate method should be replaced with the explicit assignment of the Amazon Order ID, as follows: amazonOrderReferenceId: 'YOUR_AMAZON_ORDER_REFERENCE_ID'.

Management change amount based on shipping address

The management of the modification of the amount based on the shipping address selected by the user, is handled only if the merchant has configured the shipping url on the Nexi back office configuration page for Amazon Pay and is asked to show the widget for the collection of shipping data (shipping parameter to Y in the request phase). With these conditions, every time the user changes the shipping address, in the Amazon address widget, the address that has just been selected is notified to the operator. The response expected by the merchant is a POST with the content-type plain / text and in the body the amount, modified or not, and other parameters must appear.

Payment Notification Message

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 Except the “#” character. In case of MyBank you can only use: / - : ( ) . , +
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation	AN 40 CHAR
address1	Address	AN
address2	First address detail	AN
address3	Second address detail	AN
city	City	AN

countryCode	Country code	AN
postalCode	Postal code	AN
stateRegion	State	AN

Mac Calculation

For the reply message, the string to sign must contain the following fields:

- codTrans
- address1
- address2
- address3
- city
- countryCode
- postalCode
- stateRegion
- chiave segreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>address1=<val>address2=<val>address3=<val>city=<val>countryCode=<val>postalCode=<val>stateRegion=<val><chiaveSegreta>)

In response, the merchant must send the new amount calculated based on the shipping address selected by the customer. In the response parameters you must use the same codTrans used to send the customer to the cash page.

Payment Result Message

Name	Description	Format
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. es.: 5000 is 50,00 €	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts	AN MIN 2 MAX 30 Excluding "#" character. In case of activation of the MyBank service, the only special characters that can be used are: / -: (). , +
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

Mac Calculation

For the reply message, the string to sign must contain the following fields codTrans

- divisa
- importo
- chiave segreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

Paypal

Activation

In order to enable this payment method you should go in the back office Nexi in the “PayPal” Tab, in the menu "Pagamenti alternativi", where you should insert your PayPal business account and enabling this payment flagging the “abilita” box present in the Tab

For the correct setup of the payment method you must apply some changes in your profile of the PayPal account: how to change your profile.

XPay handles the Smart Payment Button mode provided by Paypal.

Recurring Payment

In order to enable recurrences in your PayPal account, you need to contact PayPal customer support so that "Reference Transaction" can be activated.To find out whether the service is enabled, you need to consult the "BILLINGAGREEMENTACCEPTEDSTATUS" parameter (1 enabled, 0 not enabled).

Payment

Payment with PayPal is compatible and follows the specifications of the following solutions:

- Single Payment
- Recurring Payment
- XPay Build: basic and recurring payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
	paypalCustom	Additional field that remains in the PayPal order detail. Corresponds to the “Custom number” PayPal field (PAYMENTREQUEST_0_CUSTOM).	
	paypalInvoiceID	Identifies the invoice of the merchant for PayPal, is a unique number so the merchant cannot use the same value for more than one order. The PayPal order detail corresponds to the “Merchant order no.” field (PAYMENTREQUEST_0_INVNUM).	
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	XML coded

Payment Result and Notification Message

This table indicates the fields provided in response to PayPal payments.

Mandatory	Name	Description	Format
✓	PAYERID	Unique identifier of the user's PayPal account.	AN 13 CHAR.
✓	PAYMENTINFO_0_TRANSACTIONID	Unique identifier of the payment transaction.	AN
✓	PAYMENTREQUEST_0_SHIPTONAME	Name and surname attached to the shipping address.	AN 128 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTREET	First shipping address field	AN 100 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTREET2	Second shipping address field. Optional.	AN 100 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCITY	Shipping address city	AN 40 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTATE	Shipping address country or province. The PayPal country code list can be found here.	AN 40 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOZIP	Postal Code	AN 20 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCOUNTRYCODE	Country Code	AN 2 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCOUNTRYNAME	Country	AN 20 CHAR.
	BILLINGAGREEMENTACCEPTEDSTATUS	Indicates whether the customer accepts recurring payments (valued with "1" if he accepts otherwise with "0")	N
	BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

NOTE:

- If you want to enable “recurring” transactions you must contact the customer service of Paypal in order to activate the "Reference Transaction".
  To know if the service is active it is necessary to consult the Outcome parameter "BILLINGAGREEMENTACCEPTEDSTATUS" (1 enabled, 0 not enabled).

- XPay manages the Smart Payment Button and Full Page Redirect modes, available by Paypal. It is possible to enable them in the Paypal section of the Nexi back office.

Paypal - Pay in 3 installments

Payment in instalments with PayPal allows purchases with a value between EUR 30 and EUR 2,000 to be spread over three monthly instalments.

Activation

In order to enable this payment method you should go in the back office Nexi in the “PayPal” Tab, in the menu "Pagamenti alternativi", where you should insert your PayPal business account and enabling this payment flagging the “abilita” box present in the Tab

For the correct setup of the payment method you must apply some changes in your profile of the PayPal account: how to change your profile.

Payment

XPay handles the Smart Payment Button mode provided by Paypal.

Payment with PayPal is compatible and follows the specifications of the following solutions:

- Single Payment
- XPay Build: basic payment
- I-Frame

However, it undergoes the following changes at start-up, outcome and payment notification:

Mandatory	Name	Description	Format
	importo	Amount to be authorised expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. With the payment method "PayPal - Pay in 3 instalments" the minimum amount allowed is 30 €, the maximum amount is 2000 €.	N MAX 8
	paypalCustom	Additional field that remains in the PayPal order detail. Corresponds to the “Custom number” PayPal field (PAYMENTREQUEST_0_CUSTOM).	
	paypalInvoiceID	Identifies the invoice of the merchant for PayPal, is a unique number so the merchant cannot use the same value for more than one order. The PayPal order detail corresponds to the “Merchant order no.” field (PAYMENTREQUEST_0_INVNUM).	
	shipping	If the payment method supports this function, shipping data are provided in response. Possible values: - "N": no shipping data are returned - "S": shipping data is returned This parameter replaces the XPay back office configuration, where it is possible to choose whether to receive the shipping data for payment methods without using the 'shipping' parameter.	XML coded

Payment Result and Notification Message

This table indicates the fields provided in response to PayPal payments.

Mandatory	Name	Description	Format
✓	PAYERID	Unique identifier of the user's PayPal account.	AN 13 CHAR.
✓	PAYMENTINFO_0_TRANSACTIONID	Unique identifier of the payment transaction.	AN
✓	PAYMENTREQUEST_0_SHIPTONAME	Name and surname attached to the shipping address.	AN 128 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTREET	First shipping address field	AN 100 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTREET2	Second shipping address field. Optional.	AN 100 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCITY	Shipping address city	AN 40 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOSTATE	Shipping address country or province. The PayPal country code list can be found here.	AN 40 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOZIP	Postal Code	AN 20 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCOUNTRYCODE	Country Code	AN 2 CHAR.
✓	PAYMENTREQUEST_0_SHIPTOCOUNTRYNAME	Country	AN 20 CHAR.
	BILLINGAGREEMENTACCEPTEDSTATUS	Indicates whether the customer accepts recurring payments (valued with "1" if he accepts otherwise with "0")	N
	BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

Oney

Activation

To make this Payment METHOD available on the checkout page, it is necessary to set up and activate the service by accessing the page dedicated to Oney of the back office in the “Alternative Payments” menu. In this section, to activate the service, it will be necessary to enter the onboarding data received from Oney and select the type of offer to be displayed on the checkout page (3 or 4 instalments with or without fees).
While proceeding with activation, a call will be made to Oney to retrieve the business transactions associated with the merchant. If this call fails, the service will not be enabled.
Depending on the indications of Oney and the modifications made on the Oney terminal, it will be necessary to update the business transactions with the dedicated button available on this page

Payment

Payment with Oney follows the specifications of Simple Payment, however it undergoes the following changes in the Initiation Message:

Initiation Message Payment

Mandatory	Name	Description	Format
✓	nome	Customer name	AN MAX 150
✓	cognome	Customer surname	AN MAX 150
✓	Buyer_email	Cardholder’s email. If the Buyer_email is not valid (it contains the + character or is more than 100 characters long), the standard “mail” parameter is considered.	AN MAX 100 + character not permitted
✓	Buyer_homePhone	Home phone number. At least one of the parameters between “Buyer_homePhone” and “Buyer_msisdn” must be populated. The prefix is required (e.g. "+39").	N MAX 15 Permitted values: ^(\\+)([0-9]{10.15})$
✓	Buyer_msisdn	Mobile phone number. At least one of the parameters between “Buyer_homePhone” and “Buyer_msisdn” must be	^(\\+)([0-9]{10,15})$

		populated. The prefix is required (e.g. "+39").	
✓	Buyer_account	Buyer account on merchant site	AN MAX 64
✓	Buyer_honorific	Customer civility: 0 = Unknown 1 = Mr 2 = Madame 3 = Miss	N MAX 1
✓	Buyer_type	Customer type: 1 = Company 2 = Individuals	N MAX 1
✓	Bill_country	Codice nazione ISO 3166-1 alpha-3 (per fatturazione).	AN 3
✓	Bill_country_label	Delivery country name	AN MAX 38
✓	Bill_street	Street number, street type and street name	AN MAX 38
✓	Bill_cap	Codice postale di fatturazione	AN MAX 10
✓	Bill_city	Delivery city name	AN MAX 100
✓	shipIndicator	Shipping type. Possible values: - 01 = Shipping to the billing address - 02 = Shipping to another address verified by the merchant - 03 = Shipping to an address other than the billing address - 04 = Shipping to or pick-up at the store (store address must be specified in the “destinationAddress” item) - 05 = Digital goods, including online services, electronic gift cards, claim codes - 06 = Travel and event tickets (not shipped) - 07 = Other: for example games, digital services not	N MAX 2

		shipped, electronic media subscriptions.	
✓	deliveryDate	Expected delivery date	DATA yyyy-MM-dd
✓	deliveryMode	Delivery Mode. Possible values are: - 1 = Collection of the goods in the merchant store - 2 = Collection in a third party point (like ups, alveol, etc.) - 3 = Collection in an airport, train station or travel agency - 4 = Carrier (La Poste, Colissimo, UPS, DHL...or any private carrier) - 5 = Electronic ticket issuance, download, etc.	N MAX 2
✓	deliveryTimeframe	Indicator on the delivery period of the goods: 01 = Immediate Delivery (Electronic Delivery). 02 = Same day delivery. 03 = Night delivery. 04 = Delivery in two or more days.	N MAX 2
✓	Dest_country	Country code (ISO3166-1 alpha-3)	AN MAX 3
✓	Dest_country_label	Country label	AN MAX 38
✓	Dest_street	Delivery address	AN MAX 38
✓	Dest_city	Destination city	AN MAX 40
✓	Dest_cap	Destination address post code	AN MAX 10
✓	Item_category_n	Category code. The possible values are: 1 = Food & drinks 2 = Auto & motorcycle 3 = Culture & entertainment 4 = Home & garden	N

		5 = Home appliances 6 = Bidding and multi purchasing 7 = Flowers & gifts 8 = Computers & Software 9 = Health & beauty 10 = Personal services 11 = Professional services 12 = Sport 13 = Clothing & accessories 14 = Travel & tourism 15 = Hifi, photo e video 16 = Telephone & communication Delivery cost and insurance cost must be present with category_code equal to 11, for anti-fraud checks. The amount must be reported in the total amount of the cart (itemsAmount), this can be higher or equal to the amount of the Payment (standard amount field).	
✓	Item_code_n	Item code no. Must be identical to the code of the merchant or the marketplace specified in the cart.	AN MAX 256
✓	Item_description_n	Product description	AN MAX 256
✓	Item_amount_n	Individual element amount no.	N
✓	Item_quantity_n	Item quantity no.	N MAX 3
	Buyer_company	Customer’s Company name. Required field if Buyer_type=1	N MAX 32
	Buyer_fax	Buyer Fax number	N MAX 15
	Buyer_birth_date	Date of birth of the customer.	DATA YYYY-MM-DD

	Buyer_birth_country	Buyer’s Brith Country code (ISO3166-1 alpha-3)	AN MAX 3
	Buyer_citizenship_country	Buyer’s citizenship Country code (ISO3166-1 alpha-3)	AN MAX 3
	Bill_street2	Second line billing address	AN MAX 38
	Bill_street3	Third line billing address	AN MAX 38
	Dest_street2	Second line delivery address	AN MAX 38
	Dest_street_3	Third line delivery address	AN MAX 38
	Dest_pickupPoint	Pickupoint name. Required field if shipIndicator 04 o 02	AN MAX 100
	Dest_name	Recipient Name. This parameter is required field when the field "shipIndicator" is valorized with "03" or if the field "destinationNameIndicator" is valorized with "02".	AN MAX 32
	Dest_surname	Recipient Surname. This parameter is required field when the field "shipIndicator" is valorized with "03" or if the field "destinationNameIndicator" is valorized with "02".	AN MAX 32
	Dest_honorific	Recipient Honorific: 0 = Unknown 1 = Mr 2 = Madame 3 = Miss This parameter is required field when the field "shipIndicator" is valorized with "03" or if the field "destinationNameIndicator" is valorized with "02".	N
	Dest_phone	Recipient phone number. This parameter is required field when the field "shipIndicator" is valorized	AN MAX 15 Valori ammessi:

		with "03" or if the field "destinationNameIndicator" is valorized with "02". The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	destinationNameIndicator	Indicates whether the account name is the same as the shipping name: 01 = Account name identical to shipping address name. 02 = Account name different from the shipping address name. Default is set to "01".	N
✓	Item_main_n	This parameter signals to Oney if it is the main product. 1 = if it is the main product (the most expensive) 0 = the item is not the main item. If no item will be indicated as main item, XPay will set the first item	AN
	itemsNumber	Number of Items. Minimum value 1, if not specified only one item is considered	N
✓	itemsAmount	Total cart amount. Only the amount (“amount” field) will be considered for instalments. The expected value is always “itemsAmount” >= “amount”.	N
✓	oney_offerta	Possible values: - "3X" to offer only 3 installments - 4X" to offer only 4 installments - 3X4X" to offer both 3 and 4 installments	AN
✓	oney_commissione	For a single transaction, merchant can decide to vary the default behavior by valuing:	AN

	- N to indicate not to apply the commission on the single transaction - S to indicate that the commission is applied to the single transaction All values other than N are considered S

NOTE:

The "item" fields refer to the product in the cart. Oney needs information about all the products in the shopping cart, the letter "n" (e.g. Item_category_n) refers to the product numbering (e.g. Item_category_1, Item_code_1, Item_category_2, etc...).

The goods or service must be provided only when the order on the XPay side goes into the "Accounted Refundable"(Contabilizzato Rimborsabile) status. You can check the status of a transaction through the back office portal or via the back office Collections API.

Payment notification: Pending status

With PagoDIL, it will be necessary to manage any additional “Pending” notification before the final positive or negative notification sent by XPay.
Once the payment has been completed by the user, the new pending outcome can be received.
While handling the outcome, XPay will update the order and, if requested in the payment call, notification will be made to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.
In this phase, in the event of immediate collection, the order is not accounted for as it is in a non-final status.
Also, since the payment is in a non-final state, you must not process the order.
The notification message (and outcome) in case of pending outcome, in addition to the standard parameters, will report additional parameters, the outcome PEN and will not have codAuth.

Back office operations

From the back office portal it is possible to carry out the standard operations carried out for the card payments:

- Cancellation of the entire authorized amount.
- Total accounting of the authorized amount. The order will be shown in state "Reimbursable Accounted"(“Contabilizzato Rimborsabile”). Only in this state the merchant will be able to send the goods. They are possible also more partial contabilizations until the attainment of the total one, but only once caught up the total contabilization it will be possible to send the goods.
- Refunds of the accounted amount, 1 or more refunds can be made until the amount of the order is reached.
- See the detail of the transaction containing the standard data.

PagoDIL

Activation

To make this payment method available on the checkout page, it is necessary to set up and activate the service by accessing the page dedicated to PagoDIL of the XPay back office in the “Alternative Payments” menu. In this section, to activate the service, it will be necessary to enter the merchant ID provided by Cofidis and the threshold of amounts and instalments within which the user will view the payment method on the checkout page.

Payment

It is possible to integrate the service with the Simple Payment and XPay Build solutions. Integration through Simple Payment is also available in selectedcard mode by populating the parameter with PAGODIL.
Payment with PagoDIL follows the specifications of **Simple Payment**, but however has the following differences during the payment initiation, result and notification phases:

Payment initiation message: additional fields for PagoDIL

Mandatory	Name	Description	Format
✓	nome	Customer name	AN MAX 150
✓	cognome	Customer surname	AN MAX 150
✓	importo	Amount to be authorised expressed in cents without separator, the first 2 numbers on the right represent cents, e.g.: 5000 corresponds to 50.00. **Minimum value that can be used with PagoDIL: "10000" (100 euro).**	N MAX 8
✓	mail	Email address of the buyer. At least one of the parameters between “mail” and “Buyer_msisdn” must be populated.	
✓	TCONTAB	The field identifies the collection mode that the merchant wants to apply to the individual transaction. If populated with:	

		- C (immediate), the transaction, if authorized, is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - D (deferred), or if the field is not provided, the transaction, if authorized, is managed according to the settings defined in the terminal's profile. Immediate collection is the standard set by Nexi. If you want to manage deferred collections, request activation from technical support. Once enabled, in the case of deferred collection, the collection responsibility is assigned to the merchant, who can manage it from the back office, via API, or at the automatic deadline communicated during profile configuration.	
✓	Buyer_msisdn	Mobile phone number. At least one of the parameters between “Buyer_homePhone” and “Buyer_msisdn” must be populated. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
✓	itemsNumber	Quantity of elements, it is possible to specify at the most 10 cart elements. If the purchase exceeds 10 different items, the merchant must report the most significant items in terms of Unit Price by Quantity. In any case, XPay will send PagoDIL the first 10 elements received.	N MAX 2

✓	Item_code_n	Item code no. Must be identical to the code of the merchant or the marketplace specified in the cart.	AN MAX 256
✓	Item_quantity_n	Item quantity no.	N MAX 3
✓	Item_amount_n	Individual element amount no.	N MAX 10
✓	Item_description_n	Item description no.	AN MAX 250
✓	shipIndicator	Shipping type. Possible values: - 01 = Shipping to the billing address - 02 = Shipping to another address verified by the merchant - 03 = Shipping to an address other than the billing address - 04 = Shipping to or pick-up at the store (store address must be specified in the “destinationAddress” item) - 05 = Digital goods, including online services, electronic gift cards, claim codes - 06 = Travel and event tickets (not shipped) - 07 = Other: for example games, digital services not shipped, electronic media subscriptions.	N MAX 2
	OPTION_CF	Customer tax code	AN MAX 16
	Dest_street	Delivery address	AN MAX 38
	Dest_street2	Second line delivery address	AN MAX 38
	Dest_street_3	Third delivery address line	AN MAX 38

	Dest_city	Destination city	AN MAX 40
	Dest_state	Delivery province abbreviation Mandatory if shipIndicator 01, 02, 03, 04	AN MAX 2
	Dest_cap	Destination address post code	AN MAX 10
	Dest_country	Delivery country code in ISO 3166-1 alpha-3 format. Mandatory if shipIndicator 01, 02, 03, 04	AN MAX 3
	Buyer_homePhone	Home telephone number. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	Bill_street	Billing address	AN MAX 40
	Bill_street2	Second billing address line	AN MAX 10
	Bill_street3	Third billing address line	AN MAX 10
	Bill_city	Billing city	AN MAX 100
	Bill_state	Billing province abbreviation	AN MAX 2
	Bill_cap	Billing post code	AN MAX 8
	Bill_country	ISO 3166-1 alpha-3 country code (for billing).	AN 3
	itemsAmount	Total cart amount. Only the amount (“amount” field) will be considered for instalments. The expected value is always “itemsAmount” >= “amount”.	N
	numberOfInstalment	Number of financing instalments. If the number is not provided in input (or it is not numerical), the maximum number of	N MAX 3

		instalments permitted for the product(s) established when entering into the agreement with Cofidis will be used.	
	pagodilOfferID	Code identifying the Cofidis financial product that the Merchant wants to use for financing. Corresponds to the product code with a length of 2 for Cofidis systems. Warning: if the number is not provided in input, the system will use the only product code established when the agreement was entered into. If multiple product codes were established when the agreement was entered into, this number is mandatory	N MAX 10
	frequencyOfInstallment	Frequenza di pagamento delle rate della dilazione. Valori ammessi: 1 = Mensile. Se errato o non indicato sarà utilizzato il valore di default su Cofidis	N MAX 1
	pagodilSGP	Value to be used to specify a particular promotion.	AN MAX 10
	externalClass	Usable for any identification, grouping and reporting requested by the Merchant. For example, for distribution of internal commissions, incentives or analyses.	AN MAX 30
	Item_category_n	Category code. The possible values are: 1 = Food and beverages 2 = Cars and Motorcycles 3 = Culture and	N

		Entertainment 4 = Home and Garden 5 = Domestic Appliances 6 = Multiple Offers and Purchases 7 = Flowers and Gifts 8 = Computers & Software 9 = Health and Beauty 10 = Personal Services 11 = Professional Services 12 = Sport 13 = Clothing and Accessories 14 = Travel and Tourism 15 = Hifi, Photos and Videos 16 = Telephones and Communications	
	destinationNameIndicator	Specifies whether the name on the account corresponds to the name specified for shipping: 01 = Account name identical to the shipping address name. 02 = Account name different from the shipping address name. “01” is populated by default. If destinationNameIndicator = 02, the following fields will be used: name (Dest_name), surname (Dest_surname) and Buyer_msisdn.	N
	chUsualIp	IP address of the customary device.	AN MAX 40
	nbPurchaseAccount	Number of purchases of this account in the last 6 months	N MIN 1 MAX 4
	nbPurchaseAmount	Cumulative amount of orders placed by the customer in the last 6 months.	N MAX 10

	chAccDate	Date of account activation on the merchant's website	DATA yyyy-MM-dd
	chFirstPurchaseDate	Date of first customer purchase on the merchant's website	DATA yyyy-MM-dd
	chLastPurchaseDate	Date of last customer purchase on the merchant's website.	DATA yyyy-MM-dd

NOTES:

- The "item" fields refer to the cart product. Cofidis needs information regarding the products present in the cart, letter "n" (e.g., Item_quantity_n) refers to the product numbering (e.g., Item_quantity_1, Item_code_1, Item_quantity_2, etc.).
- If a mandatory parameter is not present or is incorrect, the checkout page will not display the button.
  To help developers identify the reason in the browser console, in test environments, a log will be displayed with the reason for the error.
  If an optional parameter is incorrect, it will not be sent to PagoDIL.

Payment notification: Pending status

With PagoDIL, it will be necessary to manage any additional "Pending" notification before the final positive or negative notification sent by XPay.
Once the payment has been completed by the user, the new pending outcome can be received.
While handling the outcome, XPay will update the order and, if requested in the payment call, notification will be made to the address indicated in the "urlpost" parameter, with possible cancellation in case of failure.
In this phase, in the event of immediate collection, the order is not accounted for as it is in a non-final status.
Also, since the payment is in a non-final state, you must not process the order.
The notification message (and outcome) in case of pending outcome, in addition to the standard parameters, will report additional parameters, the outcome PEN and will not have codAuth.

Mandatory	Name	Description	Format
✓	esito	Only value permitted PEN	AN
✓	ProcedureCode	Dossier number type	AN MAX 2
✓	DossierNumber	Dossier number	AN MAX 12
✓	AcceptanceNumber	Acceptance number	AN MAX 10
✓	RejectionCode	Rejection reason	AN MAX 5
✓	IdDocType	Possible values: 3-Passport, 4-ID card, 5-Driver's licence	AN MAX 12
✓	IdDocNumber	Document number	AN MAX 14
✓	BillingReference	Billing reference	AN MAX 40

On conclusion of the pending notification, there will be a redirect to the receipt or the result page. Subsequently, the notification with the final result will be received.

Final notification message: additional fields for PagoDIL

Obbligatorio	Nome	Descrizione	Formato
✓	codAut	Authorisation code assigned by the credit card issuer, present only with authorisation granted. Only value permitted: PDIL	AN
✓	numeroMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
✓	eventType	Type of event that triggered the notification, only possible value: FINAL	AN

Back Office Operations

From the back office, merchants can perform standard operations carried out for cards:

- Accounting: total accounting of the authorised amount is permitted (subsequent to notification with final result)
- Refunds/Cancellations: only total refunds/cancellations are possible, always after final confirmation.

NOTES:

- Accepted PagoDIL practices will be found in the back office in the " Autorizzato " or " Contabilizzato " status based on the type of collection set up on the merchant's terminal.
- The PagoDIL practices denied or in error will be found in the back office in the " Rifiutato " status.

Pagolight

Activation

In order to make this payment method available on the till page, it is necessary to configure and activate the service by accessing the Pagolight page of the XPay back office, within the 'Alternative Payments' menu. In this section, you will need to enter the merchant key provided by Pagolight to activate the service.
Below are the instructions for activating Pagolight in your e-commerce: Pagolight activation guide.

Payment

It is possible to integrate the service via Simple Payment and XPay Build. Integration via Simple Payment is also available in selectedcard mode by enhancing the parameter with 'PAGOLIGHT'.
Payment with Pagolight is compatible with and follows the specifications of the following solutions:

- Easy Payment
- XPay Build: basic Payment

However, it undergoes the following changes at the start of payment:

Mandatory	Name	Description	Format
✓	importo	amount to be authorised expressed in cents without separator, the first 2 numbers on the right represent the cents, e.g.: 5000 corresponds to 50.00. **Values allowed by Pagolight:** **- Minimum amount: '6000' (60 euro).** **- Maximum amount: '500000' (5000 euro).**	N MAX 8

Back Office Operations

Merchants from the back office will only be able to make total or partial reversals on orders shown as booked.

Deposit Methods

Nexi provides two ways to manage your deposits:

- Using the profile specifications set during configuration
- Using the TCONTAB parameter within the Payment Initiation call

When managing receipts through the use of profiles, the default time for posting the transaction is set to midnight on the day in which the transaction takes place. There is, however, the option of extending the number of days (MAX 5), and deferring a decision on which operation to carry out when the deadline is reached: either processing or cancelling the transaction.

Using the TCONTAB parameter, the merchant can manage each transaction deposit dynamically by setting the parameter to "C" for immediate deposit, even if the profile has been set to deferred accounting.
If this parameter is set to "D" or is not populated, the merchant can manage the transaction through the Nexi back office or the back office APIs. If this doesn’t occur, then the authorised payment is managed according to whatever is shown in the profile.

XPAY BUILD

Xpay Build is a Nexi solution that allows you to include XPay in your Ecommerce in a complete customizable way with a low impact on PCI – DSS standards.

What's XPay Build?

XPay Build is an approach that allows the merchant to host the payment form within their portal, without redirecting the customer to the XPay checkout page, avoiding having to manage the card data.
In fact, the fields where the cardholder enters this information are contained in an iFrame connected to the XPay server, ensuring the security of the card data and at the same time making the shopping experience better.
Xpay Build makes available HTLM interface components ready to be used as input fields and bottons to receive cardholder's informations. They are configurable through a Javascript library downloadable from XPay server.
The forms concerns both card data and the choise of alternative payment methods qualified on your profile as ApplePay, Paypal, Klarna PayNow Sofort, etc.
At a technical level, the entered card data is managed by the Javascript library which communicates them to the XPay server.
A token is generated and the library returns it to merchant's server to be used to precess the payment through API.

XPay Build includes:
Automatic formatting of card information
Translation of the indications of the form in the customer's preferred language
Customizable style to match the appearance of the payment form with the look & feel of your portal.

Are pre-requisites necessary?

The integration in this mode requires that the merchant page is hosted on a "secure url" (https), because the card data while never passing on the merchant's server, are collected by the Nexi iframes hosted on the pages of the merchant itself, and therefore accessible from scripts for the front end.
The PCI certification level required is SAQ A (the one with questionnaire), not SAQ- D (as for server to server integration, much more expensive)

Important information

- **Privacy policy**: you must report the **Nexi privacy policy**, available at the link **https://www.nexi.it/privacy/xpay.html** .
  We advise you to quote the indicated link directly on the page, so that the text is always updated.

- **Accepted payment circuits and security protocols:** the **logos of the accepted payment circuits** and of the **activated security protocols**, which can be downloaded from the **download area** of the Nexi website, must be displayed and kept up-to-date on the website.

Payment circuits require the above information to be entered on the payment page, where the user enters their card details.

Description

The architecture and payment process are described in the web version of XPay Build, which uses a Javascript SDK client.

The XPay Build solution consists of the following elements:

- Custom cash page hosted on the merchant domain with certificate (https) containing DIV html specific for the inclusion of iFrame by Javascript Nexi

• Non-intrusive XPay Javascript library hosted on the cash page that, after appropriate configuration, is able to build iFrame containing the form for card data or the list of alternative payment methods such as ApplePay, Paypal (etc)

• Merchant's Backend receives the xpayNonce (random code valid for the single transaction) and uses it for server-to-server payment through API PayXpayNonce

Do not forget

- The xpayNonce can only be used once and has a 10-minute deadline: if these two conditions are not met, the payment will return an error
- Management of payment retry is delegated to the merchant: this means that, if there is an error in the first payment attempt but the merchant is authorized to use n attempts for each order number, it will be merchant's responsibility to reissue the form data acquisition and request the generation of a second xpayNonce, re-engaging in fact a new payment
- The SDK executes javascript calls in CORS (Cross Origin Resource Sharing) mode; it is necessary to verify that the merchant's network infrastructure does not prevent it in any way
- The XPay Build solution is not compatible with the DCC service

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/build

Card data collection form

To implement the XPay Build solution, some steps are required:

SDK Xpay inclusion

In order to start, include the XPay javascript SDK in the header of your page:

TEST ENVIRONMENT URL

```
<script
    src="https://int-ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

PRODUCTION ENVIRONMENT URL

```
<script
    src="https://ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

The alias parameter must be evaluated with the apiKey (or alias) of the merchant

XPay uses the following Content Security Policy:

default-src 'self' 'unsafe-inline' 'unsafe-eval' https:; img-src 'self' 'unsafe-inline' 'unsafe-eval' https: data:; frame-ancestors https:;

Create the payment form

To allow the SDK to create an item hosted on XPay, for the secure collection of card data, enter an empty div with a unique id within the form.
Within your page you can provide a component where you will enter the validation messages of the card data, XPay will take care to validate and provide any error messages to your cash page, while the visualization and graphic personalization of the message will be by the merchant page. In the example the div xpay-card-errors will be used to show the errors. The payment call must be from the merchant's server and not be done client-side. For this reason the form has as its action a merchant endpoint, to which the form post will be executed and from which the call will be made to the “pagaNonce” to make the payment with the xpayNonce provided by the SDK.

Environment configuration

Once the page is loaded, to initialize the SDK, call the function:

XPay.init();

After that configure the SDK with the function:

XPay.setConfig(config);

Passing as parameter the object containing the payment configuration. The tables below show the structure

Mandatory	Name	Description	Format
•	baseConfig	Object whose structure is shown in the tables below	JSON
•	paymentParams	Object whose structure is shown in the tables below	JSON
•	customParams	Object whose structure is shown in the tables below	JSON
	language	Language identifier	AN Possible values: XPay.LANGUAGE.ITA, XPay.LANGUAGE.JPN, XPay.LANGUAGE.SPA, XPay.LANGUAGE.RUS, XPay.LANGUAGE.FRA, XPay.LANGUAGE.ARA, XPay.LANGUAGE.ENG, XPay.LANGUAGE.GER, XPay.LANGUAGE.CHI, XPay.LANGUAGE.POR
	serviceType		AN
	requestType		AN

Object baseConfig

Mandatory	Name	Description	Format
•	apiKey	Alias assigned by Nexi to merchant	AN MAX 30
•	enviroment	Implementation environment	AN

Object paymentParams

Mandatory	Name	Description	Format
✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	transactionId	Payment identification code consisting of alphanumeric characters, excluding the # " ' characters. The code must be unique for each authorization request.	AN MIN 2 MAX 30
✓	currency	The code of the currency with which the amount is expressed	AN MIN 3 MAX 3 admitted only EUR
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	
✓	url	Url of the merchant towards which the gateway directs the user at the completion of the transaction passing, in GET, the response parameters with the result of the transaction. The value of the field must begin with "http://" or "https://" and the standard ports 80 or 443 must be used. The parameter is mandatory, but is only used for Alternative Payments Methods, it is ignored for cards.	AN MAX 500
✓	url_back	Url called in case the user decides to abandon the transaction during the payment phase on the checkout page	In case of esito=ANNULLO, the merchant may decide to send the user back to the payment page

		(outcome=CANCEL) or in case the call contains formal errors (outcome=ERROR). The value of the field must begin with "http://" or "https://" and the standard ports 80 or 443 must be used. The parameter is mandatory, but is only used for Alternative Payment Methods, it is ignored for cards.	with the same transaction code.
	urlPost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.The parameter is used only for Alternative Payment Methods, it is ignored for cards.	AN MAX 500

Object customParams

Mandatory	Nome	Descrizione	Format
	3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the request for 3DS exemption in all OneClick payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with: - "SCA": the 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- secretKey

SAMPLE STRING
MAC = HASH SHA1(codeTrans=<val>divisa=<val>importo=<val><secretKey>)

Separate the fields of the credit card data collection form

This mode allows you to separate each element of the card data, so to allow the merchant a free positioning within his own page.

The XPay Build initialization part remains unchanged respect to what is described in the previous paragraph.

To create the three distinct elements for collecting card data, you will need to specify the XPay.OPERATION_TYPES.SPLIT_CARD option within the "create" function. Then run the "mount" function by specifying the id of the three divs, unique within the page, in which to draw the different elements. In order, the "mount" function accepts the div for the pan, the one for the expiration date and lastly the div for the cvv:

```
    style={
        common:{
            color: "#ff00AA",
            fontSize: "17px",
           ":hover": {
                color: "#12AA12"
         },
         error:{
            color: "#ff0000",
           fontSize: "Arial, monospace"
         },
    };
    //Creating the card element object
    var card = XPay.create(XPay.OPERATION_TYPES.SPLIT_CARD, style);
   card.mount("xpay-pan", "xpay-expiry", "xpay-cvv");
}
```

The element accepts a json to customize the form that will be issued, for details on the configuration fields, their meaning and possible values, refer to the "Creating and viewing card data element" paragraph.

As in the unique version, it is possible to specify which card brands the build accepts, specifying, when creating the div, an array containing the brands to accept.

```
    //   Creating the card element object
    var acceptedCards = [XPay.CardBrand.MASTERCARD, XPay.CardBrand.VISA];
    var card = XPay.create(XPay.OPERATION_TYPES. SPLIT_CARD, style,
acceptedCards);
    card.mount("xpay-pan", "xpay-expiry", "xpay-cvv");
}
```

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol with XPay Build, refer to the 3D Secure Management section

Creating and displaying card data element

To create the element that will handle the card data you must use the function:

var card = XPay.create(XPay.OPERATION_TYPES.CARD, style);

Passing the object containing the style configuration of this element as a second parameter. The tables below show the structure

Mandatory	Name	Description	Format
	common	Object that describes the standard style with which the form will be shown. Its structure is described in the table below.	JSON
	error	Object that describes the style of the form in case of errors. Its structure is described in the table below.	JSON
	correct	Object that describes the style of the form in case of NO errors. Its structure is described in the table below	JSON

Mandatory	Name	Description	Format
	color	Coincide with property 'color' of CSS.	hexadecimal
	fontFamily	Coincide with property ' font-family ' of CSS.	Use valid 'font-family'
	fontSize	Coincide with property ' font-size ' of CSS.	Accepted format: -17px -1.3em - 10%
	fontStyle	Coincide with property ' font-style' of CSS.	Possible: -normal -italic - oblique
	fontVariant	Coincide with property ' font-variant' of CSS.	Use valid 'font-variant'
	letterSpacing	Coincide with property ‘letter-spacing’ of CSS.	Accepted format: -17px -1.3em - 10%
	textDecoration	Coincide with property ‘text-decoration’ of CSS.	Use valid 'text-decoration'
	textShadow	Coincide with property ‘text-shadow’ of CSS.	Use valid 'text-shadow'

You can also customize the pseudo classes by including the specific configuration for each of them in the correct, error and common objects. Each object that describes the style of a pseudo-class may contain the fields described in the table above.
Example:

```
var style = {
    common: {
        color: '#FF0033',
        ':hover': {
            color: '#FF3300'
        }
    }
};
```

You can custom the following pseudo classed:

- :placeholder
- :selection
- :focus
- :hover
- :focus::placeholder
- :hover::placeholder
- :focus::selection
- :hover::selection

To show the inputs of cards use the function:

card.mount("xpay-card");

passing as parameter div id in which they will be shown.

It is possible to specify which card brands are accepted by XPay Build by specifying an array containing the brands to be accepted. Possible brands are:

- XPay.CardBrand.AMEX
- XPay.CardBrand.DINERS
- XPay.CardBrand.MAESTRO
- XPay.CardBrand.MASTERCARD
- XPay.CardBrand.VISA
- XPay.CardBrand.JCB
- XPay.CardBrand.UPI

```
// Creation of the object of the card element
    var acceptedCards = [XPay.CardBrand.MASTERCARD, XPay.CardBrand.VISA];

    var card = XPay.create(XPay.OPERATION_TYPES.CARD, style, acceptedCards);
    card.mount("xpay-card");
```

If the acceptedCards array is not specified, or is empty, all the brands enabled on the merchant profile are accepted. If a brand not supported by the merchant is inserted into the array, it will be ignored.

Creating buttons for alternative payment methods

Through SDK you can create buttons that allow the customer to use other payment methods. To do this, use the function:

var buttons = XPay.create(XPay.OPERATION_TYPES.PAYMENT_BUTTON, []);

passing as second parameter an empty array to display all the payment methods available for your profile or an array containing only the desired methods (always considering those active on your profile). You can choose from the following payment methods:

- XPay.PaymentMethods.APPLEPAY
- XPay.PaymentMethods.AMAZONPAY
- XPay.PaymentMethods.PAYPAL
- XPay.PaymentMethods.MYBANK
- XPay.PaymentMethods.ALIPAY
- XPay.PaymentMethods.WECHATPAY
- XPay.PaymentMethods.GIROPAY
- XPay.PaymentMethods.IDEAL
- XPay.PaymentMethods.EPS
- XPay.PaymentMethods.BCMC (Bancontact)
- XPay.PaymentMethods.P24 (Przelewy24)
- XPay.PaymentMethods. SKRILL
- XPay.PaymentMethods. SKRILL1TAP
- XPay.PaymentMethods. PAYU
- XPay.PaymentMethods. BLIK
- XPay.PaymentMethods. MULTIBANCO

To display these bottons use the function:

buttons.mount("xpay-btn");

passing as parameter div id in which they will be shown.

Management of events triggered by SDK

The events to manage for the correct use of the XPay Build solution are the following:

- 'XPay_Ready' which communicates the loading of the paper data form or the buttons for alternative methods
- 'XPay_Payment_Started' which is triggered when the user selects an alternative payment method
- 'XPay_Card_Error' which communicates any validation errors of the inputs present in the form
- 'XPay_XpayNonce' which communicates the xpayNonce, generated with the card data entered by the cardholder, to be sent to the merchant's server to continue with the payment via the 'payXpayNonce' API

The script of the merchant page will have to worry about listening to the two events following their own implementation choices.
The only event to be managed if you implement the part of buttons that manages alternative payment methods is:

- 'XPay_Payment_Result' which communicates the outcome of the payment for Paypal, ApplePay and Google Pay in the full redirect version, in case of non-fullredirect use, therefore with pop up on the merchant page, it will be used for all payment methods. The management of the event is the task of the merchant's script.

NOTES:
Similarly, it is not possible to manage the other payment methods (MyBank, etc.) for security limitations of the different types of payment, in these cases the current management of the cash pages with url, urlBack and possibly urlPost remains valid.

Create xpayNonce

To generate xpayNonce, that will be used by the merchant server to make the payment, you have to use the function:

XPay.createNonce("payment-form", card);

passing as the first parameter the id of the form used to contain the card data and as a second parameter the card object generated previously through the SDK.

In this phase, when the createNonce function is called up, an iframe for 3D Secure authentication will be opened on the interface side; once authentication by the user has been completed, the nonce will be obtained with which to proceed to payment.

In the response JSON, in addition to the nonce, the object "dettaglioCarta" with the following structure is reported:

“dettaglioCarta”: {
“brand”: “MASTERCARD”,
“tipoProdotto”: “PROPRIETARY ATM - DEBIT - N”,
“prepagata”: “N”,
“pan”: “525599******9992”,
“scadenza”: “202012”,
“regione”: ““,
“nazionalita”: “USA”
}

Mandatory	Name	Description	Format
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table Card Type Coding	AN MAX 100
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200

✓	prepagata	It is enhanced with S or N, if the card is prapaid or not	AN
✓	pan	credit card number masked. In plain text only the first 6 and last 4 digits	N MIN 16 MAX 19 NNNNNN******NNNN
✓	scadenza	Credit card expiry date	DATA aaaamm
✓	regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30
✓	hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for payment.	AN 28 CHAR.

NOTES:

- The dynamic 3D Secure service can be activated by contacting Nexi support. This service can be used to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all payments.
- The card data collection form has no border, but it is possible to draw a border around the div:

  id="xpay-card" style="border: 1px solid #cdcd;max-width: 300px;

- The nonce can only be used once and has a time limit of 10 minutes: if these two conditions are not met, the payment will return an error.
- The management of the payment retries is delegated to the merchant: this means that if there is an error in the first payment attempt but the merchant is authorised to use n attempts for each order number, it will be the merchant's responsibility to re-issue the card data capture form and request the generation of a second nonce, effectively re-entering a new payment.
- The SDK performs javascript calls in CORS (Cross Origin Resource Sharing) mode; it is necessary to verify that the merchant's network infrastructure does not prevent them in some way.
- The XPay Build solution is not compatible with the DCC service.
- The iframe responsible for the 3D Secure procedure cannot be resized or positioned.

Basic payment

The merchant backend receives the xpayNonce along with all other fields in the form and, upon optional validation of the output mac, initiates a payment with the RESTful pagaNonce API described below. Note that the order data to be used for payment (amount, currency, order number) are those sent by the merchant at this stage; all data sent by the merchant in the xpayNonce generation step are stored by XPay (together with the xpayNonce itself), but used only for a consistency check between the two phases (to make sure that the request for a new xpayNonce and its use for a payment are generated by the same entity and for the same purpose). However, it is essential that the backend merchant, in the server to server phase, supply the correct data to XPay.

The management of the outcome (through the parsing of the pay payXpayNonce response) is entrusted to the merchant, as per the practice of payments via RESTful API.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/build/pagamento-base

URI
ecomm/api/hostedPayments/pagaNonce

METHOD
POST

ACCEPT
application/json

Initiation message

Name	Description	Format
apiKey	Alias assigned by Nexi to merchant	AN MAX 30
codiceTransazione	Payment identification code consisting of alphanumeric characters, excluding the # and _ characters. The code must be unique for each authorization request.	AN MIN 2 MAX 30
importo	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
divisa	Transaction identifier assigned by the merchant. Only admitted 978 (Euro)	N MAX 3

xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36
timeStamp	Timestamp in millisecond format	N 13 CHAR
tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment It is necessary to pass this parameter inside the "parametriAggiuntivi" object and inside the MAC calculation as a parameter before the timestamp.	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

MAC Calculation

MAC Calculation For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment Result Message: required fields

Name	Description	Format
esito	Result of the request (Possible values OK, KO)	AN MAX 2
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
codiceConvenzione	Merchant code assigned by the acquirer (where expected)	AN MAX 15
data	Transaction date	DATA MAX 8 aaaammgg
ora	Transaction time	DATA hh:mm:ss
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
tipoTransazione	Indicates the payment method. See the table Transaction Type Coding for possible values. In case of payment with negative result an empty string will be sent	AN MAX 20
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table Restful API Error Codes Table messaggio -> error details	JSON
timeStamp	Timestamp in millisecond format	N 13 CHAR
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- The codiceTransazione, importo, divisa, and apiKey parameter must be the same as the XpayNonce request, otherwise an invalid data error will be received. This error can also occur if more than 10 minutes have passed since the xpayNonce was generated.

- In the event of a KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and calling the createNonce directly, indicating "true" as the last parameter:
  XPay.createNonce("payment-form", card, undefined, true);
  The html code that forces the SCA is received in response, in order to obtain a new nonce to be used in the payNonce API.

- The XPay Build solution is not compatible with retries.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.

If you are instead interested in a solution that allows the end customer to store their credit card data, and use it later to make purchases more quickly, refer to the OneClick solution.

Recurring Payments are also identified with the term “MIT” (Merchant Initiated Transaction). MITs are broken down into:

- Scheduled: debited with defined frequency (e.g. first of each month).
- Unscheduled: debited with undefined frequency.

It is necessary to notify XPay support of the type of debits that will be made by your store, as it is necessary to properly configure the assigned Nexi profile.

It is not permitted to use contract numbers created through MIT Scheduled payments to carry out MIT Unscheduled transactions, and vice versa.

At a technical level, this service consists of two stages:

- First Payment
- Subsequent Payments

The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/build/pagamento-ricorrente

First payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.

If you are instead interested in a solution that allows the end customer to store their credit card data, and use it later to make purchases more quickly, refer to the OneClick solution

Create a contract through a valid xpayNonce. During the nonce creation phase, the following parameters must be included in the "config" object:

Mandatory	Name	Description	Format
✓	requestType	The field must be enhanced with: "PP"	AN
✓	serviceType	The field must be enhanced with: "paga_multi"	AN

And in the object "customParams" the following:

Mandatory	Name	Description	Format
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes

The xpayNonce field is the generated xpayNonce with the creaNonce API. The transactionCode, importo, currency, and apiKey must be the same as the XpayNonce request, otherwise an invalid data error will be received. This error can also occur if more than 10 minutes have passed since the xpayNonce was generated. In the case where the codiceGruppo field is present, the contract will be created for the group, otherwise only for the terminal associated with the alias.

URI
ecomm/api/hostedPayments/pagaNonceCreazioneContratto

METHODO
POST

ACCEPT
application/json

Payment Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30

✓	codiceTransazione	Payment identification code consisting of alphanumeric characters, excluding the # and _ characters. The code must be unique for each authorization request.	AN MIN 2 MAX 30
✓	importo	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	divisa	Transaction identifier assigned by the merchant. Only admitted 978 (Euro)	N MAX 3
✓	xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used	AN MIN 5 MAX 30
✓	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment It is necessary to pass this parameter inside the "parametriAggiuntivi" object and	

		inside the MAC calculation as a parameter before the timestamp.	
	mail	Buyer’s email address to which the payment result will be sent.	AN MAX 150
	nome	Name of the person who made the payment.	AN MAX 150
	cognome	Surname of the person who made the payment.	AN MAX 150
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 Excluding the # ‘ “ characters For MyBank: AN MAX 140 CHAR anche you can use just these special characters/ - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order. This data will also be reported in the report that can be queried from the back office	AN MAX 200

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Payment Result Message

Mandatory	Name	Description	Format
✓	esito	Result of the request (Possible values OK, KO)	AN MAX 2
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	codiceAutorizzazione	Confirmation code issued by the card issuer	AN MAX 6
✓	codiceConvenzione	Merchant code assigned by the acquirer where expected	AN MAX 15
✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	ora	Transaction time	DATA hh:mm:ss
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
✓	tipoTransazione	Indicates the payment method. See the table Transaction Type Coding for possible values. In case of payment with negative result an empty string will be sent	AN MAX 20
✓	errore	Only present when the result is ko. It is an object containing:	JSON

		codice -> error code, see table Restful API Error Codes Table messaggio -> error details	
✓	timeStamp	Timestamp in millisecond format	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table Card Type Coding	AN MAX 100
✓	scadenzaPan	Payment card expiry date	DATE yyyymm
✓	pan	credit card number masked. In plain text only the first 6 and last 4 digits	N MIN 16 MAX 19 NNNNNN******NNNN

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

In the event of a KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and calling the createNonce directly, indicating "true" as the last parameter:
XPay.createNonce("payment-form", card, undefined, true);
The html code that forces the SCA is received in response, in order to obtain a new nonce to be used in the payNonce API.

Subsequent Payment

Every time the registered user makes a subsequent purchase, the e-commerce must send, to Nexi, a call with the data of the contract previously registered in the first payment stage.

For server-to-server mode, the services exposed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and the responses are a JSON formatted object. Alternatively, non-Rest APIs are available where communication is managed synchronously (with https + a series of parameters and values). The result message is an xml managed on the same connection.

The endpoints of the environments are as follows:

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it

URI
ecomm/api/recurring/pagamentoRicorrente

METHOD
POST

ACCEPT
application/json

Subsequential payment initiation message: required fields

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 5 MAX 30
✓	codiceTransazione	Payment identification code consisting of alphanumeric	AN MIN 2 MAX 30

		characters, excluding the # and _ characters. The code must be unique for each authorization request.	
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
✓	divisa	Only accepted 978 for Euro	N MAX 3
✓	scadenza	Credit card expiry date	DATA aaaamm
✓	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation	AN 40 CHAR
	parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message. In the following table an example of parameters:	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
	mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
	nome	Name of the person who made the payment.	AN MAX 150
	cognome	Surname of the person who made the payment.	AN MAX 150

	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 Excluding the # ‘ “ characters For MyBank: AN MAX 140 CHAR anche you can use just these special characters/ - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order. This data will also be reported in the report that can be queried from the back office	AN MAX 200
	TCONTAB	The field identifies the collection method that the merchant wants to apply to the single transaction, if valued with: - C (immediata) the transaction if authorized is also collected without further intervention by the operator and without considering the default profile set on the terminal. - D (differita) or the field is not entered the transaction if authorized is managed according to what is defined by the terminal profile	AN MAX 20

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- scadenza
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val> divisa=<val>scadenza=<val>timeStamp=<val><chiaveSegreta>)

NOTES:
If the 'scadenza' parameter is not used in the start-up parameters, include it in the MAC calculation without valorising it

Payment Result Message: required fields

Name	Description	Format
esito	Operation result (Possible values OK, KO)	AN MAX 2
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15
data	Transaction date	DATA MAX 8 aaaammgg
ora	Transaction time	DATA hh:mm:ss
nazione	Credit card countr	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30
brand	Type of card used by the user to make payment. The possible values are shown in the table Card Type Coding	AN MAX 100
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
tipoTransazione	Indicates the payment method. See the table Transaction Type Coding for possible values. In case of payment with negative result an empty string will be sent	AN MAX 20
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table Restful API Error Codes Table messaggio -> error details	JSON
timeStamp	Timestamp in millisecond format.	N 13 CHAR

mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation	AN 40 CHAR

Payment Result Message: optional fields

Name	Description	Format
dettagliCarta	Object whose structure is shown in the following table	JSON

dettagliCarta Element

Name	Description	Format
maskedPan	Masked pan of used card	AN
expiry	Expiring date	DATA aaaamm
hashPan	hashPan to be verified for association.	AN
hashAlg	Algorithm used	AN
updateTime	Date of last update of the card data	DATA
updateChannel	"N.D." "BACK OFFICE" "PAYMENT" "CIRCUITI"	AN
state	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

MAC Calculation

For the transaction result message, the string to sign must contain the following fields

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- Transactions executed through recurring payments cannot be partially accounted for.
- If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. " parametriAggiuntivi ": {}

- Contract numbers created through MIT Scheduled payments cannot be used to make MIT Unscheduled transactions and vice versa
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

OneClick Payment

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/build/pagamento-oneclick

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.

At a technical level, the management of this solution is divided into 2 phases:

- First payment
- Subsequent payments

The first payment and subsequent payments are subject to Strong Customer Authentication (SCA), the customer will then be redirected to the 3DS protocol for authentication.

First payment

Create a contract through a valid xpayNonce. During the nonce creation phase, the following parameters must be included in the "config" object:

Mandatory	Name	Description	Format
✓	requestType	The field must be enhanced with: "PP"	AN
✓	serviceType	The field must be enhanced with: "paga_oc3d". ‘paga_multi’ to have the option of also making recurring payments	AN

And in the object "customParams" the following:

Mandatory	Name	Description	Format
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes

The xpayNonce field is the generated xpayNonce with the creaNonce API. The transactionCode, importo, currency, and apiKey must be the same as the XpayNonce request, otherwise an invalid data error will be received. This error can also occur if more than 10 minutes have passed since the xpayNonce was generated. In the case where the

codiceGruppo field is present, the contract will be created for the group, otherwise only for the terminal associated with the alias.

URI
ecomm/api/hostedPayments/pagaNonceCreazioneContratto

METHODO
POST

ACCEPT
application/json

Payment Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
✓	codiceTransazione	Payment identification code consisting of alphanumeric characters, excluding the # and _ characters. The code must be unique for each authorization request.	AN MIN 2 MAX 30
✓	importo	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	divisa	Transaction identifier assigned by the merchant. Only admitted 978 (Euro)	N MAX 3
✓	xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used	AN MIN 5 MAX 30
✓	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message. In the following table an example of parameters	AN MAX 4000 do not use these name, they are used by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL
	mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
	nome	Name of the person who made the payment.	AN MAX 150
	cognome	Surname of the person who made the payment.	AN MAX 150
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 Excluding the # ' " characters For MyBank: AN MAX 140 CHAR anche you can use just these special characters/ - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order. This data will also be reported in the report that can be queried from the back office	AN MAX 200

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.

Payment Result Message

Mandatory	Name	Description	Format
✓	esito	Result of the request (Possible values OK, KO)	AN MAX 2
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	codiceAutorizzazione	Confirmation code issued by the card issuer	AN MAX 6
✓	codiceConvenzione	Merchant code assigned by the acquirer where expected	AN MAX 15
✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	ora	Transaction time	DATA hh:mm:ss
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
✓	tipoTransazione	Indicates the payment method. See the table Transaction Type Coding for possible values. In case of payment with negative result an	AN MAX 20

		empty string will be sent	
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see table Restful API Error Codes Table messaggio -> error details	JSON
✓	timeStamp	Timestamp in millisecond format	N 13 CHAR
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table Card Type Coding	AN MAX 100
✓	scadenzaPan	Payment card expiry date	DATE yyyymm
✓	pan	credit card number masked. In plain text only the first 6 and last 4 digits	N MIN 16 MAX 19 NNNNNN******NNNN

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTE:

In the event of a KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and calling the createNonce directly, indicating "true" as the last parameter:
XPay.createNonce("payment-form", card, undefined, true);
The html code that forces the SCA is received in response, in order to obtain a new nonce to be used in the payNonce API.

Subsequent payment

Nonce creation

To make a subsequent OneClick payment, create a Nonce by referring to the Card data collection form section, making the following changes:

- Add the following parameters to the "config" object:

Name	Description	Format
requestType	The field must be enhanced with: "PR"	AN
serviceType	The field must be enhanced with: "paga_oc3d "	AN

- Add the following parameter in the "customParams" object:

Name	Description	Format
num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes

- Optional fields:

Name	Description	Format
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the request for 3DS exemption in all OneClick payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with:	AN

	- "SCA": the 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.

Payment

To make the payment, refer to the section 3D Secure Subsequent Payment

NOTES:

- By contacting Nexi support you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick payments.

Card Renewal

Make a 3D Secure payment and simultaneously change the pan and expiration of a contract. The API receives as input the parameters relating to the transaction and the nonce generated by calling the card data collection form, which is responsible to perform the 3D Secure phase.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/build/rinnovo-carta

In the nonce creation phase is necessary:

- include the following parameters in the 'config' object:

Obbligatorio	Nome	Descrizione	Formato
✓	requestType	The field must be enhanced with: "PP"	AN
✓	serviceType	The field must be enhanced with: "paga_multi" in the case of a card renewal for a recurring contract or with "paga_oc3d"	AN

- include in the 'customParams' object the parameter "num_contratto":

Obbligatorio	Nome	Descrizione	Formato
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 MAX 30 Except the “+” character and the quotes

The xpayNonce field is the nonce generated with the api creaNonce. The transaction code, amount, currency, and apiKey must be the same as the call to the api creaNonce, otherwise an invalid data error is received. This error can also be obtained if the nonce was generated more than 10 minutes ago. In the event that the GroupCode field is present, the contract will be created for the group, otherwise only for the terminal associated with the alias.

URI
ecomm/api/recurring/rinnovoCarta3DS

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 5 - MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3
✓	xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.

✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	scadenzaContratto	Contract expiration date	DATE dd/mm/yyyy
	mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 Excluding the # ' " characters For MyBank: AN MAX 140 CHAR anche you can use just these special characters/ - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
	codiceFiscale	Tax Code to be disassociated from the PAN.	AN 16 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Result message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 2 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
✓	codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
✓	data	Transaction date	DATE MAX 8 yyyymmdd
✓	ora	Transaction time	DATE hh:mm:ss
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR.
✓	brand	Type of card used by the user to make payment. The possible values are shown in the table Card Type Coding	AN MAX 100
✓	tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N)	AN MAX 200 CHAR.

		Example: VISA CLASSIC - CREDIT - N	
✓	tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first payment status KO. Therefore not usable for new recurrences.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

Card Verification

With XPay Build, it is possible to perform a card verification operation with the amount of 0 with no tokenization, in order to check the validity of the card entered by the customer.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/build/verifica-carta

Creazione nonce

It is necessary to follow the instructions in the "Card data collection form" section, configuring the config object as in the following example. It is necessary to send an amount equal to 0 (zero) and insert the "requestType" parameter in the "config" object, evaluating it to "VC:"

```
var config = {
        baseConfig: {
                apiKey: ${requestScope.alias},
                enviroment: XPay.Environments.INTEG //enviroment:
        XPay.Environments.PROD for production environment
        },
        paymentParams : {
                amount : “0”,
                transactionId : ${requestScope.codTrans},
                currency : ${requestScope.divisa},
                timeStamp : ${requestScope.timestamp},
                mac : ${requestScope.mac}
        },
        customParams:{
                nome: "nome",
                email: "test@test.it"
        },
        language: XPay.LANGUAGE.ITA,
        requestType: "VC",
        }
}
```

Card verification

URI
ecomm/api/recurring/verificaCarta3DS

METHOD
Post

ACCEPT
Application/json

Initiation message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
verificaCarta	Valued with "true"	Boolean
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation message: optional fields

Name	Description	Format
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
codiceTransazioneBuild	This parameter must match the transaction code sent in the xpayNonce creation with the build mode. If the call to creaNoncePrimoVericaCarta is used, it must not be passed or, if passed, left blank.	AN
codiceFiscale	Tax Code to be disassociated from the PAN.	AN 16 CHAR.
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Result Message

Name	Description	Format
esito	Payment result (OK or KO)	AN MAX 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

If 3D Secure payment is enabled for the transaction, during creation of the xpayNonce the user will automatically be redirected, using the JavaScript SDK, to a modal popup to complete the process. In that popup the user will be able to enter 3D Secure credentials as usual. At the end of the authentication stage, the popup will automatically close and this will engage the process described above. From the point of view of hosted payments integration on the page for collecting card details, the presence of 3D Secure is completely transparent. The xpayNonce will be made available only upon completion of the credential capture process, which will be initiated automatically by the SDK in any case

3D Secure 22

The 3D Secure 2.2 service is managed through the enhancement of the JSON information Security object whose content is considered in the 3D Secure 2.2 section

The following shows the different ways in which it is possible to manage the security protocol.

• Enhancing the json information security object within the payment configuration json:

```
var config = {
        baseConfig: {
                apiKey: ${requestScope.alias},
                enviroment: XPay.Environments.INTEG
        },
        paymentParams : {
                amount : ${requestScope.importo},
                transactionId : ${requestScope.codTrans},
                currency : ${requestScope.divisa},
                timeStamp : ${requestScope.timestamp},
                mac : ${requestScope.mac},
                urlBack: ${requestScope.urlMerchant},
                url: ${requestScope.urlMerchant},
                urlPost: ${requestScope.urlNotifica},
        },
        customParams:{
                paypalInvoiceID : "INVOICE_NUM",
        },
        informazioniSicurezza: {
                transType: "01",
        },
```

```
        language : XPay.LANGUAGE.ITA,
        serviceType: "paga_rico",
        requestType: "PP",
        }


XPay.setConfig(config);
```

• Enhancing the information in the call to create the xpayNonce:

```
        var payForm = document.getElementById('payment-form');
        payForm.elements['pagaBtn'].addEventListener("click", function () {
            this.disabled = true;

            var infoSicurezza = {};
            infoSicurezza.transType = "01";

        XPay.createNonce("payment-form", card, infoSicurezza);
        });
});
```

• Call the XPay function XPay.setInformazioniSicurezza() to enhance the information. The method can be called at any time once the SDK js is initialized. If you choose to use this mode pay attention that the data will be used to perform 3D only if the method is invoked before the XPay.createNonce () call.

```
        var payForm = document.getElementById('payment-form');
        payForm.elements['pagaBtn'].addEventListener("click", function () {
            this.disabled = true;

            var infoSicurezza = {};
            infoSicurezza.transType = "01";
            XPay.setInformazioniSicurezza(infoSicurezza);
            XPay.createNonce("payment-form", card);
        });
});
```

NOTES:

- If there are errors in the 3D Secure 2.2 parameters sent, you will receive the "esito_informazioniSicurezza" parameter, valued with "Y". For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.

Alternative payment methods

Through the XPay Build SDK it is possible to create buttons that allow the customer to use alternative payment methods.

You need to use the following function:

var buttons = XPay.create(Xpay.OPERATION_TYPES.PAYMENT_BUTTON, []);

passing as a second parameter an empty array to display all the payment methods available for your profile or an array containing only the desired methods (always considering those active on your profile). You can choose from the following payment methods:

- XPay.PaymentMethods.GOOGLEPAY
- XPay.PaymentMethods.APPLEPAY
- XPay.PaymentMethods.BANCOMATPAY
- XPay.PaymentMethods.PPRO_MYBANK
- XPay.PaymentMethods.ALIPAY
- XPay.PaymentMethods.WECHATPAY
- XPay.PaymentMethods.GIROPAY
- XPay.PaymentMethods.IDEAL
- XPay.PaymentMethods.BCMC
- XPay.PaymentMethods.EPS
- XPay.PaymentMethds.P24
- XPay.PaymentMethods.SKRILL
- XPay.PaymentMethods.MULTIBANCO
- XPay.PaymentMethods.SATISPAY
- XPay.PaymentMethods.AMAZONPAY
- XPay.PaymentMethods.PAYPAL

To display the buttons it is then necessary to use the function:

buttons.mount("xpay-btn");

passing as parameter the id of the div in which they will be displayed.

Methods of integration and outcome management

By default, the behavior and outcome management of alternative payment methods with XPay Build is different:

- With Google Pay and Apple Pay, once you click on the payment method, a section will open on the Apple or Android device through which it will be possible to proceed with the transaction.
- With PayPal, clicking the button causes the opening of a popup browser window, containing the PayPal payment page.

With these APMs the only event to manage is:

- XPay_Payment_Result

With the other APMs the user is redirected to the payment page of the chosen method. The outcome of the payment is returned via the parameters url, url_back and urlPost (if valued, optional field) passed in the "paymentParams" object:

Mandatory	Name	Description	Format
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500
✓	url_back	Recall url, in case the user decides to abandon the transaction during the payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). The field value must start with “http://” or “https://” and the standard ports 80 or 443 must be used.	AN MAX 200 In caso di esito=ANNULLO l'esercente può decidere di rimandare l'utente sulla pagina di pagamento con il medesimo codice transazione
	urlPost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security	AN MAX 500

	protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.

APM Lightbox

You can use this solution to manage the outcome of all alternative payment methods in the same way.
Through this method, once the alternative payment method has been selected, XPay will open a new popup browser window where the user can make the payment.
It is possible to request to manage payment methods using this method by specifying the "fullRedirect" parameter to false in the payment configuration json:

```
var config = {
        baseConfig: {
                apiKey: ${requestScope.alias},
                enviroment: XPay.Environments.INTEG,
                fullRedirect: false
        },
paymentParams : {
        amount : ${requestScope.importo},
        transactionId : ${requestScope.codTrans},
        currency : ${requestScope.divisa},
```

Once the payment is complete, the outcome of the transaction will be communicated to the merchant's page via the XPay_Payment_Result event as is the case for the Apple Pay, Google Pay and PayPal methods.
Since the payment outcome is communicated via the event, the url and urlBack parameters of the paymentParams object are not considered by XPay if specified, however it is possible to use the optional urlPost parameter always in the same object:

Mandatory	Name	Description	Format
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500

LIGHTBOX

Lightbox is the solution that Nexi makes available to integrate the XPay payment gateway with its Ecommerce portal, allowing its customers to make payments without being redirected to external pages

How it works?

The lightbox solution uses a javascript SDK provided by Nexi that once configured, with the parameters related to the payment, shows an iframe that covers the entire browser window. In this window you will see the Nexi cash page where the customer will make the payment. Once the payment is finished, a javascript event will be returned to the merchant page that will manage the transaction outcome.

Important information

- **Privacy policy**: you must report the **Nexi privacy policy**, available at the link **https://www.nexi.it/privacy/xpay.html** .
  We advise you to quote the indicated link directly on the page, so that the text is always updated.

- **Accepted payment circuits and security protocols:** the **logos of the accepted payment circuits** and of the **activated security protocols**, which can be downloaded from the **download area** of the Nexi website, must be displayed and kept up-to-date on the website.

Payment circuits require the above information to be entered on the payment page, where the user enters their card details.

Notes

- This solution is compatible only with payment cards
- This solution is compatible with the DCC service

To implement the XPay Lightbox solution, some steps are required

GiHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/lightbox/pagamento-base

InclusionSDK XPay

In order to start, include the script with the XPay javascript SDK in the header of your page:

TEST

```
<script
    src="https://int-ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

PRODUZIONE

```
<script
    src="https://ecommerce.nexi.it/ecomm/XPayBuild/js?alias=ALIAS_MERCHANT">
</script>
```

Alias parameter has to be value as merchant apiKey (or alias).

Environment configuration

Once loaded, to initialized SDK, cal the function:

XPay.init();

After that configure SDK through the function:

XPay.initLightbox(config);

passing the object containing the payment configuration as a parameter. The tables below show the structure:

Mandatory	Name	Description	Format
✓	baseConfig	Object whose structure is shown in the tables below	JSON
✓	paymentParams	Object whose structure is shown in the tables below	JSON

✓	customParams	N parameters can be specified that will be returned in the result messages	JSON
✓	language	Language identifier	AN Possibili valori: XPay.LANGUAGE.ITA, XPay.LANGUAGE.JPN, XPay.LANGUAGE.SPA, XPay.LANGUAGE.RUS, XPay.LANGUAGE.FRA, XPay.LANGUAGE.ARA, XPay.LANGUAGE.ENG, XPay.LANGUAGE.GER, XPay.LANGUAGE.CHI, XPay.LANGUAGE.POR

Object baseConfig

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
✓	enviroment	Implementation environment	AN possible values: XPay.Environments.INTEG, XPay.Environments.PROD

Object paymentParams

Mandatory	Name	Description	Format
✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	transactionId	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorization request.	AN MIN 2 MAX 30
✓	currency	The code of the currency with which the amount is expressed	AN MIN 3 MAX 3 admitted only EUR

✓	timeStamp	Timestamp in milliseconds format	N 13 CHAR
✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the instructions at the end of this chapter: Calculation MAC	AN 40 CHAR
	urlPost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- secretKey

SAMPLE STRING

MAC = HASH SHA1(codeTrans=<val>divisa=<val>importo=<val><secretKey>)

3D Secure 2.2

To manage 3D Secure 2.2 protocols, you have to call this function:

XPay.setInformazioniSicurezza({});

passing as paramater the JSON object which content is described in 3D Secure 2.2 section

Payment initiation

To start the payment it is necessary to call up the function:

XPay.openLightbox();

Management of events triggered by the SDK

The only event to be managed for the integration of the lightbox solution is 'XPay_Payment_Result' which, at the end of the transaction, communicates the outcome payment details.
The mac string, which is required for the validation of the result, will also be returned in the event.
For the calculation of the mac, the string must contain the fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

NOTES

XPay_Payment_Result 'which is the only event to be managed for the integration of the lightbox solution, which communicates the outcome of the payment and other details. Card Type Coding. With this solution, the “selectedcard” parameter is only available for cards, not for alternative payment methods.

Notification

With the Lightbox solution you can manage the outcome of transactions through a server-to-server call. For details of the call refer to the notification section of the Codebase

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.

If you are instead interested in a solution that allows the end customer to store their credit card data, and use it later to make purchases more quickly, refer to the OneClick solution.

Recurring Payments are also identified with the term “MIT” (Merchant Initiated Transaction). MITs are broken down into:

- Scheduled: debited with defined frequency (e.g. first of each month).
- Unscheduled: debited with undefined frequency.

It is necessary to notify XPay support of the type of debits that will be made by your store, as it is necessary to properly configure the assigned Nexi profile.

It is not permitted to use contract numbers created through MIT Scheduled payments to carry out MIT Unscheduled transactions, and vice versa.

At a technical level, this service consists of two stages:

- First Payment
- Subsequent Payments

The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

First payment

A first transaction must be generated, assigning a token that allows Nexi to save the pairing between the user and the used payment card.

Management of recurring subsequent payments

For subsequent payments, an API provided by Nexi must be used. This API requires as parameters the token generated with the first payment and other parameters related to the transaction to be performed.

NOTES:

- Transactions executed through recurring payments cannot be partially accounted for.

First Payment

To make the first payment, follow the instructions in the Payment Management section, adding the following parameters to the customParams object:

Mandatory	Name	Description	Format
✓	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	tipo_servizio	The field must be enhanced with: "paga_multi"	AN MAX 30
✓	tipo_richiesta	- PP (first payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
	gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment It is necessary to pass this parameter inside the MAC calculation as a parameter after the “importo” parameter.	

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first payment status KO. Therefore not usable for new recurrences.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12

months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Recurring Subsequent Payment

To make subsequent payments follow the instructions in the section Subsequent Payment (Recurring Payment and One Click Payment)

NOTES:

- Transactions executed through recurring payments cannot be partially accounted for.

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.

At the technical level, the management of this solution is divided into 2 phases:

- First payment
- Recurring Subsequent payments

First payment

A first transaction must be generated, assigning a token that allows Nexi to save the pairing between the user and the used payment card.

The first payment is subject to Strong Customer Authentication (SCA), the customer will therefore be redirected to the 3DS protocol for authentication.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/lightbox/pagamento-oneclick/primo-pagamento

Management of recurring subsequent payments

For subsequent payments, an API provided by Nexi must be used. This API requires as parameters the token generated with the first payment and other parameters related to the transaction to be performed.

GitHub XPay sample request:
https://github.com/NexiPayments/XPay/tree/master/lightbox/pagamento-oneclick/pagamenti-successivi

First Payment

To make the first payment, follow the instructions in the Payment Management section, adding the following parameters to the customParams object:

Name	Description	Format
num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Except the “+” character and the quotes
tipo_servizio	The field must be enhanced with: "paga_multi"	AN MAX 30
tipo_richiesta	- PP (first payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first payment status KO. Therefore not usable for new recurrences.

Recurring Subsequent Payment

To make subsequent payments follow the instructions in the section 3D Secure Subsequent Payment

IFRAME

You can integrate XPay directly into your e-commerce using the i-frame mode. Payment initiation does not change from the codice base.

How does it work?

The customer, during the transaction, remains on the merchant's e-commerce, while sensitive data continues to be managed in Nexi's secure environment with limited impact on PCI certification by remaining eligible with SAQ A.

Important information

- **Privacy policy: please refer to Nexi's privacy policy, available at the link** https://www.nexi.it/privacy/xpay.html .
  We suggest to report inside the page directly the link indicated, so that the text is always updated.
- **Enabled security circuits and protocols: the logos of accepted payment circuits and enabled security protocols, which can be downloaded from the** area download **of the Nexi website,** must be displayed and kept up-to-date on the website.

The payment circuits require the above information to be entered on the payment page, where the user enters their card details.

NOTES :

- The MyBank alternative payment method is not compatible with the i-Frame solution.

SERVER TO SERVER

Nexi also makes other types of more structured solutions available to merchants, where sensitive data relating to the transaction are handled directly by the merchant's server. This allows complete customisation of the payment experience, but requires PCI DSS security certification to be achieved, with the exception of recurring payments where the card details are not transmitted by the merchant.

The services displayed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and responses are formatted JSON objects.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server

The environment endpoints are as follows:

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it

The individual URIs and messages for each of the available services will be described below.

3D Secure Payments

Make a payment with 3D Secure authentication, this service involves the use of two APIs: one for 3D Secure verification and one for payment.
In the first step, the 'autenticazione3DS' API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure; it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlRisposta" request parameter. With the parameter "xpayNonce" received in response, the second API "paga3DS" is used to execute the payment.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server/pagamento-3D Secure

3D Secure Control

URI
ecomm/api/paga/autenticazione3DS

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
scadenza	Credit card expiry date	yyyymm
cvv	Three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	AN MAX 4 CHAR.
importo	Amount to be collected, expressed in euro cents with no separators.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito	AN MAX 500 CHAR.

	idOperazione xpayNonce timeStamp mac and, in the case of error, also codice and messaggio.	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

Initiation Message: optional fileds

Name	Description	Format
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON
3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the request for 3DS exemption in all OneClick payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with: - "SCA": the 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.	AN
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- divisa
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(apiKey=<val>codiceTransazione=<val>divisa=<val>importo=<val>timeStamp=<val><SecretKey>)

Success result message with html

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Success result message with nonce

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
warning	Object used to report errors in the 3D Secure 2.2 parameters sent. The structure is shown in the following table.	

Warning object

Name	Description	Format
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Failed result message

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC calculation if html or error is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><secretKey>)

MAC Calculation if nonce is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASHSHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val>< secretKey>)

NOTES:
This allows a xpayNonce to be created for use in making a payment with 3D Secure.
If a call requires the use of 3D Secure (due to a 3D Secure card and a merchant with the function enabled), a JSON will be returned containing the html code for carrying out 3D Secure. The subsequent xpayNonce will only be returned if the authentication is successful. The xpayNonce will be returned to the urlResponse address.
Otherwise, the API will return the error code described above.

The dynamic 3D Secure service can be activated by contacting Nexi support. This service can be used to send a 3D Secure exemption request, which will be evaluated by the card issuer and possibly accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all payments.

The Server to Server solution is not compatible with retries.

Payment

URI
ecomm/api/paga/paga3DS

METHOD
Post

ACCEPT
application/json

Payment Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
Importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(apiKey=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val> timeStamp=<val><SecretKey>)

Payment Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	DATE MAX 8 yyyymmdd
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
tipoTransazione	Transaction type, indicates the payment method. See the table here for possible	

	values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, see table message -> error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- This carries out a payment transaction with 3D Secure.
  The xpayNonce is the xpayNonce obtained from the authentication3DS API, which takes care of saving card details and carrying out the 3D Secure process.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

MOTO Payments

This service carries out server-to-server MOTO payment transactions. It is designed for merchants who wish to integrate with their own system the function to request credit card payment authorisations, where details are communicated by the cardholder to the merchant via email, telephone, etc. This allows merchants to both request credit card details and communicate the payment result through their own management system.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server/pagamento-moto

URI
ecomm/api/paga/pagaMOTO

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.
pan	Credit card number	AN MAX 100 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the payment result will be sent.	AN MAX 150 CHAR.
nome	Name of the person who made the payment.	AN MAX 150 CHAR.
cognome	Surname of the person who made the payment.	AN MAX 150 CHAR.
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- pan
- scadenza
- cvv
- importo
- divisa
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(apiKey=<val>codiceTransazione=<val>pan=<val>scadenza=<val>cvv=<val> importo=<val>divisa=<val>timeStamp=<val><SecretKey>)

Payment Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	DATE MAX 8 yyyymmdd
ora	Transaction time	DATE hh:mm:ss
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, see table message -> error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
Asynchronous POST notifications are not performed. The result is a JSON object containing the response parameters.
If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. " parametriAggiuntivi ": {}

Payments with External 3D Secure MPI

The service allows an e-commerce transaction to be carried out in 3D Secure server-to-server mode. To use it, it is necessary to have an MPI (Merchant Plug In) that manages holder authentication using 3D Secure protocols. XPay is used to forward authorisation requests, also passing on data obtained from the 3D Secure authentication process.
This service requires the merchant to obtain PCI-DSS certification.
The specifications presented below are for simple payment (oneshot), if you are interested in performing MIT, CIT and ASI via external MPI please refer to the next section MIT-CIT-ASI

URI
ecomm/api/paga/pagaMPI

METHOD
Post

ACCEPT
application/json

Payment Initiation Message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
	pan	Credit card number	AN MAX 100 CHAR.
✓	scadenza	Credit card expiry date	DATE yyyymm
✓	cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	AN MAX 4 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.

✓	eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
	ppo	Payment from wallet (Apple pay, etc.)	AN MIN 2 MAX 30
	dsTransId	Contains any 3DS Server Transaction Id generated in the case of 3D Secure 2.2	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- pan
- scadenza
- cvv
- importo
- divisa
- eci
- xid
- cavv
- ppo
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1 (apiKey=<val>codiceTransazione=<val>pan=<val>scadenza=<val>cvv=<val>importo=<val>divisa=<val>eci=<val>xid=<val>cavv=<val>ppo=<val>timeStamp=<val><SecretKey>)

Payment Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.
✓	data	Transaction date	DATE MAX 8 yyyymmdd
✓	tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
✓	eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	errore	Only present when the result is ko. It is an object containing: code -> error code, see table message > error details	AN
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
	ppo	Payment from wallet (Apple pay, etc.)	AN MIN 2 MAX 30

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

Below is the function for generating the 'xid' parameter in the case of payments with 3D Secure 2:

```
public static String generateXiD()
{
try {
byte bytes[] = new byte[20];
SecureRandom random = SecureRandom.getInstance("SHA1PRNG");
random.nextBytes(bytes);
return new String(java.util.Base64.getEncoder().encode(bytes));
} catch (NoSuchAlgorithmException ex) {
return "XXX";
}
}
```

MIT-CIT-ASI

The service enables MIT, CIT and ASI in 3D Secure server-to-server mode. In order to use it, it is necessary to have an MPI (Merchant Plug In) that handles holder authentication using the 3D Secure protocols. XPay is used to forward authorisation requests, also passing on data obtained from the 3D Secure authentication process.
This service requires the merchant to obtain PCI-DSS certification.

URI
ecomm/api/paga/pagaMPI

METHOD
Post

ACCEPT
application/json

Payment Initiation Message

Mandatory	Name	Description	Format
✓	mitFramework	Object required to handle MIT, CIT and ASI transactions.	Object JSON
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	pan	Credit card number	AN MAX 100 CHAR.
✓	scadenza	Credit card expiry date	DATE yyyymm
✓	cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	AN MAX 4 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.

✓	eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
	ppo	Payment from wallet (Apple pay, etc.)	AN MIN 2 MAX 30
	dsTransId	Contains any 3DS Server Transaction Id generated in the case of 3D Secure 2.2	AN

Object mitFramework

Mandatory	Name	Description	Format
✓	operazione	compliant values are described in the table MIT Framework parameters	AN
	networkData	Mandatory if parameter 'operazione' is set to: - UCOF_CIT_PR - UCOF_MIT - RECURRING_MIT - ASI_AUTH_CIT - ASI_AUTH_MIT The value of this parameter is returned by XPay in response to the API if the 'operazione' parameter is set to: - UCOF_CIT - RECURRING_CIT - ASI_COF_UNSCH - ASI_COF_RECUR - ASI_NOCOF	AN
	dataStanza	This parameter is mandatory for MIT Mastercard operations, and the value of this field is returned in the first CIT payments. This parameter indicates the year, month, and day when the data necessary for clearing will be prepared and provided	

MAC Calculation
For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- pan
- scadenza
- cvv
- importo
- divisa
- eci
- xid
- cavv
- ppo
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1 (apiKey=<val>codiceTransazione=<val>pan=<val>scadenza=<val>cvv=<val>importo=<val>divisa=<val>eci=<val>xid=<val>cavv=<val>ppo=<val>timeStamp=<val><SecretKey>)

Payment Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN MAX 3 CHAR.
✓	data	Transaction date	DATE MAX 8 yyyymmdd
✓	tipoTransazione	Transaction type, indicates the payment method. See the table	AN MAX 20 CHAR.

		here for possible values. If the payment result is negative, an empty string will be sent.	
✓	eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	errore	Only present when the result is ko. It is an object containing: code -> error code, see table message > error details	AN
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
	ppo	Payment from wallet (Apple pay, etc.)	AN MIN 2 MAX 30
	networkData	This field contains the code to be used to make subsequent payments.	
	dataStanza	Date on which the data necessary for clearing will be prepared and provided. This information is required for subsequent MIT Mastercard payments.	

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTE:

- In the case of invalid MIT framework parameters, the API returns an error 99 and message 'invalid mit framework parameters'.
- The API for simple payments, first payments and subsequent payments (MIT, CIT, ASI) is the same: it is always necessary to call up the API pagaMPI by passing the mitFramework object when required.
- In subsequent MIT, CIT and ASI payments, the card data (pan and expiry) must also be sent.
- Below is the function for generating the 'xid' parameter in the case of payments with 3D Secure 2:

```
public static String generateXiD()
{
try {
byte bytes[] = new byte[20];
SecureRandom random = SecureRandom.getInstance("SHA1PRNG");
random.nextBytes(bytes);
return new String(java.util.Base64.getEncoder().encode(bytes));
} catch (NoSuchAlgorithmException ex) {
return "XXX";
}
}
```

- If, in addition to an external MPI, one also has cards already tokenized for MIT, CIT or ASI operations, it will be possible to reuse them with XPay by composing the networkData, thus avoiding the first payment operation via Mit Framework on XPay gateway.

The networkData parameter consists of sub-elements, each of which is structured as follows:

- Identification code: two characters, defining the content of the sub-field
- Element length: two characters, defining the length of the data
- Data, variable length: which contains the data.

Identification code, possible values:

- Financial Network Code and BankNet Reference Number (MasterCard)
  - Identification code: 01
  - Format: an: 9
  - Description: Unique transaction identification code generated by the MasterCard network.

- TID (Visa)
  - Identification code: 03
  - Format: an: 15
  - Description: Unique transaction identification code generated by the Visa network.

- Validation Code (Visa)
  - Identification code: 05
  - Format: an: 4
  - Description: Unique transaction identification code generated by the Visa network.

- Acquirer Transaction Identifier (Nexi Payments)
  - Identification code: 06
  - Format: AN: 15

It is not necessary to send all the fields, it is sufficient to send the data you have received from the 3D Secure server. Below is an example of some networkData accepted by XPay:

- 0109MNWSACZF40
- 0315483034086190313

Recurring Payment - One Click Payment

Recurring payments allow the merchant to tokenise the customer's card data, so that recurrences can be made for services such as subscriptions. If, on the other hand, one is interested in a solution that allows the end customer to store card data, and use it later to make purchases more quickly, a OneClick solution must be implemented.
On a technical level, the management of these services is mainly divided into 2 phases:

- First payment
- Subsequent payments

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server/pagamento-ricorrente-pagamento-in-un-click

First Payment

A first transaction must be generated, assigning a contract code that allows Nexi to save the match between the user and the payment card used. This first transaction can be a real payment, or just a card verification without any charge to the user.

Management of recurrences/sequential payments

The handling of subsequent payments between the recurring and OneClick services is different.

RECURRING

Subsequent payments can be made in two ways:

Synchronous call

When you need to debit a previously registered contract, your system must send Nexi a call with the details of the previously registered contract during the first payment.
For server-to-server mode, the services exposed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and the responses are a formatted JSON object.

Batch files

Subsequent payments can also be handled via batch files, a solution whereby a file containing a list of recurrences to be executed is uploaded into the Nexi environment: the file is processed by the XPay gateway, which will execute the indicated transactions and return a file with the outcomes.

Transactions executed by means of recurring payments cannot be cashed in or partially reversed.

ONECLICK

To perform an Oneclick subsequent payment, the dedicated 'Pagamento Successivo 3DSecure' API must be called up.

3D Secure Card Verification

It performs a card verification with 3D Secure authentication, with no charge to the customer, and simultaneously tokens the card for use in subsequent recurring or OneClick payments. This service involves the use of two APIs.
In the first step, the 'autenticazione3DS' API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure; it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlRisposta" request parameter. With the parameter "xpayNonce" received in response, the second API "verificaCarta3DS" is used to perform the card verification.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click/verifica-carta-3D Secure

3D Secure Authentication

URI
ecomm/api/recurring/creaNonceVerificaCarta

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
pan	Credit card number	AN MAX 100 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	AN MAX 4 CHAR.
urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito	AN MAX 500 CHAR.

	idOperazione xpayNonce timeStamp mac and, in the case of error, also code and message.	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fields

Name	Description	Format
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- pan
- scadenza
- cvv
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1(apiKey=<val>pan=<val>scadenza=<val>cvv=<val>timeStamp=<val><SecretKey>)

Success result message with html

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
mac	Message Authentication Code. Transaction signature field. For calculation	AN 40 CHAR.

	details, see the end of this chapter: MAC Calculation.	

Success result message with nonce

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
warning	Object used to report errors in the 3D Secure 2.2 parameters sent. The structure is shown in the following table.	

Warning object

Name	Description	Format
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Failed result message

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC calculation if html or error is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><secretKey>)

MAC Calculation if nonce is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASHSHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val>< secretKey>)

NOTES:
This allows a xpayNonce to be created for use in calling a cardVerification3DS.
If a call requires the use of 3D Secure (due to a 3D Secure card and a merchant with the function enabled), a JSON will be returned containing the html code for carrying out 3D Secure. The subsequent xpayNonce will only be returned if the 3D Secure authentication is successful. The xpayNonce will be returned to the urlResponse address.

An error message is returned if the card is not 3D Secure or the merchant has not enabled the function.

Verification of card authorisation

URI
ecomm/api/recurring/verificaCarta3DS

METHOD
Post

ACCEPT
application/json

Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fields

Name	Description	Format
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment	

	It is necessary to pass this parameter inside the "parametriAggiuntivi" object and inside the MAC calculation as a parameter before the timestamp.	
scadenzaContratto	Contract expiration date	DATE dd/mm/yyyy
codiceTransazioneBuild	This parameter must match the transaction code sent in the xpayNonce creation with the build mode. If the call to creaNoncePrimoVericaCarta is used, it must not be passed or, if passed, left blank.	AN
codiceFiscale	User Tax Code. Optional.	AN MAX 16 CHAR.
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(apiKey=<val>xpayNonce=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Payment result (OK or KO)	AN MAX 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

3D Secure First Payment

Make a payment with 3D Secure authentication, simultaneously tokenize the card for use in subsequent recurring or OneClick payments. This service involves the use of two APIs: one for 3D Secure verification and one for payment.
In the first step, the "creaNoncePrimo3DS" API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure; it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlRisposta" request parameter. With the parameter "xpayNonce" received in response, the second API "fprimoPagamento3DS" is used to execute the payment.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamwnto-ricorrente-pagamento-in-un-click/primo-pagamento-3D Secure

3D Secure Authentication

URI
ecomm/api/recurring/creaNoncePrimo3DS

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
pan	Credit card number	AN MAX 100 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	AN MAX 4 CHAR.

importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito idOperazione xpayNonce timeStamp mac and, in the case of error, also code and message.	AN MAX 500 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fields

Name	Description	Format
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- divisa
- importo
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>divisa=<val>importo=<val> timeStamp=<val><SecretKey>)

Success result message with html

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Success result message with nonce

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
warning	Object used to report errors in the 3D Secure 2.2 parameters sent. The structure is shown in the following table.	

Warning object

Name	Description	Format
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Failed result message

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC calculation if html or error is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><secretKey>)

MAC Calculation if nonce is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASHSHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val>< secretKey>)

NOTES:

This allows a xpayNonce to be created for use in making a payment.
If a call requires the use of 3D Secure (due to a 3D Secure card and a merchant with the function enabled), a JSON will be returned containing the html code for carrying out 3D Secure. The subsequent xpayNonce will only be returned if the authentication is successful. The xpayNonce will be returned to the urlResponse address.
Otherwise, the API will return the xpayNonce directly for use in making subsequent payments.

Payment

URI
ecomm/api/recurring/primoPagamento3DS

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the payment result will be sent.	AN MAX 150 CHAR.
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ' " characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
scadenzaContratto	Contract expiry date	DATA dd/mm/yyyy
codiceFiscale	User Tax Code. Optional.	AN 16 CHAR.
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED payment - U forces a first MIT UNSCHEDULED payment It is necessary to pass this parameter inside the "parametriAggiuntivi" object and inside the MAC calculation as a parameter before the timestamp.	
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><SecretKey>)

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.

Transaction Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	yyyy/mm/dd
ora	Transaction time	hh:mm:ss
nazione	Credit card country	AN MAX 30 CHAR.
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- This carries out a 3D Secure payment and registers a contract code at the same time.
  The API receives in the input the parameters relating to the transaction and the xpayNonce generated with the creaNoncePrimo3DS API.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

OneClick 3D Secure Subsequent Payment

Make a subsequent OneClick payment with 3D Secure authentication, this service involves the use of two APIs: one for 3D Secure verification and one for payment.
In the first step, the "creaNonceRico3DS " API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure; it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlResponse" request parameter. With the parameter "xpayNonce" received in response, the second API "pagamentoRicorrente3DS" is used to execute the payment.

3D Secure Authentication

URI
ecomm/api/recurring/creaNonceRico3DS

METHOD
Post

ACCEPT
Application/json

Payment Initiation Message: required fields

Nome	Descrizione	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 5 MAX 30
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. It must be equal to the amount that was sent to Apple for the token generation	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3

urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito idOperazione xpayNonce timeStamp mac and, in the case of error, also code and message.	AN MAX 500
timeStamp	Timestamp in milliseconds	N 13 CRT
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 MAX 10
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Payment Initiation Message: optional fields

Nome	Descrizione	Format
scadenza	Credit card expiry date	DATA aaaamm
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON
3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the request for 3DS exemption in all OneClick payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with: - "SCA": the 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.	AN
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For the transaction start message, the string to be signed must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- codiceGruppo
- timeStamp
- chiaveSegreta

STRING SAMPLE
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val> importo=<val>codiceGruppo=<val>pan=<val> timeStamp=<val><chiaveSegreta>)

NOTE:

- By contacting Nexi support you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick payments.

Success result message with html

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Success result message with nonce

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
warning	Object used to report errors in the 3D Secure 2.2 parameters sent. The structure is shown in the following table.	

Warning object

Name	Description	Format
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Failed result message

Name	Description	Format
esito	Operation result	AN MIN 2 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC calculation if html or error is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC= HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><secretKey>)

MAC Calculation if nonce is received

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASHSHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val>< secretKey>)

Payment

To make the payment it is necessary to receive the call from Nexi at the address indicated in the urlRisposta parameter. This call must be verified using the following parameters:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

After checking the call, the payment request must be made according to the following indications.

URI
ecomm/api/recurring/pagamentoRicorrente3DS

METHODO
Post

ACCEPT
Application/json

Payment initiation Message: required fields

Nome	Descrizione	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. It must be equal to the amount that was sent to Apple for the token generation	N MAX 8

divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	N MAX 3
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 36
timeStamp	Timestamp in milliseconds	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Payment initiation Message: optional fields

Nome	Descrizione	Format
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the initiation message.	JSON Avoid these :TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON

MAC Calculation

For the transaction initiation message, the string to be signed must contain the following fields:

- apiKey
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apikey=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timestamp=<val><chiaveSegreta>)

Payment Result Message: required fields

Nome	Descrizione	Format
esito	Operation result (possible values OK, KO)	AN MAX 2
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15
data	Transaction date	DATA MAX 8 aaaammgg
ora	Transaction time	DATA hh:mm:ss
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for payment (e.g. Europe).	AN MAX 30
brand	Type of card used by the user to make payment. The possible values are shown in the table here.	AN MAX 100
tipoProdotto	If enabled, the description of the card type used for the payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
tipoTransazione	Transaction type, indicates the payment method. See the table here for possible values. If the payment result is negative, an empty string will be sent.	AN MAX 20

errore	Only present when the result is ko. It is an object containing: code -> error code, see table message > error details	JSON
timeStamp	Timestamp in milliseconds	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Payment Result Message: optional fields

Name	Description	Format
dettagliCarta	Object whose structure is shown in the following table	JSON

dettagliCarta Element

Name	Description	Format
maskedPan	Masked pan of used card	AN
expiry	Expiring date	DATA aaaamm
hashPan	hashPan to be verified for association.	AN
hashAlg	Algorithm used	AN
updateTime	Date of last update of the card data	DATA
updateChannel	"N.D." "BACK OFFICE" "PAYMENT" "CIRCUITI"	AN
state	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

MAC Calculation

For the transaction outcome message, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timestamp=<val><chiaveSegreta>)

NOTES:

- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

- E' possibile effettuare OneClick Payment utilizzando numeri contratto creati da transazioni MIT scheduled e unscheduled.

Recurring Payment

When you need to make a charge on a previously registered contract, your system must send a call which contains the details of the previously registered contract, integrated with the recording of the first payment or 3D Secure card verification.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click/pagamento-successivo**

URI
ecomm/api/recurring/pagamentoRicorrente

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the Payment result will be sent.	AN MAX 150 CHAR.
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
scadenza	Credit card expiry date	yyyymm

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- scadenza
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>scadenza=<val>timeStamp=<val><SecretKey>)

Payment Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	yyyy/mm/dd
ora	Transaction time	hh:mm:ss
nazione	Credit card country	AN MAX 30 CHAR.
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Result Message: optional fields

If the contract belongs to a terminal with the "Card Data Alignment from the Circuit" function, the Card details property is also evaluated. Please refer to the Contracts API for defining the object.

Name	Description	Format
dettagliCarta	Object whose structure is shown in the following table	JSON

dettagliCarta Element

Name	Description	Format
maskedPan	Masked pan of used card	AN
expiry	Expiring date	DATA aaaamm
hashPan	hashPan to be verified for association.	AN
hashAlg	Algorithm used	AN
updateTime	Date of last update of the card data	DATA
updateChannel	"N.D." "BACK OFFICE" "PAYMENT" "CIRCUITI"	AN
state	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

Payment Result Message: additional fields for Amazon Pay

This table indicates the fields provided in response to Amazon Pay Payments.

Name	Description	Format
amazonpay	Contains the response XML file provided by Amazon through the authorization API. For more information on the XML file see the Amazon technical specifications	XML coded

To find out the possible error messages in case of a negative result with Amazon Pay, refer to the following page.
For possible error messages in the event of a negative outcome with Paypal, refer to the "DoReferenceTransaction" API on the following page.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- Transactions executed through recurring Payments cannot be partially accounted for.

If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. "parametriAggiuntivi": {}

Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Card Renewal 3D Secure

Make a payment with 3D Secure authentication, and simultaneously change pan and expiry of a contract. This service involves the use of two APIs: one for 3D Secure verification and one for payment.
In the first step, the "creNonceRico3DS" API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure; it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlRisposta" request parameter. With the parameter "xpayNonce" received in response, the second API "rinnovoCarta3DS" is used to execute the payment.

Authentication

URI
ecomm/api/recurring/creaNonceRico3DS

METODO
Post

ACCEPT
Application/json

Payment Initiation Message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8

✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3
✓	xpayNonce	Code assigned by XPay for use in the Payment request.	AN MAX 36 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	scadenza	Card expiration date	DATE aaaamm
	informazioniSicurezza	JSON object whose structure is described in section 3DSecure 2.2. It is necessary for the operation of the 3DSecure 2.2 service	Object
	3dsDinamico	To use this parameter, dynamic 3D Secure must be enabled on the merchant's terminal. This service allows a 3D Secure exemption request to be sent which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick payments. With this field you can request the exemption or force 3D Secure authentication. It is possible to value the parameter with:	

		- "SCA": 3D Secure will be requested from the customer on the payment. - "EXEMPT": the request for exemption will be sent.	
	softDecline	In case of a KO result with error code 96, it is possible to retry the payment by reusing the same transaction code and passing this field set to 'S'. You will receive in response the html code that will force the SCA to obtain a new nonce to be used in the pagaNonce api.	AN

Mac Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- codiceGruppo
- timeStamp
- chiaveSegreta

SAMPLE STRING

*MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>*codiceGruppo=*<val>timeStamp=<val><chiaveSegreta>)*

NOTES:

- If the 'GroupCode' parameter is not used in the start-up parameters, include it in the MAC calculation as if it were not valued.
- By contacting Nexi support, it is possible to activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service has been enabled, Nexi will automatically send the 3DS exemption request in all payments

Result Message with html

Obbligatorio	Nome	Descrizione	Formato
✓	esito	Operation result	AN MAX 2 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	html	html code to be printed on the user's browser for 3D-Secure authentication	
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR

Result Message with nonce

Obbligatorio	Nome	Descrizione	Formato
✓	esito	Operation result	AN MAX 2 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	xpayNonce	Code assigned by XPay to be used for the payment request	AN MAX 36
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.

✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR
	warning	Object used to report errors in 3D Secure 2.2 parameters sent.	Object

Negative Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC calculation with html or error

For the transaction outcome message, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

MAC calculation with nonce

For the transaction outcome message, the string to be signed must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING

*MAC = HASH SHA1(esito=<val>idOperazione=<val>*xpayNonce=<val>*timeStamp=<val><chiaveSegreta>)*

URI
ecomm/api/recurring/rinnovoCarta3DS

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 = Euro	AN MAX 3
✓	xpayNonce	Code assigned by XPay for use in the Payment request.	AN MAX 36 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction	AN 40 CHAR

		signature field. For calculation details, see the end of this chapter: MAC Calculation.	
	codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
	scadenza	Card expiration date	DATE aaaamm
	mail	Buyer’s email address to which the Payment result will be sent.	AN MAX 150
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 Excluding the # ‘ “ characters For MyBank: AN MAX 140 CHAR anche you can use just these special characters/ - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
	codiceFiscale	Tax Code to be disassociated from the PAN.	AN 16 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Result message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 2 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
✓	codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
✓	data	Transaction date	DATE MAX 8 yyyymmdd
✓	ora	Transaction time	DATE hh:mm:ss
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	regione	If enabled, this will return the global region associated with	AN MAX 30 CHAR.

		the card used for Payment (e.g. Europe).	
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table Card Type Coding	AN MAX 100
✓	tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
✓	tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTES:

- In case of renewal with negative outcome, the contract will be updated with the new card and marked with the first Payment status KO. Therefore not usable for new recurrences.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

Contract Update

This solution provides for the possibility of a contract update on the same card.
With the PSD2 directive, in the case of term/pricing changes on recurring contracts, the following call must be used to better protect the merchant.
Unlike card renewal, which allows the user to change or otherwise have to re-enter the card data, the contract update will perform the SCA without allowing the card to be changed.
This service involves the use of two APIs: a 3D Secure verification API and an update API.
In the first step, the "creNonceAggiornaContratto" API responds with a JSON file containing the HTML code necessary for entering the data useful for 3D Secure, it is up to the receiver to print the HTML received on the user's browser.
Once authentication by the user has been completed, the result is returned to the address indicated in the "urlRisposta" request parameter. With the "xpayNonce" parameter received in response, the second API "aggiornaContratto" is used to execute the payment.

3D Secure Authentication

If the contract is of the MDES/VTSM (Circuit Tokenisation) type, the api will return an error indicating to use card renewal, as the contract update service is not supported.

URI
ecomm/api/recurring/creaNonceAggiornaContratto

METHOD
Post

ACCEPT
Application/json

Initiation Message: required fields

Name	Description	Format
apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30

importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro)	AN MAX 3
urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito idOperazione xpayNonce timeStamp mac and, in the case of error, also code and message.	AN MAX 500
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Initiation Message: optional fields

Name	Description	Format
codiceGruppo	Code assigned by Nexi during activation. If not provided during activation, the field should not be valorized.	AN MIN 4 MAX 10
scadenza	Card expiry date. Valorize the parameter if you want to update the credit card expiration date, otherwise do not valorize it	DATA aaaamm
cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is	AN MAX 4

	mandatory or not depends on the rules in application for each individual acquirer.	
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	Object
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- codiceGruppo
- timeStamp
- chiaveSegreta

SAMPLE STRING

*MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>*codiceGruppo=*<val>timeStamp=<val><chiaveSegreta>)*

Positive Results Message con html

Name	Description	Format
esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 - MAX 30
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Positive Results Message con nonce

Name	Description	Format
esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 - MAX 30
xpayNonce	Code assigned by XPay for use in the Payment request.	AN MAX 36
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
warning		Object

Oggetto Warning

Name	Description	Format
esito_informazioniSicurezza	Valued with "Y", it indicates that there are errors in the 3D Secure 2.2 parameters sent. If the parameters are correct, this field is not returned. For more information about any warnings returned, use the API Warning or consult the detail of the order in the XPay back office.	

Negative Results Message

Name	Description	Format
esito	Operation result	AN MAX 7 CRT
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Contract Update

URI
ecomm/api/recurring/aggiornaContratto

METHOD
Post

ACCEPT
Application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro)	AN MAX 3
xpayNonce	Code assigned by XPay for use in the Payment request.	AN MAX 36
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Initiation Message: optional fields

Name	Description	Format
codiceGruppo	Code assigned by Nexi during activation. If not provided during activation, the field should not be valorized.	AN MIN 4 MAX 10
scadenzaContratto	Card expiry date. Valorizzare il seguente parametro se si vuole aggiornare la data di scadenza della carta di credito, altrimenti non valorizzarlo	DATA aaaamm
mail	Customer email	AN MAX 150
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
codiceFiscale	User Tax Code	AN MAX 16
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For this message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
*MAC = HASH SHA1(*apiKey=<*val*>numeroContratto=<*val*> codiceTransazione=<*val*> importo=<*val*>*divisa*=<*val*>xpayNonce=<*val*>*timeStamp*=<*val*><*chiaveSegreta*>*)*

Positive Results Message

Name	Description	Format
esito	Operation result (OK, KO)	AN MAX 7
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 - MAX 30
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
codiceConvenzione	Merchant code assigned by the acquirer. Where required	AN MAX 15
data	Transaction date	DATA MAX 8 aaaammgg
ora	Ora transazione	DATA hh:mm:ss
nazione	Credit card country	AN ISO 3166-1 alpha-3
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30
brand	Type of card used by the user to make Payment. The possible values are shown in the table Card Type Coding	AN MAX 100
tipoProdotto	If enabled, the description of the card type used for the Payment is returned.	AN MAX 200

	The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Esempio: VISA CLASSIC - CREDIT – N	
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Negative Results Message

Name	Description	Format
esito	Operation result	AN MAX 7 CRT
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Recurring MOTO Subsequent Payment

First Payment

This service carries out a server-to-server MOTO Payment transaction at the same time as the contract is registered for use in subsequent recurring or Card on File Payments.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server/pagamento-ricorrente-moto

URI
ecomm/api/recurring/primoPagamentoMOTO

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
scadenza	Credit card expiry date	yyyymm
cvv	Three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards.	N MAX 4 CHAR.

	For AMEX cards only, it is a four-digit code and is found on the front of cards.	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the Payment result will be sent.	AN MAX 150 CHAR.
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ' " characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
codiceFiscale	User Tax Code. Optional.	AN 16 CHAR.
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.
tipo_contratto	This parameter is required for merchants who conduct both scheduled and unscheduled transactions: - S forces a first MIT SCHEDULED Payment - U forces a first MIT UNSCHEDULED Payment It is necessary to pass this parameter inside the "parametriAggiuntivi" object and inside the MAC calculation as a parameter before the timestamp.	

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- pan
- cvv
- scadenza
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val> divisa=<val>pan=<val>cvv=<val>scadenza=<val>timeStamp=<val><SecretKey>)

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first Payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Transaction Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	yyyy/mm/dd
ora	Transaction time	hh:mm:ss
nazione	Credit card country	AN MAX 30 CHAR.
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, see table message > error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. " parametriAggiuntivi ": {}

Recurring Subsequent Payment

When you need to make a charge on a previously registered contract using a MOTO type transaction, your system must send a call which contains the details of the previously registered contract, integrated with the recording of the first Payment.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-moto#2-pagamenti-successivi

URI
ecomm/api/recurring/pagamentoRicorrenteMOTO

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
scadenza	Credit card expiry date	yyyymm
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the Payment result will be sent.	AN MAX 150 CHAR.
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message.	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- scadenza
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceTransazione=<val>importo=<val>divisa=<val>scadenza=<val>timeStamp=<val><SecretKey>)

Payment Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	yyyy/mm/dd
ora	Transaction time	hh:mm:ss
nazione	Credit card country	AN MAX 30 CHAR.
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Result Message: optional fields

Name	Description	Format
dettagliCarta	Object whose structure is shown in the following table	JSON

dettagliCarta Element

Name	Description	Format
maskedPan	Masked pan of used card	AN
expiry	Expiring date	DATA aaaamm
hashPan	hashPan to be verified for association.	AN
hashAlg	Algorithm used	AN
updateTime	Date of last update of the card data	DATA
updateChannel	"N.D." "BACK OFFICE" "PAYMENT" "CIRCUITI"	AN
state	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- Transactions executed through recurring Payments cannot be partially accounted for.

If you do not wish to append additional parameters, you can:

- Leave the field out of the JSON
- Leave the contents of the JOSN object empty

E.g. " parametriAggiuntivi ": {}

Multi-Currency Payment

The multi-currency payment is managed through Dynamic Currency Choice (DCC), a service created through collaboration between Nexi and Global Blue, which allows holders of international Visa and MasterCard credit cards to make purchases in their own currency with a guaranteed exchange rate at the time of payment.

The DCC service is currently available in 39 currencies.

If it is, the service will provide the exchange rate to the user, who may choose to either accept the offered rate and proceed with own currency, or remain in Euro.

At a technical level, management of these services is divided into 3 main stages, which recall the following APIs:

1. Obtain the XPay exchange rate and ask the customer for acceptance to proceed with own currency or in Euro, using the verificaDCC API described below.
2. Carry out the xpayNonce request and any 3D Secure authentication, using the creaNonce API
3. Make the Payment request with the xpayNonce and exchange rate ticket obtained, using the pagaDCC API.

This service requires the merchant to achieve PCI DSS certification.

Github XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/server-to-server/pagamento-multivaluta

Verification

URI
ecomm/api/etc/verificaDCC

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- pan
- importo
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>pan=<val>importo=<val>timeStamp=<val><secretKey>)

Result Message

Name	Description	Format
ticket	Exchange rate request identifier provided by Global Blue.	AN MAX 25 CHAR.
divisaDCC	DCC currency code	AN 3 CHAR.
importoDCC	Amount expressed in the currency indicated in DCCCurrency.	N MAX 9 CHAR.
importoDCCdecimali	Indicates how many decimal places are in the DCCAmount field.	N MAX 2 CHAR.
tassoDiCambio	Indicates the exchange rate applied by Global Blue.	N 8.4
scadenzaTassoDiCambio	Indicates the date and time the exchange rate will expire.	yyyymmddhhss
MarkUp	Indicates the mark-up provided by Global Blue.	N 8.4
decimalMarkUp	Indicates how many decimal places are in the MarkUp field.	N MAX 2 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
This returns the exchange information which will be shown to the cardholder for acceptance at the time of purchase, and which will subsequently be used in the pagaDCC API.
The “importoDCCdecimali” field shows the number of decimal places used in the importo.

Generate XpayNonce

After verification and once the customer has been allowed to choose whether to transact in own currency or in Euro, this API allows a xpayNonce to be created for use in making the Payment.
Where 3D Secure is expected, a JSON will be returned containing the html code for carrying out 3D Secure. The subsequent xpayNonce will only be returned if the authentication is successful. The xpayNonce will be returned to the urlRisposta address.
Otherwise, the API will return the xpayNonce directly for use with the Payment.

The details for the XpayNonce request are as follows:

URI
ecomm/api/hostedPayments/creaNonce

METHOD
Post

ACCEPT
application/json

Initiation Message: required fileds

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
cvv	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	AN MAX 4 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.

urlRisposta	Url to which XPay redirects and will return the result in GET using the following parameters: esito idOperazione xpayNonce timeStamp mac and, in the case of error, also code and message.	AN MAX 500 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fileds

Name	Description	Format
informazioniSicurezza	JSON object whose structure is described in the 3D Secure 2.2 section. It is necessary for the 3D Secure 2.2 service to work	JSON
3dsDinamico	In order to use this parameter it is necessary that the merchant terminal has dynamic 3D Secure enabled. This service allows you to send a request for 3D Secure exemption which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the request for 3DS exemption in all OneClick Payments. With this field it is possible to request the exemption or force 3D Secure authentication. It is possible to value the parameter with: - "SCA": the 3D Secure will be requested from the customer on the Payment. - "EXEMPT": the request for exemption will be sent.	AN
softDecline	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.	AN

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- divisa
- importo
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>divisa=<val>importo=<val>timeStamp=<val><SecretKey>)

Result Message: no 3D Secure

Name	Description	Format
esito	Operation result	AN MAX 7 CRT
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
xpayNonce	Code assigned by XPay for use in the Payment request.	AN MAX 36 CRT
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table Restful API Error Codes Table messaggio -> error details	AN
timeStamp	Timestamp in millisecond format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
dettaglioCarta	Array whose structure is described in the following table	Array

Object dettaglioCarta

Name	Description	Format
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CRT
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200
prepagata	It is valued with S or N based on whether the card is a prepaid or not	AN
pan	credit card number masked. In plain text only the first 6 and last 4 digits	N MIN 16 MAX 19 NNNNNN******NNNN
scadenza	Credit card expiry date	DATE aaaamm
regione	Credit card global region of origin if qualified (eg.: Europa)	AN MAX 30 CRT
nazionalita	It shows the nationality of the card that made the Payment	AN 3 CRT Codifica ISO 3166-1 alpha-3

Result Message: no 3D Secure

Name	Description	Format
esito	Operation result	AN MAX 7 CRT
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
html	HTML code to be printed on the user's browser for 3D Secure authentication.	
timeStamp	Timestamp in millisecond format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC calculation without 3D Secure

For the result message if you receive the xpayNonce, the string to be signed must contain the following fields:
esito

- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

MAC Calculation using 3D Secure or in case of errors

For the result message if you receive the html or in case of error, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Payment

This service makes a Payment in a currency other than Euro if the cardholder has accepted the proposed exchange rate through the verificaDCC service.

URI
ecomm/api/etc/pagaDCC

METHOD
Post

ACCEPT
application/json

Payment Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
ticket	Exchange rate request identifier provided by Global Blue.	AN 25 CHAR.
xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	
importoDCC	Amount expressed in the currency indicated in DCCCurrency.	N MAX 9 CHAR.
divisaDCC	DCC currency code	N MAX 9 CHAR.
tassoDiCambioAccettato	Set to YES if the customer has accepted the transaction in the card currency, set to NO if the customer has declined and the transaction will continue to be processed in Euro.	AN YES/NO
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
pan	Credit card number	AN MAX 19 CHAR.
cvv	Three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	N MAX 4 CHAR.
scadenza	credit card expiry date	yyyymm
parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message. In the following table an example of parameters	AN MAX 4000 The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- ticket
- tassoDiCambioAccettato
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>ticket=<val>tassoDiCambioAccettato=<val> timeStamp=<val><SecretKey>)

Transaction Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
data	Transaction date	yyyy/mm/dd
ora	Transaction time	hh:mm:ss
nazione	Credit card country	AN MAX 30 CHAR.
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- The pagaNonce field is only requested if 3D Secure has been used. In this case, the transactionCode, importo and currency fields must be the same ones as used in the create xpayNonce.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.
- It is possible to use the DCC service only with simple Payments and OneClick

PLUGIN CMS

If you already have an e-commerce platform, you can integrate XPay into your e-commerce in a few clicks.

Nexi solutions are compatible with the main e-commerce platforms on the market.

Implementation is quick and easy. Nexi provides free plugins for the main e-commerce platforms.

Below are the guides for the correct module management.

Storeden

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

From the following link you can view the installation and configuration guide: Storeden Activation Guide.

For more information you can consult the Storeden website.

Support

For expert assistance on the plugin contact Storeden support.

Italiaonline

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

To activate the gateway within the Italiaonline back office, consult the operating manual in your Customer Area in the section reserved for e-commerce service.

For more information, you can consult the Italiaonline website.

Support

To receive specialized assistance on the plugin, contact Italiaonline support.

Shopify

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

From the following link you can view the installation and configuration guide: How to update the Xpay app on Shopify.
For more information, you can consult the Shopify website.

Support

For specialist plugin assistance, contact Shopify Support.

Wordpress

XPay

The Nexi XPay Payment extension for Wordpress, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.
To use this plugin, the **Woocommerce** module must be installed on the Wordpress site.

Installation

The Nexi XPay plugin for Wordpress is available for free at the Wordpress.org site, from which it will be possible to check the compatible versions.
It is possible to install the extension using the appropriate installer made available by Wordpress.

1. Log into the Wordpress administrative panel.
2. Make sure you have installed the Woocommerce plugin.
3. In the left navigation bar, select **Plugins** > **Add new**.
4. On the new page, enter **Nexi XPay** in the search bar.
5. Locate the XPay plugin and click **Install now**.

The installation phase is completed, proceed with the configuration.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log into the Wordpress administrative panel.
2. In the navigation bar on the left, select **Plugins** > **Installed plugins**.
3. On the new page look for the **Nexi XPay** plugin in the list and click **Settings**.
4. Proceed with the configuration of the module:

Payment module configuration

Field	Description
Enable/Disable	Enable the Nexi XPay Payment module.
Payment page language	Set the language of the Payment page.

Accounting	The field identifies the Payment method that the merchant wants to apply to the single transaction, if entered with: - **Immediate** if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred** if authorized, the transaction is managed according to what is defined by the terminal profile.
Enable/Disable TEST mode	Enable or disable test mode. Register in the test area to receive your credentials.

Gateway Nexi XPay Configuration

Field	Description
Enable 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Alias	Code provided by Nexi to the seller.
MAC key	Code provided by Nexi to the seller.

OneClick configuration

Field	Description
Enable OneClick	Enable OneClick mode. For more information on this mode refer to the section Payment Methods

Recurring configuration

To use this mode, you need to install the Woocommerce Subscription plugin

Campo	Description
Enable/Disable Recurring	Enable recurring Payments. For more information on this method, refer to the Payment Methods section
Alias recurring Payments	Code provided by Nexi to the seller.
MAC key recurring Payments	Code provided by Nexi to the seller
Group	Code provided by Nexi to the seller

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to carry out successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production
Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards

With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

OneClick Payment

The integration of this solution allows the end customer to store their credit card data, and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Recurring Payment
This solution allows you to purchase products with recurring charges (eg subscriptions).

During the first Payment, a token is assigned that allows Nexi to save the pairing between the user and the Payment card used
Subsequent Payments will be made automatically on the date set in the subscription product settings.
To use this mode, you need to install the Woocommerce Subscription plugin.
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Woocommerce side, selecting the appropriate products and the customer who wishes to make the purchase.
An email will be sent to the customer containing a link to make the Payment. The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service.
Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- Skrill
- PayU
- Blik
- Multibanco
- PagoDIL

NOTES:

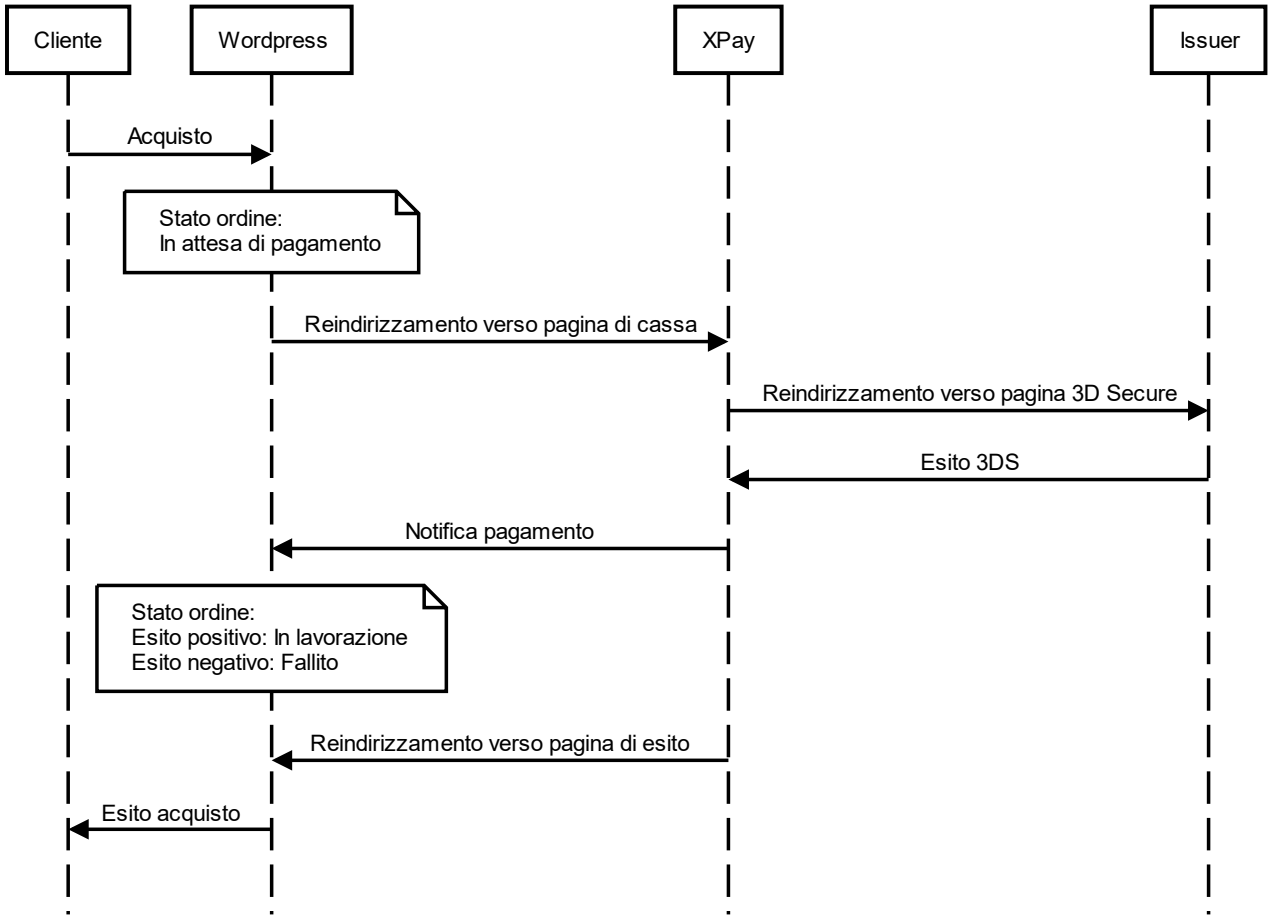
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

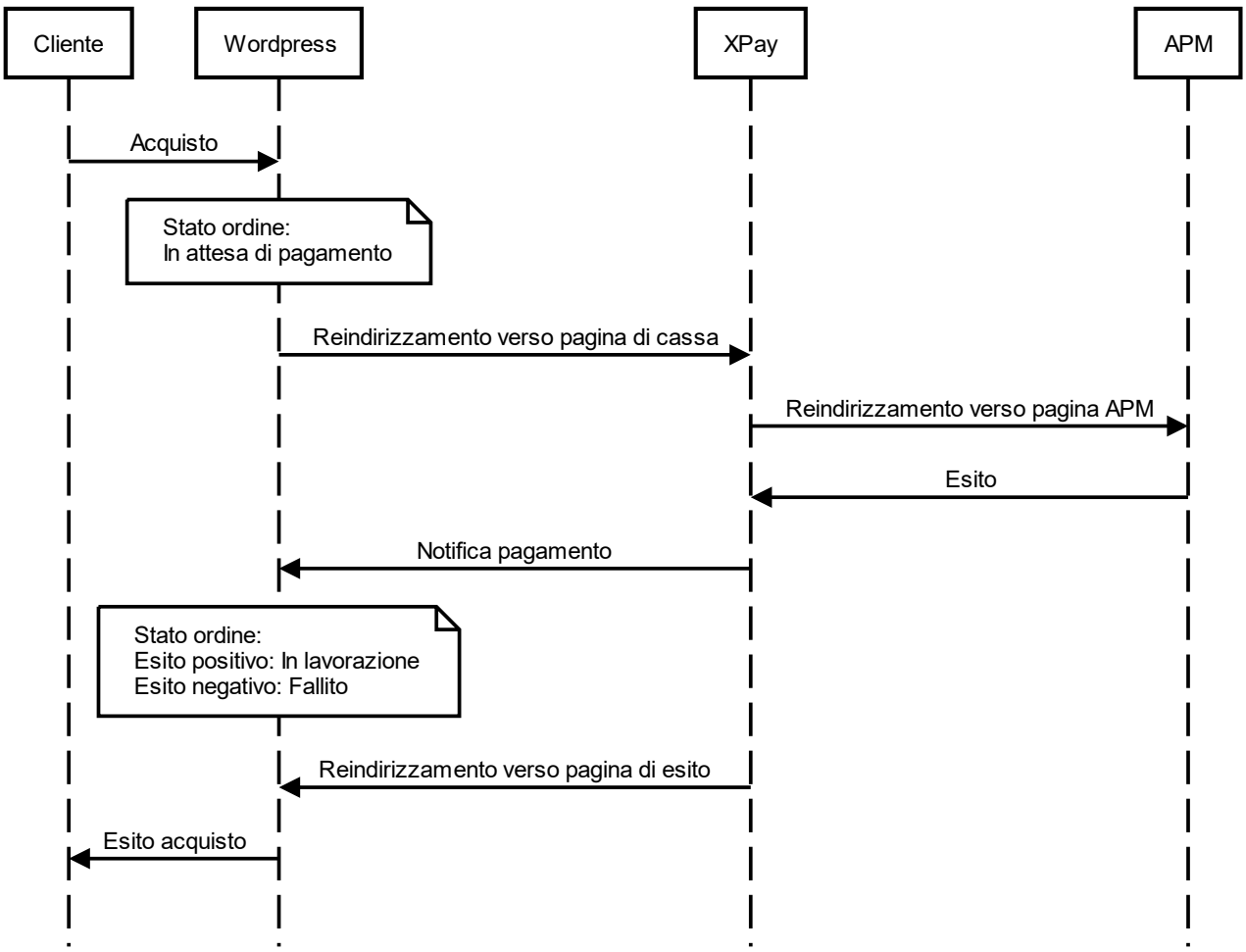
Payment by cards, OneClick, Pay-By-Link

The Payment flow is shown below with relative status changes on the Woocommerce side in case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The Payment flow is shown below with relative status changes on the Woocommerce side in case of Payment via alternative Payment methods.



Back office functionality

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting is usually done automatically by NEXI, at midnight of the same day
- **Contabilizzato**: the Payment has been accounted.
- **Negato**: the Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by refunding the customer and changing the status of the Woocommerce order. Below are the operations to be performed:
1. Log into the Wordpress administrative panel.
2. In the navigation bar on the left, select **Woocommerce** > **Orders**.
3. Click on the order to be refunded.
4. In the **Product** section click on **Refund** button and select the products to be refunded.

XPay Build

The XPay Build extension for Wordpress offers the possibility of directly hosting the Payment form within your e-commerce site, with the ability to customize colors and fonts, maintaining high security standards and at the same time avoiding having to manage the Payment card details.
This extension reduces the number of steps required to complete the Payment.
To use this plugin, the **Woocommerce** module must be installed on the Wordpress site.

Installation

The Nexi XPay Build plugin for Wordpress is available for free at the Wordpress.org site, from which it will be possible to check the compatible versions.
It is possible to install the extension using the appropriate installer made available by Wordpress.

1. Log in to the Wordpress administrative panel.
2. Make sure you have installed the Woocommerce plugin.
3. In the left navigation bar, select **Plugins** > **Add new**.
4. On the new page enter **Nexi XPay Build** in the search bar.
5. Locate the XPay plugin and click **Install now**.

The installation phase is completed, proceed with the configuration.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log into the Wordpress administrative panel.
2. In the navigation bar on the left, select **Plugins** > **Installed Plugins**.
3. On the new page look for the **Nexi XPay Build** plugin in the list and click on **Settings**.
4. Proceed with the configuration of the module:

Payment module configuration

Field	Description
Attiva/Disattiva	Enable the Nexi XPay Payment module.
Lingua pagina di Payment	Set the language of the Payment page.
Contabilizzazione	The field identifies the Payment method that the merchant wants to apply to the single transaction, if completed with: - **Immediate** if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred** if authorized, the transaction is managed according to what is defined by the terminal profile.
Abilita/Disabilita la modalità TEST	Enable or disable test mode. Register in the test area to receive your credentials.

Gateway Nexi XPay configuration

Campo	Description
Abilita 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Alias	Code provided by Nexi to the seller.
Chiave MAC	Code provided by Nexi to the seller.

OneClick configuration

Campo	Description
Abilita OneClick	Enable OneClick mode. For more information on this method, refer to the Payment Methods section

Style configuration

In this section it will be possible to customize the card data entry form.

Field	Description
Font	Font family (eg. Arial).
Font size	Font size in pixels.
Font style	Style of the font entered (eg. Italic).

Font variant	Variant of the font style (eg. Small-caps)
Letter spacing	Space between characters (eg. normal).
Border color	Color of the form border.
Error border color	Color of the form border in case of errors.
Placeholder color	Color of the suggestions inside the form.
Text color	Color of the card data entered.

Recurrence configuration
To use this mode, you need to install the Woocommerce Subscription plugin.

Field	Description
Enable/Disable recurring Payments	Enable recurring Payments. For more information on this method, refer to the Payment Methods section
Recurring Payment alias	Code provided by Nexi to the seller.
Recurring Payments MAC key	Code provided by Nexi to the seller.
Group	Code provided by Nexi to the seller.

Environment Configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in a test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production
Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards
This solution creates a Payment form on the checkout page of the e-commerce site in which to enter the card data, without redirecting the customer to external cash pages, but at the same time avoiding having to manage the card data.
In fact, the fields where this information is entered are contained in an iFrame connected to the XPay server, guaranteeing the security of the card data and at the same time making the shopping experience better.

OneClick Payment
The integration of this solution allows the end customer to memorize the data of his credit card and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data, while in the case of subsequent Payments it will show a form in which to enter only the CVV (optional).
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Recurring Payment
This solution allows you to purchase products with recurring charges (eg subscriptions). During the first Payment, a token is assigned that allows Nexi to save the pairing between the user and the Payment card used
Subsequent Payments will be made automatically on the date set in the subscription product settings.
To use this mode, you need to install the Woocommerce Subscription plugin.
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Woocommerce side, selecting the appropriate products and the customer who wishes to make the purchase.
An email will be sent to the customer containing a link to make the Payment. The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- Skrill
- PayU
- Blik
- Multibanco
- PagoDIL

NOTES:

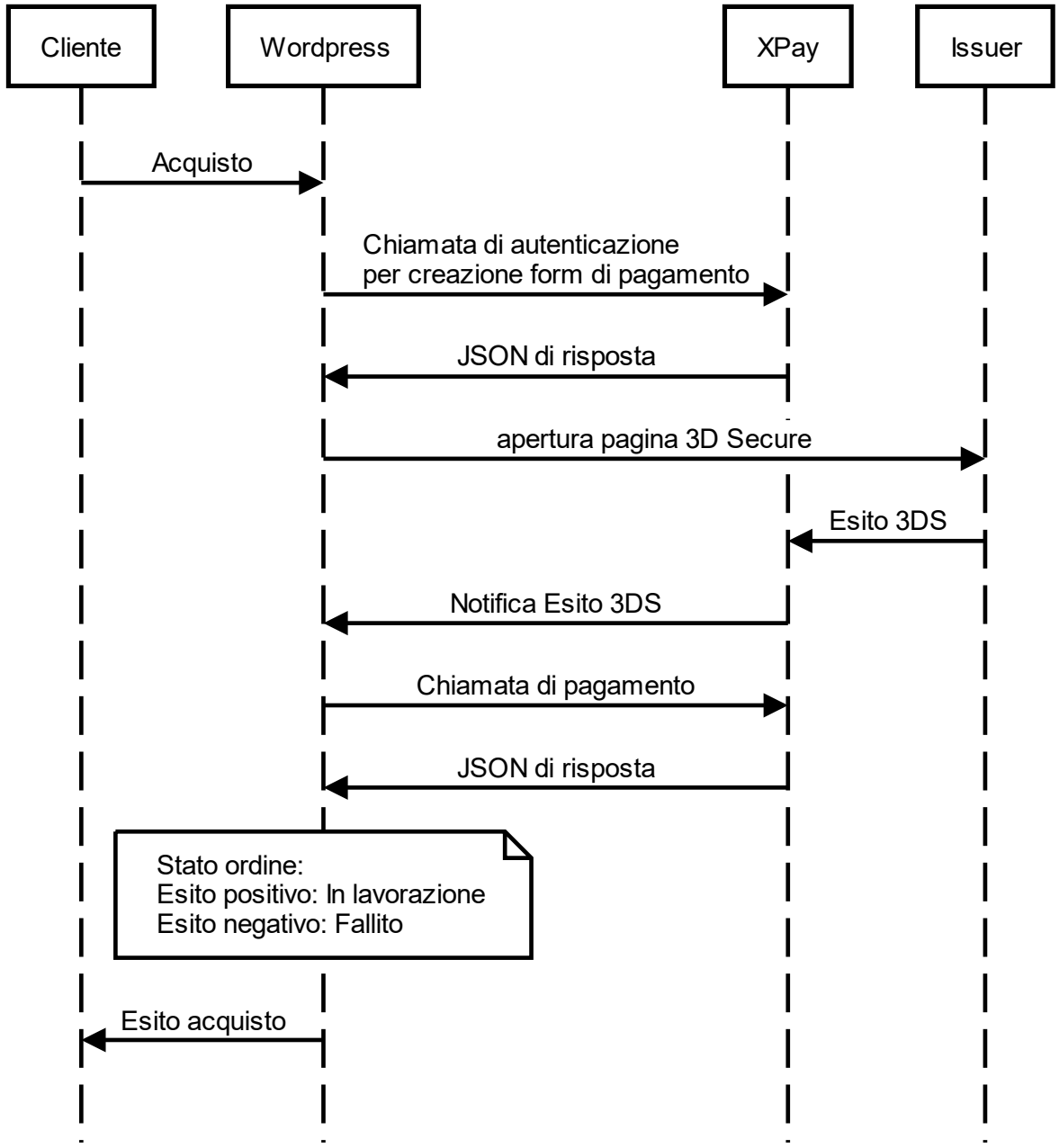
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

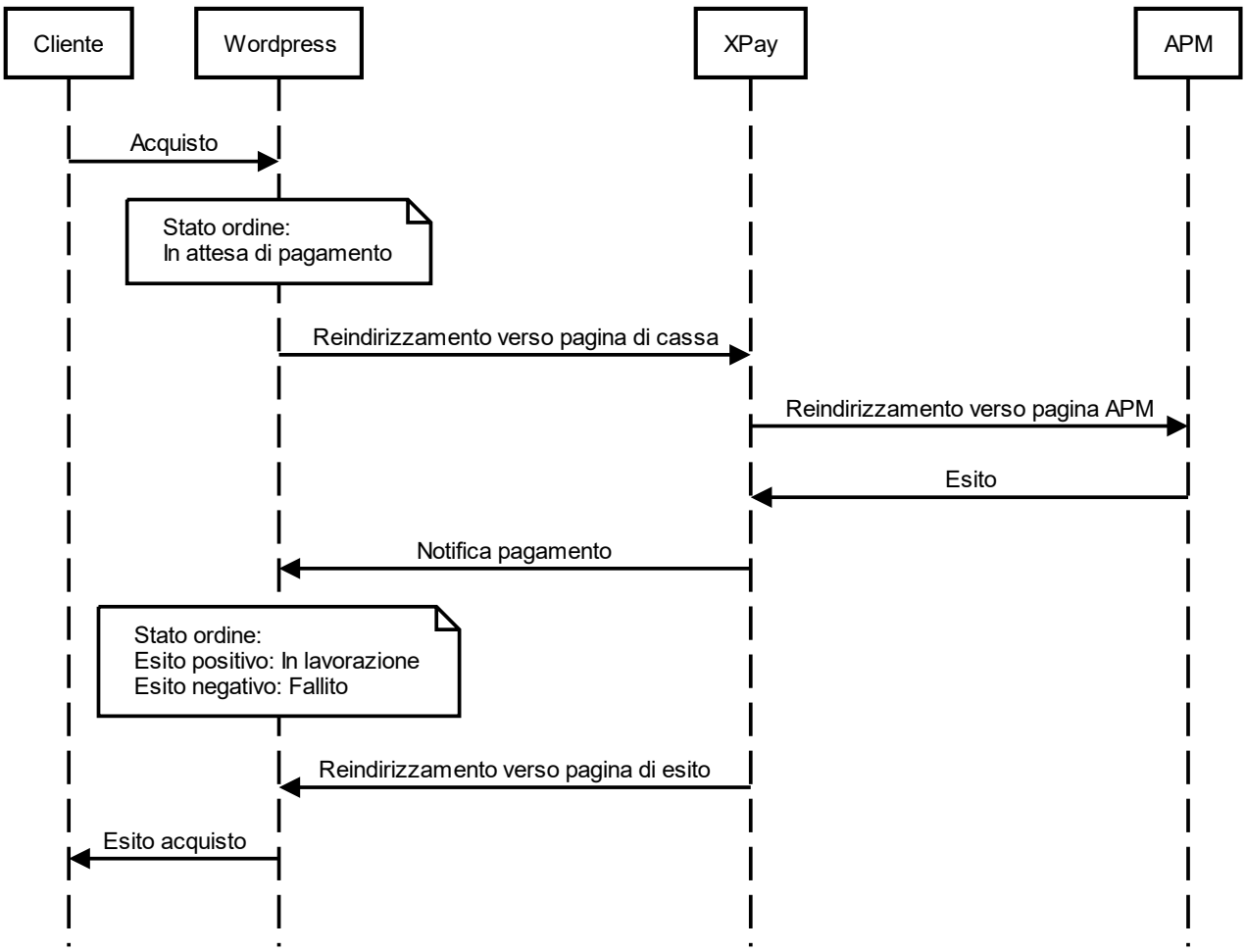
Payment by cards, OneClick, Pay-By-Link

The Payment flow is shown below with relative status changes on the Woocommerce side in case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The Payment flow is shown below with relative status changes on the Woocommerce side in case of Payment via alternative Payment methods.



Back office functionality

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting usually takes place automatically by NEXI, at midnight of the same day
- **Contabilizzato**: the Payment has been accounted.
- **Negato**: the Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by refunding the customer and changing the status of the Woocommerce order. Below are the operations to be performed:

1. Log into the Wordpress administrative panel.
2. In the navigation bar on the left, select **Woocommerce** > **Orders**.
3. Click on the order to be refunded.
4. In the **Product** section click on the **Refund** button and select the products to be refunded.

Prestashop

XPay

Nexi XPay Payment extension for Prestashop 1.7and 8 allows you to integrate XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for Prestahop 1.7 and 8 is available for free on the Prestashop Addons website, from which it will be possible to check the compatible versions.
It is possible to install the extension through the appropriate installer made available by Prestashop.

Prestashop 1.7/8

1. Log into the Prestashop administrative panel.
2. In the navigation bar on the left, select **Modules** > **Modules Manager**.
3. On the new page, select **Load module** top right.
4. Upload the plugin downloaded from the site Prestashop Addons.

The installation phase is completed, proceed with the configuration.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:

Prestashop 1.7

1. Log into the Prestashop 1.7/8 administrative panel.
2. In the navigation bar on the left, select **Modules** > **Modules Manager**.
3. On the new page, look for the plugin **Nexi XPay** in the list and click **Configure**.

Proceed with the configuration of the module:

Options

Field	Description
Payment page language	Set the language of the Payment page.
Accounting	The field identifies the Payment method that the merchant wants to apply to the single transaction, if entered with: - **Immediate** if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred** if authorized, the transaction is managed according to what is defined by the terminal profile.
Enable TEST mode	Enable or disable test mode. Register in the test area to receive your credentials.
Enable 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Alias	Code provided by Nexi to the seller.
MAC Key	Code provided by Nexi to the seller.
Enable OneClick	Enable OneClick mode. For more information on this mode refer to the section Payments methods

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in a test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production

Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards
With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

OneClick Payment

The integration of this solution allows the end customer to memorize the data of his credit card and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Prestashop side, selecting the appropriate products and the customer who wishes to make the purchase.
By clicking on the button "Send an email to the customer with the link to make the Payment" an email will be sent to the customer containing a link to make the Payment.
The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service.
Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- PagoDIL

NOTES:

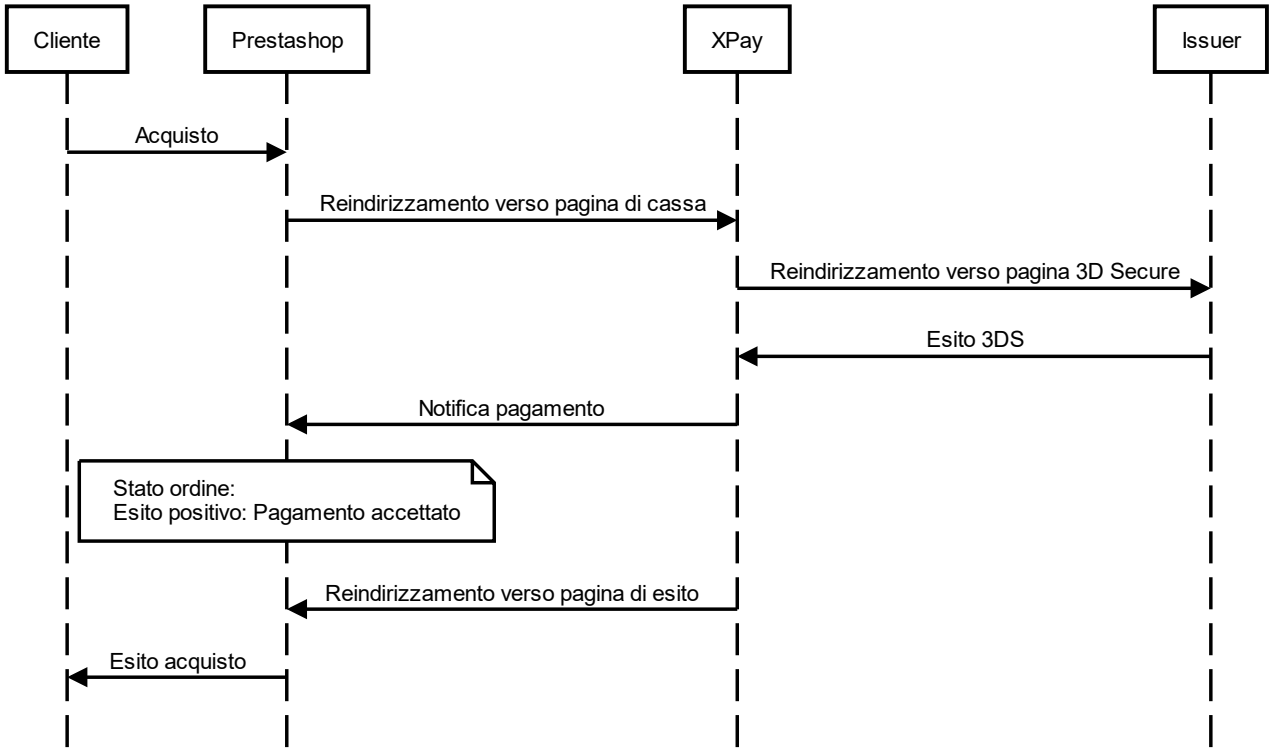
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

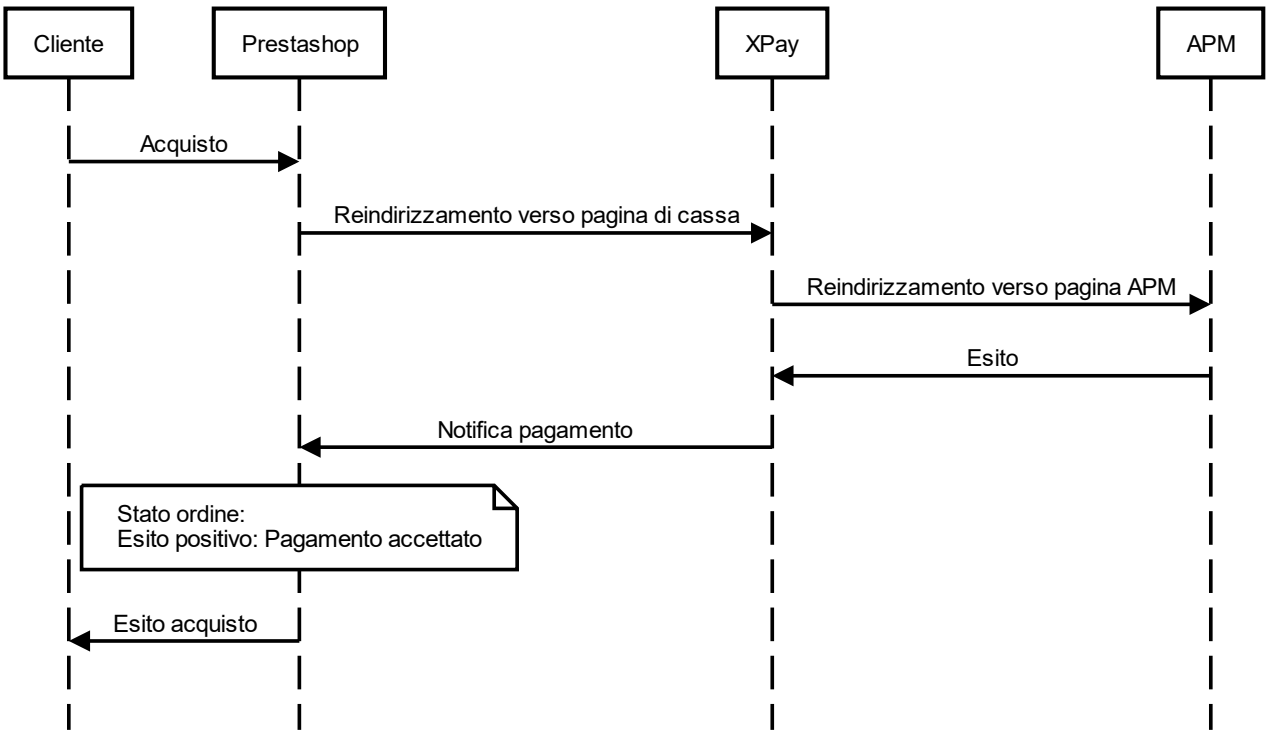
Payment by cards, OneClick, Pay-By-Link

The Payment flow is shown below with relative status changes on the Prestashop side in case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The Payment flow is shown below with relative status changes on the Prestashop side in case of Payment through alternative Payment methods.



Back office

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting is usually done automatically by NEXI, at midnight of the same day
- **Contabilizzato**: the Payment has been accounted.
- **Negato**: the Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by reimbursing the customer. Below are the operations to be performed:

1. Log into the Prestashop administrative panel.
2. Select in the navigation bar on the left **Orders**.
3. Click on the order to be refunded.
4. In the section **Nexi XPay Payments details** enter the amount to be reversed and click on the **Refund** button.

Accounting
It is possible to carry out total or partial accounting operations. This operation will post the desired amount on the XPay gateway.
By default, accounting takes place automatically at midnight, use this option only in the case of non-standard terminal configurations.
Below are the operations to be performed:

1. Log into the Prestashop administrative panel.
2. Select in the navigation bar on the left **Orders**.
3. Click on the order to be refunded.
4. In the section **Nexi XPay Payments details** enter the amount to be accounted and click on the **Account** button.

XPay Build

The XPay Build extension for Prestashop 1.7 and 8 offers the possibility to directly host the Payment form within your e-commerce site, with the ability to customize colors and fonts, maintaining high safety standards and at the same time avoiding having to manage Payment card data.
This extension reduces the number of steps required to complete the Payment.

Installation

The Nexi XPay plugin for Prestashop 1.7 and 8 is available for free at the following link.
It is possible to install the extension through the appropriate installer made available by Prestashop.

Prestashop 1.7/8

1. Log into the Prestashop administrative panel.
2. In the navigation bar on the left, select **Modules** > **Modules Manager**.
3. On the new page, select **Load module** top right.
4. Load the plugin downloaded from the following link.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:

Prestashop 1.7/8

1. Log into the Prestashop administrative panel.
2. In the navigation bar on the left, select **Modules** > **Modules Manager**.
3. On the new page, look for the plugin **Nexi XPay Build** in the list and click **Configure**.

Proceed with the configuration of the module:

Options

Field	Description
Payment page language	Set the language of the Payment page.
Accounting	The field identifies the method of collection that the merchant wants to apply to the single transaction, if completed with: - **Immediate** if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred** if authorized, the transaction is managed according to what is defined by the terminal profile.
Enable TEST mode	Enable or disable test mode. Register in the test area to receive your credentials.
Enable 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Alias	Code provided by Nexi to the seller.
MAC Key	Code provided by Nexi to the seller.
Enable OneClick	Enable OneClick mode. For more information on this method, refer to the Payment Methods section

Style configuration

In this section it will be possible to customize the card data entry form.

Field	Description
Font family	Font family (eg Arial).
Font size	Font size in pixels.
Font Variant	Style of the inserted font (eg Italic).
Letter spacing	Space between characters (eg normal).
Border color	Color of the form border.
Border color in case of errors	Color of the form border in case of errors.
Placeholder color	Color of the suggestions inside the form.
Text color	Color of the card data entered.

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to carry out successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production

Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards

This solution creates a Payment form on the checkout page of the e-commerce site in which to enter the card data, without redirecting the customer to external cash pages, but at the same time avoiding having to manage the card data.
In fact, the fields where this information is entered are contained in an iFrame connected to the XPay server, guaranteeing the security of the card data and at the same time making the shopping experience better.

OneClick Payment

The integration of this solution allows the end customer to store their credit card data, and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data, while in the case of subsequent Payments it will show a form in which to enter only the CVV (optional).
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Prestashop side, selecting the appropriate products and the customer who wishes to make the purchase.
By clicking on the button "Send an email to the customer with the link to make the Payment" an email will be sent to the customer containing a link to make the Payment.
The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service.
Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay

- PayPal
- Bancomat Pay
- PagoDIL

NOTES:

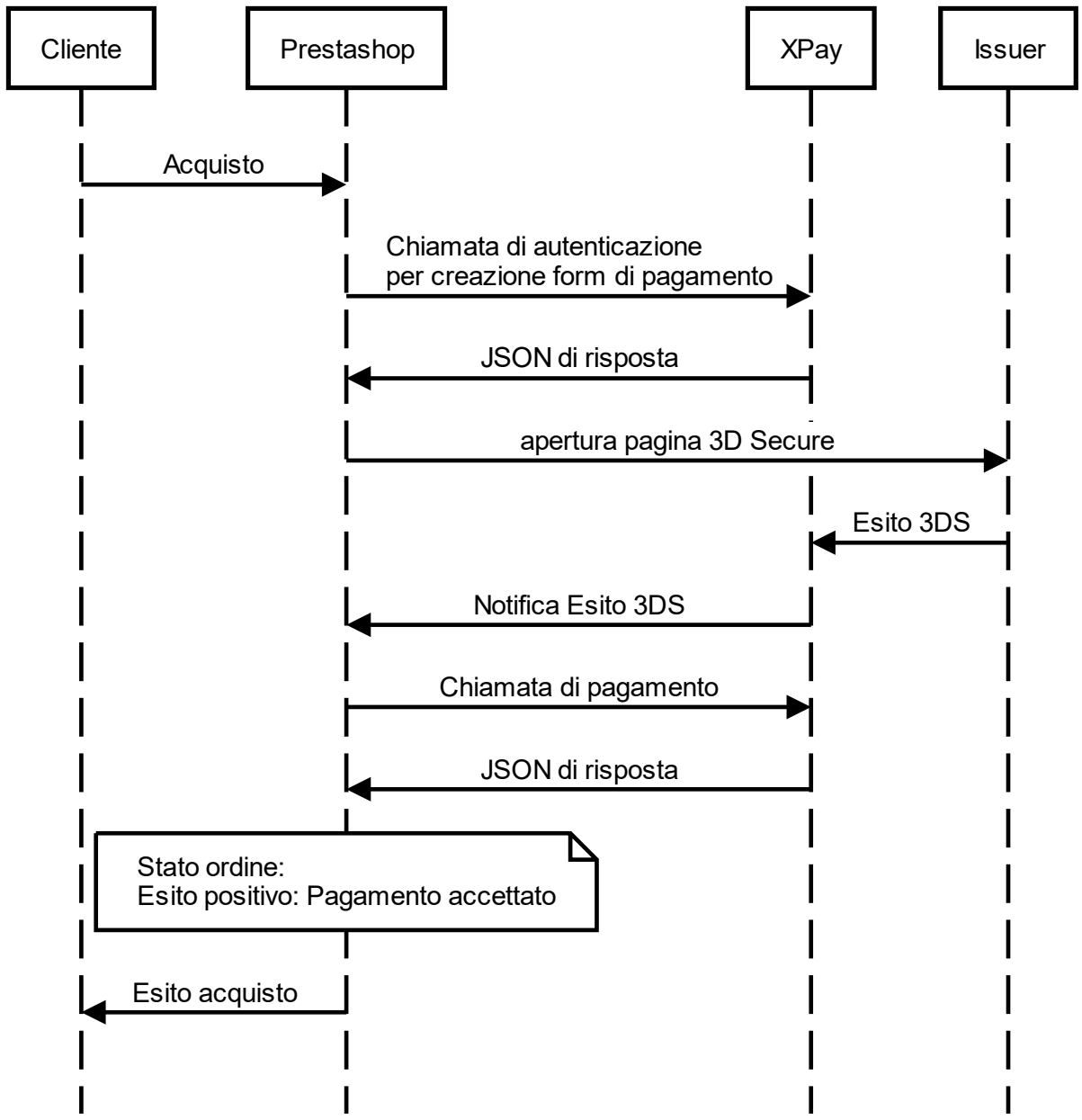
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

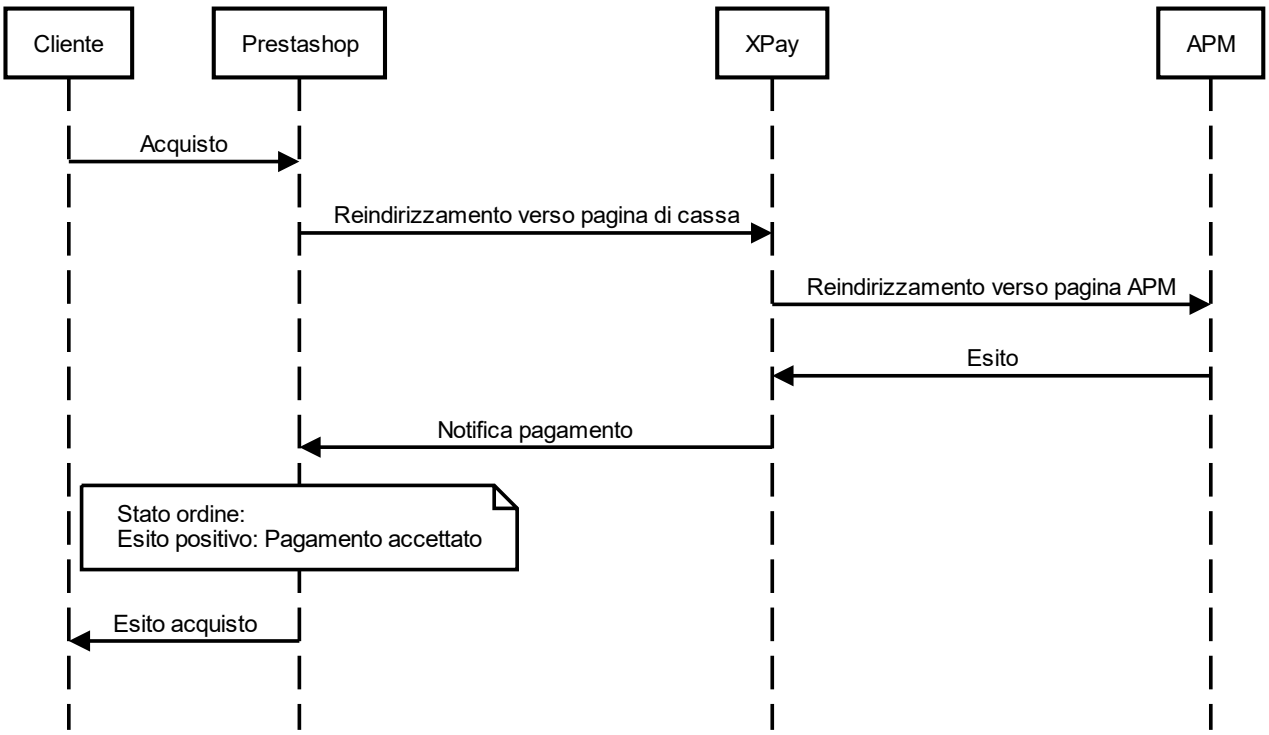
Payment by cards, OneClick, Pay-By-Link

The Payment flow is shown below with relative status changes on the Prestashop side in case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The Payment flow is shown below with relative status changes on the Prestashop side in case of Payment through alternative Payment methods.



Back office functionality

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting is usually done automatically by NEXI, at midnight of the same day
- **Contabilizzato**: the Payment has been accounted.
- **Negato**: the Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by reimbursing the customer. Below are the operations to be performed:
1. Log in to the Prestashop administrative panel.
2. In the navigation bar on the left, select **Orders**.
3. Click on the order to be refunded.
4. In the **Nexi XPay Payment details** section enter the amount to be reversed and click on the **Refund** button.

Accounting

It is possible to carry out total or partial accounting operations. This operation will post the desired amount on the XPay gateway.
By default, accounting takes place automatically at midnight, use this option only in case of non-standard terminal configurations.
Below are the operations to be performed:
1. Log in to the Prestashop administrative panel.
2. In the navigation bar on the left, select **Orders**.
3. Click on the order to be refunded.
4. In the **Nexi Xpay Payment details** section, enter the amount to be accounted and click on the **Account** button.

Magento

Magento 2

The Nexi XPay Payment extension for Magento 2, allows you to integrate the XPay Payment gateway without further implementation on your site.

It manages the customer's transfer from the merchant's ecommerce site to the Nexi secure environment and vice versa.

The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for Magento 2 is available for free in the Magento Adobe Magento Marketplace, from which it will be possible to check the compatible versions.

It is possible to install the extension via Composer.

Installation via Composer

Before proceeding, verify that Composer is installed in your environment. Below is the list of commands to be executed for installation:

1. Install the plugin

```
composer require iplusservice/xpay
```

2. Enable the plugin

```
bin/magento module:enable IPlusService_XPay
```

3. Run the update command

```
bin/magento setup:upgrade
```

4. Clear the cache

```
bin/magento cache:flush
```

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log into the Magento administrative panel.
2. In the navigation bar on the left, select **Negozi** (**Stores**)
> **Configurazione** (**Configuration**).
3. In the new menu on the left, select **Vendite** (**Sales**) > **Metodi di Payment** (**Payment methods**) > **Nexi XPay**.
4. Proceed with the configuration of the module:

Options

Field	Description
Enabled	Enable the Nexi Payment module.
Enable TEST mode	Enable or disable test mode. Register in the test area to receive your credentials.
Enable OneClick	Enable OneClick mode. For more information on this method, refer to the Payment Methods section.
Enable 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Accounting	The field identifies the Payment method that the merchant wants to apply to the single transaction, if filled with: - **Immediate**, if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred**, if authorized, the transaction it’s managed according to what is defined by the terminal profile.
Timeout Pay-By-Link	Maximum time in hours for which the Pay-By-Link link will be usable. For more information on this Payment method, refer to the Payment Methods section
Payment page language	Set the language of the Payment page.

Credentials

In this section there are the fields Alias and MAC key. These parameters are provided directly by Nexi.

Environmental configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers. For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to carry out successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production

Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is recommended to carry out a proof of Payment with a real card with the passage in production.

Payment Methods

The Nexi XPay plugin provides customers with different Payment methods:

Payment by cards

With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

OneClick Payment

The integration of this solution allows the end customer to memorize the data of his credit card and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Magento side, selecting the appropriate products and the customer who wishes to make the purchase.
An email will be sent to the customer containing a link to make the Payment. The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service.
Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- Skrill
- PayU
- Blik
- Multibanco
- PagoDIL

NOTES:

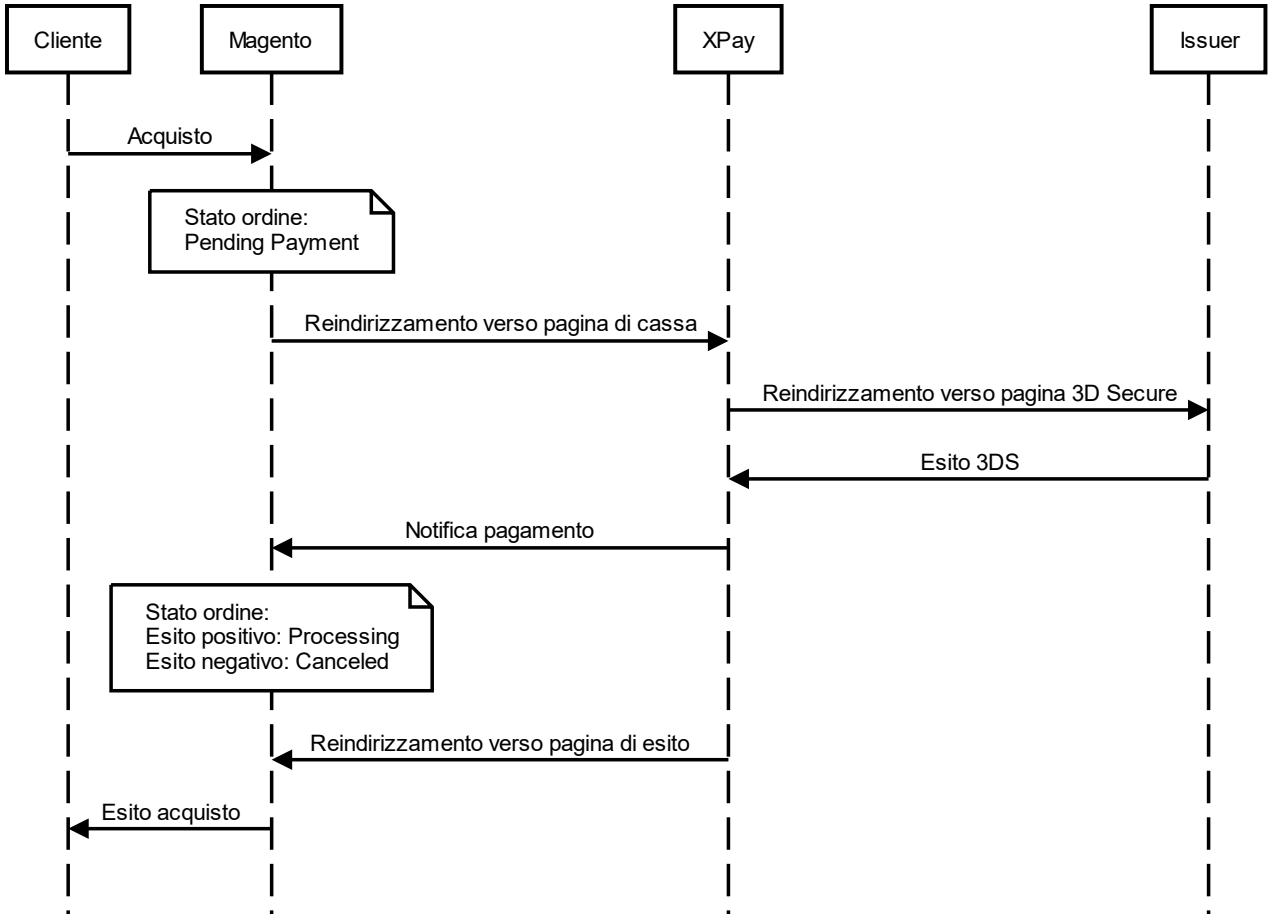
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

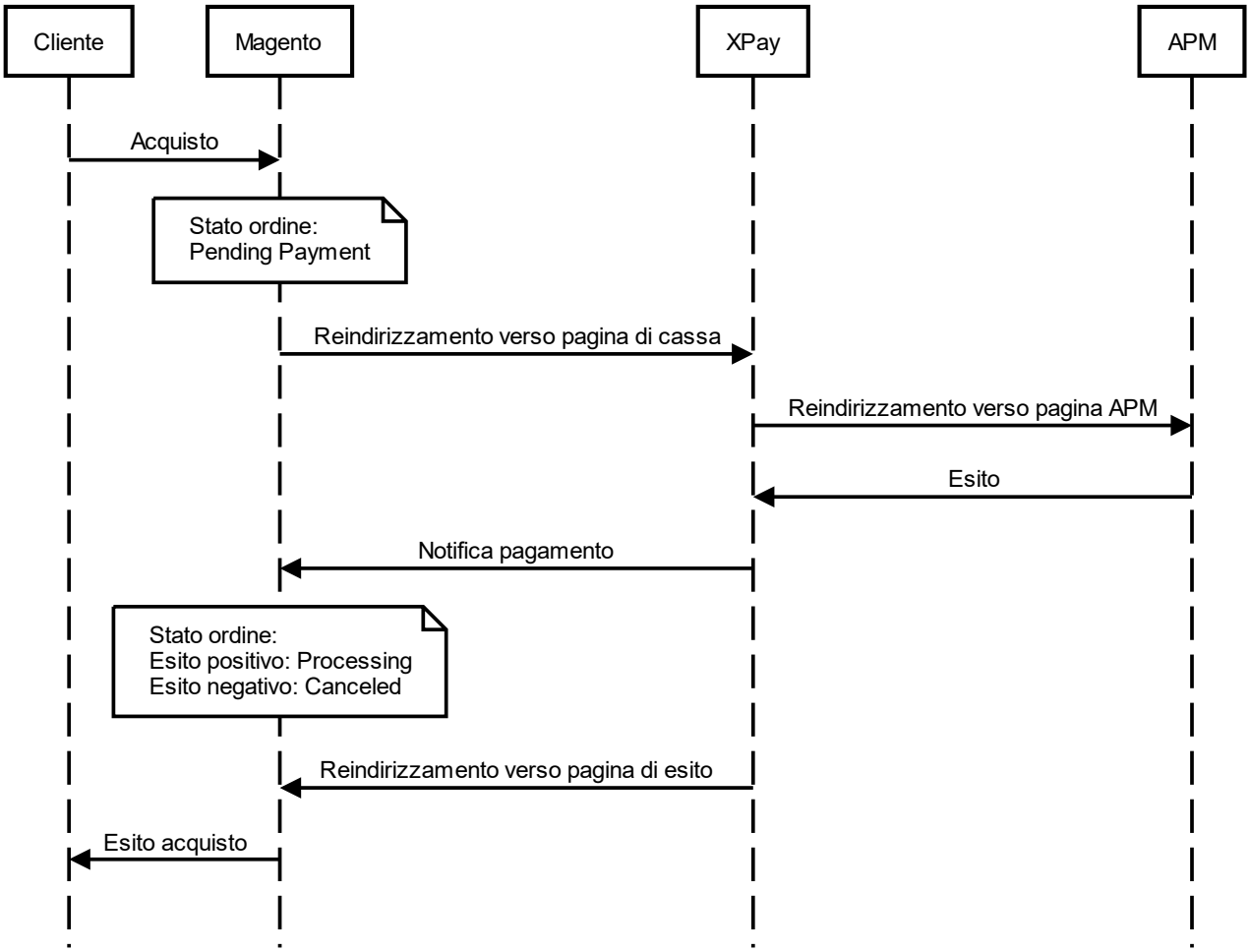
Payment by cards, OneClick, Pay-By-Link

The Payment flow is shown below with related changes in order status on the Magento side in case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The following shows the Payment flow with relative status changes on the Magento side in case of Payment through alternative Payment methods.



NOTE:

- If the customer, once redirected to the XPay checkout page for Payment, clicks the "back" button of the browser, he will return to the Magento site with an empty cart. This is because Magento, not receiving any information, is unable to retrieve the previous cart. The correct procedure is to click the "Cancel Operation" button on the XPay gateway page.

Back office functionality

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting usually takes place automatically by NEXI, at midnight of the same day

- **Contabilizzato**: the Payment has been accounted.
- **Negato**: The Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by refunding the customer and changing the Magento order status. Below are the operations to be performed:

1. Log into the Magento administrative panel.
2. Select in the navigation bar on the left **Vendite** (**Sales**) > **Ordini** (**Orders**).
3. Select the order to refund.
4. In the left menu, select **Fatture** (**Invoices**) and click on the corresponding invoice.
5. Select **Nota di credito** (**Credit Memo**) top right.
6. At the bottom of the page it is now possible to make a refund by clicking on the **Rimborso** (**Refund**) button. There is the **Quota di adeguamento** (**Adjustment Fee**) field where you can change the amount in order to proceed with a partial refund.

NOTES:

XPay's retry attempts, which allow the customer to have 3 payment attempts on the checkout page, cannot be used with the Nexi XPay plugin for Magento: with this module, the customer is redirected to Magento's outcome page in the event of a negative outcome, from which he/she will have the option of returning to the checkout page to proceed with the payment again.

Magento 2 Build

The XPay Build extension for Magento 2 offers the possibility to directly host the Payment form within your e-commerce site, with the ability to customize colors and fonts, maintaining high security standards and at the same time avoiding having to manage Payment card details.
This extension reduces the number of steps required to complete the Payment.

Installation

The Nexi XPay Build plugin for Magento 2 is available for free in the Magento Adobe Magento Marketplace, from which it will be possible to check the compatible versions. The plugin is compatible with Magento Open Source.

It is possible to install the extension via Composer..

Installation via Composer

Before proceeding, verify that Composer is installed in your environment. Below is the list of commands to be executed for installation:
1. Install the plugin

```
composer require iplusservice/xpaybuild
```

2. Enable the plugin

```
bin/magento module:enable IPlusService_XPayBuild
```

3. Run the update command

```
bin/magento setup:upgrade
```

4. Clear the cache

```
bin/magento cache:flush
```

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log into the Magento administrative panel.
2. In the navigation bar on the left, select **Negozi** (**Stores**)
> **Configurazione** (**Configuration**).
3. In the new menu on the left, select **Vendite** (**Sales**) > **Metodi di Payment** (**Payment methods**) > **Nexi XPay Build**.
4. Proceed with the configuration of the module:

Options

Field	Description
Enabled	Enable the Nexi Payment module.
Enable TEST mode	Enable or disable test mode. Register in the test area to receive your credentials.
Enable OneClick	Enable OneClick mode. For more information on this method, refer to the Payment Methods section
Enable 3D secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Accounting	The field identifies the Payment method that the merchant wants to apply to the single transaction, if entered with: - **Immediate** if authorized, the transaction is also collected without further intervention by the merchant and without considering the default profile set on the terminal. - **Deferred** if authorized, the transaction is managed according to what is defined by the terminal profile.
Timeout Pay-By-Link	Maximum time in hours for which the Pay-By-Link link will be usable. For more information on this Payment method, refer to the Payment Methods section
Payment page language	Set the language of the Payment page.

Credentials

In this section there are the fields Alias and MAC key. These parameters are provided directly by Nexi.

Style configuration

In this section it will be possible to customize the card data entry form.

Field	Description
Font family	Font family (eg Arial).
Font size	Font size.
Font style	Style of the inserted font (eg Italic).
Font variant	Variant of the inserted font (eg Small-caps).
Letter spacing	Space between characters (eg normal).

Border color	Color of the form border.
Border color in case of error	Color of the form border in case of errors.
Placeholder color	Color of the suggestions inside the form.
Text color	Color of the card data entered.
Preview	Preview of the card data entry form.

Environment configuration
The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in a test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production
Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay Build plugin provides customers with different Payment methods:

Payment by cards
This solution creates a Payment form on the checkout page of the e-commerce site in which to enter the card data, without redirecting the customer to external cash pages, but at the same time avoiding having to manage the card data.
In fact, the fields where this information is entered are contained in an iFrame connected to the XPay server, guaranteeing the security of the card data and at the same time making the shopping experience better.

OneClick Payment

The integration of this solution allows the end customer to memorize the data of his credit card and use them later to make purchases with a few clicks. In the case of a first Payment XPay will show the form for entering the card data, while in the case of subsequent Payments it will show a form in which to enter only the CVV (optional).
The Payment method can only be activated by subscribing to the Nexi XPay Pro service.

Pay-By-Link

This solution involves generating an order on the Magento side, selecting the appropriate products and the customer who wishes to make the purchase.
An email will be sent to the customer containing a link to make the Payment. The customer will be redirected to the checkout page of the ecommerce site.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- Skrill
- PayU
- Blik
- Multibanco
- PagoDIL

NOTES:

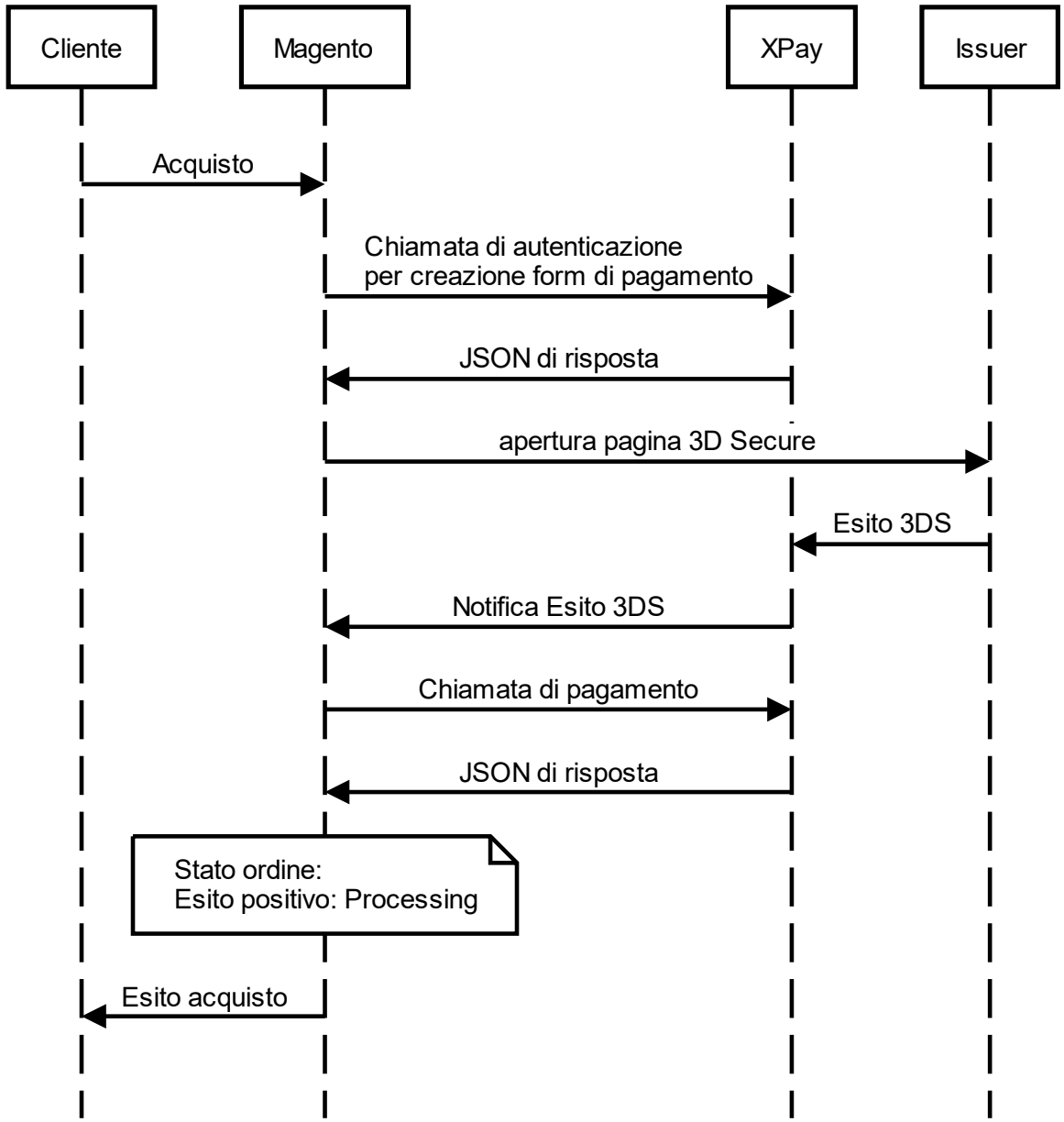
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

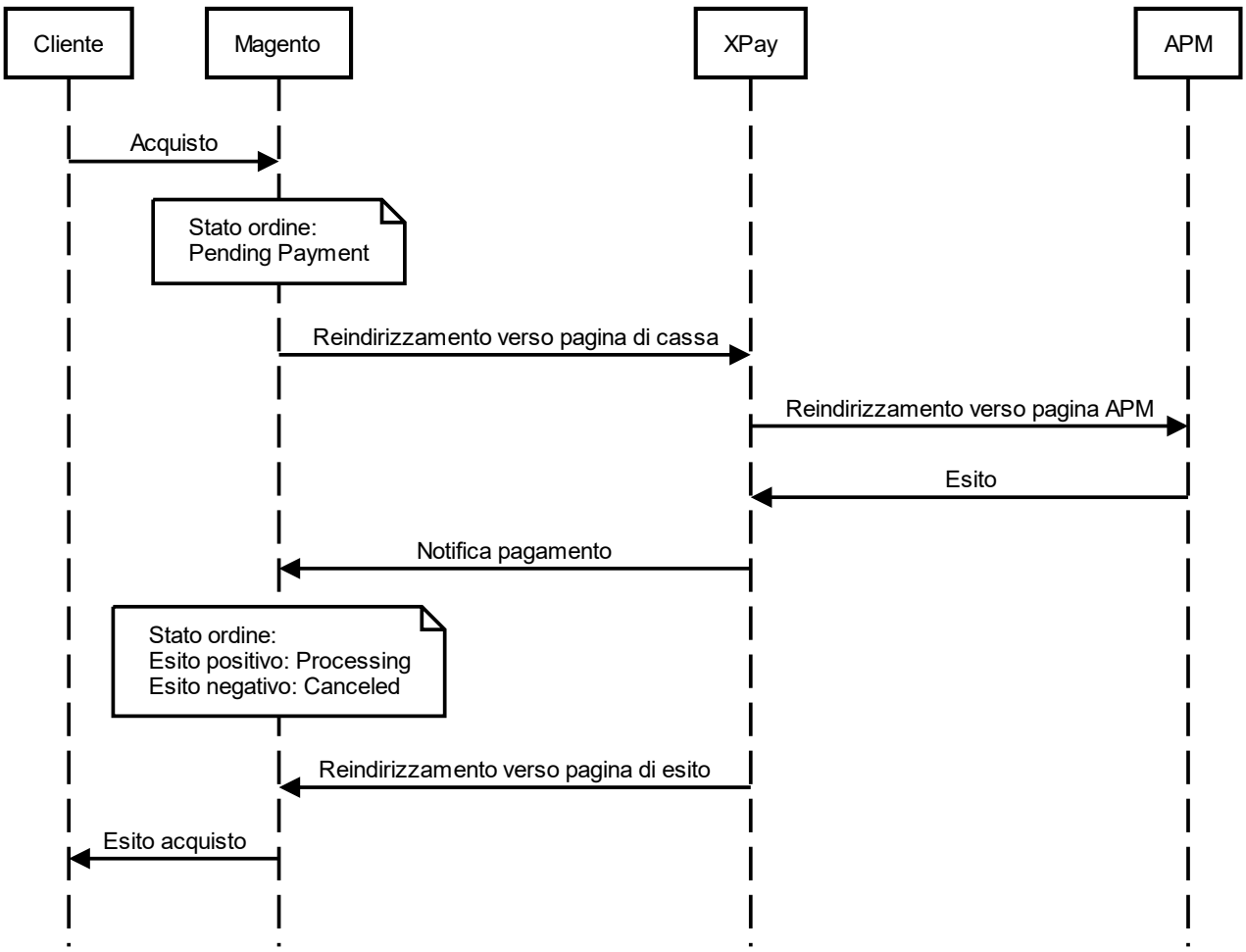
Payment by cards, OneClick, Pay-By-Link

Shown below is the Payment flow with relative status changes on the Magento side in the case of card Payment, oneclick Payment and Pay-By-Link.



Alternative Payment methods (APM)

The Payment flow is shown below with relative status changes on the Magento side in case of Payment through alternative Payment methods.



NOTE:

- If the customer, once redirected to the XPay checkout page for Payment, clicks the "back" button of the browser, he will return to the Magento site with an empty cart. This is because Magento, not receiving any information, is unable to retrieve the previous cart. The correct procedure is to click the "Cancel Operation" button on the XPay gateway page.

In the details of each order, the plugin provides information relating to transactions such as the details of the card used and the status of Payments on the XPay gateway.
Below are the statuses that can be viewed in the order details:

- **Autorizzato**: the Payment has been authorized, not yet accounted for. Accounting is usually done automatically by NEXI, at midnight of the same day
- **Contabilizzato**: the Payment has been booked.
- **Negato**: The Payment was not authorized. It will therefore not be accounted for.
- **Rimborsato**: the Payment, previously recorded, has been fully refunded to the user.
- **Contabilizzato Parz**.: a partial collection of the authorized amount was made on the Payment.
- **Rimborsato Parz**.: a partial refund of the accounted amount was made on the Payment.

Refund

It is possible to carry out total or partial refund operations. This operation will reverse the desired amount by refunding the customer and changing the Magento order status. Below are the operations to be performed:

1. Log into the Magento administrative panel.
2. Select in the navigation bar on the left **Vendite** (**Sales**) > **Ordini** (**Orders**).
3. Select the order to refund.
4. In the left menu select **Fatture** (**Invoices**) and click on the corresponding invoice.
5. Select **Nota di credito** (**Credit Memo**) top right.
6. At the bottom of the page it is now possible to make the refund by clicking on the button **Rimborso** (**Refund**). There is the **Quota di adeguamento** (**Adjustment Fee**) field where you can change the amount in order to proceed with a partial refund.

BigCommerce

The Nexi XPay payment extension for BigCommerce makes it possible to integrate the XPay payment gateway without further implementations on your site.
It manages the customer's transfer from the merchant's e-commerce site to the Nexi secure environment and vice versa.
The customer remains on the merchant's e-commerce site until checkout, and is then redirected to the XPay gateway to make the payment.

Installation

The XPay payment method is available for free among the additional providers offered by BigCommerce. XPay is activated on the checkout page once the configuration process is completed.

Configuration

Instructions are provided below on how to correctly configure the Nexi XPay plugin:

1. Log in to the BigCommerce admin panel.
2. In the left menu, click on **Impostazioni**
3. On the new page, click on **Pagamenti**
4. In the **Provider Aggiuntivi** section, find **Nexi XPay**, and click on the **configura** button.
5. Proceed with configuring the module by selecting the **XPay with Alias and chiave di Mac** option:

Options

Field	Description
Test mode	Enables or disables test mode. Register in the test area to receive your credentials
Alias	Code provided by Nexi to the seller
MAC key	Code provided by Nexi to the seller
Tipo transazione	The field identifies the collection mode that the merchant wants to apply to the individual transaction. If populated with: **Authorize & Capture**: the transaction, if authorized, is also captured without further intervention by the merchant and without considering the default profile set on the terminal. **Authorize only**: the transaction, if authorized, is managed according to the settings defined in the terminal's profile.

OneClick	Enables OneClick mode. For more information on this mode, refer to the Payment methods section
3D Secure 2	The 3D Secure 2 protocol, adopted by major international card networks (Visa, MasterCard, American Express), introduces authentication methods that can enhance and expedite the cardholder's shopping experience.
Display Name	Name displayed in the BigCommerce checkout.

Test and Production

It is highly advisable to test the plugin in the test environment before entering production codes.
You can obtain the test credentials (alias and MAC key) by contacting Nexi support through the email tech.ecommerce@nexi.it

Transfer to production
After the test phase, it will be possible to enter the production codes and disable the plugin test mode. It is advisable to perform a payment test with a real card when transferring to production.

Payment methods

The Nexi XPay plugin makes various payment methods available to customers:

Card payment
With this solution, customers remain on the merchant’s e-commerce site until checkout. They are then redirected to the Nexi environment to make the payment, to then return to the merchant’s site once the transaction is completed.

OneClick Payment
The integration of this solution enables end customers to save their credit card data and use them later on to make purchases in just a few clicks. During the first payment, XPay will display the form for the entry of card data, while during later payments it will display the card data previously entered or the possibility to enter new card data.
The payment method may be activated only with a subscription to the Nexi XPay Pro service.

Alternative payment methods (APM)
The plugin makes a number of alternative payment methods available. By selecting the desired method, the customer will be redirected to the checkout page of the selected payment service. A list of supported payment methods is provided below:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- Giro Pay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay
- Skrill
- Multibanco

Opencart

The Nexi XPay Payment extension for Opencart, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the customer's transfer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for Opencart is available for free at the Opencart.com website, from which it will be possible to check the compatible versions.
It is possible to install the extension through the installer made available by Opencart:
1. Log in to the Opencart administrative panel.
2. In the left navigation bar and select **Extensions** > **Installer**.
3. Upload the file downloaded from the site www.opencart.com.

The installation phase is completed, proceed with the configuration.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log in to the Opencart administrative panel.
2. In the navigation bar on the left, select **Extensions** > **Extensions**.
4. Select **Payments** under **Choose the extension type**.
5. Locate the plugin **Nexi XPay** in the list and click on the **Edit** button:
6. Proceed with the configuration of the module:

Options

Field	Description
Enable/Disable	Enable or disable the Payment module.
Nexi Alias	Code provided by Nexi to the seller.
Nexi key MAC	Code provided by Nexi to the seller.
Language	Set the language of the Payment page.
Enable 3D Secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.

Enable/Disable TEST Mode	Enable or disable test mode. Register in the test area to receive your credentials.
Nexi Alias TEST	Code recoverable in the test area.
Nexi key MAC TEST	Code recoverable in the test area.

Environment configuration
The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in a test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production

Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

Il plugin Nexi XPay mette a disposizione ai clienti diverse modalità di Payment:

Payment by cards
With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay

NOTES:

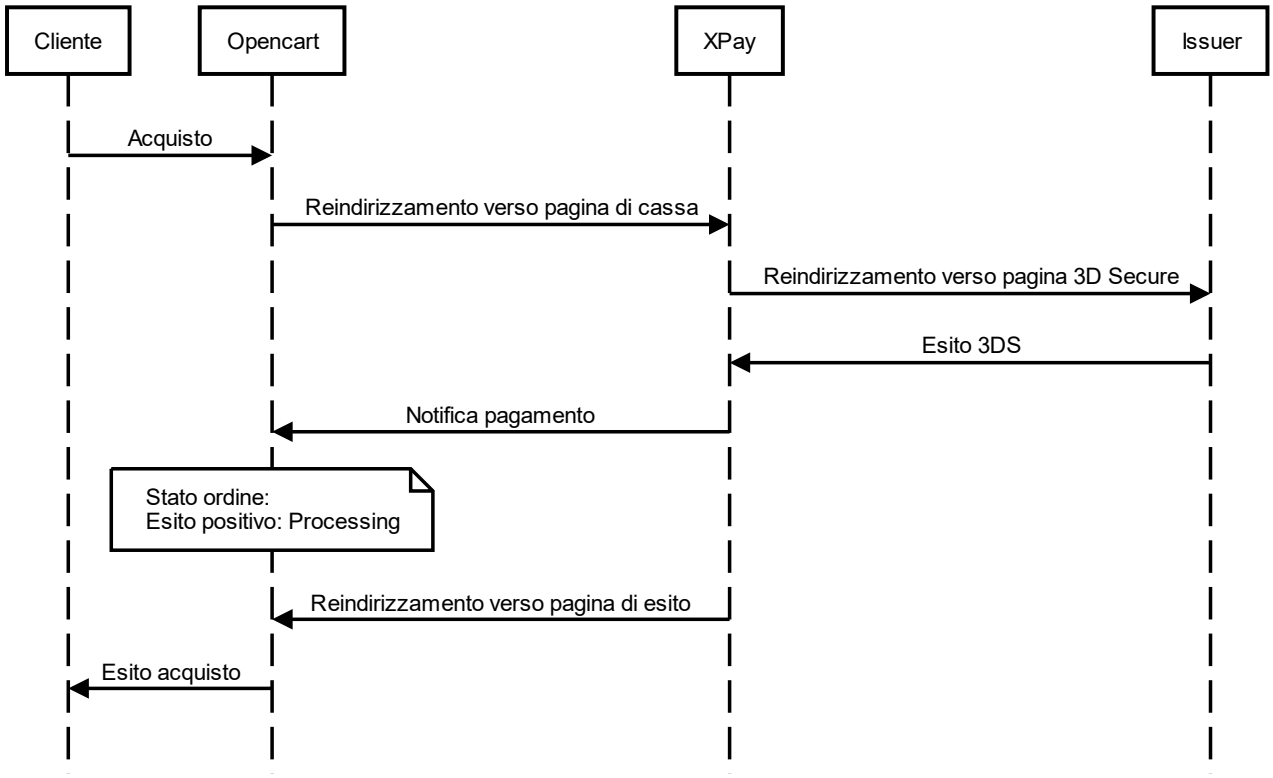
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

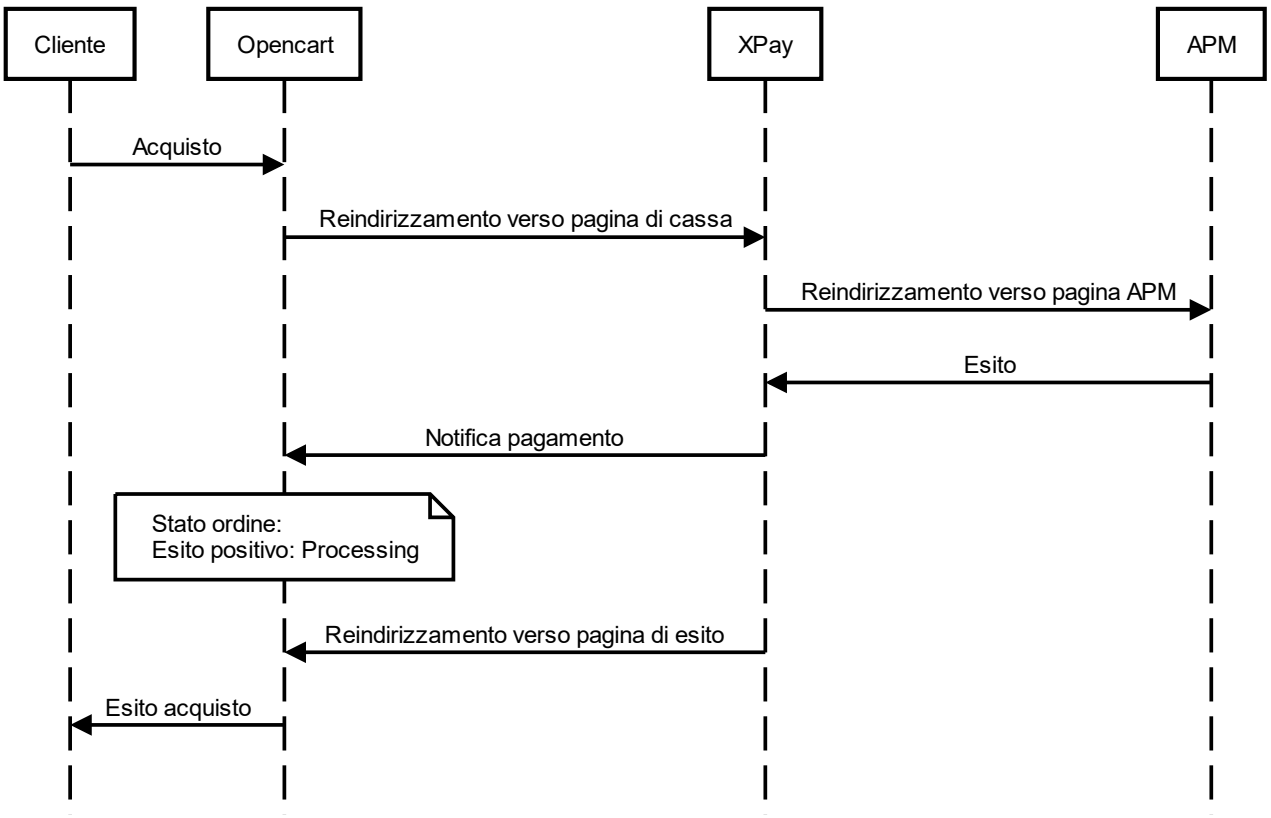
Payment by cards

The Payment flow with relative status changes on the Opencart side in case of card Payment is shown below.



Alternative Payment methods (APM)

The following shows the Payment flow with relative status changes on the Magento side in case of Payment through alternative Payment methods.


Cliente
Opencart
XPay
APM
Acquisto
Reindirizzamento verso pagina di cassa
Reindirizzamento verso pagina APM
Esito
Notifica pagamento
Stato ordine:
Esito positivo: Processing
Reindirizzamento verso pagina di esito
Esito acquisto

Farmakom

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

From the following link you can view the installation and configuration guide: Farmakom activation guide. Or contact the toll-free number **800 687 197** to receive support in activation

For more information you can consult the FarmaKom website.

Support

To receive specialized assistance on the plugin, contact Farmakom support.

Zencart

The Nexi XPay Payment extension for Zencart, allows you to integrate the XPay Payment gateway without further implementation on your site.

It manages the customer's transfer from the merchant's ecommerce site to the Nexi secure environment and vice versa.

The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for Zencart is available free of charge at Zen-cart.com, from which it will be possible to check the compatible versions.
It is possible to install the extension via FTP:
1. Upload the .zip file to the Zencart root.
2. Unzip the file.
3. Log into the Zencart administration panel.
4. In the navigation bar at the top of the page, select **Modules** > **Payment**
6. Select **Nexi XPay** in the list.
7. Click on the **Install** button in the right window.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log in to the Zencart administrative panel
2. In the navigation bar on the left, select **Modules** > **Payment**.
3. On the new page select the **Nexi XPay** plugin in the list and click the **Edit** button.
4. Proceed with the configuration of the module:

Options

Field	Description
Enable/Disable	Abilita o disabilita il modulo di Payment.
Nexi Alias	Code provided by Nexi to the seller
Nexi key MAC	Code provided by Nexi to the seller
Language form	Set the language of the Payment page.
Enable 3D Secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new

	authentication methods, able to improve and speed up the cardholder's shopping experience.
Enable/Disable TEST Mode	Enable or disable test mode. Register in the test area to receive your credentials.
Nexi Alias TEST	Code recoverable in the test area.
Nexi key MAC TEST	Code recoverable in the test area.

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers. For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production

Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is recommended to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards

With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay

NOTES:

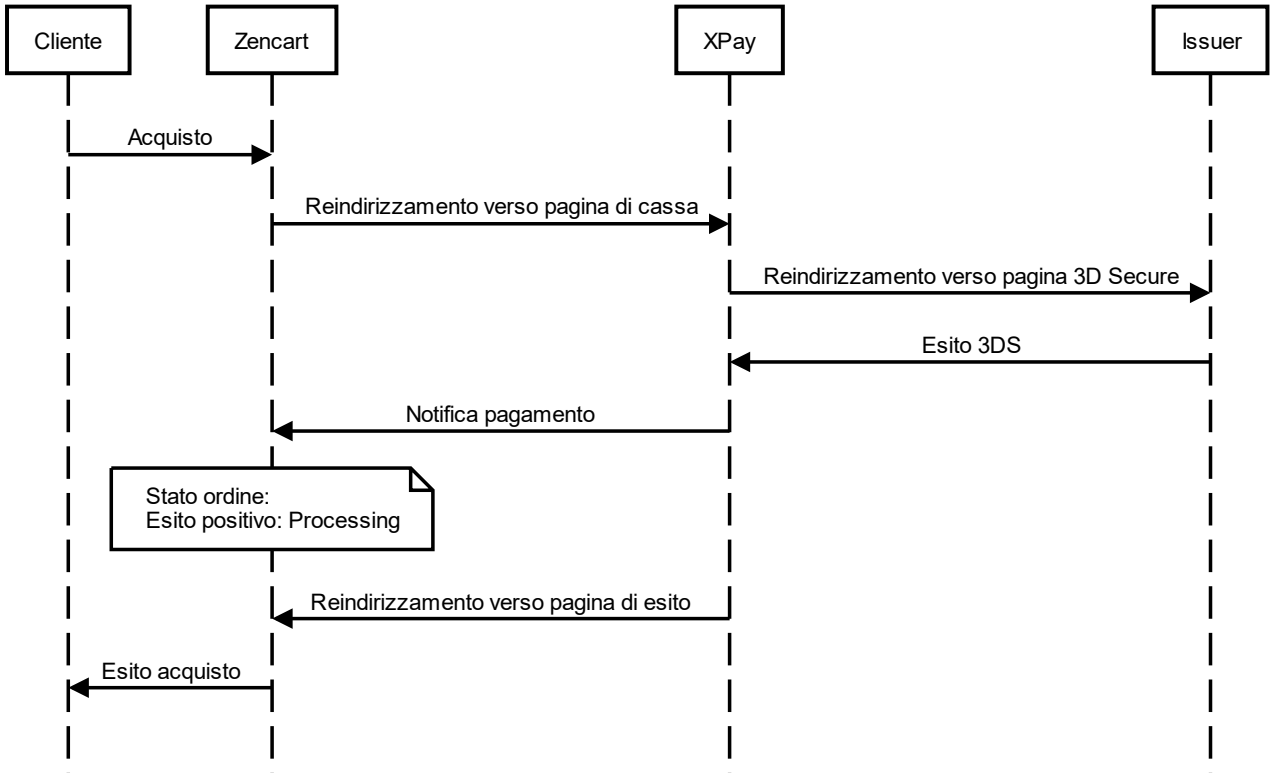
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

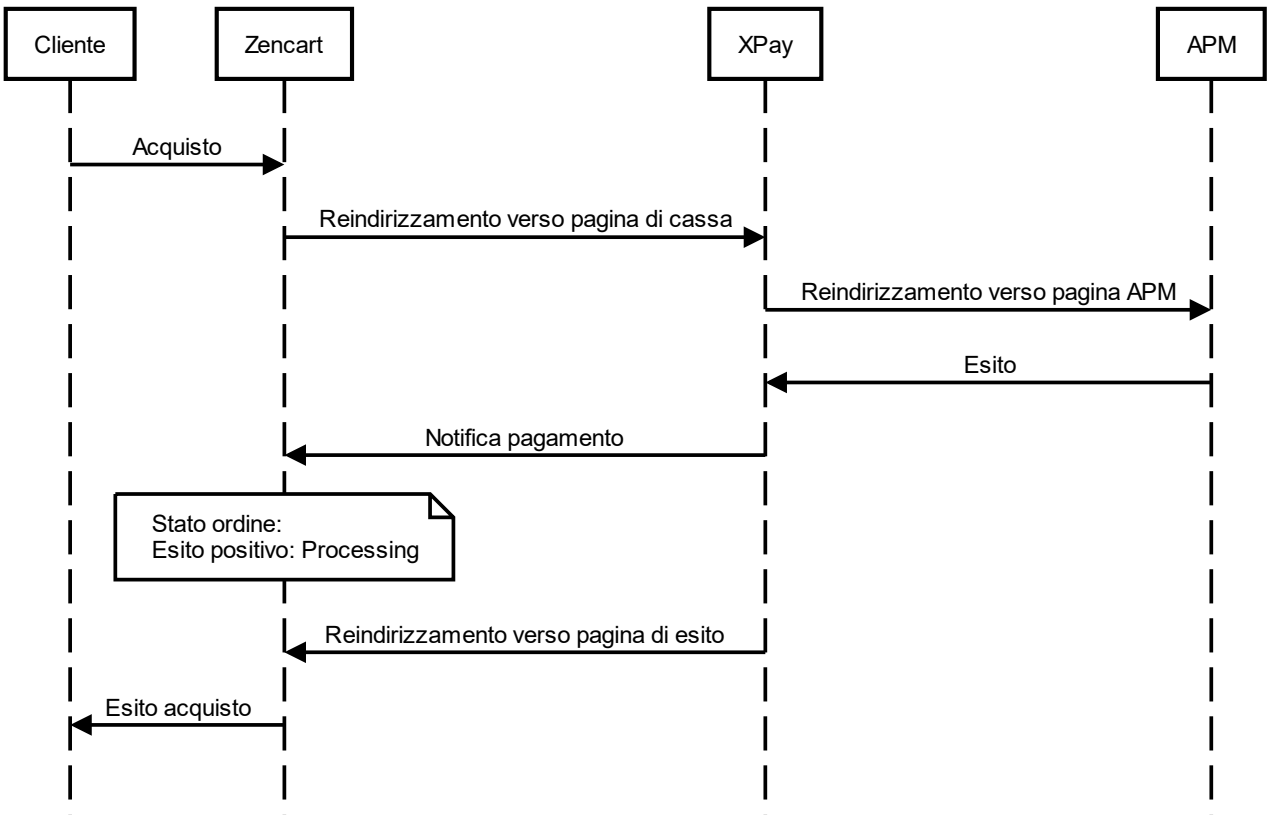
Payment by cards

The Payment flow is shown below with relative status changes on the Zencart side in case of card Payment.



Alternative Payment methods (APM)

The following shows the Payment flow with relative status changes on the Magento side in case of Payment through alternative Payment methods.


Cliente
Zencart
XPay
APM
Acquisto
Reindirizzamento verso pagina di cassa
Reindirizzamento verso pagina APM
Esito
Notifica pagamento
Stato ordine:
Esito positivo: Processing
Reindirizzamento verso pagina di esito
Esito acquisto

Salesforce

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

From the following link you can view the installation and configuration guide: Salesforce Commerce Cloud Activation Guide.

The plugin can be downloaded via the following link: Salesforce plugin.

Support

For specialist plugin support, contact Salesforce Support.

OsCommerce

The Nexi XPay Payment extension for OsCommerce, allows you to integrate the XPay Payment gateway without further implementation on your site.

It manages the customer's transfer from the merchant's ecommerce site to the Nexi secure environment and vice versa.

The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for OsCommerce is available for free at the Apps Marketplace site, from which it will be possible to check the compatible versions.
It is possible to install the extension via FTP:
1. Upload the .zip file to the OsCommerce root.
2. Unzip the file.
3. In the **admin** folder add the following code at the end of the **includes/boxes/modules.php** file

```
$cl_box_groups[sizeof($cl_box_groups)-1]['apps'][] = array('code' => 'nexixpay.php', 'title' => 'Nexi XPay', 'link' => tep_href_link('nexixpay.php'));
```

4. Log in to the OsCommerce administrative panel.
5. In the left navigation bar, select **Modules** > **Payment**
6. Click on the **+ Install Module (n)** button on the top right.
6. Select **Nexi XPay** in the list.
7. Click on the **+ Install Module** button in the right window.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log in to the OsCommerce administrative panel
2. Select in the navigation bar on the left **Modules** > **Payment**.
3. In the new page select the **Nexi XPay** plugin in the list and click the **Edit** button.
4. Proceed with the configuration of the module:

Options

Field	Description
Enable/Disable	Abilita o disabilita il modulo di Payment.

Nexi Alias	Code provided by Nexi to the seller.
Nexi key MAC	Code provided by Nexi to the seller.
Language form	Set the language of the Payment page.
Enable 3D Secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Enable/Disable TEST Mode	Enable or disable test mode. Register in the test area to receive your credentials.
Nexi Alias TEST	Code recoverable in the test area.
Nexi key MAC TEST	Code recoverable in the test area.

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production
Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is advisable to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards
With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction**.**

Alternative Payment methods (APM)
The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay

NOTES:

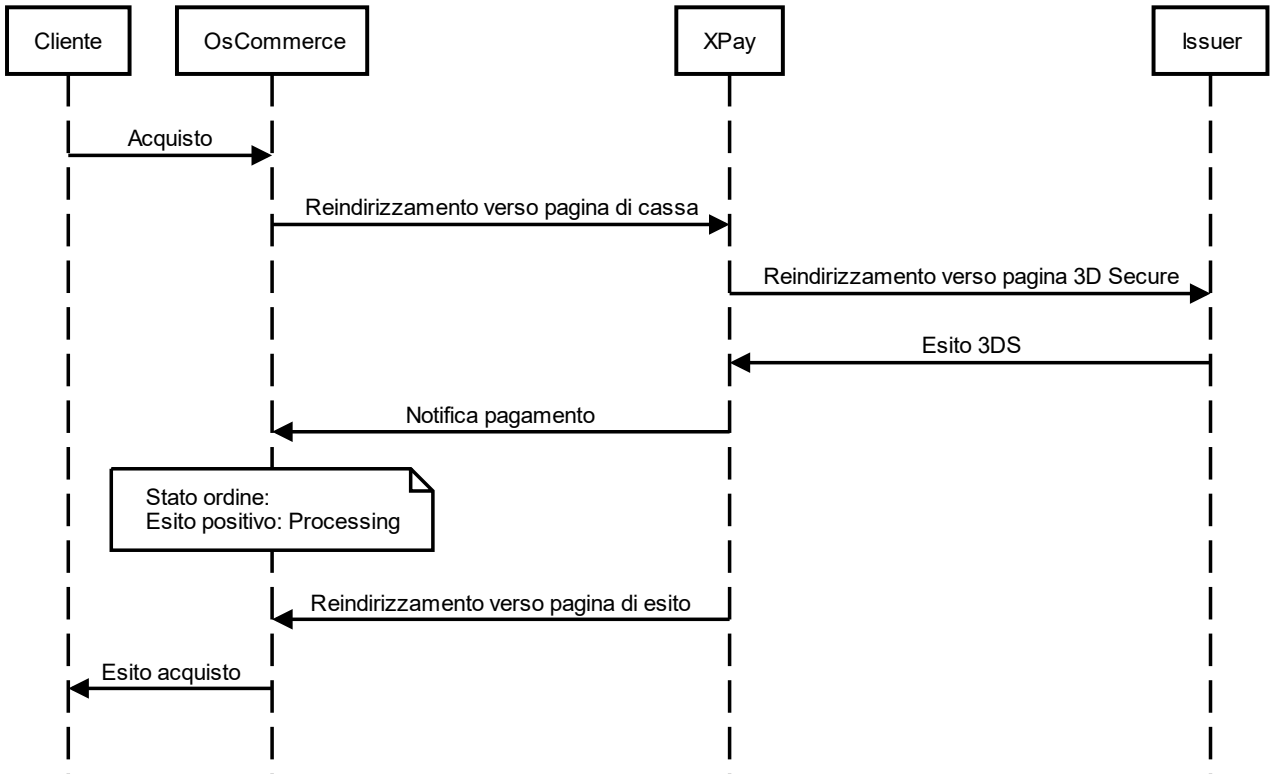
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

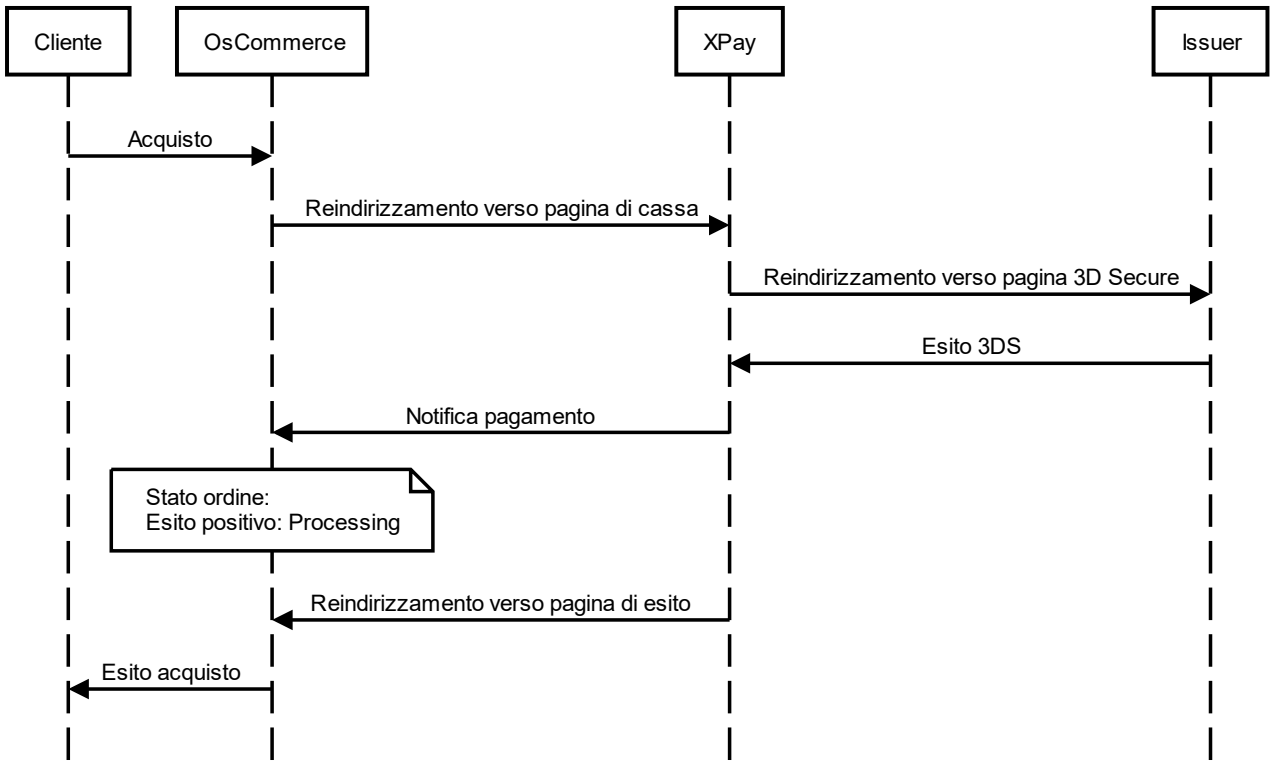
Payment by card

The Payment flow is shown below with relative status changes on the OsCommerce side in case of card Payment.



Alternative Payment methods (APM)

The following shows the Payment flow with relative status changes on the Magento side in case of Payment through alternative Payment methods.


Cliente
OsCommerce
XPay
Issuer
Acquisto
Reindirizzamento verso pagina di cassa
Reindirizzamento verso pagina 3D Secure
Esito 3DS
Notifica pagamento
Stato ordine:
Esito positivo: Processing
Reindirizzamento verso pagina di esito
Esito acquisto

SmallPay

The SmallPay plugin offers the possibility to apply instalment payments on any purchase and to debit each instalment monthly on the customer’s card through recurring, automatic payments.

Setup

The plugin for XPay is available for the e-commerce platforms:

- **Prestashop**
- **Woocommerce**
- **Magento**

Support

To receive specialised support on plugins, contact SmallPay support.

Virtuemart

The Nexi XPay Payment extension for Virtuemart, allows you to integrate the XPay Payment gateway without further implementation on your site.

It manages the customer's transfer from the merchant's ecommerce site to the Nexi secure environment and vice versa.

The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Installation

The Nexi XPay plugin for Virtuemart is available for free at the Joomla Extension site, from which it will be possible to check the compatible versions.
It is possible to install the extension through the Extension Manager installer made available by Joomla:
1. Log into the Joomla administrative panel.
2. In the navigation bar at the top of the page, select **Extension** > **Manage**.
3. Upload the file downloaded from the Joomla Extension site.
4. In the left menu select **Manage**.
5. Look for **Nexi XPay** in the list.
6. Enable the extension by clicking on the appropriate button.
7. In the navigation bar at the top of the page, select **Virtuemart** > **Payment Methods**.
8. In the new page select the **Nexi XPay** plugin in the list and click the **Edit** button.
9. Click the **New** button at the top of the page.
10. In the new page select enter **Nexi XPay** in the **Payment Name** field and **Nexi XPay** as the **Payment Method**
11. Click on the **Save** button at the top of the page.
The installation phase is completed, proceed with the configuration.

Configuration

Below are the instructions to correctly configure the Nexi XPay plugin:
1. Log into the Joomla administrative panel.
2. In the navigation bar at the top of the page, select **Virtuemart** > **Payment Methods**.
3. On the new page click on the **Nexi XPay** plugin in the list.
4. Select **Configuration** section.
5. Proceed with the configuration of the module:

Options

Field	Description
Nexi Alias	Code provided by Nexi to the seller.
Nexi key MAC	Code provided by Nexi to the seller.
Language	Set the language of the Payment page.
Enable 3D Secure 2.0	The 3D Secure 2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's shopping experience.
Enable/Disable TEST Mode	Enable or disable test mode. Register in the test area to receive your credentials.
Nexi Alias TEST	Code recoverable in the test area.
Nexi key MAC TEST	Code recoverable in the test area.

Environment configuration

The plugin creates and updates order statuses via POST notifications sent by Nexi servers.
For each notification sent, Nexi must receive the http 200 status code as a response.
It is therefore necessary that the merchant servers accept the notifications sent by Nexi, otherwise the plugin will not work correctly.

Test and production

It is highly recommended to test the plugin in the test environment, before entering the production codes.
It is possible to obtain the test credentials (alias and mac key) by registering in the XPay test area. You will need to copy the credentials present in the "Simple Payment" section.
In the area there will also be test cards that can be used to perform successful and negative transactions. In this phase it is necessary to verify that the orders are created correctly, also checking the details of the orders.

Passage to production
Once the test phase is finished, it will be possible to enter the production codes and disable the test mode of the plugin. It is recommended to carry out a proof of Payment with a real card with the passage in production.

Payment methods

The Nexi XPay plugin provides customers with various Payment methods:

Payment by cards

With this solution, the customer remains on the merchant's e-commerce until checkout. It is redirected to the Nexi environment to make the Payment and then return to the merchant's site at the end of the transaction.

Alternative Payment methods (APM)

The plugin offers several alternative Payment methods. By selecting the desired method, the customer will be redirected to the checkout page of the chosen Payment service. Below is a list of supported Payment methods:

- Google Pay
- Apple Pay
- MyBank
- AliPay
- WeChat Pay
- GiroPay
- iDEAL
- Bancontact
- EPS
- Przelewy24
- Amazon Pay
- PayPal
- Bancomat Pay

NOTES:

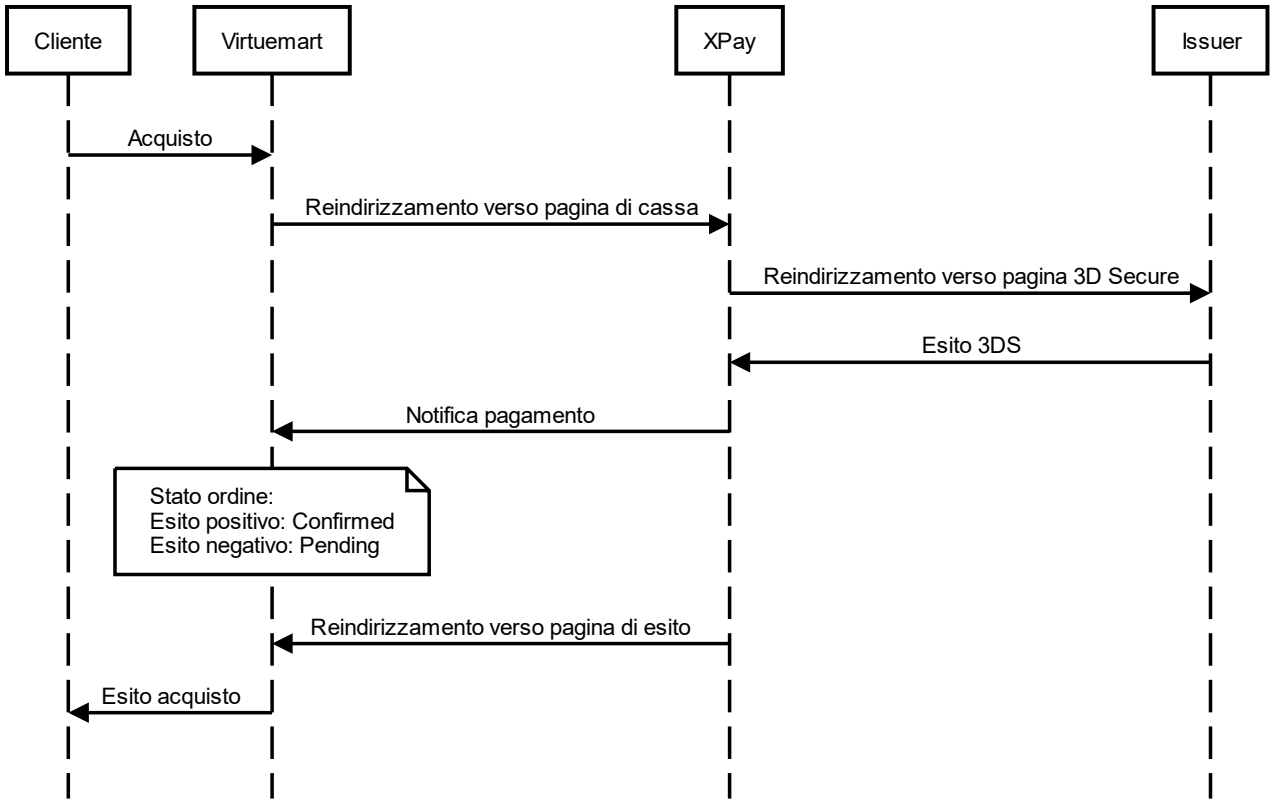
- Once you have enabled a new payment method from the XPay back office, you will need to make a save in the plugin configuration to update the APM list and show the new payment method in the ecommerce site checkout.

- The option to cancel the transaction in case of failed notification is not available with the Bancomat Pay Payment method: in case of anomalies on the notification there could be a mismatch between the order status returned by the plugin and the actual status of the transaction on the Nexi side. You could have the following scenario: the Payment on Bancomat Pay side is correctly carried out with a positive result, but due to a problem on the notification the plugin is not able to update the order status putting it in processing.

Payment flow

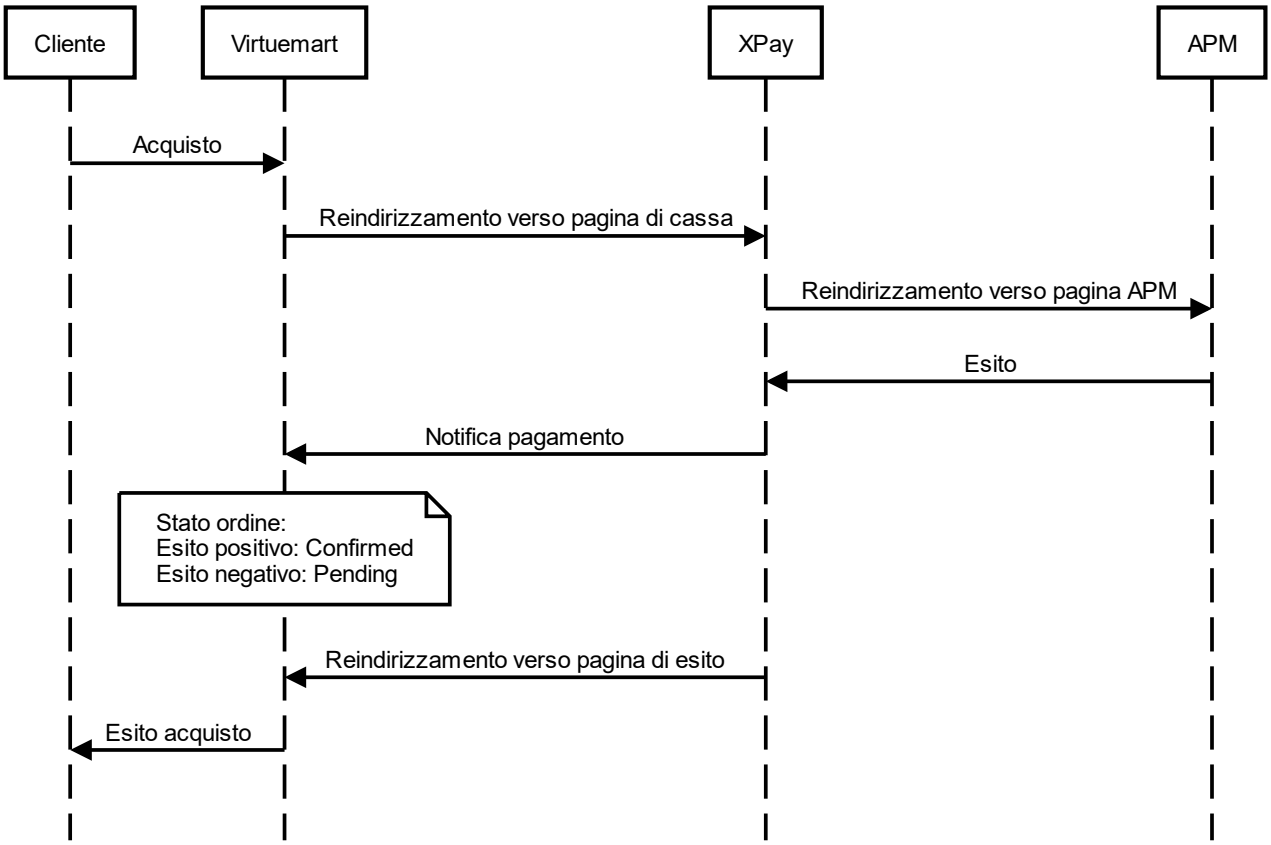
Payment by cards

The Payment flow with relative status changes on the Virtuemart side in case of Payment by cards is shown below.



Alternative Payment methods (APM)

The following shows the Payment flow with relative status changes on the Magento side in case of Payment through alternative Payment methods.



MigliorShop

The Nexi XPay Payment extension for Storeden, allows you to integrate the XPay Payment gateway without further implementation on your site.
It manages the transfer of the customer from the merchant's ecommerce site to the Nexi secure environment and vice versa.
The customer stays on the merchant's e-commerce site until checkout, then is redirected to the XPay gateway to make the Payment.

Setup

To activate XPay on Migliorshop, consult the guide in your customer area.
For more information you can consult the Migliorshop website.

Support

For specialist assistance, please contact Migliorshop Support: assistenza@sferadesign.it .

ReStore

ReStore makes XPay available among the Payment gateways.
ReStore customers can activate the service without making software integrations, simply by providing the credentials of their terminals.

Setup

XPay can be activated via the ReStore platform at any time.

For more information you can consult the ReStore website.

Support

For specialist assistance contact ReStore Support: support@restore.shopping .

eDock

Social Commerce is the new frontier of e-commerce and opens the possibility of selling online even to small retailers.
Thanks to the partnership between Nexi, eDock and e-motion you can sell on Facebook, Instagram and WhatsApp like you never thought before!

Setup

To activate eDock see the page: Activating eDock.

Support

Per assistenza specialistica contatta il Supporto di eDock.

LifePay

The **LifePay** payment extension (Nexi XPay for Liferay) makes it possible to integrate the XPay payment gateway without further implementations on your site.
It manages the customer's transfer from the merchant's e-commerce site to the Nexi secure environment and vice versa.
The customer remains on the merchant's e-commerce site until checkout, and is then redirected to the XPay gateway to make the payment.

Installation

For more information, you may consult the web page dedicated to the plugin in the Liferay marketplace https://marketplace.liferay.com/p/lifepay-nexi-xpay-liferay-payment

Support

For specialised support, contact Nextmind Support at the email address *supportoapp@nextmind.it*.

Pcommerce

With Pcommerce you can activate XPay directly in the settings, it requires no external integration and no further configuration. XPay is natively integrated into the platform and you can activate it by simply providing the required credentials.

Installation

Activation of XPay can be performed at any time directly in the configurations of the Pcommerce platform.

Support

For specialised assistance, please contact our Technical Support: support@pcommerce.it

Contact:

- Tel: 0773.164.61.65
- mail: info@pcommerce.it

Ecwid

The Nexi XPay payment extension for Ecwid allows you to integrate the XPay payment gateway without any further implementations on your site.
It handles the transfer of the customer from the merchant's ecommerce site to the secure Nexi environment and vice versa.
The customer remains on the merchant's ecommerce site until checkout, then is redirected to the XPay gateway to make payment.

Installation

For the activation of XPay on Ecwid see the guide on the Ecwid site.

Support

For specialised assistance, please contact Ecwid Support:
ec.partneraccount@lightspeedhq.com.

SAP Commerce Cloud

With the XPay Plug in you can quickly and easily integrate payment functionality for your SAP Commerce Cloud platform. SAP Commerce Cloud allows you to analyse and optimise the customer experience with a 360-degree view of each customer journey. Digital experience monitoring provides analysis and insight into how the performance of your e-commerce platform affects the customer experience and business profits.

Installation

The Plug In can be downloaded directly from the SAP Commerce Cloud site (https://store.sap.com/dcp/en/product/display-0000060496_live_v1/Nexi Commerce Plugin for SAP Commerce Cloud), where you will need to fill in a form in order to be contacted later by the Nexi team

Support

For specialised assistance, please contact SAP Support.

Scontrino

Scontrino.com is the first Italian e-commerce platform, operational for over 20 years. It has helped thousands of merchants, artisans, producers, and entrepreneurs start an online business in a simple and effective way. With Scontrino.com, you can open a personal e-commerce website with your own domain and manage it independently without any special technical skills, integrating it with social channels as well!

The Nexi XPay payment extension for Scontrino allows you to integrate the XPay payment gateway without any additional implementation on your website.

It manages the customer's transfer from the merchant's e-commerce website to the secure Nexi environment and vice versa.

The customer remains on the merchant's e-commerce website until the checkout moment, then gets redirected to the XPay gateway to make the payment.

Installation

To activate XPay on Scontrino, please refer to the guide on the Scontrino website.

Support

For specialized assistance, please contact the Scontrino Support.

SDK FOR APP

Introduzione

This solution allows you to integrate an SDK made available by Nexi within your Android or iOS application, so you can use dedicated methods to make payments through the XPay gateway and methods to manage payments made.
Through the SDKs for Android and iOS it is possible to implement different types of payments and services such as:

- **Simple payment:** opening of the classic XPay payment page, where the customer will have to enter the card details and proceed with the authentication.
- **Native form:** allows you to host a form within the app in which the customer can directly enter card data and proceed with authentication, without being redirected to external payment pages..
- **Payment in one tap:** during the first payment, the card details are tokenized, in order to allow the customer to make subsequent payments faster.
- **Back office services:** there are methods to manage reversals, accounting operations, payment details, etc...

For each operating system it is possible to download a demo app in order to verify the functioning of the SDKs and test some features such as simple payment and the native form.
Further information on other services made available by the SDKs and further details on the demo apps can be found in the dedicated sections:

- iOS
- Android
- iOS e Android services

To comply with the content security policy specifications, it is useful to include the following header:
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' https:; img-src 'self' 'unsafe-inline' 'unsafe-eval' https: data:; frame-ancestors https:;

Getting Started

Nexi makes the SDK for the iOS platform available on the public GitHub repository. By linking to it, you can download the SDK directly from your development environment.

NOTES: if you do not use the SDK provided by Nexi, in the development of the APP it is necessary to comply with the specifications published in the Apple documentation, where the indications on the supported webview are reported. Also refer to the Apple Pay section.

At the following site is moreover available for download a reference App in source format that can be used as an example for version how to integrate the sdk.

To add the framework within the app, follow the steps below:

- Open XCode (requires Xcode 10.2+) in the app project
- Remove any references to old frameworks added as "Embedded binaries"
- If it is not already present in the project, install Cocoapods following the guide
- Add the following instructions to the generated Podfile:

  platform :ios, '9.0'
  use_frameworks!
  target 'TARGET_NAME' do
  pod 'Nexi_XPay' (if ypu want to use a specific version, you can indicate it with 'numero_versione'. The possible values are listed in the iOS SDK Versions table)
  end

- From the terminal, run the "pod install" command in the project folder, in this way the framework (XPaySDK) will be downloaded and added to your app.

If you are using **Objective-C**: In the project's BuildSettings, choose "Always Embed Swift Standard Libraries" -> YES

NOTES:

• The framework is compiled with Swift version 5, so it can not be used on projects with older versions.
• With this version it is available the compilation with "bitcode" enabled.

WebView

Here are some indications about the most used WebView:

- **Safari View Controller**: this is the recommended view as it is compatible with all Nexi SDKs and with any version of the IOS operating system on the device.
- **WKWebView**: compatible with Nexi SDKs. With this view, Apple Pay is only compatible from version 1.2.5 of the SDK and if the device has the latest version of the IOS operating system. AmazonPay is not usable.
- **UIWebView**: is not compatible for use with the Nexi SDK (supported by Apple until 2020).

XPay initialisation

In order to be able to use the SDK in your app, you need to first initialise XPay main class as follows:

```
let xPay = XPay(secretKey: “SECRET_KEY”)
```

secretKey: the secret key issued to the merchant

NOTES:

- It is strongly recommended NOT to include the secret key within your app, but to have it available via a back end runtime request.
- For information on managing your Mac settings, contact Nexi's technical contact details.

Practical Example

Usage example:

```
xPay._SynchronousPayments.SelectedEnvironmen = .test
```

Below is an example of how to use the APIs:

```
@IBAction func doReverse(sender: AnyObject) {
    let apiReverseRequest = ApiReverseRequest(alias: “ALIAS_MERCHANT”,
    nOrderPM: 500, importo: 1, currency: CurrencyUtils.EUR)
```

```
        self.xPay._Back office.reverse(apiReverseRequest) { (response, error) in
            if error != nil {
        print(error!.Error.Message!)
}
else {
        if(response!.IsSuccess) {
            print(response!.OperationId)
}
else {
        print(response!.Error.Message)
}
}
}
}
```

The example API accepts an incoming request which has been built using the following parameters:

- Merchant's alias
- Order number
- Amount to be reversed
- Currency used for the reversal

APIs are splitted in functional areas:

- Back office
- ControlliSicurezza
- FrontOffice
- GestioneContratti
- HostedPayments
- PagamentiSincroni
- PrimiPagamentiRecurring
- Ricorrenze

Before each API is actually invoked, it is possible to define the current execution environment. The possible values are:

- .test: Test environment
- .prod: Production environment

Change domain

If you want to change the domain of all HTTP calls, within a certain scope, you need to set it using the following method:

xPay._FrontOffice.setDomain(“https://nuovodominio.it”)

Before each API is actually invoked, it is possible to set call timeouts. The value is in milliseconds and is set to 30 seconds by default.

When calling the corresponding API method (in this case ".reverse"), the relevant request and callback will be given in input, and these will communicate the outcome and any result. If the request is successful, the error object will be nil. If it is unsuccessful, the error object will be populated with the error messages and their relative codes. If successful, you need to verify the IsSuccess variable to ensure that the response is valid. If the variable is set to true, the response is valid. Alternatively, all you need to do is invoke the response!.Error.Message variable to get the error message. In the case of a valid response, you will find values relating to the specific response within the "response" variable.

Details for each API (area, request and response) are documented in the "API List" paragraph.

NOTES:
Each request can be coupled with additional parameters, where this has previously been agreed between the merchant and Nexi. Example:

apiReverseRequest.ExtraParameters[“ParameterName”] = “ParameterValue”

Errors and exceptions

Exceptions triggered by APIs are always intercepted and returned as part of the Error variable. This is true for both the error object and the response object (in the case of an invalid response).
The standard error codes that can be used are as follows:

- ResponseCodes.MAC_ERROR -> THIS INDICATES A SECURITY ERROR
- ResponseCodes.SERVER_ERROR

Easy Payment

For a Payment request, a request object must be prepared in the following manner:

```
let apiFrontOfficeQPRequest = ApiFrontOfficeRequestQP(alias:
"ALIAS_MERCHANT", codTrans: "NUMERO_ORDINE", currency:
CurrencyUtilsQP.EUR, amount: 1000, mac: "")
```

Below is an example of how to use the XPay Payment page, with the previously created request:

```
xPay._FrontOffice.paga(apiFrontOfficeQPRequest, parentController: self) { (response) in

    if response.IsValid {

        if response.Error != nil && !(response.Error!.Message).isEmpty {

            message = "Errore durante il pagamento:
            \(response.Error!.Message)"
        } else {

            if response.IsCanceled {
            message = "Transazione annullata"
        } else {

            if response.Mac == "MacCalcolatoLatoServer" { // Verificare
            paragrafo successivo
            message = "Transazione andata a buon fine"
            } else {
            message = "Mac errato"
            }
        }
        } else {
            message = "Transazione negata"
        }
        view?.displaySimpleAlert(title: title, message: message)
}
```

After completing the payment, it will be necessary to retrieve the MAC in the response: *response.Mac*

and compare it with the MAC calculated on the server side in order to validate the outcome received from XPay.

NOTES:

If you want to implement Apple Pay on the XPay checkout page, it is necessary to pay attention to the type of WebView used. According to Apple's guidelines, this specific payment method can only work through SFSafariViewController and WKWebView. Starting from SDK version 1.1.5, you can use SFSafariViewController by calling the method xPay._FrontOffice.pagaSafari.

REQUEST

CLASS
ApiFrontOfficeQPRequest

METHOD
Pay

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.

NOTE:

In the Payment request, you can send optional parameters using the following method:

apiFrontOfficeQPRequest.addExtraKey("nomeparametro","valoreparametro");

RESPONSE

CLASS
ApiFrontOfficeQPResponse

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
brand	Credit card network	AN MAX 100 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	AN hh:mm:ss
isValid()	If this is true, the response is valid. If it is not true, the error parameter will be populated.	True/false
error	Element containing the error code and description: code -> error code, see table message -> error details	OBJ

Optional parameters

Name	Description	Format
extraParameters	Additional optional parameters	AN

NOTES:

- All 3D Secure and Payment procedures are entrusted to the Front Office WebView.
- To enable browsing of web pages, use the "navigation" parameter.
- If a call provides for the possibility of using the 3D secure, the callback can be used to check if the user has canceled the operation from the WebView opened by the Payment process (or generation of XpayNonce). In this case, both the response object and the error object will be "nil".

One tap Payment

To implement this method, the merchant must generate a token at the first payment stage, which will be associated with the card with which the payment is made. For subsequent payments, the merchant will have to make a call to the Nexi API using the previously generated token.

First Payment

To manage an initial Payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_oc3d”. ‘paga_multi’ to have the option of also making recurring payments	AN MIN 2 - MAX 30 CHAR.
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
✓	tipo_richiesta	- PP (first Payment) used for first	AN 2 CHAR.
	gruppo	The “gruppo” value is assigned by Nexi during activation	

IN PRACTICE

apiFrontOfficeQPRequest.addExtraKey("tipo_servizio"," paga_oc3d");
apiFrontOfficeQPRequest.addExtraKey("num_contratto",""); // contract number to be associated with the card that the user will use for Payment.
apiFrontOfficeQPRequest.addExtraKey("tipo_richiesta","PP");
apiFrontOfficeQPRequest.addExtraKey("gruppo","")// The “gruppo” value is assigned by Nexi during activation.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.
- By contacting Nexi support you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick Payments.

Subsequent Payment

To make a Payment on a previously registered contract, set the parameter "*tipo_richiesta* " with "PR", or, refer to the section “3D Secure Subsequent Payment”.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so that recurrences can be made for services such as subscriptions.
If, on the other hand, you are interested in a solution that allows the end customer to store their card data, and subsequently use it to make purchases more quickly, refer to the OneClick solution.

First Payment

To manage an initial Payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MIN 2 - MAX 30 CHAR.
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
✓	tipo_richiesta	- PP (first Payment) used for first	AN 2 CHAR.
	gruppo	The “gruppo” value is assigned by Nexi during activation	

IN PRATICA

apiFrontOfficeQPRequest.ExtraParameters["tipo_servizio"] = "paga_multi";
apiFrontOfficeQPRequest.ExtraParameters["tipo_richiesta"] = "PP";
apiFrontOfficeQPRequest.ExtraParameters["num_contratto"] = ""; // numero contratto da associare alla carta che l'utente userà per il pagamento.
apiFrontOfficeQPRequest.ExtraParameters["gruppo"] = ""; // viene assegnato in fase di attivazione da Nexi

Subsequent Payment

To make a Payment on a previously registered contract, set the parameter "*tipo_richiesta* " with "PR", or, refer to the section “3D Secure Subsequent Payment”.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Native Form

To facilitate the native integration by the developers, a specific control was created that can be used only through the Xcode Interface Builder, called "Native Form". This UIView is able to collect the data entered by the user, without making them usable or readable in any way by the developer. Once integrated, it will be possible to invoke the "createNonce" method to get back the token with which it is possible to conclude the Payment via S2S call.

Useful information on configuring the "Form Nativa" control:

- 2 display modes are available to facilitate integration into different layouts. The first one is called "Inline" and allows to have a data collection view on a single line occupying little space inside the page. The second one is the "Multi", which, unlike the first one, has a larger layout (recommended dimensions: height -> 150) and presents the input fields on 2 lines.
- The use of the in-app keyboard associated with the native form is not mandatory (although very recommended for security reasons), but it is still possible to activate/deactivate it via Interface Builder.
- Both layouts of the native form foresee by default an animation in case there is an error in the card data entered by the user (shake animation). The latter can be deactivated by setting the property "shakeOnErrors" to false (also by Interface Builder).
- To meet the need for customization, you can configure the background color of the buttons and text on the in-app keyboard. To do this simply use the "setKeyboard (background: UIColor)" and "setKeyboard (text: UIColor)" methods available in the CardFormMulti or CardFormInline object.
- Always with regard to customization it is possible to configure the colors of the texts and errors that occur within the native form. Properties must be set: fontColor (UIColor) and errorColor (UIColor). Customisation of fonts is not foreseen.

Here are the procedures to use the native form:

• Draw a UIView within your Interface Builder.
• Set "CardFormMulti" or "CardFormInline" as the custom class according to your preferences, in the "Module" section write "XPaySDK".
• Connect the View (Form Nativa) to the relative ViewController, creating a special variable that for convenience we will call "cardForm".
• To be able to create the XpayNonce starting from the newly created "cardForm" object, simply call the "createNonce" method. Below is an example of a code:

```
do {
try cardForm.createNonce(parent: self, secretKey: “”, alias: “”, environment: .test,
amount: 1, currency: CurrencyUtils.EUR,
codTrans: “”, handler: { (response, error) in if error != nil {
```

```
message = error!.Error.Message
} else {
if let xpayNonceResponse = response {
if xpayNonceResponse.IsSuccess {
// If the XpayNonce was created go to result page self.view?.goToResult(codTrans:
vc.codTrans!, amount: vc.amount!)
// HERE IN YOUR APPLICATION YOU MUST USE THE XPAYNONCE TO MAKE
THE SERVER TO SERVER PAYMENT
} else {
message = response!.Error.Message
}
} else {
// User has canceled the 3D Secure Payment
message = "Payment canceled by user"
}
} catch XPayError.JailbrokenDevice {
print("Jailbroken Device")
} catch CardException.INVALID_CARD {
print(“Invalid data”)
} catch let error {
print(error)
}
```

• The "INVALID_CARD" exception indicates that the user has entered invalid card data according to the various validation algorithms. The following are the specifics of this methodology:

REQUEST

CLASS
createNonce

Mandatory	Name	Description	Format
✓	parent	ViewController from which it is invoked	ViewController
✓	secretKey	Secret key for calculating the mac (fixed value communicated by Nexi during the activation phase).	AN
✓	alias	Identification code of the merchant profile (fixed value	AN MAX 30

		communicated by Nexi during the activation phase)	
✓	environment	Execution enviroment	AN Possible values: XPay.Environments.INTEG, XPay.Environments.PROD
✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	currency	978 per Euro	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 NO #. If MyBank you canuse only: / - : ( ) . , +
✓	handler	The function that listens to the API call	AN

RESPONSE

CLASS
ApiCreaNonceResponse

Mandatory	Name	Description	Format
✓	result	Result of the request.	AN ok / ko

✓	operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in millisecond format.	N 13 CRT
✓	xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

PAYMENT

Once the nonce is received, Payment can be made via the pagaNonce API.

Recurring and OneClick

You can implement recurring and OneClick payments by using the **createNoncePP** method instead of the "createNonce" method in the first card registration payments. Below is an example of code:

```
do {
try cardForm.createNoncePP(parent: self, secretKey: "", alias: "", environment: .test,
amount: 1, currency: CurrencyUtils.EUR,
codTrans: "", handler: { (response, error) in if error != nil {
message = error!.Error.Message
} else {
if let nonceResponse = response {
if nonceResponse.IsSuccess {
// If the Nonce was created go to result page self.view?.goToResult(codTrans:
vc.codTrans!, amount: vc.amount!)
// HERE IN YOUR APPLICATION YOU MUST USE THE NONCE TO MAKE THE
SERVER TO SERVER PAYMENT
} else {
message = response!.Error.Message
}
} else {
// User has canceled the 3D Secure payment
message = "Payment canceled by user"
}
} catch XPayError.JailbrokenDevice {
print("Jailbroken Device")
} catch CardException.INVALID_CARD {
print("Invalid data")
} catch let error {
print(error)
}
```

Below are the specifics of this methodology:

REQUEST

CLASS
createNoncePP

Mandatory	Name	Description	Format
✓	parent	ViewController from which it is invoked	ViewController
✓	secretKey	Secret key for calculating the mac (fixed value communicated by Nexi during the activation phase).	AN
✓	alias	Identification code of the merchant profile (fixed value communicated by Nexi during the activation phase)	AN MAX 30
✓	environment	Execution enviroment	AN Possible values: XPay.Environments.INTEG, XPay.Environments.PROD
✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	currency	978 per Euro	AN MAX 3
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice	AN MIN 2 MAX 30 NO #. If MyBank you canuse only: / - : ( ) . , +

		more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
✓	handler	The function that listens to the API call	AN

RESPONSE

CLASS
ApiCreaNoncePrimoPagamento3DSResponse

Mandatory	Name	Description	Format
✓	result	Result of the request.	AN ok / ko
✓	operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in millisecond format.	N 13 CRT
✓	xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

PAYMENT

Once the nonce is received, Payment can be made via the pagaNonce API.

SUBSEQUENT PAYMENTS

- To perform a recurrence, it is necessary to call up the dedicated API pagamentoRicorrente
- To perform a subsequent OneClick payment you must follow the specifications Pagamento successivo 3DS

Apple Pay

To facilitate Merchants in the Apple Pay integration we offer a simplified development approach that allows the merchant application to be dependent just on the Xpay SDK and not on Apple Pay (which is already included).

To use ApplePay you have to create a certificate through Apple portal, then upload it on Xpay Back office. In this way, calls from the app on which the certificate was generated will be validated by the XPay Server.

Here below the steps to integrate Apple Pay through XPay SDK:

- To create a certificate and upload it to the XPay Back Office.
- Enable Apple Pay via the Target Capabilities and generate a valid Id merchant.
- Have your ViewController extended from the "ApplePayViewController" class.
- To start the Payment process through Apple Pay, call the "payWithApple" method inherited from the ViewController. Here is an example of code:

```
do {
let appleRequest = ApplePayRequest(merchantId: “”, secretKey: “”, alias: “”,
displayName: “”, amount: 1, currency: “EUR”, country: )
“IT”, codTrans: “”
appleRequest.SelectedEnvironment = .test
appleRequest.ShippingFields = true
appleRequest.BillingFields = true
try payWithApple(request: appleRequest!, handler: { (response, error) in {
if error != nil {
// Error during Payment process
print(error!.Error.Message)
} else {
if response != nil {
// Payment was completed
print(response!.Brand)
} else {
// Error during Payment process
print(response!.Error.Message!)
}
}
}
}})
} catch let error as XPayError {
print(error.description!)
} catch {
print(error.localizedDescription)
}
```

Through the closure above it is possible to manage a flow similar to a normal Payment in WebView.

The following are the specifics of this methodology:

REQUEST

CLASS
payWithApple

METHOD
ApplePayRequest

Mandatory	Name	Description	Format
✓	merchantId	Code assigned by Nexi	AN
✓	secretKey	Secret key for calculating the mac (fixed value communicated by Nexi during the activation phase).	AN
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	displayName	Name dispayed during ApplePay Payment	AN
✓	amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8
✓	currency	978 per Euro	AN MAX 3
✓	country	Nationality of merchant	AN MIN 2 MAX 30

✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be univocal for every authorization request, only in case of negative result of the authorization the merchant can re-propose the same request with the same codTrans for another 2 times, during configuration the operator can choose to decrease the 3 attempts	AN MIN 2 MAX 30 Excluded character #. In case of MyBank you can only use: / - : ( ) . , +
✓	SelectedEnvironment	Execution enviroment	AN
✓	ShippingFields	Shipping address	AN
✓	BillingFields	Billing address	AN

RESPONSE

CLASS
ApiApplePayResponse

Mandatory	Name	Description	Format
✓	authCode	Confirmation code issued by the card issuer.	AN MAX 6
✓	billingContact	JSON with info received about Billing (received by Apple)	JSON
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100

✓	country	Credit card nation	AN MIN 2 MAX 30
✓	date	Transaction date	DATA gg/mm/aaaa
✓	productType	Credit card type	AN MIN 2 MAX 30
✓	shippingContact	JSON with info received about Shipping (received by Apple)	JSON
✓	transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 MAX 30

NOTE:

The Payment process is implemented by the SDK using the "applePay" REST API.

Jailbreak Control

To avoid the use of devices with Jailbreak on board, the XPay framework will not work on such devices to deal with any security issues during Payment processes. Developers are given the chance to handle the returned exception in case a Jailbreak is detected.

Below is an example of integration:

```
do {
xPay = try XPay(secretKey: XPayConstants.SECRET_KEY)
} catch {
// Eccezione restituita nel caso in cui il dispositivo presenti Jailbreak
print("Jailbroken Device")
}
```

Getting Started

Nexi provides the Android platform SDK on the public GitHub repository. By linking to it, you can download the SDK directly from your development environment.

At the following site is moreover available for download a reference App in source format that can be used as an example for version how to integrate the sdk.

In addition to the XPay SDK, it is necessary to import some libraries, follow the steps listed below:

- Open Android Studio on the project corresponding to the merchant's app (which should already have been done).
- Go to the gradle file of the "app" module, where the dependencies are contained.
- Add the following libraries to the dependencies:
  dependencies {
  implementation 'com.android.support:appcompat-v7:27.1.1'
  implementation 'com.android.volley:volley:1.1.1'
  implementation 'com.google.code.gson:gson:2.8.5' // Libreria di XPay
  implementation 'it.nexi.xpay:XPaySDK:1.2.1' // (it is possible to specify number version)
  // If you want to use also GooglePay
  implementation 'com.google.android.gms:play-services-wallet:16.0.1'
  // If you want to use Custom Chrome Tabs
  implementation 'com.android.support:customtabs:27.1.0'
  }

XPay initialisation

In order to be able to use the SDK in your app, you need to first initialise XPay main class as follows:

XPay xPay = new XPay(application_context, secret_key);

application_context: this is the internal context for the merchant's app
secret_key: the secret key issued to the merchant

NOTES:
It is strongly recommended NOT to include the secret key within the app, but to request it at Runtime from your Back End. For the Simple/One-Tap/Recurrent payment method, the possibility is provided to initialise the SDK without a secret key, the mac will then have to be calculated server-side and sent to the app when needed:

XPay xPay = new XPay(context_applicazione);

Practical Example

Below is an example of how to use the APIs:

```
        private void doEnableContract() {
                ApiEnableContractRequest apiEnableContractRequest = new
ApiEnableContractRequest (
                        "ALIAS_MERCHANT”,
                        "NUMBER_CONTRACT"
                );

        xPay.ContractManagement.setEnvironment(EnvironmentUtils.Environment.TEST);
                xPay.ContractManagement.setTimeout(20000);
                xPay.ContractManagement.enableContract(apiEnableContractRequest,
                new ApiResponseCallback<ApiEnableContractResponse>() {
                        @Override
                        public void onSuccess(ApiEnableContractResponse response) {
                                Log.i("EnableContract", response.getOperationId());
                        }

                        @Override
                        public void onError(ApiErrorResponse error) {
                                Log.i ("EnableContract", "Message: " +
error.getError().getMessage());
                        }
                 });
        }
```

The example API accepts an incoming request which has been built using the following parameters:

- Merchant's alias
- Number of the contract to enable

APIs are splitted in diffent functional areas:

- Back office
- ControlliSicurezza
- FrontOffice
- GestioneContratti
- HostedPayments
- PagamentiSincroni
- PrimiPagamentiRecurring
- Ricorrenze

Before each API is actually invoked, it is possible to define the current execution environment. The possible values are:

- EnvironmentUtils.Environment.TEST: Test environment
- EnvironmentUtils.Environment.PROD: Production environment

If you want to change the domain of all HTTP calls, within a certain scope, you need to set it using the following method:

xPay._FrontOffice.setDomain("https://nuovodominio.it")

Before each API is actually invoked, it is possible to set call timeouts. The value is in milliseconds and is set to 30 seconds by default.

When calling the corresponding API method (in this case ".enableContract"), the relevant request and callback will be given in input, and these will communicate the outcome and any result.
If successfully executed, the onSuccess method will be invoked for the callback supplied, and this will receive the specified API response in the input.

Details for each API (area, request and response) are documented in the "API List" paragraph.

NOTES:
Each request can be coupled with additional parameters, where this has previously been agreed between the merchant and Nexi. Example:

apiAbilitaContrattoRequest.addExtraKey("ParameterName", "ParameterValue");

Errors and Exceptions

Exceptions triggered by APIs are always intercepted and returned using the callback's **onError** method, within the **ApiErrorResponse** object type:

```
@Override
public void onError(ApiErrorResponse error) {
    /***the error variable contains the errors generated***/
}
```

The getError() method is within this object; it returns the corresponding API simplified error and will contain both an error code and an error message.
The standard error codes that can be used are as follows:

- ResponseCodes.MAC_ERROR -> THIS INDICATES A SECURITY ERROR
- ResponseCodes.SERVER_ERROR

NOTES:

✓ To enable logs use the following code:

XPayLogger.DEBUG = true;

✓ In the case of problems with minimisation and shrinkage, add the following R8 directive to exclude the sdk from the minimisation and shrinkage process:

*-keep class en.nexi.** { *; }*

For a Payment request, a request object must be prepared in the following manner:

```
ApiFrontOfficeQPRequest apiFrontOfficeQPRequest = null;
try {
        apiFrontOfficeQPRequest = new
        ApiFrontOfficeQPRequest("checkoutQP",”ORDER_NUMBER”,
        CurrencyUtilsQP.EUR, 1000);
        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();
        } catch (MacException e) {
            e.printStackTrace();
}
```

It will be necessary to handle the MacException: exception generated in case an error occurs on the Mac control or calculation.

Below is an example of how to use the XPay Payment page, with the previously created request:

```
xPay.FrontOffice.paga(apiFrontOfficeQPRequest, navigationEnabled, new
FrontOfficeCallbackQP()   {
        @Override
        public void onConfirm(ApiFrontOfficeQPResponse
apiFrontOfficeQPResponse) {
            if(apiFrontOfficeQPResponse.isValid()) {
                Log.i(TAG, "Valid response, operation confirmed by user");
            }
            else {
                Log.i(TAG, "Invalid response");
                        THIS INDICATES A SECURITY ERROR
            }

        }

        @Override
        public void onCancel(ApiFrontOfficeQPResponse
apiFrontOfficeQPResponse) {
            Log.i(TAG, "Operation cancelled by user");
        }
    }
 );
```

XPay’s callback allows 2 "return" methods. The first - onConfirm - is invoked if the user makes a Payment, regardless of whether the Payment is successful or not. This can be

verified using the "isValid ()" method. The second - onCancel - is invoked if the user cancels the Payment.

The "navigationEnabled" parameter is a boolean variable: it allows WebView navigation if set to true, if set to false the customer will not be able to use the navigation keys (device "back" button) to navigate between the XPay checkout pages.

REQUEST

CLASS
ApiFrontOfficeQPRequest

METHOD
Pay

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.

NOTE:

In the Payment request, you can send optional parameters using the following method:

apiFrontOfficeQPRequest.addExtraKey("nomeparametro","valoreparametro");

RESPONSE

CLASS
ApiFrontOfficeQPResponse

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
brand	Credit card network	AN MAX 100 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	AN hh:mm:ss
isValid()	If this is true, the response is valid. If it is not true, the error parameter will be populated.	True/false
error	Element containing the error code and description: code -> error code, see table message -> error details	OBJ

NOTES:

- All 3D Secure and Payment procedures are entrusted to the Front Office WebView.
- To enable web page browsing, use the "navigationEnabled" parameter.
- In the case of problems with minimisation and shrinkage, add the following R8 directive to exclude the sdk from the minimisation and shrinkage process:

  *-keep class en.nexi.** { *; }*

One tap Payment

To implement this method, the merchant must generate a token at the first payment stage, which will be associated with the card with which the payment is made. For subsequent payments, the merchant will have to make a call to the Nexi API using the previously generated token.

First Payment

To manage an initial Payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_oc3d”. ‘paga_multi’ to have the option of also making recurring payments	AN MIN 2 - MAX 30 CHAR.
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
✓	tipo_richiesta	- PP (first Payment) used for first	AN 2 CHAR.
	gruppo	The “gruppo” value is assigned by Nexi during activation	

IN PRACTICE

apiFrontOfficeQPRequest.addExtraKey("tipo_servizio"," paga_oc3d");
apiFrontOfficeQPRequest.addExtraKey("num_contratto",""); // contract number to be associated with the card that the user will use for Payment.
apiFrontOfficeQPRequest.addExtraKey("tipo_richiesta","PP");
apiFrontOfficeQPRequest.addExtraKey("gruppo","")// The “gruppo” value is assigned by Nexi during activation.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.
- By contacting Nexi support you can activate the dynamic 3D Secure service. This service allows you to send a 3D Secure exemption request which will be evaluated by the card issuer and eventually accepted. Once the service is enabled, Nexi will automatically send the 3DS exemption request in all OneClick Payments.

Subsequent Payment

To make a Payment on a previously registered contract, set the parameter "*tipo_richiesta* " with "PR", or, refer to the section “3D Secure Subsequent Payment”.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so that recurrences can be made for services such as subscriptions.
If, on the other hand, you are interested in a solution that allows the end customer to store their card data, and subsequently use it to make purchases more quickly, refer to the OneClick solution.

First Payment

To manage an initial Payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MIN 2 - MAX 30 CHAR.
✓	num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
✓	tipo_richiesta	- PP (first Payment) used for first	AN 2 CHAR.
	gruppo	The “gruppo” value is assigned by Nexi during activation	

IN PRATICA

apiFrontOfficeQPRequest.ExtraParameters["tipo_servizio"] = "paga_multi";
apiFrontOfficeQPRequest.ExtraParameters["tipo_richiesta"] = "PP";
apiFrontOfficeQPRequest.ExtraParameters["num_contratto"] = ""; // numero contratto da associare alla carta che l'utente userà per il pagamento.
apiFrontOfficeQPRequest.ExtraParameters["gruppo"] = ""; // viene assegnato in fase di attivazione da Nexi

Subsequent Payment

To make a Payment on a previously registered contract, set the parameter "*tipo_richiesta* " with "PR", or, refer to the section “3D Secure Subsequent Payment”.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.
- Contracts that remain unused for more than 12 months are subject to expiry determined by card circuit rules. For subscriptions with a periodicity of more than 12 months, it is therefore necessary to implement an action to keep these contracts active: a recurrence transaction of 1 cent followed by a reversal is sufficient.

Native Form

To facilitate the native integration by the developers, a specific control has been created that can also be used by XML and Designer of Android Studio, called "Native Form". This View is able to collect the data entered by the user, without making them usable or readable in any way by the developer. Once integrated, it will be possible to invoke the "createNonce" method to get back the token with which it is possible to conclude the Payment via S2S call.

Useful information on configuring the "Form Nativa" control:

- 2 display modes are available to facilitate integration into different layouts. The first one is called "Inline" and allows to have a data collection view on a single line occupying little space inside the page. The second one is the "Multiline", which unlike the first one, has a larger layout (recommended dimensions: height -> 150dp) and presents the input fields on 2 lines.
- The use of the in-app keyboard associated with the native form is not mandatory (although very recommended for security reasons), but it can be disabled by setting the "enableInAppKeyboard" property to false (also as an attribute by Designer).
- Both layouts of the native form foresee by default an animation in case there is an error in the card data entered by the user (shake animation). The latter can be deactivated by setting the "enableShakeAnimation" property to false (also as an attribute by Designer).
- To meet the need for customization, you can configure the background color of the buttons and text on the in-app keyboard. To do this, simply use the "keyboardBackground =" color_desiderato "and" keyboardTextColor = "color_desiderato" "attributes available in the CardFormViewMultiline or CardFormViewInline object.

Here are the procedures to use the native form:

• Using the Android Studio Designer, add one of the following Views to your XML layout, based on your needs and available space:
it.nexi.xpay.CardFormView.CardFormViewInline
it.nexi.xpay.CardFormView.CardFormViewMultiline

• Connect the View (Form Nativa) to the desired activity (or Fragment etc), creating a special variable that for convenience we will call "cardForm".

• To be able to create the XpayNonce starting from the newly created "cardForm" object, simply call the "createNonce" method. Here is an example of code:

```
try {
cardFormMultiline.createNonce(mContext, “ALIAS”, "SECRET_KEY",1,
CurrencyUtils.EUR, "CODTRANS-"
+ System.currentTimeMillis(), EnvironmentUtils.Environment.TEST,new
ApiResponseCallback<ApiCreaNonceResponse>() {
@Override
public void onSuccess(ApiCreaNonceResponse response) {
if (response.isSuccess())
Log.i("XPAY", "OK, xpayNonce: " + response.getXpayNonce());
else
Log.i("XPAY", "NON OK, error msg: " + response.getError().getMessage());
}
@Override
public void onError(ApiErrorResponse error) {
Log.e("XPAY", "ERROR, error msg: " + error.getError().getMessage());
}
});
} catch (DeviceRootedException e) {
Log.e("XPAY", "Rooted device");
e.printStackTrace();
} catch (InvalidCardException ex) {
Log.e("XPAY","Invalid card input");
}
```

Here are the specifications of this methodology

METHOD
createNonce

Mandatory	Name	Description	Format
✓	context	Context Android	context
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	secretKey	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN

✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	currency	978 per Euro	AN MAX 3
✓	transCode	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 NO #. If MyBank you can only use: / - : ( ) . , +
✓	environment	Execution enviroment	AN

RESPONSE

CLASS
ApiCreaNonceResponse

Mandatory	Name	Description	Format
✓	result	Result of the request.	AN ok / ko
✓	operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in millisecond format.	N 13 CRT
✓	xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

Recurring and OneClick

It is possible to implement recurring and OneClick payments by using the **createNoncePP** method instead of the "createNonce" method in the first card registration payments.
Below is an example of code:

```
try {
cardFormMultiline.createNoncePP(mContext, "ALIAS", "SECRET_KEY",1,
CurrencyUtils.EUR, "CODTRANS-"
+ System.currentTimeMillis(), EnvironmentUtils.Environment.TEST,new
ApiResponseCallback<ApiCreaNoncePrimoPagamento3DSResponse>() {
@Override
public void onSuccess(ApiCreaNoncePrimoPagamento3DSResponse response) {
if (response.isSuccess())
Log.i("XPAY", "OK, nonce: " + response.getNonce());
else
Log.i("XPAY", "NON OK, error msg: " + response.getError().getMessage());
}
@Override
public void onError(ApiErrorResponse error) {
Log.e("XPAY", "ERROR, error msg: " + error.getError().getMessage());
}
});
} catch (DeviceRootedException e) {
Log.e("XPAY", "Rooted device");
e.printStackTrace();
} catch (InvalidCardException ex) {
Log.e("XPAY","Invalid card input");
}
```

Here are the specifications of this methodology

METHOD
createNoncePP

Mandatory	Name	Description	Format
✓	context	Context Android	context
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	secretKey	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN
✓	amount	Amount to be authorized in hundredths of euro without separator, the first 2 numbers on the right represent the euro cents, eg .: 5000 corresponds to € 50.00	N MAX 8
✓	currency	978 per Euro	AN MAX 3
✓	transCode	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 NO #. If MyBank you can only use: / - : ( ) . , +
✓	environment	Execution enviroment	AN

RESPONSE

CLASS
ApiCreaNoncePrimoPagamento3DSResponse

Mandatory	Name	Description	Format
✓	result	Result of the request.	AN ok / ko
✓	operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in millisecond format.	N 13 CRT
✓	xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

PAYMENT

Once you have received the nonce, you can make the payment via the API pagaNonceCreazioneContratto.

SUBSEQUENT PAYMENT

- To perform a recurrence, it is necessary to call up the dedicated API pagamentoRicorrente
- To perform a subsequent OneClick payment you must follow the specifications Pagamento successivo 3DS

Payment Chrome Custom Tabs

Starting with version 1.1.1 of the XPay Android SDK, it has been introduced the possibility to make a Payment through Google's Chrome Custom Tabs. The integration mode is the same for QP cash pages, only the name of the method used (payChrome) changes. We report the parameters for convenience:

REQUEST

CLASS
pagaChrome

METHODO
ApiFrontOfficeQPRequest

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 Except the “#” character. In case of MyBank you can only use: / - : ( ) . , +
✓	amount	Amount expressed in euro cents without separators	N MAX 9
✓	currency	978 per Euro	AN MAX 3

RESPONSE

CLASS
ApiFrontOfficeQPResponse

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
✓	error	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
✓	amount	Amount expressed in euro cents without separators	N MAX 9
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 NO #. In case of MyBank you can use only: / - : ( ) . , +
✓	currency	978 per Euro	AN MAX 3
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100
✓	date	Transaction date	DATA gg/mm/aaaa
✓	time	Transaction time	AN hh:mm:ss

✓	authCode	Confirmation code issued by the card issuer	AN MAX 6
✓	isValid()	If true, the answer will be valid, otherwise the error parameter will be evaluated	AN
	extraParameters	Optional extra parameters	AN

In the case of initialisation of the SDK without a secret key, once the payment has been completed and the user has closed the ChromeTab, only the alias and codTrans fields will be valorised in the response received in the onSuccess() method.

To check the status of the payment, it will be necessary to invoke the paymentResult method (again, passing the relevant mac code in the request and checking the one in the response):

```
ApiPaymentResultRequest request = new ApiPaymentResultRequest(response.getAlias(),
response.getCodTrans(), mac);
xPay.HostedPayments.paymentResult(request, new ApiResponseCallback() {
@Override
public void onSuccess(ApiPaymentResultResponse response) {
//TODO response.getPaymentQP()
}

@Override
public void onError(ApiErrorResponse error) {
//TODO response.getPaymentQP()
}
}
);
```

NOTE:
Payment via Custom Tabs makes integration with Amazon Pay compatible. But unlike previous WebView, a default page is presented at the end of each Payment to invite the user to close the Chrome page. At this point the SDK carries out a check on the transaction code, returning the outcome of the Payment to the developer.

To use the Chrome Custom Tabs, as specified at the beginning of the documentation, you must include the library: implementation 'com.android.support:customtabs:27.1.1' within the gradle.

As for the customization you can set the color of the toolbar through the method:

xPay.FrontOffice.setToolbarColor(it.nexi.xpay.R.color.keyboard_background_color);

PAYMENT

Once the nonce is received, Payment can be made via the pagaNonce API.

Google Pay

To facilitate the integration of Google Pay by merchants, a simplified development method was made available, making the merchant application "dependent" only by XPay SDK and not by Google Pay (which is included in its indoor).

To be able to release an app that uses Google Pay on the store, you need to request a production access through the Google form (at the link: https://developers.google.com/pay/api/android/guides/test-and -deploy / deploy-your-application). While for the tests carried out in the "demo" environment some registration or certificate generation is not necessary. The "nexi" gateway is already managed and included in the SDK.

Below are the steps to integrate Google Pay via the XPay SDK:

- You need to include Google Play services, AppCompat and a line in AndroidManifest. (Following the instructions at the link:https://developers.google.com/pay/api/android/guides/setup)
- To have the XPK XPay class externally to your Activity, (the GooglePayActivity class of the XPK (it.nexi.xpay.GooglePay.GooglePayActivity).
- To begin the Payment process through Google Pay, call the "payWithGoogle" method inherited from the Activity. Below is an example of a code:

```
GooglePayRequest googleRequest = new GooglePayRequest("alias", "secret_key",
"terminalId", "EUR","IT", 1, "Merchant Name",
“CODTRANS”+System.currentTimeMillis());
//Imposto ambiente
googleRequest.setEnvironment(EnvironmentUtils.Environment.TEST);
// Imposto parametri di fatturazione
JSONObject billingParameters = new JSONObject();
try {
billingParameters.put("format", "FULL");
billingParameters.put("format", "FULL");
billingParameters.put("phoneNumberRequired", true);
} catch (JSONException e) {
e.printStackTrace();
}
googleRequest.setBillingParameters(billingParameters);
buttonGooglePay.setOnClickListener(new View.OnClickListener() {
@Override
public void onClick(View v) {
payWithGoogle(mContext, googleRequest, new GooglePayCallback() {
@Override
public void onCancel() {
Log.i("GOOGLEPAY", "CANCEL");
}
@Override
```

```
public void onSuccess(ApiGooglePayResponse response) {
Log.i("GOOGLEPAY", "OK");
}
@Override
public void onError(ApiErrorResponse error) {
Log.e("GOOGLEPAY", "ERROR" + error.getError().getMessage());
}
});
}});
```

Through the above mentioned callback it is possible to manage a flow similar to a normal Payment in WebView.

If you want to enable or disable your "Pay with Google" button, you can do so by invoking the "checkGooglePayAvailability" method, which is always present in the "GooglePayActivity" activity. Here is an example of code:

```
checkGooglePayAvailability(EnvironmentUtils.Environment.TEST, billingParameters, new
IGooglePayListener() {
@Override
public void onGooglePayAvailable(boolean isAvailable) {
Log.i("GPay", "Google Pay is: " + isAvailable
}
});
```

NOTE:

- This solution is only compatible with Chrome Custom Tabs.

Root Control

To avoid the use of rooted devices, the XPay library will not work on such devices to deal with any security issues during Payment processes. Developers are given the option to handle the returned exception if root permissions are detected on the devices.

Below is an example of integration:

```
try {
xPay = new XPay(this, SECRET_KEY);
} catch (DeviceRootedException e) {
Log.e(TAG, “Device is rooted” + e.getMessage());
}
```

Back office Deposit

This service performs a journal processing operation. Partial amounts and multiple operations may be allowed, depending on the characteristics of the terminal.

REQUEST

CLASS
ApiContabilizzaRequest

METHOD
contabilizza

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Transaction signature field	AN 40 CHAR.

RESPONSE

CLASS
ApiContabilizzaResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

Return/Refund

This service carries out a cancellation or refund depending on the status of the transaction. Partial amounts and multiple transactions may be allowed, depending on the merchant's configuration.

REQUEST

CLASS
ApiStornaRequest

METHOD
Storna

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ' " characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Transaction signature field	AN 40 CHAR.

ESPONSE

CLASS
ApiStornaResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

NOTES:
Once the order has been authorised, only a total transaction cancellation is possible.

Order List

This service carries out a cancellation or refund depending on the status of the transaction. Partial amounts and multiple transactions may be allowed, depending on the merchant's configuration.

REQUEST

CLASS
ApiReportOrdiniRequest

METHOD
reportOrdini

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
from	Filter by date from	dd/mm/yyyy
to	Filter by date to	dd/mm/yyyy
channel	Filter by Payment method used for the order, with multiple channels able to be queued. Possible values: - All - MyBank - CreditCard - PayPal	
statuses	Filter by order status, with multiple statuses able to be queued.	AN
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ' " characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.

RESPONSE

CLASS
ApiReportOrdiniResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
reports	Orders element whose structure is shown in the following table.	

Reports element

Name	Description	Format
nMerchant	Terminal assigned to the merchant by Nexi.	AN MIN 2 - MAX 30 CHAR.
transCode	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Transaction amount expressed in euro cents with no separator.	N MAX 9 CHAR.
currency	978 for Euro	
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
brand	Credit card network	AN
PaymentType	Type of Payment made.	AN
operationType	Type of operation carried out.	AN
transactionTypeExtended	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
pan	Credit card number	N MAX 19 CHAR.
parameters	Additional parameters	AN
status	Order status	AN
transactionDate	Transaction date	dd/mm/yyyy
operationDate	Operation date	dd/mm/yyyy
serviceType	Type of service used for the transaction.	AN

name	Customer name	AN MIN 2 - MAX 30 CHAR.
surname	Customer surname	AN MIN 2 - MAX 30 CHAR.
email	Customer email	AN MAX 150 CHAR.

NOTES:
This allows to query XPay in order to obtain a list of transactions, by applying different filter conditions. Amongst other things, this makes available those details needed to invoke the orderDetails API.

Possible values for statuses:

- Autorizzato
- Negato
- Annullato
- Incassato
- Rimborsato
- NonCreato
- IncParziale
- RimbParziale

Order Details Query

This service carries out a cancellation or refund depending on the status of the transaction. Partial amounts and multiple transactions may be allowed, depending on the merchant's configuration.

REQUEST

CLASS
ApiSituazioneOrdineRequest

METHOD
situazioneOrdine

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ' " characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.

RESPONSE

CLASS
ApiSituazioneOrdineResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
reports	Orders element whose structure is shown in the following table.	

Reports element

Name	Description	Format
nMerchant	Terminal assigned to the merchant by Nexi.	AN MIN 2 - MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Transaction amount expressed in euro cents with no separator.	N MAX 9 CHAR.
currency	978 for Euro	
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
brand	Credit card network	AN
PaymentType	Type of Payment made.	AN
operationType	Type of operation carried out.	AN
transactionTypeExtended	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
pan	Credit card number	N MAX 19 CHAR.
parameters	Additional parameters	AN
status	Order status	AN
transactionDate	Transaction date	dd/mm/yyyy
operationDate	Operation date	dd/mm/yyyy
serviceType	Type of service used for the transaction.	AN
name	Customer name	AN MIN 2 - MAX 30 CHAR.
surname	Customer surname	AN MIN 2 - MAX 30 CHAR.
email	Customer email	AN MAX 150 CHAR.
details	Reports element whose structure is as defined in the following table.	

Details element

Name	Description	Format
name	Customer name	AN MIN 2 - MAX 30 CHAR.
surname	Customer surname	AN MIN 2 - MAX 30 CHAR.
email	Customer email	AN MAX 150 CHAR.
unapprovedAmount	Unapproved amount	N MAX 9 CHAR.
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
status	Order status	AN
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
operations	Details element whose structure is shown in the following table.	

Operations element

Name	Description	Format
operationType	Operation type	AN
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
status	Order status	AN
creationDate	Creation date	DATE
user	Merchant operator requesting the operation.	AN

Pay-by-Link link request

The service allows you to obtain a Payment link that, for example, sent by e-mail to the customer allows him to be sent back to the XPay Payment pages and complete the transaction in safety.

REQUEST

CLASS
ApiPay-by-LinkRequest

METHOD
richiestaPay-by-Link

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 – MAX 30 CRT
amount	Amount expressed in euro cents without	N MAX 9 CRT
timeout	Number of hours the generated Payment link will remain valid.	N MAX 4 CRT
redirectUrl	Merchant URL to which the gateway directs the user to complete the transaction by passing, in GET, the response parameters with the result of the transaction	AN MAX 500

RESPONSE

CLASS
ApiPay-by-LinkResponse

Name	Description	Format
result	Request result	AN MAX 30 CRT
operationId	Transaction identifier assigned by Nexi	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CRT
Pay-by-LinkUrl	Contains the link to be used to make the Payment	AN

Security checks
Blacklist inclusion

Add blacklist of a Fiscal code or contract.

CLASS
ApiAggiungiBlackListRequest

METHOD
aggiungiBlackList

RICHIESTA

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
type	Type of search if with fiscal code (CodiceFiscale) or contract code (CodiceContratto)	AN MIN 2 MAX 30
value	Depending on the type of search, enter the tax code or the contract code	AN MIN 2 MAX 30
description	Description to be assigned to the contract	AN

Response

CLASS
ApiAggiungiBlackListRequest

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Blacklist removal

It deletes from the black list a previously loaded Fiscal code or contract.

CLASS
ApiRimuoviBlackListRequest

METHOD
rimuoviBlackList

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
type	Type of search if with fiscal code (CodiceFiscale) or contract code (CodiceContratto)	AN MIN 2 MAX 30
value	Depending on the type of search, enter the tax code or the contract code	AN MIN 2 MAX 30

RESPONSE

CLASS
ApiAggiungiBlackListRequest

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Blacklist Check

It checks the presence in black list given a contracted Fiscal code, in case it returns the detail.

REQUEST

CLASS
ApiControllaBlackListRequest

METHOD
controllaBlackList

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
type	Type of search if with fiscal code (CodiceFiscale) or contract code (CodiceContratto)	AN MIN 2 MAX 30
value	Depending on the type of search, enter the tax code or the contract code	AN MIN 2 MAX 30

RESPONSE

CLASS
ApiControllaBlackListResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
blackListElements	Arrays whose structure is defined in the following table	Array

Name	Description	Format
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
dataType		AN
listedValue		AN
description	Description to be assigned to the contract	AN
dCreation	Contract creation date	DATA

Report blacklist

Allows you to query on any blacklist associated with the terminal, returns the list of contracts / tax codes present.

CLASS
ApiReportBlackListRequest

METHOD
reportBlackList

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
type	Type of search if with fiscal code (CodiceFiscale) or contract code (CodiceContratto)	AN MIN 2 MAX 30

RESPONSE

CLASSE
ApiReportBlackListResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
blackListElements	Arrays whose structure is defined in the following table	Array
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
dataType		AN

listedValue		AN
description	Description to be assigned to the contract	AN
dCreation	Contract creation date	DATA

CF/PAN Check existance

CLASS
ApiControllaEsistenzaCFPanRequest

METHOD
controllaEsistenzaCFPan

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
taxCode	User CF (Codice fiscale)	AN MAX 16 CRT
hashPan	hashPan where you want to verify association	
group	Code assigned by Nexi during activation	AN MIN 5 MAX 30 CRT

RESPONSE

CLASS
ApiControllaEsistenzaCFPanResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
cfPans	Arrays whose structure is defined in the following table	Array
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
taxCode	User CF Codice fiscale	AN MAX 16

expire	Card expiry date	DATA aaaamm
status	Order Status	AN
hashPan	hashPan where you want to verify association	
dRegistration	Operation data	DATA

CF/PAN delate

CLASS
ApiRimuoviCFPanRequest

METHOD
rimuoviCFPan

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
taxCode	User CF (Codice fiscale)	AN MAX 16 CRT
hashPan	hashPan where you want to verify association	
group	Code assigned by Nexi during activation	AN MIN 5 MAX 30 CRT

RESPONSE

CLASSE
ApiRimuoviCFPanResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

CF/PAN association report

CLASS
ApiReportAssociazioniCFPanRequest

METHOD
reportAssociazioniCFPan

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
type	Type of search if with fiscal code (CodiceFiscale) or contract code (CodiceContratto)	AN MIN 2 MAX 30
value	Depending on the type of search, enter the tax code or the contract code	AN MIN 2 MAX 30
group	Code assigned by Nexi during activation	AN MIN 5 MAX 30

RESPONSE

CLASS
ApiReportAssociazioniCFPanResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
cfPans	Arrays whose structure is defined in the following table	Array
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30

taxCode	User CF Codice fiscale	AN MAX 16
expire	Card expiry date	DATA aaaamm
status	Order Status	AN
hashPan	hashPan where you want to verify association	
dRegistration	Operation data	DATA

Creation of a physical POS contract

The service allows you to upload a contract for recurring Payments or card on file starting from a Payment card transaction carried out on a POS.

CLASS
ApiContrattoDaPOSFisicoRequest

METHOD
creaContrattoDaPOSFisico

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
contractPOS	Object contractPOS whose structure is described in the following table	contractPOS
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30 CRT
idPhysicalPOS	Identifier of the terminal where the transaction was made	N MAX 8 CRT
authCode	Confirmation code issued by the card issuer	AN MAX 6 CRT
stan	Optional code received from the physical POS	AN MAX 6 CRT
amount	Amount expressed in euro cents without separators	N MAX 9 CRT
serviceDescription	Field in which the merchant can specify a description of the type of service offered. This field will also be reported in the text of the email sent to the cardholder. For the MyBank service, the field is sent to the bank to be included in the description of	AN MAX 2000 For MyBank: AN MAX 140 CRT and you can use only: / - : ( ) . , + For PAYPAL: AN MAX 127 CHAR

	the SCT format but is truncated to the 140th character	
email	Customer Mail	AN MAX 150 CRT
transactionDate	Transaction date	DATA gg/mm/aaaa

RESPONSE

CLASS
ApiContrattoDaPOSFisicoResponse

Name	Description	Format
Result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Cancellation of contract

The merchant enabled to manage recurring Payments, OneClickPay / Card on file can delete contract codes matched to users' cards through this service.

CLASS
ApiAggiungiBlackListRequest

METHOD
aggiungiBlackList

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30

RESPONSE

CLASS
ApiCancellaContrattoResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Enabling contract

The merchant enabled to manage recurring Payments, OneClickPay / Card on file can enable contracts previously disabled through this service.

CLASS
ApiAbilitaContrattoRequest

METHOD
abilitaContratto

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30

RESPONSE

CLASS
ApiAbilitaContrattoResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Contract disabling

The merchant enabled to manage recurring Payments, OneClickPay / Card on file can disable contracts linked to users' cards through this service. The contract in the deactivated state can be restored and only the possibility of carrying out operations is suspended.

CLASS
ApiDisabilitaContrattoRequest

METHOD
disabilitaContratto

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30

RESPONSE

CLASS
ApiDisabilitaContrattoResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT

Requesting contracts

It allows to query the contracts registered for the Recurring services, OneClickPay / Card on file, with some filter criteria.

CLASS
ApiQueryContrattiRequest

METHOD
queryContratti

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
taxCode	Description to be assigned to the contract	AN MAX 16 CRT
dRegistrationFrom	Search by date to	DATA
dRegistrationTo	Search by date from	DATA

RESPONSE

CLASS
ApiQueryContrattiResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
contracts	Arrays whose structure is defined in the following table	Array

nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
groupCode	Code assigned by Nexi during activation	AN MIN 5 MAX 30

Contract detail

It allows to promptly query a registered contract for Recurring services, OneClickPay / Card on file, and obtain detailed information.

CLASS
ApiDettagliContrattiRequest

METHOD
dettaglioContratto

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
taxCode	User CF	AN MAX 16 CRT
dRegistrationFrom	Search by date to	DATA
dRegistrationTo	Search by date from	DATA

REPSPONSE

CLASSE
ApiDettagliContrattiResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
contractDetails	Arrays whose structure is defined in the following table	Array

nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
groupCode	groupCode	AN MIN 5 MAX 30
dActivation	Contract attivation date	AN
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 In case of MyBank you can only use: / - : ( ) . , +
taxCode	User CF	AN MAX 16
hashPan	hashPan to be verified for association.	AN
cardType	Card type	AN
statusFirstPayment	First Payment status	AN

Hosted Payments

The merchant carries out its own data collection page, without limitations from the point of view of the user experience. The page must contain a form with the fields necessary for the transaction. The type of PCI certification questionnaire required is SAQ A-EP.

CLASS
ApiCreaNonceRequest

METHOD
creaNonce

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
card	Object whose structure is defined in the following table	card
amount	Amount expressed in euro cents without separators	N MAX 9
currency	978 per Euro	AN MAX 3
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 In case of MyBank you can only use: / - : ( ) . , +
pan	Credit card pan	N MIN 16 MAX 19
month	Credit card expiration month	N MAX 2
year	Credit card expiration year	N MAX 4

cvc	CVV2 / CVC2 code consisting of 3 numbers on the back of the VISA, MASTERCARD, MAESTRO, DINERS and JCB credit cards. 4DBC composed of 4 numbers on the front of the AMERICAN EXPRESS cards. The obligation depends on the rules set by the individual acquirers.	N

RESPONSE

CLASS
ApiCreaNonceResponse

Name	Description	Format
result	Request result	AN ok/ko
operationId	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

NOTE:
The actual Payment must be done on the merchant Back End, in Server to Server mode, using the XpayNonce returned by creaNonce. If a 3D Secure alias is passed, a WebView will open to complete the procedure, after which the ApiCreaNonceResponse response will be returned.

Synchronous Payments

Payments with External 3D Secure MPI

This service carries out server-to-server 3D Secure e-commerce transactions. It is designed for merchants who have their own MPI (Merchant Plug In) for handling the cardholder authentication stage using 3D Secure protocols. XPay is therefore used to forward the authorisation requests, and to transfer the data previously obtained in the 3D Secure process.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiPagaMPIRequest

METHOD
pagaMPI

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.

currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.

RESPONSE

CLASS
ApiPagaMPIResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
codTrans	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 6 CHAR.
currency	978 for Euro	N 3 CHAR.
date	Transaction date	DATE dd/mm/yyyy
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.
eci	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
xid	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.
cavv	3D Secure data. See table	AN MIN 2 - MAX 30 CHAR.

Server-to-server SSL E-commerce Payments

This service carries out server-to-server SSL e-commerce Payment transactions. It is designed for merchants who wish to integrate with their own APP the function to request credit card Payment authorisations without using 3D Secure, where details are collected directly from the form of the merchant's site/APP.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiPagaSSLRequest

METHOD
pagaSSL

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ' " characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.

RESPONSE

CLASS
ApiPagaSSLResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN MIN 2 - MAX 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
region	Credit card global region of origin	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.

M.O.T.O Payments

This service performs a Payment transaction M.O.T.O. Server to Server is intended for those wishing to integrate on their system the function of request authorization of Payments by credit card, whose data have been communicated by the cardholder to the merchant by mail, telephone, etc. provides that the operator manages, through his own management system, both the request for credit card data and the communication of the result of the Payment.

CLASS
ApiPagaMOTORequest

METHOD
pagaMOTO

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 Except the “#” character. In case of MyBank you can only use: / - : ( ) . , +
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	AN

amount	Amount to be authorised, expressed in euro cents with no separator.	N MAX 9
currency	978 per Euro	AN MAX 3
email	Customer Mail	AN MAX 150
name	Customer name	AN MIN 2 MAX 30
surname	Customer surname	AN MIN 2 MAX 30
pan	Credit card pan	N MIN 16 MAX 19
month	Credit card expiration month	N 2 MAX
year	Credit card expiration year	N MAX 4
cvc	CVV2 / CVC2 code consisting of 3 numbers on the back of the VISA, MASTERCARD, MAESTRO, DINERS and JCB credit cards. 4DBC composed of 4 numbers on the front of the AMERICAN EXPRESS cards. The obligation depends on the rules set by the individual acquirers.	N

RESPONSE

CLASS
ApiPagaMOTOResponse

Name	Description	Format
result	Result of the request.	AN ok/ko
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
authCode	Confirmation code issued by the card issuer.	AN MAX 6
convCode	Confirmation code issued by the card issuer	AN MIN 2 MAX 30
date	Transaction date	DATA gg/mm/aaaa
time	Transaction time	AN hh:mm:ss

country	Credit Card nation	AN MIN 2 MAX 30
region	Macro region credit card origin	AN MIN 2 MAX 30
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100
productType	Credit card type	AN MIN 2 MAX 30
transactionType	Indicates the manner in which the Payment occurred. The possible values are indicated in the Transaction type encoding table	AN MIN 2 MAX 30

Subsequential First Payment

The integration of Recurring, OneClickPay or Card On File services allows the end customer to store their credit card data on Nexi systems, and use them later to make purchases with just one click or sending by the merchant occurrences (for example for subscription services or billing). At the technical level, the management of these services is divided mainly into 2 phases:

1. Activation and / or first Payment

A first transaction must be generated, assigning a contract code that allows Nexi to save the combination between the user and the used Payment card, for subsequent purchases. This first transaction can be a real Payment, or just a verification of the card without charging the user.
For first Payment, the sequence of services to be used is as follows:
3D Secure:

- creaNoncePrimoPayment3DS - to manage 3D Secure authentication
- primoPayment3DS - to manage Payment and contract registration

No 3D Secure:

- primoPaymentSSL - to manage Payment and contract registration

In the recording-only situation with card verification, the sequence of APIs to be used is as follows:

3D Secure:

- creaNonceVerificaCarta - to manage 3D Secure authentication
- verificaCarta3DS - To manage the validity verification of the card and register the contract

No 3D Secure:

- verifcaCartaSSL - To manage the validity verification of the card and register the contract

2. Management of subsequent Payments
The management of subsequent Payments between OneClick Payments and recurring at a technical level is similar. The merchant application / website must follow the Recurrences section.

Recurring SSL Card Verification

This service carries out a verification of card authorisation without server-to-server 3D Secure to register the contract for use in subsequent recurring or Card on File/OneClickPay Payments.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiVerificaCartaSSLRequest

METHOD
verificaCartaSSL

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	
nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
groupCode	Code assigned by Nexi during activation.	AN MIN 2 - MAX 30 CHAR.
contractExpires	For recurring Payments, indicates when the expiry date for the option contract occurs.	DATE dd/mm/yyyy

Optional parameters

Name	Description	Format
email	Customer email	AN MAX 150 CHAR.
description	Description assigned to the contract.	AN
TaxCode	User Tax Code	AN 16 CHAR.

RESPONSE

CLASS
ApiVerificaCartaSSLResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

Recurring SSL First Payment

This service carries out a server-to-server SSL e-commerce Payment transaction at the same time as the contract is registered for use in subsequent recurring or Card on File/OneClickPay Payments.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiPrimoPaymentSSLRequest

METHOD
primoPaymentSSL

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
groupCode	Code assigned by Nexi during activation.	AN MIN 2 - MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards.	

	For AMEX cards only, it is a four-digit code and is found on the front of cards.	
contractExpires	For recurring Payments, indicates when the expiry date for the option contract occurs.	DATE dd/mm/yyyy

Optional parameters

Name	Description	Format
email	Customer email	AN MAX 150 CHAR.
description	Description assigned to the contract.	AN
TaxCode	User Tax Code	AN 16 CHAR.

RESPONSE

CLASS
ApiPrimoPaymentSSLResponse

Required Parameters

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN MIN 2 - MAX 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
region	Credit card global region of origin	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first Payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.

3D Secure Card Verification

Use of this service occurs in 2 stages. In the first step, card details are sent and the SDK takes care of managing the 3D Secure and returning the xpayNonce. With the XpayNonce received in response, the APP proceeds to recall the second 3DS card verification service.

This service requires the merchant to achieve PCI DSS certification.

Create xpayNonce

REQUEST

CLASS
ApiCreaNonceVerificaCartaRequest

METHOD
creaNonceVerificaCarta

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ

RESPONSE

CLASS
ApiCreaNonceVerificaCartaResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.

NOTES:
This allows a xpayNonce to be created for use in calling a verificaCarta3DS.
If the card needs to be authenticated using 3D Secure, a WebView will open in order to complete the procedure. The response ApiCreaNonceVerificaCartaResponse will be returned after this has been completed.

Verification of card authorisation

REQUEST

CLASS
ApiVerificaCarta3DSRequest

METHOD
verificaCarta3DS

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.
nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
groupCode	Code assigned by Nexi during activation.	AN MIN 2 - MAX 30 CHAR.
contractExpires	For recurring Payments, indicates when the expiry date for the option contract occurs.	DATE dd/mm/yyyy

Optional parameters

Name	Description	Format
email	Customer email	AN MAX 150 CHAR.
description	Description assigned to the contract.	AN
taxCode	User Tax Code	AN 16 CHAR.

RESPONSE

CLASS
ApiVerificaCarta3DSResponse

Name	Description	Format
result	Result of the request.	AN OK / KO
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

NOTES:

- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

Recurring 3D Secure First Payment

This service carries out a 3D Secure Payment transaction at the same time as the contract is registered for use in subsequent recurring or OneClickPay/Card on File Payments. Use of this service occurs in 2 stages. In the first step, card details are sent and the SDK takes care of managing the 3D Secure and returning the xpayNonce. With the XpayNonce received in response, the APP proceeds to recall the second Payment service.

This service requires the merchant to achieve PCI DSS certification.

Create xpayNonce

REQUEST

CLASS
ApiCreaNoncePrimoPayment3DSRequest

METHOD
creaNoncePrimoPayment3DS

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
card	Element containing Payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.

RESPONSE

CLASS
ApiCreaNoncePrimoPayment3DSResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.

NOTES:
This allows a xpayNonce to be created for use in calling the firstPayment3DS service.
If the card needs to be authenticated using 3D Secure, a WebView will open in order to complete the procedure. The response ApiCreaNoncePrimoPayment3DSResponse will be returned after this has been completed.

Payment and contract registration

REQUEST

CLASS
ApiPrimoPayment3DSRequest

METHOD
primoPayment3DS

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.

nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
groupCode	Code assigned by Nexi during activation.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
contractExpires	For recurring Payments, indicates when the expiry date for the option contract occurs.	DATE dd/mm/yyyy

Optional parameters

Name	Description	Format
email	Customer email	AN MAX 150 CHAR.
description	Description assigned to the contract.	AN
TaxCode	User Tax Code	AN 16 CHAR.

RESPONSE

CLASS
ApiPrimoPayment3DSResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN MIN 2 - MAX 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
region	Credit card global region of origin	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first Payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

M.O.T.O. First Payment

Make a Payment transaction M.O.T.O. Server to Server simultaneously records the contract for use in subsequent Payments.

CLASS
ApiPrimoPaymentMOTORequest

METHOD
primoPaymentMOTO

REQUEST

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
groupCode	Code assigned by Nexi during activation.	AN MIN 5 MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
amount	Amount expressed in euro cents with no separators.	N MAX 9
currency	978 per Euro	AN MAX 3
card	Object whose structure is defined in the following table	card

contractExpires	Indicates for recurring when it is the end date of the optional contract	DATA gg/mm/aaaa
email	Customer Mail	AN MAX 150
description	Description to be assigned to the contract	AN
taxCode	User CF	AN MAX 16
pan	Credit card number	N MIN 16 MAX 19
month	Credit card expiry month	N MAX 2
year	Credit card expiry year	N MAX 4
cvc	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	N

RESPONSE

CLASS
ApiPrimoPaymentMOTOResponse

Name	Description	Format
result	Result of the request.	AN ok/ko
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 16
timeStamp	Timestamp in millisecond format.	N 13 CRT
authCode	Confirmation code issued by the card issuer.	AN MAX 6
convCode	Merchant code assigned by the acquirer.	AN MIN 2 MAX 30
date	Transaction date	DATA gg/mm/aaa
time	Transaction time	AN hh:mm:ss
country	Credit card country	AN MIN 2 MAX 30

region	Credit card global region of origin	AN MIN 2 MAX 30
brand	Type of card used by the user to make Payment. The possible values are shown in the table here	AN MAX 100
productType	Credit card type	AN MIN 2 MAX 30
transactionType	Indicates the manner in which the Payment occurred. The possible values are indicated in the Transaction type encoding table	AN MIN 2 MAX 30

NOTES:

- In the first Payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization. Diners do not allow the use of this amount, if you have an agreement with this circuit, you will need to make a first Payment of 1 cent which Nexi will recognize as a card verification operation with tokenization and the amount will not be charged.

Recurring/OneClick

Subsequent Payment

When you need to make a charge on a previously registered contract, your system must send a call which contains the details of the previously registered contract, integrated with the recording of the first Payment.

REQUEST

CLASS
ApiPaymentRicorrenteRequest

METHOD
PaymentRicorrente

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
nContract	Code allowing to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
month	Credit card expiry month	mm
year	Credit card expiry year	yyyy
groupCode	Code assigned by Nexi during activation.	AN MIN 2 - MAX 30 CHAR.

RESPONSE

CLASS
ApiPaymentRicorrenteResponse

Required Parameters

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN MIN 2 - MAX 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
region	Credit card global region of origin	AN MIN 2 - MAX 30 CHAR.
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.

NOTES:

- Transactions executed through recurring Payments cannot be partially accounted for.

M.O.T.O. subsequent Payment

Every time the registered user makes a subsequent purchase, the e-commerce must send a call to Nexi with the data of the contract registered in the first Payment stage.

REQUEST

CLASS
ApiPaymentRicorrenteMOTORequest

METHOD
PaymentRicorrenteMOTO

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30
amount	Amount expressed in euro cents without separators	N MAX 9
currency	978 per Euro	AN MAX 3
month	Credit card expiry month	N MAX 2
year	Credit card expiry year	N MAX 4

RESPONSE

CLASS
ApiPaymentRicorrenteMOTOResponse

Name	Description	Format
result	Result of the request.	AN ok / ko
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
authCode	Confirmation code issued by the card issuer.	AN MAX 6
convCode	Merchant code assigned by the acquirer.	AN MIN 2 MAX 30
date	Transaction date	DATA gg/mm/aaaa
time	Transaction time	AN hh:mm:ss
country	Credit card country	AN MIN 2 MAX 30
region	Credit card global region of origin	AN MIN 2 MAX 30
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100
productType	Credit card type	AN MIN 2 MAX 30
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 MAX 30

NOTES:

- Transactions executed through recurring Payments cannot be partially accounted for.

3D Secure Subsequent Payment

When you need to charge a previously registered contract, your system have to send a call with the data of the contract previously registered with the first Payment. This type of call will require the inclusion of the 3D Secure code also on recurring Payments.

Generate xpayNonce

REQUEST

CLASSE
ApiCreaNoncePaymentRicorrente3DSRequest

METHODO
creaNoncePaymentRicorrente3DS

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
nContract	Code that allows to save the pairing between the user and the used Payment card	AN MIN 5 MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 MAX 30 Except the “#” character. In case of MyBank you can only use: / - : ( ) . , +
amount	Amount expressed in euro cents without separators	N MAX 9
currency	978 per Euro	AN MAX 3
month	Credit card expiry month	N MAX 2
year	Credit card expiry year	N MAX 4

groupCode	Code assigned by Nexi during activation	AN MIN 5 MAX 30

RESPONSE

CLASS
ApiCreaNoncePaymentRicorrente3DSResponse

Name	Description	Format
result	Result of the request.	AN ok / ko
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

Payment

REQUEST

CLASSE
ApiPaymentRicorrente3DSRequest

METHODO
PaymentRicorrente3DS

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may	AN MIN 2 MAX 30 Except the “#” character. In case of MyBank you can only use: / - : ( ) . , +

	choose to decrease this to less than 3 attempts.	
amount	Amount expressed in euro cents without separators	N MAX 9
currency	978 per Euro	AN MAX 3
xpayNonce	Code assigned by XPay to be used for the Payment request	AN MAX 36

RESPONSE

CLASSE
ApiPaymentRicorrente3DSResponse

Name	Description	Format
result	Result of the request.	AN ok / ko
operationId	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
authCode	Confirmation code issued by the card issuer.	AN MAX 6
convCode	Merchant code assigned by the acquirer.	AN MIN 2 MAX 30
date	Transaction date	DATA gg/mm/aaaa
time	Transaction time	AN hh:mm:ss
country	Credit card country	AN MIN 2 MAX 30
region	Credit card global region of origin	AN MIN 2 MAX 30
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100
productType	Credit card type	AN MIN 2 MAX 30
transactionType	Indicates the Payment method. See the table here for possible values.	AN MIN 2 MAX 30

NOTES:

- Transactions executed through recurring Payments cannot be partially accounted for.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.

Varie

DCC Verification Service

Currency Choice is a service born from the collaboration between Nexi and Global Blue. It allows international Visa and MasterCard credit card holders to make purchases in their own currency, with an exchange rate guaranteed at the time of Payment.

The Currency Choice service is currently available in the currencies that can be found here.
This service allows to verify whether the currency of the Payment card used is one of the 38 available. If it is, the service will provide the exchange rate to the user, who may choose to either accept the offered rate and proceed with own currency, or remain in euro.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiVerificaDCCRequest

METHOD
verificaDCC

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
pan	Credit card number	N MAX 19 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.

RESPONSE

CLASS
ApiVerificaDCCResponse

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
ticket	Exchange rate request identifier provided by Global Blue.	AN 25 CHAR.
DCCcurrency	Code of the currency in which the dccAmount is expressed (e.g. 840=USD).	AN 3 CHAR.

	Only present for the DCC service. For allowed values, see the table here.	
DCCamount	Shows the value of the amount converted into the currency chosen by the payer for the transaction. The currency used is shown in the dccCurrency field. Blank space characters are added on the left until 20 characters are reached.	AN 20 CHAR.
DCCdecimalAmount	Shows the value of the amount converted into the currency chosen by the payer for the transaction. The currency used is shown in the dccCurrency field. Blank space characters are added on the left until 20 characters are reached.	AN 20 CHAR.
exchangeRate	Exchange rate	N
MarkUp	Indicates the mark-up provided by Global Blue.	N 8.4
decimalMarkUp	Indicates how many decimal places are in the MarkUp field.	N MAX 2 CHAR.

DCC Service - Payment

This service makes a Payment in a currency other than Euro if the cardholder has accepted the proposed exchange rate through the DCCVerification service.

This service requires the merchant to achieve PCI DSS certification.

REQUEST

CLASS
ApiPagaDCCRequest

METHOD
pagaDCC

Required Parameters

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
ticket	Exchange rate request identifier provided by Global Blue.	AN 25 CHAR.
amount	Amount expressed in euro cents with no separators.	N MAX 9 CHAR.
currency	978 for Euro	N 3 CHAR.
DCCcurrency	Code of the currency in which the dccAmount is expressed (e.g. 840=USD). Only present for the DCC service. For allowed values, see the table here.	AN 3 CHAR.
DCCamount	Shows the value of the amount converted into the currency chosen by the payer for the transaction. The currency used is shown in the dccCurrency field. Blank space characters are added on the left until 20 characters are reached.	AN 20 CHAR.
exchangeRateAccepted	Exchange rate accepted.	N

xpayNonce	Code assigned by XPay for use in the Payment request.	AN 36 CHAR.

Optional parameters

Name	Description	Format
pan	Credit card number	N MAX 19 CHAR.
month	Credit card expiry month	mm
year	Credit card expiry year	yyyy
cvc	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. 4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	N MAX 4 CHAR.

RESPONSE

CLASS
ApiPagaDCCResponse

Required Parameters

Name	Description	Format
result	Result of the request.	AN MAX 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN MIN 2 - MAX 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN MIN 2 - MAX 30 CHAR.
region	Credit card global region of origin	AN MIN 2 - MAX 30 CHAR.
brand	Credit card network	AN
productType	Credit card type	AN MIN 2 - MAX 30 CHAR.

3D SECURE 2.2

The new 3D Secure 2.2 protocol adopted by the main international circuits (Visa, MasterCard, American Express), introduces new authentication methods, able to improve and speed up the cardholder's purchase experience.

In particular, the new protocol allows an exchange of more information between the merchant and the card issuer, in order to allow a better assessment of the risk of the transaction, simplifying the Customer's purchase experience and improving the conversion rate at check out.

In many cases the information retrieved from the purchaser's device and the additional information passed by the merchant will be sufficient to authenticate the card holder transparently, without further interaction. In some cases, instead, for transactions that present higher risks, active authentication of the Customer will be required.

The structure of the "informazioniSicurezza" JSON object required for 3D Secure 2.2 service is described below:

Mandatory	Name	Description	Format
	transType	01 = Goods/Service Purchase 03 = Check Acceptance 10 = Account Funding 11 = Quasi-Cash Transaction 28 = Prepaid Activation and Load	AN
	buyer	Object whose structure is shown in the tables below. Contains information about the buyer.	JSON
	destinationAddress	Object whose structure is shown in the tables below. Contains information about the buyer.	JSON
	billingAddress	Object whose structure is shown in the tables below. Contains information about the buyer.	JSON
	cardHolderAcctInfo	Object whose structure is shown in the tables below. Contains information about the buyer.	JSON
	merchantRiskIndicator	Object whose structure is shown in the tables below. Contains information about the buyer.	JSON

Buyer information, "buyer" element

Mandatory	Name	Description	Format
✓	email	Buyer Mail	AN MIN 1 MAX 254
	msisdn	Mobile number. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	homePhone	Home Phone. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$

	workPhone	Work Phone. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	account	Cardholder’s ID Account	AN MAX 64

Shipping address, "destinationAddress" element

Mandatory	Name	Description	Format
✓	city	City	AN MIN 1 MAX 40
✓	countryCode	Country code (ISO3166-1 alpha-3)	AN 3 CHA
✓	street	Street	AN MIN 1 MAX 50
	street2	Address first detail	AN MAX 50
	street3	Address second detail	AN MAX 50
✓	postalCode	Postal Code	AN MIN 1 MAX 8
✓	stateCode	Province abbreviation	AN MIN 1 MAX 2

Billing address, "billingAddress" element

Mandatory	Name	Description	Format
✓	city	City	AN MIN 1 MAX 40
✓	countryCode	Country code (ISO3166-1 alpha-3)	AN 3 CHA
✓	street	Street	AN MIN 1 MAX 50
	street2	Address first detail	AN MAX 50
	street3	Address second detail	AN MAX 50

✓	postalCode	Postal Code	AN MIN 1 MAX 8
✓	stateCode	Province abbreviation	AN 2 CHA

Cardholder account information, "cardHolderAcctInfo" element

Mandatory	Name	Description	Format
	chAccDate	Account activation date on the merchant's site	yyyy-mm-dd
	chAccAgeIndicator	Account seniority indicator on the merchant's site: 01 = No account 02 = created during this transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	N
	chAccChangeDate	Date of last change of the account on merchant DB	yyyy-mm-dd
	chAccChangeIndicator	Time elaps from the last change of the cardholder's account information on the merchant's site, including the billing or shipping address, new Payment account, new user, etc ...: 01 = created during this transaction 02 = Created in the last 30 days 03 = Created between 30 and 60 days ago 04 = Created before 60 days ago	N
	chAccPwChangeDate	Date of last change of account password	yyyy-mm-dd
	chAccPwChangeIndicator	Time elapsed since the cardholder's account performed a password change or account recovery: 01 = No account 02 = created during this	N

		transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	
	nbPurchaseAccount	Number of purchases of this account in the last 6 months	N MIN 1 MAX 4 CRT
	destinationAddressUsageDate	Date of last use of this delivery address	yyyy-mm-dd
	destinationAddressUsageIndicator	Indicates when the shipping address used for this transaction was used for the first time: 01 = created during this transaction 02 = Created in the last 30 days 03 = Created between 30 and 60 days ago 04 = Created before 60 days ago	N
	destinationNameIndicator	Indicates if the account name matches the name indicated for the shipment: 01 = Account name identical to the shipping address name. 02 = different account name from the shipping address name.	N
	txnActivityDay	Number of transactions (concluded and abandoned) for this account in the previous 24 hours.	N MIN 1 MAX 3 CRT
	txnActivityYear	Number of transactions (concluded and abandoned) for this account in the previous 12 months.	N MIN 1 MAX 3 CRT
	provisionAttemptsDay	Number of card tokenization attempts in the last 24 hours	N MIN 1 MAX 3 CRT
	suspiciousAccActivity	Indicator for suspicious activity: 01 = No suspicious activity verified. 02 = Suspicious activity detected.	N

	PaymentAccAgeDate	Activation date of the Payment account	yyyy-mm-dd
	PaymentAccIndicator	Indicates when the card holder has entered the Payment account on the merchant's site: 01 = No account 02 = created during this transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	N

Merchant reliability indicator, "merchantRiskIndicator" element

Mandatory	Name	Description	Format
	deliveryEmail	Delivery email address for intangible purchases	AN MAX 254 CHA
	deliveryTimeframe	Indicator on the delivery period of the goods: 01 = Immediate Delivery (Electronic Delivery). 02 = Same day delivery. 03 = Night delivery. 04 = Delivery in two or more days.	N
	giftCardAmount	Object that contains: value: Value of the gift or prepaid card used for the transaction currency: Currency code of the gift or prepaid card used for the transaction (ISO 4217) If you use the object, both parameters are mandatory.	JSON
	giftCardCount	Number of gift or prepaid cards used. If this field is sent in the request, the 'giftCardAmount' object must also be set.	N 2 CHAR

	preOrderDate	In the case of reservation, the date on which the goods will be available	yyyy-mm-dd
	preOrderPurchaseIndicator	Indicator on the availability of the goods: 01 = Goods available. 02 = Future availability.	N
	reorderItemsIndicator	Indicates if the customer is ordering goods already purchased previously: 01 = First order. 02 = Goods already purchased previously.	N
	shipIndicator	Indicator on the type of delivery: 01 = Shipping to the billing address. 02 = Shipping to another address verified by the merchant. 03 = Delivery to a different address than the billing. 04 = Shipment or collection to the store (the address of the store must be indicated in the "destinationAddress" object). 05 = Digital goods, including online services, electronic gift certificates, recovery codes. 06 = Travel and event tickets (not sent). 07 = Other: for example games, digital services not sent, electronic media subscriptions.	N

NOTES:

- In the event of errors in the parameters sent (format, lack of mandatory fields), the "warning" object will be received with the "esito_informazioniSicurezza" parameter set to "Y". For more information about any warnings returned, use the appropriate API Warning or consult the detail of the order in the XPay back office.

3D Secure 2.2 management through redirection

The following are the parameters necessary for the 3D Secure 2.2 service to function:.

ATTENTION: the parameters are divided into 5 groups, when a parameter is used, the parameters indicated as mandatory in the group must also be sent.

Buyer Information

Mandatory	Name	Description	Format
✓	Buyer_email	Cardholder’s email	AN MIN 1 MAX 256
	Buyer_homePhone	Buyer’s home phone. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	Buyer_workPhone	Buyer’s work phone. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	Buyer_msisdn	Mobile phone. The prefix is required (e.g. "+39").	^(\\+)([0-9]{10,15})$
	Buyer_account	Buyer account on merchant site	AN MAX 64

Shipping address information

Mandatory	Name	Description	Format
✓	Dest_city	City of destination of the shipment	AN MIN 1 MAX 40
✓	Dest_country	Country code (ISO3166-1 alpha-3)	AN 3
✓	Dest_street	Delivery address	AN MIN 1 MAX 50
	Dest_street2	Second line delivery address	AN MAX 50
	Dest_street3	Third line delivery address	AN MAX 50
✓	Dest_cap	Postal code	AN MIN 1 MAX 8
✓	Dest_state	Province code	AN MIN 1 MAX 2

Billing address information

Mandatory	Name	Description	Format
✓	Bill_city	Billing city	AN MIN 1 MAX 40
✓	Bill_country	Country code (ISO3166-1 alpha-3)	AN 3
✓	Bill_street	Billing Address	AN MIN 1 MAX 50
	Bill_street2	Third billing address row	AN MAX 50
	Bill_street3	Second billing address row	AN MAX 50
✓	Bill_cap	Postal code	AN MIN 1 MAX 8
✓	Bill_state	Province code	AN MIN 1 MAX 2

Buyer account information

Mandatory	Name	Description	Format
	chAccDate	Account activation date on the merchant's site	yyyy-mm-dd
	chAccAgeIndicator	Account seniority indicator on the merchant's site: 01 = No account 02 = created during this transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	N
	chAccChangeDate	Date of last change of the account on merchant DB	yyyy-mm-dd
	chAccChangeIndicator	Time elaps from the last change of the cardholder's account information on the merchant's site, including the billing or shipping address, new Payment account, new user, etc ...: 01 = created during this transaction	N

		02 = Created in the last 30 days 03 = Created between 30 and 60 days ago 04 = Created before 60 days ago	
	chAccPwChangeDate	Date of last change of account password	yyyy-mm-dd
	chAccPwChangeIndicator	Time elapsed since the cardholder's account performed a password change or account recovery: 01 = No account 02 = created during this transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	N
	nbPurchaseAccount	Number of purchases of this account in the last 6 months	N
	destinationAddressUsageDate	Date of last use of this delivery address	yyyy-mm-dd
	destinationAddressUsageIndicator	Indicates when the shipping address used for this transaction was used for the first time: 01 = created during this transaction 02 = Created in the last 30 days 03 = Created between 30 and 60 days ago 04 = Created before 60 days ago	N
	destinationNameIndicator	Indicates if the account name matches the name indicated for the shipment: 01 = Account name identical to the shipping address name. 02 = different account name from the shipping address name.	N
	txnActivityDay	Number of transactions (concluded and abandoned) for this account in the previous 24 hours.	N

	txnActivityYear	Number of transactions (concluded and abandoned) for this account in the previous 12 months.	N
	provisionAttemptsDay	Number of card tokenization attempts in the last 24 hours	N
	suspiciousAccActivity	Indicator for suspicious activity: 01 = No suspicious activity verified. 02 = Suspicious activity detected.	N
	PaymentAccAgeDate	Activation date of the Payment account	yyyy-mm-dd
	PaymentAccIndicator	Indicates when the card holder has entered the Payment account on the merchant's site: 01 = No account 02 = created during this transaction 03 = Created in the last 30 days 04 = Created between 30 and 60 days ago 05 = Created before 60 days ago	N

Information concerning the reliability of the merchant:

Mandatory	Name	Description	Format
	deliveryEmail	Delivery email address for intangible purchases	AN
	deliveryTimeframe	Indicator on the delivery period of the goods: 01 = Immediate Delivery (Electronic Delivery). 02 = Same day delivery. 03 = Night delivery. 04 = Delivery in two or more days.	N
	gca_value	Value of the gift or prepaid card used for the transaction. The amount must be expressed in cents. If you use this parameter, the "gca_curr" field must also be sent in the request.	N

	gca_curr	Currency code of the gift or prepaid card used for the transaction (ISO 4217). If this parameter is used, the "gca_value" field must also be sent.	N
	giftCardCount	Number of gift or prepaid cards used	N
	preOrderDate	In the case of reservation, the date on which the goods will be available	yyyymmdd
	preOrderPurchaseIndicator	Indicator on the availability of the goods: 01 = Goods available. 02 = Future availability.	N
	reorderItemsIndicator	Indicates if the customer is ordering goods already purchased previously: 01 = First order. 02 = Goods already purchased previously.	N
	shipIndicator	Indicator on the type of delivery: 01 = Shipping to the billing address. 02 = Shipping to another address verified by the merchant. 03 = Delivery to a different address than the billing. 04 = Shipment or collection to the store (the address of the store must be indicated in the "destinationAddress" object). 05 = Digital goods, including online services, electronic gift certificates, recovery codes. 06 = Travel and event tickets (not sent). 07 = Other: for example games, digital services not sent, electronic media subscriptions.	N

NOTES:

- In the event of errors in the parameters sent (format, lack of mandatory fields), the "warning" object will be received with the "esito_informazioniSicurezza" parameter set to "Y". For more information about any warnings returned, use the appropriate API Warning or consult the detail of the order in the XPay back office.

BACK OFFICE API

Nexi XPay makes a back office environment available for merchants to use in managing the transactions received. Merchants who have their own management system can benefit from typically post-sale features (operational and reporting), by using API integration.

IN PRACTICE

The services can be used regardless of the way in which the Payment request is forwarded by the merchant.

The services displayed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and responses are formatted JSON objects.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice**

The environment endpoints are as follows:

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it

The individual URIs and messages for each of the available services are described below.

NB Merchants can also access the back office via the web, simply by entering their credentials.

Deposit

This service performs a journal processing operation. Partial amounts and multiple operations may be allowed, depending on the characteristics of the terminal.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/incasso**

URI
ecomm/api/bo/contabilizza

METHOD
Post

ACCEPT
application/json

Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN MAX 3 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fields

Name	Description	Format
idContabParzialePayPal	The field is present only when a PayPal transaction with Payment order Order and Authorization is being processed	
infoAPM	The infoAPM field is present only for accounting operations carried out with the apm.	Object

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- divisa
- importo
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey<val>codiceTransazione=<val>divisa=<val>importo=<val>timeStamp=<val>SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio -> error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Reversal/Refund

This service carries out a cancellation or refund depending on the status of the transaction. Partial amounts and multiple transactions may be allowed, depending on the merchant's configuration.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/api-back office/storno-rimborso

URI
ecomm/api/bo/storna

METHOD
Post

ACCEPT
application/json

Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN MAX 3 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Initiation Message: optional fields

Name	Description	Format
idContabParzialePayPal	This field is the partial accounting ID provided by paypal when the accounting is carried out. The field is mandatory only in the event that a partial paypal booking is being reversed. In all other cases (non-paypal orders, reversals of paypal total accounting) the field can be omitted (for merchants not enabled for paypal) or left blank.	

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- divisa
- importo
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>divisa=<val>importo=<val>timeStamp=<val>SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Result Message: optional fields

Name	Description	Format
infoAPM	The infoAPM field is present only for accounting operations carried out with the apm.	Object

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
The type of reversal depends on the processing status of the order:

- If it has been authorised-> Online Reversal only for the total amount authorized (cancellation with card availability updated)
- If it has not yet been processed -> Accounting Reversal (cancellation of deposit request with card availability updated)
- If it has already been processed -> Refund (previously collected sum is credited back to the cardholder)

The idContabParzialePayPal field is the id for the partial processing provided by PayPal when an order is processed. This field is only mandatory if you are reversing a PayPal partial processing. In all other cases (non-PayPal orders, reversal of fully processed PayPal transactions), the field may be omitted (for merchants who have not enabled PayPal) or left blank.

Order Details Query

This service returns the details of an order and all associated operations.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/api-back office/interrogazione-dettaglio-ordine

URI
ecomm/api/bo/situazioneOrdine

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>timeStamp=<val><SecretKey>)

Result Message: required fields

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
scadenza	Card expiry date	DATA aaaamm
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
report	Contains one or more objects whose structure is shown in the following table.	AN

Report element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MIN 2 - MAX 30 CHAR.
codiceTransazione	Identifier of the transaction to be cancelled or refunded.	AN MIN 2 - MAX 30 CHAR.
importo	Transaction amount expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	EUR (Euro)	N 3 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN 6 CHAR.
brand	Credit card network	AN
TipoPayment	Method by which the Payment was made, if the e-commerce used 3D Secure, SSL, or MOTO	AN
tipoTransazione	Indicates the transaction type. See the table here for possible values.	AN MIN 2 - MAX 30 CHAR.
nazione	Credit card country	AN MIN 2 - MAX 30 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MIN 2 - MAX 200 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
parametri	Additional parameters	AN
stato	Order status	AN
dataTransazione	Transaction date	yyyy/mm/dd

		hh:mm:ss
mail	Customer email	AN MAX 150 CHAR.
dettaglio	Contains an object whose structure is shown in the following table.	AN

Details element

Name	Description	Format
nome	Customer name	AN MIN 2 - MAX 30 CHAR.
cognome	Customer surname	AN MIN 2 - MAX 30 CHAR.
mail	Customer email	AN MAX 150 CHAR.
importo	Transaction amount expressed in euro cents with no separator.	N MAX 8 CHAR.
importoRifiutato	Refused amount expressed in euro cents without separator, the first 2 numbers on the right represent the euro cents, e.g.: 5000 corresponds to 50.00 €.	N
divisa	978 for Euro	N 3 CHAR.
stato	Order status	AN
codiceTransazione	Identifier of the transaction to be cancelled or refunded.	AN MIN 2 - MAX 30 CHAR.
parametriAggiuntivi	Additional parameters sent in the request phase	N
controvaloreValuta	Amount expressed in euro cents without separator, the first 2 numbers on the right represent the euro cents, e.g.: 5000 corresponds to 50.00 € . It corresponds to the amount in the currency chosen on the cash page.	N
decimaliValuta	Number of decimals of the currency chosen by the customer (e.g. for USD "2" is returned).	N
tassoCambio	Exchange rate applied	N
codiceValuta	Currency code. E.g. 840 = USD	N
flagValuta	Indicates whether the customer has chosen to make the Payment in the proposed currency.	N
operazioni	Contains one or more objects whose structure is shown in the following table.	AN

Operations element

Name	Description	Format
tipoOperazione	Operation carried out: authorisation, processing, cancellation, refund.	AN MAX 30 CHAR.
importo	Transaction amount expressed in euro cents with no separator.	N MAX 8 CHAR.
divisa	978 for Euro	N 3 CHAR.
stato	Order status	AN
dataOperazione	Operation date	dd/mm/yyyy
utente	User who carried out the operation.	AN
idContabParzialePayPal	The idContabParzialePayPal field is returned only if the transaction was processed using PayPal.	AN

Result Message: optional fields

Name	Description	Format
idContabParzialePayPal	The field is only present when depositing a PayPal transaction and is required for managing reversals.	

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
This returns an object which describes the transaction (details relating to order, Payment, and any other operation - processing/reversal).

The idContabParzialePayPal field is returned only if the transaction was processed using PayPal. If the operation type is "CONTAB.", this shows the PayPal ID to transfer to the reversal API for reversing the partial processing. Alternatively, if the operation type is "STORNO", it indicates which partial processing is being referred to.
If idContabParzialePayPal = "", this indicates that the reversal relates to a Sale type Payment which was not partially processed. This is only possible for "STORNO" operations. In this case, it is possible to just send the transaction code for a reversal.

Possible values per “stato”:

The “stato” field of the 'report' object array represents the accounting status of the transaction. Possible values are:

- Non Creato: the payment did not reach authorisation, a problem occurred on the previous steps (e.g. 3dSecure interruption by the user).

- Autorizzato: the payment has been authorised, not yet accounted for. Accounting takes place by default automatically by NEXI, at midnight of the same day
- Negato: payment has not been authorised. It will therefore not be accounted for.
- Annullato: the payment was authorised but then cancelled, either due to a notification error, or upon explicit action by the merchant (via back office, or via API).
- Contabilizzato: the payment has been accounted for.
- Contabilizzato Parz.: partial collection of the authorised amount was made on the payment.
- Rimborsato: the payment, previously accounted for, was fully refunded to the user.
- Rimborsato Parz.: a partial reimbursement of the amount entered in the accounts was made on the payment.
- In Corso: the transaction is in progress.

The “stato” field of the “dettaglio” object can take on the following values:

- Autorizzato

- In attesa di contab.
- Contabilizzato
- Autor. Negata
- Non valido
- Pendente
- Non generato
- Chiuso da backoffice
- Annullato

Whereas in the array of objects “operazione” the field “TipoOperazione” may take the value:

- CONTAB. with "stato"
    - Autorizzato
    - In attesa di contab.
    - Contabilizzato
    - Autor. Negata
    - Non valido
    - Sospeso
    - Chiuso da backoffice

    - Annullato
- STORNO with "stato":
    - In attesa di storno
    - Stornato
    - Storno Negato
    - Non valido
    - Storno Annullato

Order List

This allows to get a list of orders that meet the chosen filters in a request. The API can return a maximum of 15.000 orders.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/elenco-ordini**

URI
ecomm/api/bo/reportOrdini

METHOD
POST

ACCEPT
application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant. If not filled ("") all transactions will be returned, otherwise the inserted transaction will be returned.	AN MIN 2 - MAX 30 CHAR.
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
✓	periodo	Period to be searched. Max interval: 90 days	DATE
✓		Possible values for channel: All MyBank CreditCard PayPal Sofort	AN
	stato	Valuing this parameter will only return orders in a certain status (e.g. Annullato). It is possible to enter more values in this array during a search than the complete list below: - NONCREATO - AUTORIZZATO - INCASSATO	AN

	- INCPARZIALE - NEGATO - ANNULLATO - RIMBORSATO - RIMBPARZIALE - INCORSO

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- periodo
- canale
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>periodo=<val>canale=<val>timeStamp=<val><SecretKey>)

Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CHAR.
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	AN
✓	timeStamp	Timestamp in millisecond format.	N 13 CHAR.
✓	report	Orders object whose structure is shown in the following table.	AN

Report element

Mandatory	Name	Description	Format
✓	numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30 CHAR.
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CHAR.
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN MAX 3 CHAR.
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
✓	tipoPayment	Method by which the Payment was made, if the e-commerce used 3D Secure, SSL, or MOTO	AN
✓	tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
✓	pan	Masked credit card number with only the first 6 and/or the last 4 digits showing.	AN MAX 19 CHAR.
✓	parametri	Additional parameters	AN

✓	stato	Transaction outcome, possible values: - Non Creato - Autorizzato - Contabilizzato - Contabilizzato Parz. - Negato - Annullato - Rimborsato - Rimborsato Parz. - InCorso	AN
✓	dataTransazione	Transaction date	DATE dd/mm/yyyy

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:

- The order list API can return a maximum of 15000 records.
- This API is a reporting API, so it reports the accounting status of transactions. Following a reversal, executing the order list API will not result in the transaction being reversed: the status will be updated when the accounting reversal actually becomes accounting, i.e. at midnight.

Report

This API requires the data necessary to download a report scheduled by the BO. Starting from the reference date, returns the list of report instances processed closer to the date. If the reference date is not specified, the current date is used. Through the data contained in the listReport vector it will be possible to download the report itself.

In order to download the file, it is necessary to configure the reports in the back office, in the "Report" section, inserting the type, filters, data and format of the report to be generated.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/report**

URI
ecomm/api/bo/elencoReport

METHODO
Post

ACCEPT
Application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
refDate	reference date DD/MM/YYYY	DATA DD/MM/YYYY
timeStamp	Timestamp in millisecond format.	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the startup message, the string to be signed must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey<val> timeStamp=<val>chiaveSegreta>)

Result Message

Name	Description	Format
esito	Operation result (possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
timeStamp	Timestamp in millisecond format.	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
listaReport	Object whose structure is described in the following table	JSON
dataElaborazione	processing data	DATA dd/MM/yyyy HH:mi:ss
Format	Format csv or txt	AN
frequenza	Daily | Weekly | Monthly	AN
id	Report ID	AN
nomeFile	File name	AN
titolo	Title	AN

MAC Calculation

For the transaction outcome message, the string to be signed must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Download report

This API invoked with a common POST, returns the report file indicated in the idReport parameter (obtained through the ListReport API).

URI
ecomm/api/bo/downloadReport

METHOD
Get/Post

ACCEPT
Application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
timeStamp	Timestamp in milliseconds format	N 13 CRT
idReport	Report ID	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the startup message, the string to be signed must contain the following fields:

- apiKey
- timeStamp
- idReport
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey<val> timeStamp=<val>idReport=<val>chiaveSegreta>)

Result Message

The related report file is returned

Warning

This API allows you to retrieve information regarding the causes of any warnings returned during a transaction.
It is mandatory to specify at least one parameter between codiceTransazione and the pair of dates to perform the search. If both are valued, the research will be carried out by dates.
The answer will contain the "warnings" list which contains an element for the type of warning possible.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/api-backoffice/warning**

URI
ecomm/api/bo/warning

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
	dataTransazioneDal	Search by date from	AN gg/mm/aaaa hh:mm:ss

	dataTransazioneAl	Search by date to	AN gg/mm/aaaa hh:mm:ss

MAC Calculation

For the startup message, the string to be signed must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>timeStamp=<val><chiaveSegreta>)

Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
	errore	Only present when the result is ko. It is an object containing: codice -> error code, see table messaggio > error details	JSON
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	warnings	Array of objects containing information relating to the causes of the returned warnings, the structure of which is described in the following table	

Object warnings

Mandatory	Name	Description	Format
✓	tipo	Category to which the returned warnings object belongs: for errors on 3D Secure 2.2 parameters, it will be valued with "INFO_SICUREZZA".	AN
✓	campo	Object in which the fields that trigger the warning message are indicated.	Object

MAC Calculation

For this message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Active payment methods

Questa API permette di recuperare i metodi di pagamento attivi su un terminale. Vengono restituiti inoltre altre informazioni come i loghi associati ai metodi di pagamento.

URI
ecomm/api/profileInfo

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
✓	platform	Name of the CMS from which the call is being made, used by Nexi for statistical purposes. If you are not using a particular CMS, enhance with 'custom'.	AN
✓	platformVers	Version of the CMS from which the call is being made, used by Nexi for statistical purposes. If you are not using a particular CMS, please value with '0'.	AN
✓	pluginVers	Version of the CMS plugin from which the call is being made, used by Nexi for statistical purposes. If you are not using a particular CMS, please value with '0'.	AN
✓	timeStamp	Timestamp in millisecond format	N 13 CRT
✓	mac	Message Code Authentication Transaction signature field. For	AN 40 CRT

	the calculation, see the section "MAC Calculation" at the end of this section.

MAC Calculation

For the startup message, the string to be signed must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>timeStamp=<val><chiaveSegreta>)

Positive Result Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	urlLogoNexiSmall	Nexi logo with dimensions 240x60 pixels	AN
✓	urlLogoNexiLarge	Nexi logo with dimensions 480x120 pixels	AN
✓	availableMethods	Array of objects containing information on the payment method active on the terminal	Oggetto

Object: availableMethods

Mandatory	Name	Description	Format
✓	code	Payment method identification code	AN
✓	description	Payment method name	AN
✓	selectedcard	This parameter indicates how the 'selectedcard' parameter must be set during payment initiation in order to be redirected directly to the till page of that particular payment method	AN
✓	image	Link to the payment method logo	AN
✓	type	Type of payment method - CC: payment circuit, such as Visa and Mastercard - APM: alternative payment method, such as PayPal and Amazon Pay	AN
✓	recurring	This parameter indicates whether recurring payments can be made on the payment method	AN Y/N

Negative Result Message

Mandatory	Name	Description	Format
✓	esito	Outcome of the operation	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Present only in the event of a knockout. It is an object containing: code -> error code, possible values are given in the table here message -> error detail	AN
✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the section "MAC Calculation" at the end of this section.	AN 40 CRT
✓	timeStamp	Timestamp in millisecond format	N 13 CRT

Mac Calculation

- For this message, the string to sign must contain the following fields:
- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

INCASSO SENZA PENSIERI

Incasso Senza Pensieri is a value-added service dedicated to reservations (Hotels, Restaurants and Tour Operators) on the XPay Gateway.

More information on service activation and examples of use cases are available by consulting the guides:

- **XPay Hotel**
- **XPay Ristoranti**
- **Tour operator**

Compliant with all the security regulations in force, the "Incasso Senza Pensieri" service is based on the Nexi XPay platform and makes it possible to simplify reservations made remotely via all the payment instruments accepted by the merchant, making them more defensible in case of disputes.

The following types of reservations are available:

- Guaranteed Reservation: reservation, through a card verification without charging the customer. In case the customer does not come to the structure, it’s possible to charge the first night cost.
- Prepaid Refundable: reservation with payment in advance. In case of cancellations before the beginning of the stay it is possible to refund the amount totally or partially (according to the Terms and Conditions defined by the merchant).
- Prepaid not Refundable: reservation with prepaid payment. No refund is possible.
- Bundle: type of reservation dedicated to tour operators

It is also possible to do card verification operations: verification of a 0 amount card without tokenization, aimed at verifying the authenticity of the customer's card.

In order to use the service it is necessary to activate it from the back office and configure at least one structure (struttura/structure intended as an Hotel/Restaurant facility)

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri

Payment

Guaranteed booking

Reservation, through a card verification without charging the customer. In case the customer does not show up at the structure, you can charge the cost of the first night of stay.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento/prenotazione-garantita

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message: required fields

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must	AN MIN 2 - MAX 30 CHAR. In case of

		be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	MyBank you can only use: / - : ( ) . , +
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_tipoprenotazione	"GARANTITA"	

✓	dl_codicestruttura	One of the structure codes surveyed manually from back office or through the API censisciStruttura	MAX 100
✓	dl_dataprenotazione	Check-In/Start date of hire if dl_formatodata parameter is set to "PERIODO" - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with "SINGOLA" Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	dl_importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	importoNoShow	Penalty for non-cancellation, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N
✓	num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card, necessary to perform the NoShow. If not valorized, the value of the field dl_codiceprenotazione	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN MAX 40 CRT
✓	dl_oggetto	Object of the reservation. Suggested values: - TAVOLO - SALA	AN

		Mandatory only for Restaurants	
	dl_templategarantita	template GARANTITA type. If not present the value of the structure will be used. Possible values: - DATA -> the parameter "dl_datacancellazione" will become mandatory. - ORE -> the parameter "dl_orecancellazione" will become mandatory.	AN
	dl_datacancellazione	Date by which the customer can cancel the reservation.	DD/MM/YYYY HH24:MI
	dl_orecancellazione	Hours from CheckIn within which the customer can make the cancellation.	N
	dl_codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100
	dl_formatodata	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	
	dl_tipodata	You can set the parameter with: - E = "by" - F = "until" - A = "starting from"	

		In this way, based on the selection made, the buyer will be able to see the following format on XPAY: - 11.12.2020 – before 2.00 pm - 11.12.2020 – until 2.00 pm - 11.12.2020 – starting at 2.00 pm The field will be managed if the time is present in the dl_dataprenotazione field. Default value is E.	
	dl_datafineprenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	dl_numnotti	Number of nights	N
	dl_nomerichiedente	Name of reservation holder	AN MAX 256
	dl_cognomerichiedente	Surname of reservation holder	AN MAX 256
	dl_numospiti	Number of guests staying in the structure	N
	dl_ospite_X	If “dl_numospiti” is set the number of guests can be specified (dl_host_1, dl_host_2,... dl_host_[dl_number of guests]). If dl_number of guests is not present, the following will not be considered	AN MAX 3000
	dl_termcond	Identifier of the terms and conditions surveyed in the back office manually or through the API caricaTermCond.	

		If the field is not used, the default text provided by Nexi for the booking type will be automatically selected.	
	dl_termcondpost	If set to S manages the loading of the terms and conditions into the request. If the condition term code, specified in dl_termcond, is already present, the previously saved value will be used. Otherwise, the parameter dl_termcondtest_n will be evaluated.	AN
	dl_termcondtesto_n	Text of the terms and conditions to be saved and displayed on the checkout page. n is to be replaced with the languages managed by xpay (ITA, ENG). ENG is mandatory	AN
	dl_termconddescrizione	Description that will be displayed in the back office	AN
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-	AN MAX 500

		urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report	AN MAX 200

		information about the order.	
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal. Compatible with payment cards and PayPal.	

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not

exceed 4000 characters. Avoid the following parameter names because they are already used by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- importoNoShow
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>
importoNoShow=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_tipoprenotazione
- dl_codiceprenotazione (if present in request)
- dl_dataprenotazione (if in the request the field dl_datafineprenotazione is valorized, the parameter in the calculation of the mac must be valorized with the concatenation of the start and end dates of the reservation. Es. dl_dataprenotazione=30/01/202112/02/2021)
- num_contratto
- dl_termcond (if present in request)
- importoNoShow
- chiaveSegreta

SAMPLE STRING

MAC = HASH
SHA1(codTrans=<val>dl_tipoprenotazione=<val>dl_codiceprenotazione=<val>dl_dataprenotazione=<val>num_contratto=<val>dl_termcond=<val>importoNoShow=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications)

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2

For Subsequent Payment refer to the section **Pagamenti Successivi**

Guaranteed booking with penalty

Reservation by means of a card verification without charge to the customer. In the event that the customer does not cancel the stay within the time stipulated in the terms and conditions, a penalty fee agreed upon at the time of booking will be charged.

Compared to the Guaranteed Reservation, it will not be necessary to use a dedicated API (no show) for the charge. XPay will do this automatically once the maximum cancellation period has expired.

It is important to note that the pre-determined amount (penalty) will be charged in any case if the stay is not cancelled: this charge will be considered by the operator as a penalty if the customer does not show up at the property, or as a partial/total payment for the stay.

It is the responsibility of the operator, in case he receives the cancellation within the given booking deadline, to make the cancellation from the backoffice or call up the cancellation API.

This type of booking is not available for tour operators.

You must set up a POST request (the GET method is deprecated) with the format of a form submission at

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2	N MAX 8 CRT

		numbers to the right represent the euro cents.	
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR).	AN MAX 200 CRT

		For detailed information on the parameters received, please refer to the Cancellation section.	
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_tipoprenotazione	"GARANTITAPENALE"	
✓	dl_codicestruttura	One of the structure codes surveyed manually from back office or through the API censisciStruttura	MAX 100
✓	dl_dataprenotazione	Check-In/Start date of hire if dl_formatodata parameter is set to "PERIODO" - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with "SINGOLA" Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	dl_importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card, necessary to perform the NoShow. If not valorized, the value of the field dl_codiceprenotazione	AN MIN 5 MAX 30 Except the “+” character and the quotes
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter:	AN MAX 40 CRT

		MAC Calculation “Incasso Senza Pensieri”.	
✓	dl_oggetto	Object of the reservation. Suggested values: - TAVOLO - SALA Mandatory only for Restaurants	AN
	dl_templategarantita	template GARANTITA type. If not present the value of the structure will be used. Possible values: - DATA -> the parameter "dl_datacancellazione" will become mandatory. - ORE -> the parameter "dl_orecancellazione" will become mandatory.	AN
	dl_datacancellazione	Date by which the customer can cancel the reservation.	DD/MM/YYYY HH24:MI
	dl_orecancellazione	Hours from CheckIn within which the customer can make the cancellation.	N
	dl_codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100
	dl_formatodata	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in	

		the back office is considered.	
	dl_tipodata	You can set the parameter with: - E = "by" - F = "until" - A = "starting from" In this way, based on the selection made, the buyer will be able to see the following format on XPAY: - 11.12.2020 – before 2.00 pm - 11.12.2020 – until 2.00 pm - 11.12.2020 – starting at 2.00 pm The field will be managed if the time is present in the dl_dataprenotazione field. Default value is E.	
	dl_datafineprenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	dl_numnotti	Number of nights	N
	dl_nomerichiedente	Name of reservation holder	AN MAX 256
	dl_cognomerichiedente	Surname of reservation holder	AN MAX 256
	dl_numospiti	Number of guests staying in the structure	N
	dl_ospite_X	If “dl_numospiti” is set the number of guests can be specified (dl_host_1, dl_host_2,... dl_host_[dl_number of guests]). If dl_number of guests is not present, the	AN MAX 3000

		following will not be considered	
	dl_termcond	Identifier of the terms and conditions surveyed in the back office manually or through the API caricaTermCond. If the field is not used, the default text provided by Nexi for the booking type will be automatically selected.	
	dl_termcondpost	If set to S manages the loading of the terms and conditions into the request. If the condition term code, specified in dl_termcond, is already present, the previously saved value will be used. Otherwise, the parameter dl_termcondtest_n will be evaluated.	AN
	dl_termcondtesto_n	Text of the terms and conditions to be saved and displayed on the checkout page. n is to be replaced with the languages managed by xpay (ITA, ENG). ENG is mandatory	AN
	dl_termconddescrizione	Description that will be displayed in the back office	AN
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this	AN MAX 500

		field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR

	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office.	

	Compatible with payment cards and PayPal. Compatible with payment cards and PayPal.

3D Secure 2.2

To use the 3D Secure 2.2 service, please refer to section **3D Secure 2.2**

MAC Calculation

For the transaction start message, the string to be signed must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation Incasso senza pensieri

For the transaction start message, the string to be signed must contain the following fields:

- codTrans
- dl_tipoprenotazione
- dl_codiceprenotazione (to be inserted if present in request)
- dl_dataprenotazione (If the field dl_databooking is passed in the request, the parameter in the calculation of the mac must be set to the concatenation of the start and end dates of the booking. Es. dl_dataprenotazione=30/01/202112/02/2021)
- num_contratto
- dl_termcond (to be inserted if present in request)
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_tipoprenotazione=<val>dl_codiceprenotazione=<val>dl_dataprenotazione=<val>num_contratto=<val>dl_termcond=<val><chiaveSegreta>)

Note

- Additional parameters may be specified and will be returned in the result message and notification message.
  There is no limit to the number of additional parameters, but the total length of the string consisting of the parameter names and their value must not exceed 4000 characters.
  The following parameter names should be avoided because they are used by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $COGNOME, EMAIL .
  The parameters must also be configured in the XPay back office in the configuration section otherwise they will not be returned.
- For correct handling of calls, please remember to follow the standards RFC 2396 and RFC 3986
- Parameters related to the working framework (e.g. VIEWSTATE for ASP.NET applications) must not be sent
- SHA256 encoding may be used for mac calculation. You must contact the e-mail address at the bottom of this page to enable the new encoding on the terminal.

The handling of the outcome, cancellation and notification does not change from that of the solution Easy Payment. Please refer to the corresponding sections to see the returned parameters.

Penalty Payment

When the cancellation deadline expires, XPay automatically charges the penalty fee. Charges are not made overnight, to avoid disturbing customers with outcome notifications during inappropriate hours.
Upon completion of the individual penalty payment, a POST notification will be sent to the 'urlpost' parameter if set during the booking process. Below is the data sent in the notification:

Mandatory	Name	Description	Format
	numeroMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30 CRT
	importo	Transaction amount taken from the payment initiation message	N MAX 8 CRT
	divisa	The code of the currency in which the amount is expressed (EUR = Euro)	AN 3 CRT
	data	Transaction date	yyyymmdd
	orario	Transaction hour	Hhmmss
	codTrans	Code associated with the payment taken from the payment initiation message	AN MIN 2 - MAX 30 CRT
	esito	Outcome of the operation. Possible values: - OK - KO	AN MAX 7 CRT
	codAut	Authorisation code assigned by the credit card issuer, present only with authorisation granted	AN MIN 2 MAX 6 CRT
	brand	Type of card used by the user to make the payment. Possible values are as shown in the table here	AN MAX 100 CRT
	tipoTransazione	Transaction type, indicates the method of payment, only value allowed NO_3DSECURE	AN
	mail	E-mail address of the person who made the payment	AN MAX 150 CRT

	messaggio	Report a brief description of the outcome of the payment. Possible values: - Transaction successful - Transaction not authorised	AN MAX 300 CRT
	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Excluding the + character and superscripts
	eventType	Type of event triggering the notification, only possible value: PENALE	AN
	dl_codiceprenotazione	Reservation code associated with the plan	AN
	mac	Message Code Authentication Transaction signature field. For the calculation, see the section 'MAC Calculation' at the end of this section.	AN 40 CRT

No outcome e-mails will be sent to the merchant or the end customer, even in the case of unsuccessful payment.

MAC Calculation

For the outcome message, the string to be signed must contain the fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

Prepaid Refundable

Booking with advance Payment. It is possible to refund the amount in full or in part (depending on the Terms and Conditions defined by the operator) if the reservation is cancelled before the beginning of the stay.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento/prepagato-rimborsabile

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each	AN MIN 2 - MAX 30 CHAR. In case of MyBank you

		authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	can only use: / - : ( ) . , +
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_tipoprenotazione	"RIMBORSABILE"	

✓	dl_codicestruttura	One of the structure codes surveyed manually from back office or through the API censisciStruttura	MAX 100
✓	dl_dataprenotazione	Check-In/Start date of hire if dl_formatodata parameter is set to "PERIODO" - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with "SINGOLA" Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN MAX 40 CRT
✓	dl_oggetto	Object of the reservation. Suggested values:: - TAVOLO - SALA Mandatory only for Restaurants	AN
	dl_templaterimborsabile	template rimborsabile type. If not present, the value of the structure will be used. Possible values: - DATA -> Both or one of the following parameters must be indicated "dl_datarimborsototale", "dl_datarimborsoparziale". parameter "dl_importorimborsoparziale" will become mandatory if a partial refund date is specified. - ORA -> "dl_giornirimborsototale", "dl_giornirimborsoparziale", "dl_percentualerimborso", "dl_giorninorimborso" will become mandatory	AN

	dl_datarimborsototale	Total Refund Date.	DATA DD/MM/YYYY HH:MI
	dl_datarimborsoparziale	Partial refund date, must be after the full refund date.	DATA Data DD/MM/YYYY HH:MI
	dl_importorimborsoparziale	Amount of partial reimbursement, expressed in euro cents	N
	dl_giornirimborsototale	Days from the beginning of the stay, within which the customer will receive a full refund in case of cancellation of the reservation	N MAX 3
	dl_giorninorimborso	Days from the start date of the stay, within which the customer will not receive a refund in case of cancellation of the reservation	N MAX 3
	dl_giornirimborsoparziale	Days from the start date of the stay, within which the customer can receive a partial refund in case of cancellation of the reservation	N MAX 3
	dl_percentualerimborso	Percentage of the rePayment amount in case of partial rePayment	N MAX 10
	dl_tipoincasso	Type of embedding DIFFERITO o DILAZIONATO. In case of DILAZIONATO will become mandatory dl_importoprenotazione, dl_numerorate, dl_importorata_n, dl_datarata_n For more information please refer to the section Incasso Differito e Dilazionato	AN
	dl_importoprenotazione	Amount of the booking expressed in euro cents	

		without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. The parameter indicates the total amount of the transaction while the parameter 'amount' must be set to the same amount as the first instalment.	
	dl_numerorate	Number of instalments	N
	dl_importorata_n	Date of the instalment. n is the number of the instalment 1 to dl_numerorate. The amount of instalment 1 must correspond to the amount of the transaction	N
	dl_datarata_n	Date on which payment of instalment 1 is to be made. The date of instalment 1 may be left unspecified and will in any case take the date of payment as its value.	
	dl_saldoinstruttura	Indicates whether the last instalment will be paid on arrival at the accommodation. Possible values S or N	AN
	dl_codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100
	dl_formatodata	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date.	

		If not present, the default of the structure indicated in the back office is considered.	
	dl_tipodata	Allows the user to choose "between within" (E) and "up to" (F). In this way, based on the selection made, the buyer will be able to see the following format on XPAY: - 11.12.2020 – within 14:00 - 11.12.2020 – until 14:00. The field will be managed if the time is present inside the field dl_dataprenotazione. default value is E.	
	dl_datafineprenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	dl_numnotti	Number of nights	N
	dl_nomerichiedente	Name of reservation holder	AN MAX 256
	dl_cognomerichiedente	Surname of reservation holder	AN MAX 256
	dl_numospiti	Number of guests staying in the structure	N
	dl_ospite_X	If “dl_numospiti” is set the number of guests can be specified (dl_host_1, dl_host_2,... dl_host_[dl_number of guests]). If dl_number of guests is not present, the following will not be considered	AN MAX 3000
	dl_delaycharge	If valorized with "true", it will be possible to carry out	

		delayed charge operations on the reservation. If not present, the default of the structure indicated in the back office is considered. This operation is only allowed on payments in "Contabilizzato/Rimborsabile" status and within 90 days of the accounting date.	
	dl_incremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present, the default of the structure indicated in the back office is considered. This operation is only possible on transactions in "Autorizzato" status.	
	dl_termcond	Identifier of the terms and conditions surveyed in the back office manually or through the API caricaTermCond. If the field is not used, the default text provided by Nexi for the booking type will be automatically selected.	
	dl_termcondpost	If set to S manages the loading of the terms and conditions into the request. If the condition term code, specified in dl_termcond, is already present, the previously saved value will be used. Otherwise, the parameter dl_termcondtest_n will be evaluated.	AN
	dl_termcondtesto_n	Text of the terms and conditions to be saved and displayed on the checkout page. n is to be replaced with the languages managed by	AN

		xpay (ITA, ENG). ENG is mandatory	
	dl_termconddescrizione	Description that will be displayed in the back office	AN
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined	AN MAX 7

		during the service configuration process.	
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user’s Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35

	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.	

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_tipoprenotazione
- dl_codiceprenotazione (if present in request)
- dl_dataprenotazione (if in the request the field dl_datafineprenotazione is valorized, the parameter in the calculation of the mac must be valorized with the concatenation of the start and end dates of the reservation. Es. dl_dataprenotazione=30/01/202112/02/2021)
- num_contratto
- dl_termcond (if present in request)
- dl_delaycharge (if present in request)
- dl_incremental (if present in request)
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_tipoprenotazione=<val>dl_codiceprenotazione=<val>dl_dataprenotazione=<val>num_contratto=<val>dl_termcond=<val>dl_delaycharge=<val>dl_incremental=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications)

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
With this mode, the call to the gateway will be the same for both the first and subsequent Payments: XPay will handle them.
In the case of the first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
To use the solution it is necessary to send the following parameters during Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_oc3d”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized	AN MIN 4 MAX 10

Mac Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiave segreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiavesegreta>)

NOTA:

If the "gruppo" is not used in the initialization parameters, include it in the MAC calculation without valuing it.

Prepaid Not Refundable

Reservation with advance Payment. No refunds are possible.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento/prepagato-non-rimborsabile

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and	AN MIN 2 - MAX 30 CHAR. In case of MyBank you

		only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	can only use: / - : ( ) . , +
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_tipoprenotazione	"NONRIMBORSABILE"	

✓	dl_codicestruttura	One of the structure codes surveyed manually from back office or through the API censisciStruttura	MAX 100
✓	dl_dataprenotazione	Check-In/Start date of hire if dl_formatodata parameter is set to "PERIODO" - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with "SINGOLA" Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN MAX 40 CRT
	dl_codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100 CRT
	dl_formatodata	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	N MAX 8 CRT
	dl_tipodata	Allows the user to choose "between within" (E) and "up to" (F). In this way, based on the selection made, the buyer will be able to see the	

		following format on XPAY: - 11.12.2020 – within 14:00 - 11.12.2020 – until 14:00. The field will be managed if the time is present inside the field dl_dataprenotazione. default value is E.	
	dl_datafineprenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	dl_tipoincasso	Type of embedding DIFFERITO o DILAZIONATO. In case of DILAZIONATO will become mandatory dl_importoprenotazione, dl_numerorate, dl_importorata_n, dl_datarata_n For more information please refer to the section Incasso Differito e Dilazionato	
	dl_numerorate	Number of instalments	N
	dl_importorata_n	Date of the instalment. n is the number of the instalment 1 to dl_numerorate. The amount of instalment 1 must correspond to the amount of the transaction	N
	dl_datarata_n	Date on which payment of instalment 1 is to be made. The date of instalment 1 may be left unspecified and will in any case take the date of payment as its value.	
	dl_saldoinstruttura	Indicates whether the last instalment will be paid on arrival at the accommodation. Possible values S or N	AN

	dl_importoprenotazione	Amount of the booking expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. The parameter indicates the total amount of the transaction while the parameter 'amount' must be set to the same amount as the first instalment.	
	dl_numerorate	Number of instalments	N
	dl_importorata_n	Date of the instalment. n is the number of the instalment 1 to dl_numerorate. The amount of instalment 1 must correspond to the amount of the transaction	N
	dl_datarata_n	Date on which payment of instalment 1 is to be made. The date of instalment 1 may be left unspecified and will in any case take the date of payment as its value.	
	dl_saldoinstruttura	Indicates whether the last instalment will be paid on arrival at the accommodation. Possible values S or N	AN
	dl_ospite_X	If “dl_numospiti” is set the number of guests can be specified (dl_host_1, dl_host_2,... dl_host_[dl_number of guests]). If dl_number of guests is not present, the following will not be considered	AN MAX 3000
	dl_delaycharge	If valorized with "true", it will be possible to carry out delayed charge operations on the reservation. If not present, the default of the	

		structure indicated in the back office is considered. This operation is only allowed on payments in "Contabilizzato/Rimborsabile" status and within 90 days of the accounting date.	
	dl_incremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present, the default of the structure indicated in the back office is considered. This operation is only possible on transactions in "Autorizzato" status.	
	dl_termcond	Identifier of the terms and conditions surveyed in the back office manually or through the API caricaTermCond. If the field is not used, the default text provided by Nexi for the booking type will be automatically selected.	
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To	AN MAX 500

		confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200

	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.	

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_tipoprenotazione
- dl_codiceprenotazione (if present in request)
- dl_dataprenotazione (if in the request the field dl_datafineprenotazione is valorized, the parameter in the calculation of the mac must be valorized with the concatenation of the start and end dates of the reservation. Es. dl_dataprenotazione=30/01/202112/02/2021)
- num_contratto
- dl_termcond (if present in request)
- dl_delaycharge (if present in request)
- dl_incremental (if present in request)
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_tipoprenotazione=<val>dl_codiceprenotazione=<val>dl_dataprenotazione=<val>num_contratto=<val>dl_termcond=<val>dl_delaycharge=<val>dl_incremental=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
  Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications)

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
With this mode, the call to the gateway will be the same for both the first and subsequent Payments: XPay will handle them.
In the case of the first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
To use the solution it is necessary to send the following parameters during Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_oc3d”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized	AN MIN 4 MAX 10

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiave segreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiavesegreta>)

NOTA:

If the “gruppo” is not used in the initialization parameters, include it in the MAC calculation without valuing it

Bundle

Type of reservation dedicated to tour operators.

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_tipoprenotazione	To enhance with "PACCHETTO"	
✓	dl_codicestruttura	One of the structure codes surveyed manually from back office or through the API censisciStruttura	MAX 100

✓	dl_dataprenotazione	Check-In/Start date of hire if dl_formatodata parameter is set to "PERIODO" - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with "SINGOLA" Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN MAX 40 CRT
✓	dl_oggetto	Object of the reservation. Suggested values:: - TAVOLO - SALA Mandatory only for Restaurants	AN
	dl_templaterimborsabile	template rimborsabile type. If not present, the value of the structure will be used. Possible values: - DATA -> Both or one of the following parameters must be indicated "dl_datarimborsototale", "dl_datarimborsoparziale". parameter "dl_importorimborsoparziale" will become mandatory if a partial refund date is specified. - ORA -> "dl_giornirimborsototale", "dl_giornirimborsoparziale", "dl_percentualerimborso", "dl_giorninorimborso" will become mandatory	AN
	dl_datarimborsototale	Total Refund Date.	DATA DD/MM/YYYY HH:MI

	dl_datarimborsoparziale	Partial refund date, must be after the full refund date.	DATA Data DD/MM/YYYY HH:MI
	dl_importorimborsoparziale	Amount of partial reimbursement, expressed in euro cents	N
	dl_giornirimborsototale	Days from the beginning of the stay, within which the customer will receive a full refund in case of cancellation of the reservation	N MAX 3
	dl_giorninorimborso	Days from the start date of the stay, within which the customer will not receive a refund in case of cancellation of the reservation	N MAX 3
	dl_giornirimborsoparziale	Days from the start date of the stay, within which the customer can receive a partial refund in case of cancellation of the reservation	N MAX 3
	dl_percentualerimborso	Percentage of the rePayment amount in case of partial rePayment	N MAX 10
	dl_tipoincasso	Type of embedding DIFFERITO o DILAZIONATO. In case of DILAZIONATO will become mandatory dl_importoprenotazione, dl_numerorate, dl_importorata_n, dl_datarata_n For more information please refer to the section Incasso Differito e Dilazionato	AN
	dl_importoprenotazione	Amount of the booking expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00.	

		The parameter indicates the total amount of the transaction while the parameter 'amount' must be set to the same amount as the first instalment.	
	dl_numerorate	Number of instalments	N
	dl_importorata_n	Date of the instalment. n is the number of the instalment 1 to dl_numerorate. The amount of instalment 1 must correspond to the amount of the transaction	N
	dl_datarata_n	Date on which payment of instalment 1 is to be made. The date of instalment 1 may be left unspecified and will in any case take the date of payment as its value.	
	dl_saldoinstruttura	Indicates whether the last instalment will be paid on arrival at the accommodation. Possible values S or N	AN
	dl_codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100
	dl_formatodata	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	

	dl_tipodata	Allows the user to choose "between within" (E) and "up to" (F). In this way, based on the selection made, the buyer will be able to see the following format on XPAY: - 11.12.2020 – within 14:00 - 11.12.2020 – until 14:00. The field will be managed if the time is present inside the field dl_dataprenotazione. default value is E.	
	dl_datafineprenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	dl_numnotti	Number of nights	N
	dl_nomerichiedente	Name of reservation holder	AN MAX 256
	dl_cognomerichiedente	Surname of reservation holder	AN MAX 256
	dl_numospiti	Number of guests staying in the structure	N
	dl_ospite_X	If “dl_numospiti” is set the number of guests can be specified (dl_host_1, dl_host_2,... dl_host_[dl_number of guests]). If dl_number of guests is not present, the following will not be considered	AN MAX 3000
	dl_delaycharge	If valorized with "true", it will be possible to carry out delayed charge operations on the reservation. If not present, the default of the	

		structure indicated in the back office is considered. This operation is only allowed on payments in "Contabilizzato/Rimborsabile" status and within 90 days of the accounting date.	
	dl_incremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present, the default of the structure indicated in the back office is considered. This operation is only possible on transactions in "Autorizzato" status.	
	dl_termcond	Identifier of the terms and conditions surveyed in the back office manually or through the API caricaTermCond. If the field is not used, the default text provided by Nexi for the booking type will be automatically selected.	
	dl_termcondpost	If set to S manages the loading of the terms and conditions into the request. If the condition term code, specified in dl_termcond, is already present, the previously saved value will be used. Otherwise, the parameter dl_termcondtest_n will be evaluated.	AN
	dl_termcondtesto_n	Text of the terms and conditions to be saved and displayed on the checkout page. n is to be replaced with the languages managed by xpay (ITA, ENG). ENG is mandatory	AN

	dl_termconddescrizione	Description that will be displayed in the back office	AN
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7

	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user’s Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual	AN MAX 20

	Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.
xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_tipoprenotazione
- dl_codiceprenotazione (if present in request)
- dl_dataprenotazione (if in the request the field dl_datafineprenotazione is valorized, the parameter in the calculation of the mac must be valorized with the concatenation of the start and end dates of the reservation. Es. dl_dataprenotazione=30/01/202112/02/2021)
- num_contratto
- dl_termcond (if present in request)
- dl_delaycharge (if present in request)
- dl_incremental (if present in request)
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_tipoprenotazione=<val>dl_codiceprenotazione=<val>dl_dataprenotazione=<val>num_contratto=<val>dl_termcond=<val>dl_delaycharge=<val>dl_incremental=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications)

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
With this mode, the call to the gateway will be the same for both the first and subsequent Payments: XPay will handle them.
In the case of the first Payment XPay will show the form for entering the card data while in the case of subsequent Payments it will show the card data previously entered or the possibility of entering the data of a new card.
To use the solution it is necessary to send the following parameters during Payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_oc3d”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN MAX 2
gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized	AN MIN 4 MAX 10

Mac Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiavesegreta>)

NOTA:

If the "gruppo" is not used in the initialization parameters, include it in the MAC calculation without valuing it.

API

This section describes the API made available by Nexi for the service "Incasso senza Pensieri".

Structure insertion

The API allows you to censor a multilingual structure and values.

It is also possible to census a structure from the Nexi back office in the appropriate section of the reservations.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/inserimento-struttura

URI
ecomm/api/vas/ig/censisciStruttura

METHOD
Post

ACCEPT
Application/json

Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	struttura	Object containing the information of the structure to be recorded	Oggetto
✓	defaultGarantita	Object containing the default template ofGARANTITA	Oggetto

✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	multilingua	Array of objects that allows the description of the structure present on the checkout page to be displayed in different languages. Valued by means of the "descrizionePaginaCassa" parameter. The structure of the object is described below.	Oggetto

Object struttura

Mandatory	Name	Description	Format
✓	nomeStruttura	Name of the new structure to be registered	AN
✓	codice	Identification code of the new structure	AN
✓	email	Structure reference email that will be shown on the checkout page	AN MIN 1 MAX 254
✓	telefono	Structure reference phone number that will be shown on the checkout page	AN
✓	defaultGarantita	Object containing the default template of the GARANTITA reservation	
✓	defaultRimborsabile	Object containing the default template of the RIMBORSABILE reservation	
	periodo	- If set to "true", in the back office, when creating the booking link, the default date format will be shown as	AN

		PERIODO, with a start and end date for the booking. - If set to "false", in the back office, during the creation of the booking link, the default date format will be shown as SINGOLA (booking of a single day in the structure).	
	apmAttivi	The APMs do not provide the possibility to manage the no-Show with the GARANTITA, choose how you prefer to manage them: - If valorized with "true" they remain active but only to verify the card without possibility to apply no-show - If valorized with "false" they deactivate among the Payment options when this type of reservation is requested	AN
	orarioArrivo	If set to "true", in the back office, when creating the booking link, together with the check-in date will also be shown the choice of time	AN
	orarioUscita	If set to "true", in the back office, when creating the booking link, together with the check-out date will also be shown the choice of time	AN
	delayCharge	If valorized with "true", by default delayed charge operations will be allowed on bookings (excluding GARANTITA)	AN
	incremental	If valorized with "true", by default incremental operations	AN

		will be allowed on bookings (excluding GARANTITA)	
	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	email	Structure reference mail that will be shown on the checkout page	AN MAX 254 CRT
	telefono	Reference telephone number of the structure that will be shown on the checkout page	AN
	facebookId	facebookId	AN
	googleMyBusiness	Google contact	AN
	giorniPreavviso	Number of days of advance notice of payment of instalments or of the imminent expiry of full refund terms for a reservation. If not specified this is the default (2) set on the property in the back office	N

Object defaultGarantita

mandatory	Name	Descrption	Format
✓	templateGarantita	Booking conditions GARANTITA, if not specified is the default set on the structure in the back office. Possible values: - DATA -> will become mandatory “dataCancellazione” - ORA -> will become mandatory "oreCancellazione"	AN Format data DD/MM/YYYY HH:MI
	oreCancellazioneGarantita	Hours from arrival within which the customer can cancel the reservation	N

Oggetto defaultRimborsabile

Mandatory	Nome	Descrizione	Formato
✓	templateRimborsabile	Booking conditions RIMBORSABILE, if not specified is the default set on the structure in the back office. Possible values: - DATA -> will become mandatory: "dataRimborsoTotale", "dataRimborsoParziale", "importoRimborsoParziale" - ORA -> will become mandatory: "giorniRimborsoTotale", "giorniNessunRimborso", "giorniRimborsoParziale", "percentualeRimoborsoParziale"	

Object multiligua

Mandatory	Name	Description	Format
✓	parametro	Valorise with "DESCR_ESTERNA"	AN
✓	lingua	Description language. The available languages are those	AN 3

		shown in the table Codifica languageId.	
✓	valore	Description in the language indicated in the "lingua" parameter	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>timeStamp=<val><chiaveSegreta>)

Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 20 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	
✓	timeStamp	Timestamp in milliseconds format	AN 13
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Inserting terms and conditions

The API allows you to upload custom terms and conditions for use with the service Incasso senza Pensieri.
It is possible to enter the terms and conditions also from the Nexi back office in the appropriate section of the bookings.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/inserimento-termini-condizioni

URI
ecomm/api/vas/ig/caricaTermCond

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	tipo	Type of reservation for which you want to insert the terms and conditions. Possible values: - GARANTITA - RIMBORSABILE - NONRIMBORSSABILE	AN
✓	codice	New terms and conditions identification code	AN
✓	descrizione	Internal description for new terms and conditions	AN
✓	testi	Object containing the terms and conditions divided by language	Oggetto

✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object testi: required fields

Mandatory	Name	Description	Format
✓	ITA	Terms and conditions in Italian	AN
✓	ENG	Terms and conditions in English	AN
	SPA	Terms and conditions in Spanish	AN
	FRA	Termini e condizioni in French	AN
	GER	Terms and conditions in German	AN
	JPN	Terms and conditions in Japanese	AN
	CHI	Terms and conditions in Chinese	AN
	ARA	Terms and conditions in Arabic	AN
	RUS	Termini e condizioni in Russian	AN
	POR	Terms and conditions in Portoguese	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>timeStamp=<val><chiaveSegreta>)

Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 20 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	
✓	timeStamp	Timestamp in milliseconds format	AN 13
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Modification of terms and conditions

The API allows you to change the status of previously uploaded terms and conditions. It is also possible to deactivate or cancel the terms and conditions from the Nexi back office, in the appropriate section of the reservations.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/modifica-termini-condizioni

URI
ecomm/api/vas/ig/modificaStatoTermCond

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codice	New terms and conditions identification code	AN
✓	stato	Possible values: - CANCELLATO - ATTIVO - DISATTIVO	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>timeStamp=<val><chiaveSegreta>)

Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 20 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	
✓	timeStamp	Timestamp in milliseconds format	AN 13
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Delayed Charge

The API allows you to perform a delayed charge operation on a reservation.
It is also possible to perform this operation from the Nexi back office, in the appropriate section of the reservations.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/delayed-charge

URI
ecomm/api/vas/ig/pagaDelayedCharge

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codicePrenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	N MAX 3 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT

✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codicePrenotazione
- importo
- divisa
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codicePrenotazione=<val>importo=<val> divisa=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N MAX 8
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
✓	data	Transaction date	DATA MAX 8 aaaammgg

✓	ora	Transaction time	AN MAX 6 hhmmss
✓	regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Esempio: VISA CLASSIC - CREDIT – N	AN MAX 200
✓	codiceConvenzione	Merchant code assigned by the acquirer. Where required	AN MAX 15
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table Codifica tipo carta.	AN MAX 100
✓	tipoTransazione	Transaction type, indicates the Payment method. See the table Codifica Tipo Transazione for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
✓	codicePrenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTE:

The pagaDelayedCharge API, in addition to the standard error codes, may return error code 94 - operation in progress: there is already another incremental request that has not yet completed, so you must wait.

This operation is only allowed on payments in "Contabilizzato/Rimborsabile" status and within 90 days of the accounting date.

Incremental

The API allows you to perform an incremental operation on a reservation.
It is also possible to perform this operation from the Nexi back office, in the appropriate section of the reservations.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/incremental

URI
ecomm/api/vas/ig/pagaIncremental

METHOD
Post

ACCEPT
Application/json

Initiation Message

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codicePrenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	N MAX 3 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT

✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codicePrenotazione
- importo
- divisa
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codicePrenotazione=<val>importo=<val> divisa=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N MAX 8
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6

✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	ora	Transaction time	AN MAX 6 hhmmss
✓	regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Esempio: VISA CLASSIC - CREDIT – N	AN MAX 200
✓	codiceConvenzione	Merchant code assigned by the acquirer. Where required	AN MAX 15
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table Codifica tipo carta.	AN MAX 100
✓	tipoTransazione	Transaction type, indicates the Payment method. See the table Codifica Tipo Transazione for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
✓	codicePrenotazione	Unique code of the reservation. If not	AN

		valorized, the value of the “codice transazione” or “numero contratto” will be used.	
✓	importoTotaleAutorizzato	Total amount authorized (pre-authorized amount + sum of incremental amounts) expressed in eurocent without separator, the first 2 numbers to the right represent the euro cents.	N

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

NOTE:

The pagaIncremental API, in addition to the standard error codes, may return error code 94 - operation in progress: there is already another incremental request that has not yet completed, so you must wait.

This operation is only allowed on payments in "Autorizzato" status.

Payment No Show

The API allows you to charge a No Show previously registered through a reservation GARANTITA.
It is also possible to perform this operation from the Nexi back office, in the special section of the reservations.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/pagamento-no-show

URI
ecomm/api/vas/ig/PaymentNoShow

METHOD
Post

ACCEPT
Application/json

Initiation Message: required fields

Mandatory	Name	Description	Format
✓	apiKey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	N MAX 3 CRT

✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
	scadenza	Card expiry date	DATA aaaamm
	codiceGruppo	Code assigned by Nexi during activation. If not provided during activation, the field should not be valorized.	AN MIN 4 MAX 10 CRT
	parametriAggiuntivi	In this object, you can enter n parameters that will be returned in the result message. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL	Oggetto

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- scadenza
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>
codiceTransazione=<val>importo=<val> divisa=<val>scadenza=<val>
timeStamp=<val><chiaveSegreta>)

NOTE:

If the "scadenza" parameter is not used in the initiation message, include it in the MAC calculation without valuing it.

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6
✓	codiceConvenzione	Merchant code assigned by the acquirer. Where required	AN MAX 15
✓	data	Transaction date	DATA MAX 8 aaaammgg
✓	ora	Transaction time	AN MAX 6 hhmmss
✓	regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30
✓	nazione	Credit card country	AN ISO 3166-1 alpha-3
✓	tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Esempio: VISA CLASSIC - CREDIT – N	AN MAX 200
✓	brand	Type of card used by the user to make Payment. The possible values are shown in the table Codifica tipo carta	AN MAX 100

✓	tipoTransazione	Transaction type, indicates the Payment method. See the table Codifica Tipo Transazione for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	timeStamp	Timestamp in milliseconds format	N MAX 8

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Extension Report

The interrogation API makes it possible to obtain a snapshot of the instalments associated with the booking.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/api/report-dilazione

URI
ecomm/api/vas/ig/reportDilazione

METHOD
Post

ACCEPT
Application/json

Initiation message

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codicePrenotazione	Unique booking code. If not populated, the value of the transaction code or the contract number will be used.	AN
✓	timeStamp	Timestamp in millisecond format	N 13 CRT
✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the “MAC Calculation” section at the end of this chapter	AN 40 CRT

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- apikey
- codicePrenotazione
- timeStamp
- chiaveSegreta

AN EXAMPLE OF THIS STRING MAY BE
MAC = HASH SHA1(apikey=<val>codicePrenotazione=<val>timeStamp=<val><chiaveSegreta>)

Positive Result message

Mandatory	Name	Description	Format
✓	esito	Transaction result (Possible values OK, KO, CANCELLATION and ERROR)	AN MAX 7
✓	idOperazione	Transaction ID assigned by Nexi	AN MIN 2 MAX 30
✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the “MAC Calculation” section at the end of this chapter	AN 40 CRT
✓	timeStamp	Timestamp in millisecond format	N MAX 8
✓	dilazioni	Object	

Extension object

Mandatory	Name	Description	Format
✓	numeroRata	Number of the instalment	N
✓	dataRata	Date of the instalment	DATE DD/MM/YYYY
✓	importoRata	Amount of the instalment	

✓	pagamentoInStruttura	Specifies whether the payment of the last instalment will be made at the facility. Possible values true or false	AN
✓	stato	Payment status. Possible values: - TO BE PAID -> payment of the instalment is scheduled - PAID -> the instalment was paid with a positive result - UNPAID -> payment of the instalment was unsuccessful - FACILITY -> the instalment will be paid at the facility - CANCELLED -> following booking cancellation/refund, the instalment will not be paid	AN
✓	origine	Payment origin. The possible values are: - BATCH -> Payment made by the batch - MERCHANT -> After an unpaid amount, the payment was made by the merchant in the back office - PAYMAIL -> After an unpaid amount, the payment was made by the cardholder via the link sent - PAYMENT -> Instalment paid via the disputeless payment flow, valid only for the first instalment which created the extensions.	AN
✓	dataPagamento	Date of payment	DATE MM/DD/YYYY HH:MM:SS

✓	codiceTransazione	Code associated with the transaction, represents the transaction which made the payment of the instalment	AN
✓	esitoPost	Sending of result via POST. Possible values TRUE or FALSE	

Negative Result message

Mandatory	Name	Description	Format
✓	esito	Transaction result	AN MAX 7 CRT
✓	idOperazione	Transaction ID assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Present only in the case of ko result. It is an object containing: code -> error code, see table message -> error detail	AN
✓	timeStamp	Timestamp in millisecond format	N 13 CRT
✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the “MAC Calculation” section at the end of this chapter	AN 40 CRT

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

AN EXAMPLE OF THIS STRING MAY BE
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Loading of booking data

Aside from the classic Payment call, it is possible to proceed with the booking in an alternative manner.
This METHOD makes it possible to precede the Payment with a dedicated call in which the parameters of the “Incasso Senza Pensieri” service are sent to the XPay gateway.
If the parameters are correct, the gateway will return a nonce with which to proceed with Payment.

Guaranteed booking

Reservation, through a card verification without charging the customer. In case the customer does not show up at the structure, you can charge the cost of the first night of stay.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento-api/prenotazione-garantita

URI
ecomm/api/vas/ig/creaNonce

METHOD
Post

ACCEPT
Application/json

Initiation Message Payment

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN2 MAX 30 CRT
✓	incassoGarantito	Object containing the necessary information to use	Object

		the service "Incasso senza Pensieri	
✓	timeStamp	Timestamp in milliseconds format	N13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object IncassoGarantito: required fields

Mandatory	Name	Description	Format
✓	tipoprenotazione	“GARANTITA”	
✓	codicestruttura	One of the structure codes recorded by back office manually or through the API censisciStruttura	MAX 100
✓	dataprenotazione	- Check-In/Start date of hire if dl_formatodata parameter is set to “PERIODO” - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with “SINGOLA” Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	importoNoShow	Penalty for non-cancellation, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N
✓	templateGarantita	Booking conditions GARANTITA, if not specified is the default set on the structure in the back office. Possible values:	AN

		- DATA -> will become mandatory “dataCancellazione” - ORA -> will become mandatory "oreCancellazione"	
	dataCancellazione	Date by which the customer can cancel the reservation.	DATA DD/MM/YYYY HH:MI
	oreCancellazione	Hours from CheckIn within which the customer can make the cancellation	N
	codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100 CRT
	flagFormatoData	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	N MAX 8 CRT
	dataFinePrenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	numeroNotti	Number of nights	N
	nomeIntestatario	Name of reservation holder	AN MAX 256
	cognomeIntestatario	Surname of reservation holder	AN MAX 256
	numeroOspiti	Number of guests staying in the structure	N

	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	idTermCond	Identifier of terms and conditions surveyed in the back office manually or via the caricaTermCond API	

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- tipoPrenotazione
- codicePrenotazione (if present in request)
- dataPrenotazione
- importoNoShow
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>tipoPrenotazione=<val>codicePrenotazione=<val>dataPrenotazione=<val>importoNoShow=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	nonce	Code assigned by XPay for use in the Payment request.	AN MAX 35 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details,	AN 40 CRT

	see the end of this chapter: MAC Calculation.

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message: required fields

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	importoNoShow	Importo penale in caso di mancata cancellazione, espresso in centesimi di euro senza separatore, i primi 2 numeri a destra rappresentano gli euro cent, es.: 5000 corrisponde a 50,00 €	

✓	dl_nonce	Nonce received by the API creaNonce	
✓	dl_importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN 40 CRT
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available	AN MAX 7

		languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user’s Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis	AN MAX 35

		of prior agreement with the same company.	
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.	

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- importoNoShow
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>importoNoShow=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_nonce
- importoNoShow
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>
dl_nonce=<val>importoNoShow=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications).
- For the use of the Incasso Senza Pensieri service through the Back Office API Request Pay-by-Link link, it is sufficient to enter amongst the additional parameters the “dl_nonce” field received from the “creaNonce” operation.

The management of the result, cancellation and notification does not change with respect to those of the Easy Payment solution. Refer to the corresponding sections to consult the returned parameters.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (update contract) to be used when updating a contract on the same card.	AN MAX 2

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
Per utilizzare questa modalità è necessario inviare il seguente parametro in fase di creazione nonce:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (update contract) to be used when updating a contract on the same card.	AN MAX 2

To make subsequent OneClick Payments, you must make a Payment request identical to the first Payment by passing the same “num_contratto” and enhancing the “ tipo_richiesta “ parameter with “PR”.

Guaranteed booking with penalty

Reservation by means of a card verification without charge to the customer. If the customer does not cancel the stay within the time stipulated in the terms and conditions, a penalty fee agreed upon at the time of booking will be charged.

Compared to the Guaranteed Reservation, it will not be necessary to use a dedicated API (no show) for the charge. XPay will do this automatically once the maximum cancellation period has expired.

It is important to note that the pre-agreed amount (penalty) will be charged in any case if the stay is not cancelled: this charge will be considered by the operator as a penalty if the customer does not show up at the property, or as a partial/total payment for the stay.

It is the responsibility of the operator, in case he receives the cancellation within the given booking deadline, to make the cancellation from the backoffice or call up the cancellation API.

This type of booking is not available for tour operators.

URI
ecomm/api/vas/ig/creaNonce

METHOD
Post

ACCEPT
Application/json

Initiation Message Payment

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN2 MAX 30 CRT
✓	incassoGarantito	Object containing the necessary information to use	Object

		the service "Incasso senza Pensieri	
✓	timeStamp	Timestamp in milliseconds format	N13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object IncassoGarantito: required fields

Mandatory	Name	Description	Format
✓	tipoprenotazione	“GARANTITAPENALE”	
✓	codicestruttura	One of the structure codes recorded by back office manually or through the API censisciStruttura	MAX 100
✓	dataprenotazione	- Check-In/Start date of hire if dl_formatodata parameter is set to “PERIODO” - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with “SINGOLA” Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
✓	importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	importoPenale	Penalty for non-cancellation, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N
✓	templateGarantita	Booking conditions GARANTITA, if not specified is the default set on the structure in the back office. Possible values:	AN

		- DATA -> will become mandatory “dataCancellazione” - ORA -> will become mandatory "oreCancellazione"	
	dataCancellazione	Date by which the customer can cancel the reservation.	DATA DD/MM/YYYY HH:MI
	oreCancellazione	Hours from CheckIn within which the customer can make the cancellation	N
	codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100 CRT
	flagFormatoData	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	N MAX 8 CRT
	dataFinePrenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	numeroNotti	Number of nights	N
	nomeIntestatario	Name of reservation holder	AN MAX 256
	cognomeIntestatario	Surname of reservation holder	AN MAX 256
	numeroOspiti	Number of guests staying in the structure	N

	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	idTermCond	Identifier of terms and conditions surveyed in the back office manually or via the caricaTermCond API	

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- tipoPrenotazione
- codicePrenotazione (if present in request)
- dataPrenotazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val> tipoPrenotazione=<val>codicePrenotazione=<val>dataPrenotazione=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	nonce	Code assigned by XPay for use in the Payment request.	AN MAX 35 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details,	AN 40 CRT

		see the end of this chapter: MAC Calculation.

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message: required fields

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_nonce	Nonce received by the API creaNonce	
✓	dl_importoprenotazione	Reservation amount, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N MAX 8 CRT

✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation “Incasso Senza Pensieri”.	AN 40 CRT
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the	AN MAX 2000 CHAR.

		type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user’s Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20

	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the value set in the XPay back office. Compatible with payment cards and PayPal.

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val>importoNoShow=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_nonce
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>
dl_nonce=<val>importoNoShow=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications).
- For the use of the Incasso Senza Pensieri service through the Back Office API Request Pay-by-Link link, it is sufficient to enter amongst the additional parameters the “dl_nonce” field received from the “creaNonce” operation.

The management of the result, cancellation and notification does not change with respect to those of the Easy Payment solution. Refer to the corresponding sections to consult the returned parameters.

Penalty Payment

When the cancellation deadline expires, XPay automatically charges the penalty fee. Charges are not made overnight, to avoid disturbing customers with outcome notifications during inappropriate hours.
Upon completion of the individual penalty payment, a POST notification will be sent to the 'urlpost' parameter if set during the booking process. Below is the data sent in the notification:

Mandatory	Name	Description	Format
	numeroMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30 CRT
	importo	Transaction amount taken from the payment initiation message	N MAX 8 CRT
	divisa	The code of the currency in which the amount is expressed (EUR = Euro)	AN 3 CRT
	data	Transaction date	yyyymmdd
	orario	Transaction hour	Hhmmss
	codTrans	Code associated with the payment taken from the payment initiation message	AN MIN 2 - MAX 30 CRT
	esito	Outcome of the operation. Possible values: - OK - KO	AN MAX 7 CRT
	codAut	Authorisation code assigned by the credit card issuer, present only with authorisation granted	AN MIN 2 MAX 6 CRT
	brand	Type of card used by the user to make the payment. Possible values are as shown in the table here	AN MAX 100 CRT
	tipoTransazione	Transaction type, indicates the method of payment, only value allowed NO_3DSECURE	AN
	mail	E-mail address of the person who made the payment	AN MAX 150 CRT

	messaggio	Report a brief description of the outcome of the payment. Possible values: - Transaction successful - Transaction not authorised	AN MAX 300 CRT
	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Excluding the + character and superscripts
	eventType	Type of event triggering the notification, only possible value: PENALE	AN
	dl_codiceprenotazione	Reservation code associated with the plan	AN
	mac	Message Code Authentication Transaction signature field. For the calculation, see the section 'MAC Calculation' at the end of this section.	AN 40 CRT

No outcome e-mails will be sent to the merchant or the end customer, even in the case of unsuccessful payment.

MAC Calculation

For the outcome message, the string to be signed must contain the fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

Prepaid Refundable

Booking with Payment in advance. It is possible to refund the amount in full or in part (depending on the Terms and Conditions defined by the operator) if the reservation is cancelled before the beginning of the stay.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento-api/prepagato-rimborsabile

URI
ecomm/api/vas/ig/creaNonce

METHOD
Post

ACCEPT
Application/json

Initiation Message Payment

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN2 MAX 30 CRT
✓	incassoGarantito	Object containing the necessary information to use the service "Incasso senza Pensieri	Oggetto
✓	timeStamp	Timestamp in milliseconds format	N13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object IncassoGarantito

Mandatory	Name	Description	Format
✓	tipoprenotazione	Valorise with "RIMBORSABILE"	
✓	codicestruttura	One of the structure codes recorded by back office manually or through the API censisciStruttura	MAX 100
✓	dataprenotazione	- Check-In/Start date of hire if dl_formatodata parameter is set to “PERIODO” - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with “SINGOLA” Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
	templateRimborsabile	Reservation conditions RIMBORSABILE, if not specified is the default set on the structure in the back office. Possible values: - DATA -> parameters "dataRimborsoTotale", "dataRimborsoParziale", "importoRimborsoParziale" will be mandatory - ORA -> "giorniRimborsoTotale", "giorniNessunRimborso", "giorniRimborsoParziale", "percentualeRimoborsoParziale" will be mandatory	AN
	giorniRimborsoTotale	Days from the beginning of the stay, within which the customer will receive a full refund in case of cancellation of the reservation	N MAX 3 CRT
	giorniNessunRimborso	Days from the start date of the stay, within which the customer **will not** receive a refund in case of cancellation of the reservation	N MAX 3 CRT

	giorniRimborsoParziale	Days from the start date of the stay, within which the customer can receive a partial refund in case of cancellation of the reservation.	N MAX 3 CRT
	percentualeRimoborsoParziale	Percent of the repayment amount in case of partial repayment	N MAX 10 CRT
	dataRimborsoTotale	Date and time by which the customer may receive a full refund in case of cancellation of the reservation.	DATA 15/01/2021 HH:MI
	dataRimborsoParziale	Days and time by which the customer may receive a partial refund in case of cancellation of the reservation.	DATA 15/01/2021 HH:MI
	importoRimborsoParziale	Amount, expressed in eurocents, of the partial refund	N
	dataFinePrenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	numeroNotti	Number of nights	N
	nomeIntestatario	Name of reservation holder	AN MAX 256
	cognomeIntestatario	Surname of reservation holder	AN MAX 256
	numeroOspiti	Number of guests staying in the structure	N
	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	idTermCond	Identifier of terms and conditions surveyed in the back office manually or via the caricaTermCond API	

	flagIncremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present the default of the structure indicated in the back office is considered	AN
	flagDelayCharge	If valorized with "true", on the reservation it will be possible to execute delay charge operations. If not present the default of the structure indicated in the back office is considered	AN
	tipoIncasso	Type of embedding. Possible values DIFFERITO o DILAZIONATO. For more information please refer to the section Incasso Differito e Dilazionato	AN
	importoPrenotazione	Amount of the reservation expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. The value must correspond to the total amount of the booking. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	AN
	numerorate	Number of instalments into which the payment is to be divided. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	N
	dilazioni	Object, inside object “incassoGarantito”, containing information on instalments in case of "tipoIncasso" valued with DILAZIONATO	Array

Object dilazioni

Mandatory	Name	Description	Format
✓	numeroRata	Instalment number	N
✓	dataRata	Installment date	DATA DD/MM/AAA
✓	importoRata	Instalment amount	N
✓	pagamentoInStruttura	Indicates whether the payment of the last instalment will take place in the structure. Possible values true or false	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- tipoPrenotazione
- codicePrenotazione (if present in request)
- dataPrenotazione
- idTermCond
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val> tipoPrenotazione=<val>codicePrenotazione=<val>dataPrenotazione=<val> timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	nonce	Code assigned by XPay for use in the Payment request.	AN MAX 35 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. The parameter must be set to the same amount as the first instalment and not to the value of the 'importoPrenotazione'.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_nonce	Nonce received by the API creaNonce	
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC	AN 40 CRT

		Calculation “Incasso Senza Pensieri”.	
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140

		instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the	

	value set in the XPay back office. Compatible with payment cards and PayPal.

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_nonce
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_nonce=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications).
- For the use of the Incasso Senza Pensieri service through the Back Office API Request Pay-by-Link link, it is sufficient to enter amongst the additional parameters the “dl_nonce” field received from the “creaNonce” operation.
- The codicePrenotazione (if indicated) or the codiceTransazione is used as a contract and must therefore be between 5 and 30 characters long.

The management of the result, cancellation and notification does not change with respect to those of the Easy Payment solution. Refer to the corresponding sections to consult the returned parameters.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”."	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (aggiorna contratto) da utilizzare quando si vuole aggiornare un contratto sulla medesima carta.	AN MAX 2
num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
Per utilizzare questa modalità è necessario inviare il seguente parametro in fase di creazione nonce:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: "paga_1click”.	AN MAX 30
✓	num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes
	gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized.	AN MIN 4 MAX 10

To make subsequent OneClick Payments, you must make a Payment request identical to the first Payment by passing the same “num_contratto” and enhancing the “ tipo_richiesta “ parameter with “PR”.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val> divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiaveSegreta>)

Prepaid Not Refundable

Booking with Payment in advance. It is not possible to make any kind of refund.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento-api/prepagato-non-rimborsabile

URI
ecomm/api/vas/ig/creaNonce

METHOD
Post

ACCEPT
Application/json

Initiation Message Payment

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN2 MAX 30 CRT
✓	incassoGarantito	Object containing the necessary information to use the service "Incasso senza Pensieri	Oggetto
✓	timeStamp	Timestamp in milliseconds format	N13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object IncassoGarantito

Mandatory	Name	Description	Format
✓	tipoprenotazione	Valorise with "NONRIMBORSABILE"	
✓	codicestruttura	One of the structure codes recorded by back office manually or through the API censisciStruttura	MAX 100
✓	dataprenotazione	- Check-In/Start date of hire if dl_formatodata parameter is set to “PERIODO” - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with “SINGOLA” Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
	codiceprenotazione	Unique code of the reservation. If not valorized, the value of the “codice transazione” or “numero contratto” will be used.	AN MAX 100 CRT
	flagFormatoData	- If valorized with "PERIODO" the format of the reservation date is interpreted as a period, the parameter "dl_datafineprenotazione" is therefore mandatory - If valorized with "SINGOLA", the booking format is interpreted as a single date. If not present, the default of the structure indicated in the back office is considered.	N MAX 8 CRT
	dataFinePrenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS

	numeroNotti	Number of nights	N
	nomeIntestatario	Name of reservation holder	AN MAX 256
	cognomeIntestatario	Surname of reservation holder	AN MAX 256
	numeroOspiti	Number of guests staying in the structure	N
	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	idTermCond	Identifier of terms and conditions surveyed in the back office manually or via the caricaTermCond API	
	flagIncremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present the default of the structure indicated in the back office is considered	AN
	flagDelayCharge	If valorized with "true", on the reservation it will be possible to execute delay charge operations. If not present the default of the structure indicated in the back office is considered	AN
	tipoIncasso	Type of embedding. Possible values DIFFERITO o DILAZIONATO. For more information please refer to the section Incasso Differito e Dilazionato	AN
	importoPrenotazione	Amount of the reservation expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. The value must correspond	AN

		to the total amount of the booking. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	
	numerorate	Number of instalments into which the payment is to be divided. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	N
	dilazioni	Object, inside object “incassoGarantito”, containing information on instalments in case of "tipoIncasso" valued with	Array

Object dilazioni

Obbligatorio	Nome	Descrizione	Formato
✓	numeroRata	Instalment number	N
✓	dataRata	Installment date	DATA DD/MM/AAA
✓	importoRata	Instalment amount	N
✓	pagamentoInStruttura	Indicates whether the payment of the last instalment will take place in the structure. Possible values true or false	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- tipoPrenotazione
- codicePrenotazione (if present in request)
- dataPrenotazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val>
tipoPrenotazione=<val>codicePrenotazione=<val>dataPrenotazione=<val>
timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	nonce	Code assigned by XPay for use in the Payment request.	AN MAX 35 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message: required fields

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. The parameter must be set to the same amount as the first instalment and not to the value of the 'importoPrenotazione'.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_nonce	Nonce received by the API creaNonce	
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC	AN 40 CRT

		Calculation “Incasso Senza Pensieri”.	
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140

		instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the	

	value set in the XPay back office. Compatible with payment cards and PayPal.

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_nonce
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>dl_nonce=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications).
- For the use of the Incasso Senza Pensieri service through the Back Office API Request Pay-by-Link link, it is sufficient to enter amongst the additional parameters the “dl_nonce” field received from the “creaNonce” operation.
- - The codicePrenotazione (if indicated) or the codiceTransazione is used as a contract and must therefore be between 5 and 30 characters long.

The management of the result, cancellation and notification does not change with respect to those of the Easy Payment solution. Refer to the corresponding sections to consult the returned parameters.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Mandatory	Name	Description	Format
✓	flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
✓	tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (aggiorna contratto) da utilizzare quando si vuole aggiornare un contratto sulla medesima carta.	AN MAX 2
✓	num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
Per utilizzare questa modalità è necessario inviare il seguente parametro in fase di creazione nonce:

Mandatory	Name	Description	Format
✓	flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30
✓	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MAX 2
	gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized.	AN MIN 4 MAX 10

To make subsequent OneClick Payments, you must make a Payment request identical to the first Payment by passing the same “num_contratto” and enhancing the “ tipo_richiesta “ parameter with “PR”.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val> divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiaveSegreta>)

Bundle

Type of reservation dedicated to tour operators.

GitHub XPay sample code:
https://github.com/NexiPayments/XPay/tree/master/incasso-senza-pensieri/pagamento-api/prepagato-rimborsabile

URI
ecomm/api/vas/ig/creaNonce

METHOD
Post

ACCEPT
Application/json

Initiation Message Payment

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	apikey	Alias assigned by Nexi to the merchant	AN MAX 30 CRT
✓	codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN2 MAX 30 CRT
✓	incassoGarantito	Object containing the necessary information to use the service "Incasso senza Pensieri	Oggetto
✓	timeStamp	Timestamp in milliseconds format	N13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Object IncassoGarantito

Mandatory	Name	Description	Format
✓	tipoprenotazione	Valorise with "PACCHETTO"	
✓	codicestruttura	One of the structure codes recorded by back office manually or through the API censisciStruttura	MAX 100
✓	dataprenotazione	- Check-In/Start date of hire if dl_formatodata parameter is set to “PERIODO” - Date of the single day of stay/rental if the dl_formatodata parameter is valorized with “SINGOLA” Hours, minutes, seconds are optional.	DATA MAX 19 DD/MM/YYYY HH24:MI:SS
	templateRimborsabile	Reservation conditions for RIMBORSABILE and TOUR OPERATOR, if not specified is the default set on the structure in the back office. Possible values: - DATA -> parameters "dataRimborsoTotale", "dataRimborsoParziale", "importoRimborsoParziale" will be mandatory - ORA -> "giorniRimborsoTotale", "giorniNessunRimborso", "giorniRimborsoParziale", "percentualeRimoborsoParziale" will be mandatory	AN
	giorniRimborsoTotale	Days from the beginning of the stay, within which the customer will receive a full refund in case of cancellation of the reservation	N MAX 3 CRT
	giorniNessunRimborso	Days from the start date of the stay, within which the customer **will not** receive a refund in case of cancellation of the reservation	N MAX 3 CRT

	giorniRimborsoParziale	Days from the start date of the stay, within which the customer can receive a partial refund in case of cancellation of the reservation.	N MAX 3 CRT
	percentualeRimoborsoParziale	Percent of the repayment amount in case of partial repayment	N MAX 10 CRT
	dataRimborsoTotale	Date and time by which the customer may receive a full refund in case of cancellation of the reservation.	DATA 15/01/2021 HH:MI
	dataRimborsoParziale	Days and time by which the customer may receive a partial refund in case of cancellation of the reservation.	DATA 15/01/2021 HH:MI
	importoRimborsoParziale	Amount, expressed in eurocents, of the partial refund	N
	dataFinePrenotazione	Check-out Date. It will be used in the back office to search by reservation date. The hours part is optional. The parameter is mandatory if requested as dl_formatodata is “PERIODO”	AN MAX 19 DD/MM/YYYY HH24:MI:SS
	numeroNotti	Number of nights	N
	nomeIntestatario	Name of reservation holder	AN MAX 256
	cognomeIntestatario	Surname of reservation holder	AN MAX 256
	numeroOspiti	Number of guests staying in the structure	N
	datiOspiti	In this array of strings you can enter customer data, such as first and last name	Array
	idTermCond	Identifier of terms and conditions surveyed in the back office manually or via the caricaTermCond API	

	flagIncremental	If valorized with "true", on the reservation it will be possible to execute incremental operations. If not present the default of the structure indicated in the back office is considered	AN
	flagDelayCharge	If valorized with "true", on the reservation it will be possible to execute delay charge operations. If not present the default of the structure indicated in the back office is considered	AN
	tipoIncasso	Type of embedding. Possible values DIFFERITO o DILAZIONATO. For more information please refer to the section Incasso Differito e Dilazionato	AN
	importoPrenotazione	Amount of the reservation expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to €50.00. The value must correspond to the total amount of the booking. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	AN
	numerorate	Number of instalments into which the payment is to be divided. The parameter becomes mandatory if tipoIncasso=DILAZIONATO	N
	dilazioni	Object, inside object “incassoGarantito”, containing information on instalments in case of "tipoIncasso" valued with DILAZIONATO	Array

Object dilazioni

Mandatory	Name	Description	Format
✓	numeroRata	Instalment number	N
✓	dataRata	Installment date	DATA DD/MM/AAA
✓	importoRata	Instalment amount	N
✓	pagamentoInStruttura	Indicates whether the payment of the last instalment will take place in the structure. Possible values true or false	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- codiceTransazione
- tipoPrenotazione
- codicePrenotazione (if present in request)
- dataPrenotazione
- idTermCond
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>codiceTransazione=<val> tipoPrenotazione=<val>codicePrenotazione=<val>dataPrenotazione=<val> timeStamp=<val><chiaveSegreta>)

Positive Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result (Possible values OK, KO, ANNULLO e ERRORE)	AN MAX 7
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	nonce	Code assigned by XPay for use in the Payment request.	AN MAX 35 CRT
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Negative Results Message

Mandatory	Name	Description	Format
✓	esito	Operation result	AN MAX 7 CRT
✓	idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
✓	errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
✓	timeStamp	Timestamp in milliseconds format	N 13 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>xpayNonce=<val>timeStamp=<val><chiaveSegreta>)

Payment

Set up a POST request (the GET method is deprecated) with the format of a form submission at the address:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/DispatcherIG

Payment Initiation Message

This table shows required fields that have to be entered through a POST with the format of a form submission, into a redirect URL and their features

Mandatory	Name	Description	Format
✓	alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CRT
✓	importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents. The parameter must be set to the same amount as the first instalment and not to the value of the 'importoPrenotazione'.	N MAX 8 CRT
✓	divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CRT
✓	codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same	AN MIN 2 - MAX 30 CHAR. In case of MyBank you can only use: / - : ( ) . , +

		transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	
✓	url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CRT
✓	url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR). For detailed information on the parameters received, please refer to the Cancellation section.	AN MAX 200 CRT
✓	mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
✓	dl_nonce	Nonce received by the API creaNonce	
✓	dl_mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC	AN 40 CRT

		Calculation “Incasso Senza Pensieri”.	
	urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500
	mail	Customer email	AN MAX 150
	languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7
	descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140

		instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
	Note1	Field in which the merchant can report information about the order.	AN MAX 200
	Note2	Field in which the merchant can report information about the order.	AN MAX 200
	Note3	Field in which the merchant can report information about the order.	AN MAX 200
	OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN MAX 16
	infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35
	infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20
	xpayTimeout	Payment timeout, valued with the seconds of validity of the Payment session. The parameter overwrites the	

	value set in the XPay back office. Compatible with payment cards and PayPal.

N additional parameters can be specified that will be returned in the result message and notification message. There is no limit to the number of additional parameters but the overall length of the string consisting of the parameter names and their value must not exceed 4000 characters. Avoid the following parameter names because they are already used by XPay:TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NOME, $COGNOME, EMAIL

3D Secure 2.2

If you want to manage the 3D Secure 2.2 protocol, refer to the 3D Secure Management section **3D Secure 2.2**

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><chiaveSegreta>)

MAC Calculation “Incasso Senza Pensieri”

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- dl_nonce
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>dl_nonce=<val><chiaveSegreta>)

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards
- Parameters related to the working framework must not be sent (eg VIEWSTATE for ASP.NET applications).
- For the use of the Incasso Senza Pensieri service through the Back Office API Request Pay-by-Link link, it is sufficient to enter amongst the additional parameters the “dl_nonce” field received from the “creaNonce” operation.
- The codicePrenotazione (if indicated) or the codiceTransazione is used as a contract and must therefore be between 5 and 30 characters long.

The management of the result, cancellation and notification does not change with respect to those of the Easy Payment solution. Refer to the corresponding sections to consult the returned parameters.

Recurring Payment

The integration of this solution allows the merchant to tokenize the customer's card data, so they can make recurrences for services such as **subscriptions**.
To use this mode it is necessary to send the following parameters during the first Payment:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_multi”."	AN MAX 30
tipo_richiesta	- PP (first Payment) used for first paymens - RC (card renewal) used for update a card already associated with a contract - AC (aggiorna contratto) da utilizzare quando si vuole aggiornare un contratto sulla medesima carta.	AN MAX 2
num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes

For Subsequent Payment refer to the section **Pagamenti Successivi**

OneClick Payment

The integration of this solution allows the end customer to store the data of their credit card and use them later to make purchases with a few clicks.
Per utilizzare questa modalità è necessario inviare il seguente parametro in fase di creazione nonce:

Name	Description	Format
flagTokenizzazione	Valorise with"true"	AN

And send the following parameters when making the first payment:

Mandatory	Name	Description	Format
✓	tipo_servizio	The field must be set to: "paga_1click”.	AN MAX 30
✓	num_contratto	Unique code assigned by the merchant for the link with the archive containing the sensitive data of the credit card	AN MIN 5 MAX 30 Except the “+” character and the quotes
	gruppo	Code assigned by Nexi during activation. If it has not been provided during the activation phase, the field must not be valorized.	AN MIN 4 MAX 10

To make subsequent OneClick Payments, you must make a Payment request identical to the first Payment by passing the same “num_contratto” and enhancing the “ tipo_richiesta “ parameter with “PR”.

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- gruppo
- num_contratto
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val> divisa=<val>importo=<val>gruppo=<val>num_contratto=<val><chiaveSegreta>)

Deferred and Extended Collection

For refundable and non-refundable bookings made using credit cards, it is possible to select between deferred or extended collection through the “tipoIncasso” parameter populated with “DIFFERITO” or “DILAZIONATO”.

The “tipoIncasso” field is not mandatory and, if not specified, the transaction will be managed following the terminal configurations.

Deferred collection

This function is available for refundable and non-refundable bookings.

When deciding to make a booking through deferred collection, a pre-authorisation is made and the transaction will have a duration of 28 days, after which time it will be cancelled.

Deferred collection maintains the current booking settings in terms of communication and terms and conditions.

Using the deferred collection type, the booking is by default enabled for the possibility of incremental transactions, provided this is supported by the circuit rules.

When the merchant cancels or refunds a booking with deferred collection, an email will be sent to the cardholder indicating that the pre-authorisation has been cancelled. If the cancelled transaction is also multi-currency, the multi-currency cancellation/refund email will also be sent.

Two days before the expiry of the pre-authorisation, XPay will send an email to the merchant with the booking data to indicate the imminent expiry.
The email address at which the merchant will receive the notice is the email associated with the transaction code facility.

Extended collection

This function is available for refundable and non-refundable bookings.

By selecting extended collection, the merchant may indicate the extensions into which to break down the payment of the total amount of the booking.

Selection of the extended collection type requires the merchant to necessarily specify the total amount of the booking and from 2 to 12 instalments across which to break down the payment.

The instalments must meet the following conditions:

- the first instalment must have the amount equal to the amount of the transaction
- the date of the first instalment does not need to be indicated, even if present, the date of payment made by the cardholder will be considered
- the sum of the instalments must correspond to the total amount of the booking
- an instalment payment date prior to the current date cannot be specified, and each instalment must be subsequent to the previous one
- the instalments must be indicated in order of payment date
- the date of the last instalment cannot be subsequent to the booking start date
- the last instalment may be indicated as to be paid in the facility
- in the case of Pay-by-Link, the second instalment must be subsequent to the expiry of the link

When paying for a booking with future extensions, a contract will be created associated with the card used by the user at the time of payment, to be used for the payment of the instalments.

If not specified otherwise by the merchant in the call with the tipo_richiesta and tipo_servizio parameters, the contract cannot be used to make different recurring payments other than the payment of the instalments.

After the instalment plan is activated, each instalment will be paid by automatic XPay procedures at the planned date. On a daily basis, these procedures select the instalments to be paid on that day with the exclusion of plans for which there was previously an unpaid amount.

After payment of the individual instalment, a notification will be sent by post, to the “urlpost” parameter of the first instalment payment, to the merchant to report the payment made and its result. The fields sent in the notification are listed below:

Mandatory	Name	Description	Format
✓	numeroMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
✓	importo	Amount of the instalment for which the payment was made	N
✓	divisa	The code of the currency in which the amount is expressed. Only value permitted: EUR (Euro)	AN MAX 3
✓	data	Date of the transaction	DATE yyyymmdd
✓	orario	Time of the transaction	AN hhmmss
✓	codTrans	Payment identification code consisting of alphanumeric characters	AN
✓	esito	Transaction result	AN MAX 2
✓	codAut	Authorisation code assigned by the credit card issuer, present only with authorisation granted	AN MIN 2 MAX 6
✓	brand	Type of card used by the user to make the payment. The possible values are those reported in the Card type coding table.	AN MAX 100
✓	tipoTransazione	Type of transaction, indicates the manner with which the payment was made, only value permitted NO_3DSECURE	AN
✓	mail	The email address of the buyer to which to send the payment result	AN MAX 150
✓	messaggio	Provides a brief description of the payment result. The possible values are those reported in the Result coding table.	AN

✓	mac	Message Code Authentication Transaction signature field. For the calculation, see the “MAC Calculation” section at the end of this chapter	AN 40
✓	TCONTAB	The field identifies the collection mode that the merchant wants to apply to the individual transaction, only value permitted: - I (immediate) the transaction if authorised is also collected without further intervention by the merchant.	AN
✓	num_contratto	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 5 MAX 30 Excluding + character and superscripts
✓	eventType	Type of event that triggered the notification, only possible value: DILAZIONE	AN
✓	dl_codiceprenotazione	Code of the booking associated with the plan	AN
✓	dl_numerorata	Number of the instalment paid	N

If the notification fails, XPay will not cancel the transaction.

MAC Calculation

For the result message, the string to sign must contain the fields:

- codTrans
- esito
- importo
- divisa
- data
- orario
- codAut
- chiave segreta

AN EXAMPLE OF THIS STRING MAY BE

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codAut=<val><chiaveSegreta>)

A notification email will also be sent to the cardholder based on the payment result.
In the case of an OK result, the email will contain confirmation of the advance payment.
In the case of KO, an email will be sent containing a link to proceed with payment within 48 hours, with the possibility to change the card used.

Lastly, the instalment will be updated with details of the payment just made, setting it as PAID or UNPAID.

After payment of all instalments for the day, all instalments for which a previous unpaid amount has not yet been paid will be marked as unpaid.

The payment of the unpaid amount, aside from being made by the cardholder using the Pay-by-Link link received, may also be requested directly by the merchant using the dedicated function present in the details of the booking in the back office.

Instalment payment prior notice email

Also through automatic procedures, emails providing prior notice of instalment payment and of the imminent deadline of the full refund of a booking will be sent. The days of prior notice will be specified by the merchant in the facility configuration, the default will be 2.

If the card saved for the contract has expired when the instalment is to be paid, a Pay-by-Link link will be added so that the card can be renewed.

Email providing notification of the full refund deadline:

For refundable bookings, n days (by default 2) before the deadline for full refund, an email will be sent to cardholders to remind them of the refund deadline.

Management of Refunds on extended collection:

By performing a cancellation or refund (partial or total), all instalments still to be paid associated with the extension plan will be cancelled.

Furthermore, in the case of a refundable booking, if the transaction is prior to the total refund date/days, all of the instalments already paid will be cancelled/refunded, depending on the status of the individual transaction.

If the refund takes place during the partial refund period, only the instalments up to the amount of the partial refund or the percentage of the amount already paid will be cancelled.

If the refund of an instalment fails, the merchant will be responsible for providing the refund from the back office.

Irrespective of the type of booking and the cancellation periods specified in the terms and conditions, the merchant will be free to manually refund the individual instalments paid, even beyond the terms specified.

It is not possible to cancel a specific instalment without first collecting it.

EVOLVED TOKENIZATION

The MasterCard MDES for merchants and Visa VTS services work alongside the current XPay tokenization system with no technical impacts for merchants, but with the enhancement of value added services that the merchant may add.

Notifications

Status change notification

This service makes it possible to receive a notification on “contracts” (num_contratto associated with the tokenized card) which experience changes/revocations by the card circuit, to ensure that the merchant can update and intervene with its own customer.

It is possible to set the address for receiving notifications on changes of token status in the Nexi back office.

The composition of the JSON message is described below, containing the data of the contracts impacted by any changes:

Name	Description	Format
terminalId	ID of the tokenization terminal	N
timeStamp	Timestamp in milliseconds format	N 13 CRT
contracts	Arrays whose structure is defined in the following table.	Array
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Oggetto contracts:

Name	Description	Format
contractNumber	contract number	AN
tokenizationMode	Type of tokenization done, possible values are: • XPAY • VTSM • MDES	AN
eventType	Type of event that triggered the notification, the possible values are: • CONFIG-CHANGE ⌊ change of card metadata, requires the re-download of the graphic asset • CARD-CHANGE ⌊ change of card data (card renewal or change) • ACTIVATION ⌊ activation of a new token/reactivation of a token suspended previously • DEACTIVATION ⌊ deactivation of a token (cancellation) • SUSPENSION ⌊ temporary suspension of the token (may be reactivated)	AN

MAC Calculation

The MAC is calculated by performing the SHA-1 operation of the concatenation of all of the values returned, if the property is absent, a value of ““ (empty string) is assumed, according to this scheme:

MAC = terminalId + timestamp;
for each contracts (
    MAC += contractNumber + tokenizationMode + eventType;
)
MAC += stringaSegretaMerchant;
MAC = SHA-1(MAC);

Tokenization notification

After the first Payment, the contract is regularly tokenized on XPay and, at the same time, a “circuit tokenization” attempt is scheduled.

The circuit tokenization is therefore asynchronous with respect to the Payment flow, its results are sent to merchants by means of a notification identical to that described in the section of the previous paragraph.

NOTES:

- Tokenisation notifications do not need to be responded to with an HTTP status code 200: XPay does not perform notification retry or transaction cancellation procedures as it does for payments.

  - Esempio 1 { "timeStamp": "1669590135419", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_6383ec000b4dc", "tokenizationMode": "VTSM", "eventType": "ACTIVATION" }], "MAC": "7b5baf3943b96223eaf3788f93be33fc53bf540f" }
  - Esempio 2 { "timeStamp": "1669600350793", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_6144d2f616419", "tokenizationMode": "MDES", "eventType": "CONFIG-CHANGE" }, { "contractNumber": "nexi_6144d2f616419", "tokenizationMode": "MDES", "eventType": "CARD-CHANGE" }], "MAC": "2e2bb92f680549a8565f32e9f961c9aa91f796fa" }
  - Esempio 3 { "timeStamp": "1669618242781", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_6245b8d899239", "tokenizationMode": "VTSM", "eventType": "CARD-CHANGE" }], "MAC": "53254d34bd1bcb3f858ea84220fe5cf9975a201a" }
  - Esempio 4 { "timeStamp": "1669602267024", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_61c3061c899a0", "tokenizationMode": "MDES", "eventType": "SUSPENSION" }], "MAC": "6f0b854512083e481b7c0a496afb66e21ab342d9" }
  - Esempio 5 { "timeStamp": "1669604879054", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_5fafb847102f8", "tokenizationMode": "MDES", "eventType": "DEACTIVATION" }], "MAC": "97a780cd6d4a7176450ca63fd516b5235c611d99" }
  - Esempio 6 { "timeStamp": "1669631067790", "terminalId": "00002830", "contracts": [{ "contractNumber": "nexi_63848c01914d8", "tokenizationMode": "MDES", "eventType": "ACTIVATION" }, { "contractNumber": "nexi_63848c1684e3a", "tokenizationMode": "VTSM", "eventType": "ACTIVATION" }, { "contractNumber": "nexi_63848c23dc19a", "tokenizationMode": "MDES", "eventType": "ACTIVATION" }], "MAC": "fc3d05fb6274bb25b9a2655595b96326dcab36f0" }

Tokenization details

URI
ecomm/api/vas/ig/tokenizationInfo

METHOD
Post

ACCEPT
Application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned by Nexi to the merchant	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>timeStamp=<val><chiaveSegreta>)

Positive Results Message

Name	Description	Format
esito	Operation result (Possible values OK, KO)	AN MAX 2
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
codiceGruppo	Code assigned by Nexi during activation. If not provided during activation, the field should not be valorized.	AN MIN 4 MAX 10
datiToken	Object containing information about the token.	Object

Object: datiToken

Name	Description	Format
tokenType	Type of tokenization made, the possible values are: • XPAY -> normal XPay tokenization, recurring transactions are carried out with real card data • VTSM -> tokenized contract on VTS, recurring transactions are carried out with the token provided by VISA • MDES -> tokenized contract on MDES, recurring transactions are carried out with the token provided by MASTERCARD	AN
status	Indicates the status of the transaction, the possible values are: • APPROVED: only for MDES token, represents a token created, but still not active in MDES systems, therefore unusable • ACTIVE: active and usable token • DEACTIVATED: token cancelled on a definitive basis • SUSPENDED: token temporarily suspended	AN
brand	Type of card used by the user to make Payment. The possible values are shown in the table Codifica tipo carta	AN MAX 100
panLast4	Last 4 characters of PAN	N MAX 4
panExpiry	Card Expiration	DATA yyyyMM
tokenExpiry	If tokenized VTS or MDES, it represents the token expiry provided by the circuit	DATA
cardArt	String encoded in base64 which contains the image in PNG Format of the cardart. If the card-art is not provided by the circuit, a NEXI template is used	AN
foregroundColor	colour to be used for any writing on the card-art is specified by the circuit, for NEXI templates black is used (“ffffff”)	AN

PaymentAccountReference	If VTS or MDES tokenized, represents the PAR of the token (the PAR is the key that the circuits use to “group” all of the tokens of the same card	AN
hashPan	hashPan to be verified for association	N

Negative Results Message

Name	Description	Format
esito	Operation result	AN MAX 7 CRT
idOperazione	Transaction identifier assigned by Nexi	AN MIN 2 MAX 30
errore	Only present when the result is ko. It is an object containing: codice -> error code, see Table messaggio > error details	AN
timeStamp	Timestamp in milliseconds format	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

ADDITIONAL SERVICES

Contract Management

This section contains the specifications of the API dedicated to the management of contracts registered on the XPay gateway.
The term "contract" refers to the token that XPay uses to associate the card details of a customer, which is necessary to make subsequent recurring or OneClick payments.
Below is the list of APIs made available by XPay for managing contracts:

- Loading Contracts from POS transaction
- Contract cancellation
- Contract disabling
- Contract enabling
- Contract query
- Contract details
- Contract status

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/altri-servizi**

The environment endpoints are as follows:

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it

The individual URIs and messages for each of the available services are described below.

Loading Contracts from POS Transactions

This service allows contracts to be loaded for recurring or Card on File Payments, beginning with a card Payment transaction made using a POS.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/caricamento-contratto-da-transazione-pos

URI
ecomm/api/contratti/creazioneDaPosFisico

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
contratto	Contract object whose structure is shown in the following table.	AN

Contract element: required fields

Name	Description	Format
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
idPOSFisico	Identifier of the terminal where the transaction was made.	N MAX 8 CHAR.
codiceAutorizzazione	Confirmation code issued by the card issuer.	AN MAX 6 CHAR.
importo	Amount authorised by physical POS expressed in euro cents without separator, the first 2 numbers on the right represent euro cents, e.g.: 5000 corresponds to 50.00 €	N MAX 8 CHAR.
dataTransazione	Transaction date. If you don’t have second, enter “00”	DATA dd/MM/yyyy HH:mm:ss

Contract element: optional fields

Name	Description	Format
stan	Optional code received from the physical POS.	AN MAX 6 CHAR.
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
mail	Buyer’s email address to which the Payment result will be sent.	AN MAX 150 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- idPOSFisico
- codiceAutorizzazione
- stan
- importo
- descrizione
- mail
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>idPOSFisico=<val>codiceAutorizzazione=<val>stan=<val>importo=<val>descrizione=<val>mail=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Contract Cancellation

This service allows merchants who have enabled recurring, OneClickPay/Card on File Payment management to delete the contract codes that are linked to user's cards.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/cancellazione-contratto**

URI
ecomm/api/contratti/cancellaContratto

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apikey=<val>numeroContratto=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Contract Disabling

This service allows merchants who have enabled recurring, OneClickPay/Card on File Payment management to disable the contracts linked to user's cards. A contract in disabled status can be restored - it only suspends the ability to make transactions.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/disabilita-contratto

URI
ecomm/api/contratti/disabilitaContratto

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Contract Enabling

This service allows merchants who have enabled recurring, OneClickPay/Card on File Payment management to enable contracts which were previously disabled.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/abilita-contratto

URI
ecomm/api/contratti/abilitaContratto

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Contract Query

This service allows contracts registered for Recurring, OneClickPay/Card on File services to be queried by using filter criteria.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/elenco-contratti

URI
ecomm/api/contratti/queryContratti

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
codiceFiscale	User Tax Code. Optional.	AN MAX 16 CHAR.
dataRegistrazioneDa	Search by date from	AN dd/mm/yyyy hh:mm:ss
dataRegistrazioneA	Search by date to	AN dd/mm/yyyy hh:mm:ss

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceFiscale
- dataRegistrazioneDa
- dataRegistrazioenA
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceFiscale=<val>dataRegistrazioneDa=<val>dataRegistrazioneA=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
contratti	Contracts object whose structure is shown in the following table.	AN

Contracts element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
Searches are made using the parameters " numeroContratto ", " codiceFiscale ", " dataRegistrazioneDa ", and " dataRegistrazioneA ". At least one of these parameters needs to be populated in order to run a search. In the case of the nContract, the wildcard % can be used to represent one or more characters.

Contract Details

This service allows to run queries in a timely fashion for contracts registered for Recurring, OneClickPay/Card on File services, and to obtain detailed information about them.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-contratti/dettagli-contratto

URI
ecomm/api/contratti/dettagliContratto

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
codiceFiscale	User Tax Code. Optional.	AN MAX 16 CHAR.
dataRegistrazioneDa	Search by date from	AN dd/mm/yyyy hh:mm:ss
dataRegistrazioneA	Search by date to	AN dd/mm/yyyy hh:mm:ss

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceFiscale
- dataRegistrazioneDa
- dataRegistrazioenA
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>codiceFiscale=<val>dataRegistrazioneDa=<val>dataRegistrazioneA=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
contratti	Contracts object whose structure is as defined in the following table.	AN

Contracts element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30 CHAR.
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 - MAX 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
dataAttivazione	Contract activation date	AN dd/mm/yyyy hh:mm:ss
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 - MAX 30 CHAR.
codiceFiscale	User Tax Code. Optional.	AN MAX 16 CHAR.
hashPan	hashPan to be verified for association.	AN
tipoCarta	Type of card used	AN
statoPrimoPag	First Payment status	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
Searches are made using the parameters "numeroContratto", "codiceFiscale", "dataRegistrazioneDa", and "dataRegistrazioneA". At least one of these parameters needs to be populated in order to run a search. In the case of the nContract, the wildcard % can be used to represent one or more characters.

Contract Status

It allows to query the collection of contracts registered on the terminal or, if the terminal belongs to a recurring group, to the whole group.

The search is performed on the parameters “numeroContratto”, “codiceFiscale”, “dataRegistrazioneDa”, ”dataRegistrazioneA”, “dataAggiornamentoDa”, “dataAggiornamentoA”, “statoAggiornamento”. At least one of these must be evaluated in order to carry out the search. In the case of the numeroContratto, the general character% can be entered to indicate any characters.

The selection criteria related to updates work on the date of the last update of the card data, which can be modified either by back office, or by Payment or by automatic circuit procedures.

If the contract has never been updated, the activation date is used, otherwise, the date on which the card data was actually changed is indicated and the channel of the last update is indicated (BACK OFFICE, PAYMENT, CIRCUITS), in case of "no update", the channel is set to ND

In the card data, if available, the PAN hash is indicated, with its hashing algorithm. Generally XPay calculates the pan HASH during tokenization, in the case of manual uploads or channels that do not include pan hashing, the property is returned as "N.D.". It will be evaluated with the first recurrence made on the contract.

The state property of the data object Carta instead allows you to understand if the PAN has actually been "aligned" by the circuit, in particular the allowed values are:

- VALIDO - The pan has been correctly aligned by the circuit
- BLOCCATO - The pan has been signaled as "blocked" by the circuit
- NON_TROVATO - The circuit did not find information on the PAN
- NON_PARTECIPANTE - PAN is not sent to the circuit for alignment

The updateChannel property indicates through which of the update methods the last modification of the card data took place, in particular:

- N.D. - Not available / Never Updated (new / never updated contracts)
- BACK OFFICE - Card Data manually edited via back office application
- PAYMENT - Card data modified through a particular Payment anniversary
- CIRCUITI - Card data automatically modified following interaction with the circuits (Optional: if the operator signs the service)

URI
ecomm/api/contratti/statoContratti

METHOD
POST

ACCEPT
application/json

Initiation Message: required fileds

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used (also partial %=each character)	AN MIN 5 MAX 30
timeStamp	Transaction identifier assigned by the merchant.	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

Initiation Message: optional fileds

Name	Description	Format
codiceFiscale	User cf	AN MAX 16 CRT
dataRegistrazioneDa	Search by date from	AN gg/mm/aaaa hh:mm:ss
dataRegistrazioneA	Search by date to	AN gg/mm/aaaa hh:mm:ss
dataAggiornamentoDa	Search for update date from	AN gg/mm/aaaa hh:mm:ss
dataAggiornamentoA	Search for update date to	AN gg/mm/aaaa hh:mm:ss
statoAggiornamento	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- apiKey
- numeroContratto
- codiceFiscale
- dataRegistrazioneDa
- dataRegistrazioneA
- dataAggiornamentoDa
- dataAggiornamentoA
- statoAggiornamento
- timeStamp
- chiaveSegreta

SAMPLE STRING
MAC = HASH SHA1(apiKey=<valore>numeroContratto=<val>codiceFiscale=<val>dataRegistrazioneDa=<val>dataRegistrazioneA=<val>dataAggiornamentoDa=<val>dataAggiornamentoA=<val>statoAggiornamento=<val>timeStamp=<val><chiaveSegreta>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 MAX 30
listaContratti	Arrays whose structure is defined in the following table	Array

listaContratti Element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30
numeroContratto	Code allowing Nexi to save a paired link between the user and the Payment card used.	AN MIN 5 MAX 30
codiceGruppo	Code assigned by Nexi during activation	AN MIN 4 MAX 10
dataAttivazione	Contract activation date	DATA

codTrans	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30 Escluso carattere _
codiceFiscale	User CF	AN MAX 16
hashPan	hashPan to be verified for association.	AN
tipoCarta	Type of card used	AN
statoPrimoPag	First Payment status	AN
timeStamp	Timestamp in millisecond format.	N 13 CRT
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT
dettagliCarta	Object whose structure is shown in the following table	JSON

dettagliCarta Element

Name	Description	Format
maskedPan	Masked pan of used card	AN
expiry	Expiring date	DATA aaaamm
hashPan	hashPan to be verified for association.	AN
hashAlg	Algorithm used	AN
updateTime	Date of last update of the card data	DATA
updateChannel	"N.D." "BACK OFFICE" "PAYMENT" "CIRCUITI"	AN
state	"BLOCCATO" "NON_TROVATO" "VALIDO" "NON_PARTECIPANTE"	AN

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(esito=<valore>idOperazione=<val>timeStamp=<val><chiaveSegreta>)

Control Management

This section contains the specifications of the APIs dedicated to blacklist management and to matching the customer's tax code and the hash of the card pan.
Below is the list of APIs made available by XPay for contract management:

- Adding to blackList
- Cancellation from blacklist
- Checkin existence in blacklist
- Blacklist
- Verification of Tax Code/Pan pairing
- Removing Tax Code/Pan pairing
- List of associated Tax Code/Pan pairing

Adding to Blacklist

This service adds Tax Codes or contract codes to the blacklist.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/inserimento-in-blacklist

URI
ecomm/api/blacklist/aggiungi

METHOD
POST

ACCEPT
application/json

Initiation Message: required fields

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipo	Type of search - either by Tax Code (CodiceFiscale) or contract code associated with the user (CodiceContratto)	AN MIN 2 - MAX 30 CHAR.
valore	Depending on the type of search, enter either the Tax Code or the contract code.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

Initiation Message: optional fields

Name	Description	Format
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- tipo
- valore
- descrizione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(apiKey=<valore>tipo=<val>valore=<val>descrizione=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC = HASH SHA1(esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Cancellation from Blacklist

This service removes a previously entered Tax Code or contract code from the blacklist.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/cancellazione-da-blacklist

URI
ecomm/api/blacklist/rimuovi

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipo	Search by Tax Code or hashPan	AN 16 CHAR.
valore	Value	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- tipo
- valore
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>tipo=<val>valore=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Checking Existence in Blacklist

This service checks the blacklist to see if a given Tax Code or contract code is present in the blacklist. If it exists, the details are returned.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/controlla-se-in-blacklist

URI
ecomm/api/blacklist/controlla

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipo	Search by Tax Code or hashPan.	AN 16 CHAR.
valore	Value	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- tipo
- valore
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>tipo=<val>valore=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	
blacklist	Blacklist object whose structure is as defined in the following table.	AN

Blacklist element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipoDato		
valoreListato		
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
dataCreazione	Contract creation date	DATE

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Blacklists

This service allows any blacklist associated with the terminal to be queried, and it returns a list of existing contract codes/Tax Codes.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/elenco-blacklist

URI
ecomm/api/blacklist/reportBlackList

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipo	Search by Tax Code or hashPan	AN 16 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- tipo
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>tipo=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
blacklist	Blacklist object whose structure is shown in the following table.	AN

Blacklist element

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipoDato		
valoreListato		
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ‘ “ characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
dataCreazione	Contract creation date	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Verification of Tax Code/PAN Pairing

This service checks a particular Tax Code against a card's PAN hash to confirm the association status.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/verifica-abbinamento-cf-pan

URI
ecomm/api/cfpan/controllaEsistenza

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceFiscale	Tax Code to be disassociated from the PAN.	AN 16 CHAR.
hashPan	hashPan to be disassociated.	AN
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceFiscale
- hashPan
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>codiceFiscale=<val>hashPan=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	
cfpan	cfpan object whose structure is as defined in the following table.	AN

Tcpan element

Name	Description	Format
merchant	merchant	AN
cf	Tax Code	N
scadenza	Card expiry date	DATE
stato	Payment status	AN
dataRegistrazione	Registration date	DATE
hashPan	hashPan	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

Removing Tax Code/PAN Pairing

This service removes any association between a Tax Code and card PAN by running the card's hash.
It allows a CF/PAN association to be removed.
If the group field is not specified ("group": ""), the API will provide data related to the alias only. Alternatively, if the group field is specified, then the API will return all data linked to the entire group.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/eliminazione-cf-pan

URI
ecomm/api/cfpan/rimuovi

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
codiceFiscale	Tax Code to be disassociated from the PAN.	AN 16 CHAR.
hashPan	hashPan to be disassociated.	AN
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- codiceFiscale
- hashPan
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>codiceFiscale=<val>hashPan=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
It allows a CF/PAN association to be removed.
If the group field is not specified ("gruppo ": ""), the API will provide data related to the alias only. Alternatively, if the group field is specified, then the API will return all data linked to the entire group.

List of Associated Tax Codes/PANs

This service returns any associated pairings between Tax Code and hash of the card's PAN existing for a merchant profile or on a profile group.
This allows to query the collection of CF/PAN pairings which are configured for the terminal.
If the group field is not specified ("gruppo": ""), the API will provide data related to the alias only. Alternatively, if the group field is specified, then the API will return all data linked to the entire group.

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/altri-servizi/gestione-controlli/elenco-associazioni-cf-pan

URI
ecomm/api/cfpan/reportAssociazioni

METHOD
POST

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN MAX 30 CHAR.
tipo	Search by Tax Code or hashPan	AN MIN 2 - MAX 30 CHAR.
valore	Tax code or hashPan value	AN
codiceGruppo	Group assigned by Nexi.	AN MIN 4 MAX 10
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

For the initiation message, the string to sign must contain the following fields:

- apiKey
- tipo
- valore
- gruppo
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (apiKey=<val>tipo=<val>valore=<val>gruppo=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN MAX 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN MIN 2 - MAX 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
cfpan	Tcpan object whose structure is as defined in the following table.	AN

CFpan element

Name	Description	Format
merchant	merchant	AN
cf	Tax Code	AN
scadenza	Card expiry date	DATE
stato	Payment status	AN
dataRegistrazione	Registration date	AN
hashPan	hashPan	AN

MAC Calculation

For the result message, the string to sign must contain the following fields:

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING
MAC=HASH SHA1 (esito=<val>idOperazione=<val>timeStamp=<val><SecretKey>)

NOTES:
This allows to query the collection of CF/PAN pairings which are configured for the terminal.
If the group field is not specified ("gruppo": ""), the API will provide data related to the alias only. Alternatively, if the group field is specified, then the API will return all data linked to the entire group.

TABLES AND CODING

Restful API Error Codes Table

The following table describes the values of the 'code' field received in the event of a negative outcome via the XPay API:

Code	Description
1	The value for one of the input JSON parameters is incorrect
2	Requested information cannot be found
3	Incorrect MAC
4	MAC not present in the JSON request
5	More than 5 minutes have passed since the timeStamp was generated
7	apiKey does not contain a valid alias
8	Invalid contract
9	Transaction already present
12	Invalid group
13	Transaction not found
14	The card has expired
15	Card brand not allowed
16	Invalid value for current status
17	Transaction amount too high
18	Number of retry attempts finished
19	Payment rejected*
20	3DS authentication canceled
21	3DS authentication failed
22	Invalid debit card (expired or blocked)
50	Unable to calculate the MAC. Either the alias is invalid, or the incoming JSON does not comply with requirements
96	In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same card and the same amount.
97	Generic error
98	Method not yet implemented
99	Operation not allowed. The merchant does not meet requirements for performing the requested operation
100	Internal error

NOTES:

* The possible contents of the "message" field in case of outcome with code "19" are the following:

- Auth. Denied
- expired card
- restricted card
- invalid merchant
- transaction not permitted
- not sufficient funds
- incorret PIN
- no card record
- exceeds withdrawal amount limit
- no card record
- reserved for national use
- Technical problem
- Host not found

Coding: resultCode

The following table contains the possible values of the “codiceEsito” field received with some XPay solutions such as Simple Payment.

resultCode	resultDescription
0	approved: Approved/verified
20	Order not present
101	incorrect or missing parameters
102	Incorrect PAN - the specified pan cannot execute further authorisations
103	Transaction blocked if the merchant profile provides for cancellation of the transaction in the event of a failed server-to-server notification to urlpost.
104	Generic error
108	Order already registered
109	Technical error
110	Contract number already present
111	Incorrect Mac
112	Transaction denied due to VBV/SC authentication failure or authentication was not possible
113	Contract number not present in the archive
114	Merchant not enabled for multiple group Payments
115	Group Code not present
116	3D Secure cancelled by user
117	Card not authorized due to application of BIN Table rules
118	The PAN of the card is already associated with another Tax code A maximum number of cards are already associated with the indicated tax code (number agreed with Nexi) Transaction blocked due to application of blacklist rules if provided by merchant profile Error on the check between Tax Code and PAN, e.g. the check is active and the Tax Code is not passed by the merchant Unauthorised transaction Transaction blocked due to application of check rule on PAN presence verification on another contract_number if provided for by the merchant profile
119	Merchant not enabled to operate in this mode
120	Network not accepted. The request message indicated Payment was being made with one network, but the card’s PAN is associated with a different network.
121	Transaction expired due to timeout
122	Maximum number of retry attempts using the same transCode reached
400	Auth denied: Generic refusal for many possible reasons, the buyer should check the data entered or ask his bank/issuer for clarification.
401	Expired card: incorrect expiry date, the buyer must check the data entered before trying again.
402	Restricted card/invalid card number/Closed Account: invalid, incorrect or closed card, request a new payment method
403	Invalid merchant: contact support

404	Transaction not permitted to cardholder or terminal: Transaction not permitted by the card issuer. if in PSD2 perimeter retry the transaction with SCA or ask the buyer to use another payment instrument.
405	Not sufficient funds: lack of funds, ask the buyer to try again after re-establishing availability on the card or use another payment method.
406	Technical problem/format error: technical problem on authorisation systems, ask the buyer to try again or contact support
407	Host not found, Card issuer or switch inoperative: Unable to contact the issuing bank. The buyer must try again or use another payment method.
408	Soft Decline, transaction not allowed by the card issuer re-issue with authentication
409	Suspected fraud: The card issuer suspects a fraudulent payment.
410	Allowable PIN tries exceeded: the buyer has entered an incorrect PIN/authentication more times than allowed by the issuing bank. The buyer must try again or use another payment method
411	Refer to card issuer: the buyer should contact their bank for clarification. The buyer can try again after solving the problem with their bank or use another payment method
412	Expire, lost, stolen card: card may be lost, blocked or counterfeit, request a new payment method
413	Excess Reattempts: an attempt to re-submit the same transaction that has previously suffered a decline for which the circuits prohibit re-transmission. Contact the buyer to check with his bank or obtain a new payment instrument.
414	Exceeding daily paper spending limits

Coding: message

The following table contains the possible values of the “messaggio” field received as a result with some XPay solutions such as Simple Payment.

Message/resultDetails	Description
Message OK	Transaction authorised
Controllo CF	The card’s PAN is already associated with another Tax Code.
Controllo PAN	The Tax Code indicated is already associated with the maximum number of cards (number agreed with Nexi).
Controllo BLACKLIST	Transaction blocked due to application of blacklist rules as defined in the merchant profile.
Controllo CF/PAN	Error found when checking the Tax Code and PAN combination, for example the check exists and the merchant has not provided the Tax Code.
Auth. Denied	Transaction not authorized
Impossibile eseguire la Post di Notifica	Transaction blocked if the merchant profile expects a transaction to be cancelled when a server-to-server notification sent to the urlpost fails.
3D Secure annullato da utente	3D Secure authentication was not completed correctly, or was cancelled by the user.
Carta non autorizzata causa applicazione regole BIN table	Transaction blocked if the BIN table is enabled on the merchant profile and the check control fails.
Problema 3D Secure	Unable to complete the transaction due to problems with 3D Secure, for example the user did not return from the authentication stage or there were problems activating the merchant profile for the service.
expired card	Expired card or incorrect expiry date
Invalid merchant	Acquirer Merchant Code not correctly enabled or revoked.
transaction not permitted	Transaction not allowed
not sufficient funds	Transaction denied due to a lack of funds on the card for the amount requested.
Technical problem	Technical problem with the authorisation systems.

Host not found	Issuer authorisation system not available.
Transazione chiusa per time-out	The transaction ended after the set timeout period for the merchant’s profile.
Controllo PAN/CONTRATTO	Transaction blocked due to application of the rule for checking if the PAN is present on another n_contract as defined in the merchant profile.
Numero di tentativi di retry esaurito	The maximum number of ko attempts for the same transCode has been reached (the number is defined at the merchant profile level as being between 1 and 3).
soft decline	Transaction declined by card issuer because it requires strong authentication(SCA) of the customer, retry Payment.
Transazione avvenuta correttamente	The transaction was successfully completed. This message is returned for alternative payment methods.

Coding: languageId

LanguageId field coding for displaying check-out pages in one of the various languages available:

languageId	Description
ITA	Italian
ENG	English
SPA	Spanish
FRA	French
GER	German
JPN	Japanese
CHI	Chinese
ARA	Arabic
RUS	Russian
POR	Potuguese

Coding of DCCcurrency codes for DCC

Numeric currency code	Alphanumeric currency code	Description
978	EUR	EURO
036	AUD	Australian dollar
124	CAD	Canadian dollar
344	HKD	Hong Kong dollar
392	JPY	Japanese yen
756	CHF	Swiss franc
826	GBP	Pound sterling
840	USD	US dollar
986	BRL	Brazilian real (1994-)
702	SGD	Singapore dollar
784	AED	United Arab Emirates dirham
901	TWD	New Taiwan dollar
682	SAR	Saudi riyal
360	IDR	Indonesian rupiah
764	THB	Thai baht
414	KWD	Kuwait dinar
458	MYR	Malaysian ringgit
634	QAR	Qatari riyal
484	MXN	Mexican peso
710	ZAR	South Africa rand
410	KRW	South Korean won
985	PLN	Polish zloty
356	INR	Indian rupee
608	PHP	Philippine peso
203	CZK	Czechoslovak koruna
554	NZD	New Zealand dollar
152	CLP	Chilean peso
946	RON	Romanian leu
348	HUF	Hungarian forint
170	COP	Colombian peso
048	BHD	Bahraini dinar
818	EGP	Egyptian pound
191	HRK	Croatian kuna
428	LVL	Latvian lats
862	VEF	Venezuelan bolívar
400	JOD	Jordanian dinar
032	ARS	Argentine peso (1991-)
446	MOP	Macanese pataca
208	DKK	Danish krone
752	SEK	Swedish crown
643	RUB	Russian ruble

Transaction Type Coding

tipoTransazione	Description
NO_3DSECURE	The merchant is not enabled to use the Verified by Visa and Mastercard Identity Check security protocols or it was not possible to use the protocols.
3DS_FULL	The merchant is enabled for the 3D Secure protocol, the credit cardholder is registered with the service and has been properly authenticated.
3DS_MERCHANT	The merchant is enabled for the 3D Secure protocol, but the credit cardholder or the card issuer do not participate in the service.
VBV_FULL	The merchant is enabled for the Verified by Visa protocol, the credit cardholder is registered with the service and has been properly authenticated.
SC_FULL	The merchant is enabled for the Mastercard Identity Check protocol, the credit cardholder is registered with the service and has been properly authenticated.
VBV_MERCHANT	The merchant is enabled for the Verified by Visa protocol, but the credit cardholder or the card issuer do not participate in the service.
SC_MERCHANT	The merchant is enabled for the Mastercard Identity Check protocol, but the credit cardholder or the card issuer do not participate in the service.
M.O.T.O.	This value is used if it is not an e-commerce transaction (which requires the presence of the buyer who is buying through a browser) but a Mail Order Telephone Order transaction, in which the credit card data are communicated by the buyer to the merchant.
AMEX_FULL	The merchant is enabled for the AMEX SafeKey protocol, the credit cardholder is registered with the service and has been properly authenticated.
AMEX_MERCHANT	The merchant is enabled for the AMEX SafeKey protocol, but the cardholder has not activated the service.
EXPRESSCO	The transaction was carried out through a PayPal account

AMAZONPAY	The transaction was carried out with Amazon Pay
ALIPAY	The transaction was carried out with AliPay
BANCOMATPAY	The transaction was carried out with BancomatPay
BANCONTACT	The transaction was carried out with BancoContact
EPS	The transaction was carried out with EPS
GIROPAY	The transaction was carried out with GiroPay
IDEAL	The transaction was carried out with Ideal
Przelewy24	The transaction was carried out with Przelewy24
WECHAT	The transaction was carried out with WeChatPay
MY_BANK	The transaction was carried out with MyBank
MULTIBANCO	The transaction was carried out with Multibanco
BLIK	The transaction was carried out with Blik
PAYU	The transaction was carried out with PayU
SKRILL	The transaction was carried out with Skrill
SKRILL1TAP	The transaction was carried out with Skrill1Tap

Card Type Coding

brand/cardType/selectedcard
VISA
MASTERCARD - MasterCard
AMEX
JCB
MAESTRO
MY_BANK – SCT (for brand and selectedcard)
CC (only for selectedcard, allows Payment by credit cards only)
SOFORT (for brand and selectedcard)
PAYPAL (only for brand)
AMAZONPAY (for brand and selectedcard)
GOOGLEPAY (for selectedcard)
APPLEPAY (for selectedcard)
PAYPAL_BNPL (Only for selectedcard - payment via PayPal's 'Pay in 3 instalments' service)
ALIPAY (for brand and selectedcard)
WECHATPAY (for brand and selectedcard)
GIROPAY (for brand and selectedcard)
IDEAL (for brand and selectedcard)
BCMC (Bancontact, for brand and selectedcard)
EPS (for brand and selectedcard)
P24 (Przelewy24, for brand and selectedcard)
BANCOMATPAY (for brand, selectedcard, tipotransazione, and Paymenttype)
SKRILL (for brand and selectedcard)
SKRILL1TAP (for brand and selectedcard)
PAYU (for brand and selectedcard)
BLIK (for brand and selectedcard)
MULTIBANCO (for brand and selectedcard)
SATISPAY (for brand and selectedcard)

ECI, XID and CAVV Coding

The table below shows the parameters that must be sent via the ecomm/api/pay/payMPI API, depending on the outcome of the 3D Secure authentication via external MPI.

VISA/MASTERCARD/MAESTRO	Status	Eci	Cavv	Xid
PARes	Y	11	YES	YES
PARes	A	31	YES	YES
PARes	N	00	NO	NO
PARes	U	20	NO	NO

Status	Description
Y	CH passed authentication (both challenged and frictionless)
A	Attempt
N	CH Failed authentication
U	Unable to authenticate CH/ no response

Transazioni SSL	Eci	Cavv	Xid
	20	NO	NO

NOTES:

- The parameters 'cavv' and 'xid' are alphanumeric strings that are returned by the external MPI. The "eci" parameter is also data returned by the MPI, but the value may differ from that expected by the XPay gateway, so a conversion is necessary:
  - From the 3ds server Mastercard:
    - if eci=02 is received, eci=11 must be sent to XPay
    - if you receive eci=01 you need to send eci=31 to XPay
  - From 3ds server VISA:
    - if you receive eci=05 you must send eci=11 to XPay
    - if you receive eci=06 you must send eci=31 to XPay
- SSL transactions include subsequent MIT payments that do not require 3D Secure authentication to the customer.

VAT Codes

VAT Code	Description
04	VAT 4%
10	VAT 10%
22	VAT 22%
ESN1	Excluded ex art. 15
ESN2	Not subject
ESN3	Not Taxable
ESN4	VAT exempt
ESN5	Regime del margine / VAT not expost
ESN6	Inversione contabile
ESN7	VAT exception in other EU State

Invoice Status Code

Status	Description
0	Invoice token requested
1	Request user data to GYB
2	Invoice issue process started (recovery and issue code creation)
3	Invoice released correctly
4	Error in invoice issue
5	Invoice canceled by the merchant through api or back office

SDK iOS Version

The following table lists the iOS SDK versions made available by Nexi with relative compatibility with Swift and XCode versions.

SDK iOS	Swift	Xcode
1.1.5	4.2	10
1.1.6	5	10
1.2.0	5.1	11
1.2.3	5.1	11
1.2.5	5.1	11
1.2.6.3	5.1	11
1.2.7.2	5.3	12
1.2.9.2	5.3	12

MIT framework parameters

Table containing the possible values of the "operation" parameter inside the JSON mitFramework object.

Value	Description	NetworkData mandatory
UCOF_CIT	A first Payment initiated by the card holder (CIT) will be made to save the card for future purchases. Save the networkData value returned by the API for subsequent transactions (UCOF_CIT_PR, UCOF_CIT, UCOF_MIT)	No
UCOF_CIT_PR	A subsequent Payment initiated by the card holder (CIT) will be made on a previously saved card created with a UCOF_CIT or ASI_COF_UNSCH transaction. All calls of this type must specify in the input json the networkData field received in response from the first Payment (UCOF_CIT o ASI_COF_UNSCH).	Yes
UCOF_MIT	A recurrence initiated by the merchant (MIT) will be made on a card already registered with a UCOF_CIT or ASI_COF_UNSCH transaction. All calls of this type must specify in the input json the networkData field received in response from the first Payment (UCOF_CIT o ASI_COF_UNSCH).	Yes
RECURRING_CIT	A first Recurring (scheduled) Payment initiated by the card holder (CIT) will be made. Save the networkData value returned by the API for subsequent transactions (RECURRING_MIT).	No
RECURRING_MIT	A recurrence initiated by the merchant (MIT) will be made on a card previously saved with a RECURRING_CIT or ASI_COF_RECUR transaction. All calls of this type must specify in the input json the networkData field received in response from the first Payment (RECURRING_CIT o ASI_COF_RECUR).	Yes
ASI_COF_UNSCH	A card verification (ASI COF) will be executed for subsequent transactions	No

	initiated by the merchant or unscheduled card holder. Save the networkData value returned by the API for subsequent recurring transactions.	
ASI_COF_RECUR	A card verification (ASI COF) will be executed for subsequent recurring scheduled transactions. Save the networkData value returned by the API for subsequent recurring transactions.	No
ASI_NOCOF	A card verification will be executed or an order transaction will be completed without authorization. In this way the card will be verified without committing the user's funds (ASI NO COF) then authorization will be requested (ASI_AUTH_CIT or ASI_AUTH_MIT) when processing the order. Save the networkData value returned by the API for the next transaction.	No
ASI_AUTH_CIT	Authorization request for a previous card verification (ASI_NOCOF) initiated by the card holder (CIT) to complete the order. It can be of a defined or estimated amount. All calls of this type must specify in the input json the networkData field received in response by ASI_NOCOF	Yes
ASI_AUTH_MIT	Authorization request for a previous card verification (ASI_NOCOF) initiated by the operator (MIT) to process the order. It must be of a defined amount. All calls of this type must specify in the input json the networkData field received in response by ASI_NOCOF	Yes

EXAMPLE:

In order to implement a first card registration payment with subsequent recurrences, it is necessary to value the 'transaction' parameter as follows:

- First payment:
  - UCOF_CIT: if you want to proceed to execute recurrences of type unscheduled, debits with undefined frequency.
  - RECURRING_CIT: if you want to proceed to perform scheduled recurrences, debits with a defined frequency (e.g. first of each month).

- Subsequent payment:
  - UCOF_MIT: to be used if UCOF_CIT was used in the first payment.
  - RECURRING_MIT: To be used if RECURRING_CIT was used in the first payment.

HTTP/XML API

Server to Server Payments

Payment

NOTES:

- These APIs are deprecated, they remain available to pre-existing users

Merchants collect the card details on their systems, and carry out Payment transactions with or without 3D Secure, depending on the type of configuration of the merchant's XPay profile. The transaction is completed in synchronous mode for transactions without 3D Secure, or in asynchronous mode for transactions with 3D Secure.

This service requires the merchant to achieve PCI DSS certification.

1. Requesting Payment towards Nexi Payment endpoint

IN PRACTICE

A http request must be set up with the parameters/values shown below. Any corresponding fields for additional functionalities may be added (e.g. Recurring Payments, OneClick Payments), and it must be directed towards this URL:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/ServletS2S

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/ ServletS2S

2. Managing 3D Secure authentication

IN PRACTICE

If the credit card is enabled for 3D Secure authentication, the API responds with an XML containing the html code to be printed on the user's browser.

3. Managing the response upon completion of the transaction

IN PRACTICE

The user’s return to your site must be managed, and the Payment result recorded.
If the transaction does not require 3D Secure, you will receive an XML in response on the same connection as used for the request (synchronous response). If the transaction requires 3D Secure, after authentication the user returns to your site with the Payment result at the "url" address indicated in the request message. XPay also notifies the result directly to your server at the "urlpost" address indicated in the request message.

NB Below you will find characteristics for the fields to be created (name + description + format) and corresponding sample codes. You will also find information regarding the correct settings for the MAC field.

NOTES:

• These APIs are deprecated, remain available for existing users

Payment Initiation Message: required fields

This table indicates the mandatory fields that must be included in the request message, and their corresponding characteristics.

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents, i.e. 5000 represents € 50.00.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CHAR.
pan	Credit card number	AN MAX 19 CHAR.
scadenza	Credit card expiry date	yyyymm
cv2	CVV2/CVC2, three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards.	AN MAX 4 CHAR.

	4DBC, four-digit code found on the front of AMERICAN EXPRESS cards. Whether it is mandatory or not depends on the rules in application for each individual acquirer.	
Mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500 CHAR.
Tipo_richiesta	PA - value to be set for Payments	AN 2 CHAR.

Payment Initiation Message: optional fields

This table indicates optional fields which can be used for data-entry at the discretion of the merchant.

Name	Description	Format
mail	Buyer's email address to which the Payment result will be sent.	AN MAX 150 CHAR.
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ' " characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR

Parametri aggiuntivi	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values. The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.	AN MAX 4000 CHAR.
OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the Tax Code against associated PAN number are active (optional security control activated on request).	AN 16 CHAR.
selectedcard	If present, the Payment page that is shown only allows the user to make Payment using the networks or Payment methods indicated. This feature is useful for merchants who wish to enter the choice of Payment method on their own check-out page. The possible values are shown in the Card Type Coding. It is necessary to separate the values with a comma ",".	AN
TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to C (immediate), when the transaction is authorised the Payment is deposited without any further intervention on the part of the merchant and without considering the default profile set for the terminal. If set to D (deferred) or if the field is empty, when the transaction is authorised it will be handled as defined by the terminal profile.	AN 20 CHAR.
infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.
infob	Additional information about the individual Payment. This information can	AN MAX 20 CHAR.

	be transmitted to the bank on the basis of prior agreement with the same bank.

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- secretKey

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><SecretKey>)

Response message for 3D Secure authentication

This XML message is returned by XPay in response to a transaction initiation message if the credit card authentication stage is supposed to occur prior to Payment, in accordance with 3D Secure protocols. The message is forwarded using the same connection that was used for receiving the transaction initiation message. The parameters in the message are described in the following table.

Name	Description	Format
TERMINAL_ID	Store identification code transferred in the Payment initiation message (alias).	AN MAX 30 CHAR.
TRANSACTION_ID	Payment identification code transferred in the Payment initiation message in the transCode field.	AN MIN 2 - MAX 30 CHAR.
HTML_CODE	HTML code to be "printed" on the user's browser for redirection to the 3D Secure authentication page.	
MAC	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

NB: Parsing of XML responses should not be validating: thanks to the evolution of the system, additional elements will be able to be added to the messages in future. Applications must ignore unknown elements without causing malfunctions.

Example of returned XML:

<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<TERMINAL_ID>7182815</TERMINAL_ID>
<AUTHRES>
<TRANSACTION_ID>ID000000000025486A</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>MDpay default response template for web</title>
</head>
<body bgcolor="#02014E" OnLoad="OnLoadEvent();" >
<form name="downloadForm"
action="https://acsNexi.it:443/pareq/3c39e31733373131633430313331313139363030653
33430/3ds/vereqauthid=31376271324E6B684F3255447533507576647 06C56644F513D3
D"

method="POST">
<input type="hidden"
name="PaReq"
value="eJxVUm1PwjAQ/iuE79Lry9qNHE3QYVxUQtCp38zcGlgiY3SDwL+3HUO06Yd77q
XPPXfF17U1Jn4x+d4ajc+mabKVGZTFZCiUlMBhqHExXZqdxoOxTbmtNB3BiCG5QFdk83
VWtRqzfHebzLWIeACApIe4MTaJNfQnUAGTCm4EBxUC5UjOcayyjdGKhiykAZIOYb7dV6
09aR669y4A9/Zbr9u2HhOCxAMk1yYWe281rvhYFvqjivm8uF+9J7Onr+Uhjsu0rN/SNnpMJ
0h8BhZZazQD2t0BDcagxsIJ7PyYbTyrnqXLgRPuVZ0dWHue6RlQH/jrQDdPa6r8pCMVus
4vCM2x3lbGZTiCXxsL0+Q6ieH3sECEcvpJOVMgQyFZxIXryKchuSq8e/BDz1s3PsalDKW
KJAUKgkkplN9AF/OspRscDUB2tB4g8dWkXy7pV++sf1/iB2NMqeE=">
<input type="hidden"
name="TermUrl"
value="https://ecommerce.nexi.it:443/mdpaympi/MerchantServer?msgid=4766030">
<input type="hidden"
name="MD"
value="D6A7882ACB6D8D32645DA85B381FD3AD.ecdvas">
<!-- To support javascript unaware/disabled browsers -->
<noscript>
Please click the submit button below.
<input type="submit" name="submit" value="Submit">
</noscript>
</form>
<SCRIPT LANGUAGE="Javascript" >

<!-- about:blank -->
<!--
function OnLoadEvent() {
document.downloadForm.submit();
}
//-->
</SCRIPT>
</body>
</html>
]]>
</HTML_CODE>
</AUTHRES>
<MAC>e1c2597cb5fe1f066e0008469f0b70659de6be85</MAC>
</VPOSRES>

NB: the elements in italics do not form part of the html to be returned to the cardholder's browser. They indicate to the xml parser that the contents of the tag can be ignored since they contain characters specific to the xml protocol.

MAC Calculation:

For the AUTHRES message, the string to sign must contain tags and corresponding values for the following fields:

- TERMINAL_ID
- TRANSACTION_ID
- HTML_CODE
- SecretKey

The MAC will be calculated as follows:
mac= HASH SHA(<TERMINAL_ID>value</TERMINAL_ID><TRANSACTION_ID>value</TRANSACTION_ID><HTML_CODE>value</HTML_CODE>secret string)

Below is an example of the MAC calculation for an AUTHRES message:

mac= HASH SHA('<TERMINAL_ID>7182815</TERMINAL_ID>
<TRANSACTION_ID>ID000000000025469A</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<title>MDpay default response template for web</title>
</head>

<body bgcolor="#02014E" OnLoad="OnLoadEvent();" >
<form name="downloadForm"
action="https://acsNexi.it:443/pareq/3c63af6a3337313163343031363331313330333061373130/3ds/vereqauthid=33377337556F4D48656B7659417264576D436547387835513D3D
"
method="POST">
<input type="hidden"
name="PaReq"
value="eJxVUttOAjEQ/RXCq5Hetu2WDE0QTOBBggiJ+mI23cZdlQW6RcGvt10W1KYPc+
bSOXOmsCycteMHa/bOarizdZ292k6ZD7qJFAIz1tUwHy7sTsOndXW5qTTp4R4FdIahyJki
q7yGzOxupjOdKMYxBtRCWFs3HWvcHi45FRJfJwzLFBMG6BSHKltbLUlKU8IBNQjMZl95
d9QsDe+dAezdhy683/YRAhQBoF8S83206lB8KHO9eptMlth+PS9oYRS5vyoen/xMjPz3+w
BQzIA881ZTTJrbIaLPcT8JtBo/ZOvYVd+uFp0weJzq5IBt7DM8ARIDfx0Q9HS2MketZBqYn
xHYw3ZT2ZARFLzYkNva6OkYXw7liVDDF8KoxDIRCWNYBUYxDdDvhKNJFN34IB9lQiilp
CRBUyK4Ys0GmljsWgbhwny8aRsBoFiN2uWidvXB+vclfgA8Gam7">
<input type="hidden"
name="TermUrl"
value="https://ecommerce.nexi.it:443/mdpaympi/MerchantServer?msgid=4766033">
<input type="hidden"
name="MD"
value="4E7311C0EEF2F0C861D81963B419C637.ecdvas">
<!-- To support javascript unaware/disabled browsers -->
<noscript>
Please click the submit button below.
<input type="submit" name="submit" value="Submit">
</noscript>
</form>
<SCRIPT LANGUAGE="Javascript" >
<!-- about:blank -->
<!--
function OnLoadEvent() {
document.downloadForm.submit();
}
//-->
</SCRIPT>
</body>
</html>
]]>
</HTML_CODE>macCalculationExample');

The value obtained will be:
"adb669b9f5a703bd088525385a0c6d6ce77e9d6c"

Payment Result Message: required fields

For a transaction without 3D Secure, the Payment result will be sent in direct response to the request message. For a transaction with 3D Secure, the result will be received when the

user is returned to the address indicated in the "url" field, along with a notification from our server to the address indicated in the "urlpost" field.

The XML containing the Payment result consists of two sections:

- StoreRequest
- StoreResponse

The transaction initiation message fields are replicated in StoreRequest, with the exception of the "pan" field (which is only populated with the last four digits) and the cv2 field (which is replaced with the character "*"):

Name	Description	Format
alias	Store identification code transferred in the Payment initiation message.	AN MAX 30 CHAR.
importo	Transaction amount retrieved from the Payment initiation message.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed (EUR = Euro).	AN 3 CHAR.
codTrans	Code associated with the Payment retrieved from the Payment initiation message.	AN MIN 2 - MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
esito	Payment result (OK or KO)	AN 2 CHAR.
pan	Partial credit card number, only the last 4 digits are shown.	AN 4 CHAR.
scadenza	Credit card expiry date	yyyymm
cv2	This is shown as masked with: *	AN MAX 4 CHAR.
tipo_richiesta	PA	AN 2 CHAR.

The tags described in the following table can be found in StoreResponse:

Name	Description	Format
tipoCarta	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 15 CHAR.
TipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN 20 CHAR.
Regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.

Paese	If enabled, this will return the ISO 3166-1 alpha-3 code which identifies the country of the card used for Payment.	ISO 3166-1 alpha-3 code
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN 200 CHAR.
codiceAutorizzazione	Authorisation code assigned to Payment.	AN MAX 6 CHAR.
dataOra	Transaction date and time	yyyymmddThhmmss
codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods.	N MAX 3 CHAR.
descrizioneEsito	Description of the transaction result. The possible values are shown in the table here.	AN MAX 2000 CHAR.
dettaglioEsito	Shows a brief description of the Payment result. The possible values are shown in the table here.	AN MAX 200 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Result Message: optional fields

This table indicates optional fields which may be present depending on the merchant configuration.

Name	Description	Format
Parametri aggiuntivi	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values.	AN MAX 4000 CHAR.
Hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for Payment.	AN 28 CHAR.
Infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.
Infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20 CHAR.

codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.

NB: Parsing of XML responses should not be validating: thanks to the evolution of the system, additional elements will be able to be added to the messages in future. Applications must ignore unknown elements without causing malfunctions.

EXAMPLES
Below is an example of a response XML for a successful result:

```
<RootResponse>
<StoreRequest>
<alias>Payment_test_XXXX</alias>
<codTrans>XXXXXXXX-1</codTrans>
<divisa>EUR</divisa>
<importo>1</importo>
<mail>xxxxx.xxxx@xxxx.it</mail>
<scadenza>202508</scadenza>
<pan>9992</pan>
<cv2>***</cv2>
< num_contratto >123456789</ num_contratto >
< tipo_richiesta > PP </ tipo_richiesta >
< tipo_servizio > paga_multi </ tipo_servizio >
< gruppo >XXXX</ gruppo >
< descrizione >sdfgfddf gdfgdfdfggdfgdfdf</ descrizione >
</StoreRequest>
- <StoreResponse>
<tipoCarta>MasterCard</tipoCarta>
<codiceAutorizzazione>TESTOK</codiceAutorizzazione>
<dataOra>20090618T160701</dataOra>
<codiceEsito>0</codiceEsito>
<descrizioneEsito>autorizzazione concessa</descrizioneEsito>
<ParametriAggiuntivi>
<parametro1>XXXXX</parametro1>
<parametro2>XXXXX</parametro2>
</ParametriAggiuntivi>
<mac>gdfdfdgdfgdfgdfgdfr3434g345gedggdf=</mac>
</StoreResponse>
</RootResponse>
```

And here is a response XML for an unsuccessful result:

```
<RootResponse>
<StoreRequest>
<alias>Payment_test_XXXX</alias>
<codTrans>XXXXXXXX-1</codTrans>
<divisa>EUR</divisa>
<importo>1</importo>
<mail>xxxxx.xxxx@xxxx.it</mail>
```

<scadenza>202508</scadenza>
<pan>9992</pan>
<cv2>***</cv2>
< num_contratto >123456789</ num_contratto >
< tipo_richiesta > PP </ tipo_richiesta >
< tipo_servizio > paga_multi </ tipo_servizio >
< gruppo >XXXX</ gruppo >
< descrizione >sdfgfddf gdfgdfdfggdfgdfdf</ descrizione >
</StoreRequest>
- <StoreResponse>
<tipoCarta>MasterCard</tipoCarta>
<codiceAutorizzazione/>
<dataOra>20090618T160701</dataOra>
<codiceEsito>103</codiceEsito>
<descrizioneEsito>autorizzazione negata dell'emittente della carta</descrizioneEsito>
<ParametriAggiuntivi>
<parametro1>XXXXX</parametro1>
<parametro2>XXXXX</parametro2>
</ParametriAggiuntivi>
<mac>gdfdfdgdfgdfgdfgdfr3434g345gedggdf </mac>
</StoreResponse>
</RootResponse>

MAC Calculation:

For the server-to-server transaction result message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- codAut (in the XML result message this corresponds to the field: authorisationCode)
- data (in the XML result message this corresponds to the values which precede the "T" value in the field: dateTime)
- orario (in the XML result message this corresponds to the values which follow the "T" value in the field: dateTime)
- secretKey

SAMPLE STRING
MAC= HASH SHA1 (codTrans=<val>divisa=<val>importo=<val>codAut=<val>data=<val>orario=<val><SecretKey)

Payment for CardOnFile/Recurring/OneClick Registration

NOTES:

• These APIs are deprecated, remain available for existing users

Integrating recurring, CardOnFile, or OneClick Payments allows merchants to store credit card details, and use them to make subsequent Payments. At a technical level, the operation involves 2 stages: a registration or first Payment stage, where the contract is registered and associated with a credit card, and a second stage, where subsequent Payment requests are forwarded for existing contracts. Technically, the integration of services is the same. It is only at a contractual level that the merchant profile alias issued will differ.

1. Activation and/or first Payment
2. Management of recurring Payments/subsequent Payments

Activation and/or first Payment

During the first transaction, a contract code must be generated for use in subsequent purchases. This contract code allows Nexi to save a paired link between the user and the Payment card used.

IN PRACTICE

The information described in the"Codebase" must be integrated and the following specific parameters added.
3D Secure management occurs exactly as described in the "Codebase".

"First Payment" Initiation Message

Name	Description	Format
num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
tipo_richiesta	PP (first Payment)	AN 2 CHAR.
gruppo	The “gruppo” value is assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Result Message: required fields

The same information found in the "Codebase" module is received in response, along with the following specific parameters.

Name	Description	Format
num_contratto	Contract number retrieved from the initiation message.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Result Message: optional fields

The same optional information found in the "Codebase" module can be received in response, along with the following specific parameter.

Name	Description	Format
Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.

Payment on Registered Contracts

NOTES:

• These APIs are deprecated, remain available for existing users

When you need to make a charge on a previously registered contract, the message is the same as that in the first Payment described above, without the pan and cv2 fields. Payment will take place in synchronous mode with the following fields suitably populated.

Name	Description	Format
n_contract	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details during the first Payment with FP contract registration.	AN MAX 30 CHAR.
service_type	The field must be set to: “multi_pay”.	AN MAX 30 CHAR.
request_type	"PR" Payment on a registered contract	AN 2 CHAR.
group	The “group” value is assigned by Nexi during activation.	AN MIN 5 - MAX 30 CHAR.

Payment with External 3D Secure MPI

NOTES:

• These APIs are deprecated, remain available for existing users

This paragraph describes the message made available for merchants whose applications use Nexi XPay platform for sending authorisation requests. In this situation, the merchant is equipped with an MPI (Merchant Plug In), and handles the cardholder's 3D Secure authentication stage.

1. Requesting Payment towards Nexi Payment endpoint

IN PRACTICE

The XML message containing the parameters/values shown below must be sent, using the post method, to this URL:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/XPayServlet

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/XPayServlet

2. Recording the transaction result

IN PRACTICE

The Payment result must always be managed in XML format, and on the same connection as used for the request (synchronous response).

Payment Initiation Message

This table indicates the mandatory fields that must be included in the request message, and their corresponding characteristics.

Name	Description	Format
TERMINAL_ID	Merchant identification code within XPay.	AN MAX 30 CHAR.
TRANSACTION_ID	Unique code which identifies the merchant order.	AN MAX 30 CHAR.
REQUEST_TYPE	Possible values: FA: First Attempt RA: Payment request retry	AN 2 CHAR.

ACTION_CODE	Type of transaction requested. The following values are allowed: VERI: transaction requesting authorisation verification only	AN MAX 10 CHAR.
PAN	Number of the card being used in the Payment request.	N MAX 19 CHAR.
EXPIRE_DATE	Expiry date for the card being used in the Payment request.	yymm
CVV2	Security code for the card being used in the Payment request.	N MAX 4 CHAR.
AMOUNT	Amount of the Payment requested. This is a string of 9 fixed numbers, where the last two numbers represent the 2 decimal places, and no separator is used between whole numbers and decimal numbers.	AN MAX 9 CHAR.
CURRENCY	ISO code for the Payment currency, where the only value currently managed is 978 (Euro).	N 3 CHAR.
ECI	Electronic Commerce Indicator	AN 2 CHAR.
XID	Order identifier	28 byte base64 encoding
CAVV	Cardholder Authentication Verification Value	28 byte base64 encoding
VERSION_CODE	Fixed value: “01.00”	AN 5 CHAR.
MAC	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Example:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
<TERMINAL_ID>0000000050242004</TERMINAL_ID>
<AUTHONLYREQ>
<TRANSACTION_ID>T0000000000000000001</TRANSACTION_ID>
<REQUEST_TYPE>FA</REQUEST_TYPE>
<ACTION_CODE>VERI</ACTION_CODE>
<PAN>1234567890123456</PAN>
<EXPIRE_DATE>0605</EXPIRE_DATE>
<CVV2>123</CVV2>
<AMOUNT>000123056</AMOUNT>
<CURRENCY>978</CURRENCY>
<ECI>30</ECI>
<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
<VERSION_CODE>01.00</VERSION_CODE>
</AUTHONLYREQ>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- TERMINAL_ID
- TRANSACTION_ID
- PAN
- EXPIRE_DATE
- CVV2
- AMOUNT
- CURRENCY
- ECI
- XID
- CAVV
- VERSION_CODE
- secretKey

SAMPLE STRING
MAC= HASH SHA1(<TERMINAL_ID>< TRANSACTION_ID><PAN><EXPIRE_DATE>< CVV2><AMOUNT>< CURRENCY>< ECI>< XID>< CAVV>< VERSION_CODE><secretKey>)

Payment Result Message

This XML message is returned by the XPay platform in response to the AuthOnlyReq message. It uses the same connection on which the message was received, and contains the transaction result for the requested authorisation.
The following table lists the XPay parameters that are included in the message:

Name	Description	Format
TERMINAL_ID	Merchant identification code within XPay.	AN MAX 30 CHAR.
TRANSACTION_ID	Unique code which identifies the merchant order.	AN MAX 30 CHAR.
REQUEST_TYPE	Possible values: FA: First Attempt RA: Payment request retry	AN 2 CHAR.
RESPONSE	Result of the Payment requested. For possible values see the table below.	AN MAX 3 CHAR.

AUTH_CODE	This is the authorisation code obtained from the credit card issuer. If the Payment result is negative, an empty string will be sent.	AN MIN 2 - MAX 6 CHAR.
AMOUNT	Amount of the Payment requested. This is a string of 9 fixed numbers, where the last two numbers represent the 2 decimal places, and no separator is used between whole numbers and decimal numbers.	AN MAX 9 CHAR.
CURRENCY	ISO code for the Payment currency, where the only value currently managed is 978 (Euro).	N 3 CHAR.
ECI	Electronic Commerce Indicator	AN 2 CHAR.
XID	Order identifier	28 byte base64 encoding
CAVV	Cardholder Authentication Verification Value	28 byte base64 encoding
TRANSACTION_DATE	Transaction date	dd/mm/yyyy hh.mm.ss
TRANSACTION_TYPE	Transaction type, indicates the level of security for the Payment undertaken. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN 30 CHAR.
MAC	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

- **RESPONSE**: Result of the Payment requested, it can take on the following values:

RESPONSE	Description
0	Payment executed correctly
1	Payment error: incorrect message format or missing or incorrect field
3	Payment error: duplicate TRANSACTION_ID field ("FA" case) TRANSACTION_ID not found ("RA" case)
16	Payment error: TERMINAL_ID field unknown or not enabled
18	Payment error: Payment declined by credit card issuer
2	Payment error: an unexpected error occurred while processing the request
8	Payment error: incorrect MAC
17	MAXimum number of operations denied for the same TRANSACTION_ID, RA case **(*)**

(*) The maximum number of operations is set by the Payment platform

Example of a successful Payment:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<TERMINAL_ID>0000000050242004</TERMINAL_ID>
<AUTHONLYRES>
<TRANSACTION_ID>T0000000000000000001</TRANSACTION_ID>
<REQUEST_TYPE>FA</REQUEST_TYPE>
<RESPONSE>0</RESPONSE>
<AUTH_CODE>098765</AUTH_CODE>
<AMOUNT>000123056</AMOUNT>
<CURRENCY>978</CURRENCY>
<TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
<TRANSACTION_TYPE>VBV_FULL</TRANSACTION_TYPE>
<ECI>30</ECI>
<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
</AUTHONLYRES>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>
```

Example of a denied Payment:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<TERMINAL_ID>0000000050242004</TERMINAL_ID>
<AUTHONLYRES>
<TRANSACTION_ID>T0000000000000000001</TRANSACTION_ID>
<REQUEST_TYPE>FA</REQUEST_TYPE>
<RESPONSE>21</RESPONSE>
<AUTH_CODE></AUTH_CODE>
```

<AMOUNT>000123056</AMOUNT>
<CURRENCY>978</CURRENCY>
<TRANSACTION_DATE>06/07/2005 16.55.56</TRANSACTION_DATE>
<TRANSACTION_TYPE></TRANSACTION_TYPE>
<ECI>30</ECI>
<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
</AUTHONLYRES>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSRES>

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- TERMINAL_ID
- TRANSACTION_ID
- RESPONSE
- AUTH_CODE
- AMOUNT
- CURRENCY
- secretKey

THE MAC WILL BE CALCULATED AS FOLLOWS

mac= HASH SHA1(TERMINAL_ID><TRANSACTION_ID>< RESPONSE>< AUTH_CODE>< AMOUNT>< CURRENCY><secretKey>)

Generating Pay-by-Link Links

NOTES:

• These APIs are deprecated, remain available for existing users

This service allows to generate a Payment link which can be sent to customers for example by email, enabling them to be redirected to the XPay Payment pages to complete their transaction securely, without the merchant needing to worry about managing sensitive customer details. At a technical level, the implementation requires two stages:

1. Requesting an XPay Payment link

IN PRACTICE

Set up a Get request (redirect - link) or Post request (by sending a form with hidden fields) which is directed to this URL:

PRODUCTION ENVIRONMENT URL
https://ecommerce.nexi.it/ecomm/ecomm/OffLineServlet

TEST ENVIRONMENT URL
https://int-ecommerce.nexi.it/ecomm/ecomm/OffLineServlet

The request must be integrated with the parameters/values shown below, and any corresponding fields for additional functionalities may be added (e.g. Recurring Payments, OneClick Payments).
The resulting link can be inserted into an email to your customer, who, by following the link or pasting it into the browser address bar, will be redirected to the secure Nexi environment to make the Payment.

2. Managing the response upon completion of the transaction

IN PRACTICE

The user's return to your site must be managed, and the Payment result recorded. Alternatively, if you would rather not implement the response message, you will need to check the XPay back office for any transactions made.

NB Below you will find characteristics for the fields to be created (name + description + format) and corresponding sample codes. You will also find information regarding the correct settings for the MAC field.

NOTES:

• These APIs are deprecated, remain available for existing users

Payment Initiation Message: required fields

This table indicates the mandatory fields to be entered as part of the redirect URL, and their corresponding characteristics.

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN MAX 30 CHAR.
importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents, i.e. 5000 represents € 50.00.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CHAR.
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # ‘ “ characters. The code must be unique for each authorisation request. If, and only if, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN MIN 2 - MAX 30 CHAR.
url	Return URL to the website upon completion of the transaction, passing the response parameters with the transaction result using the GET method. The customer is redirected to the specified address via this parameter, both in the case of a successful transaction outcome (esito=OK) and in the case of a negative outcome (esito=KO).The value of this field must start with "http://" or "https://" and must use the standard ports 80 or 443.	AN MAX 500 CHAR.
url_back	Recall url, in case the user decides to abandon the transaction during the Payment phase on the check-out page (result = CANCELLED) or if the call contains formal errors (result = ERROR).	AN MAX 200 CHAR.

	The url will be called queuing the following parameters: **Field name** / **Description** Importo / Request amount Divisa / EUR codTrans / Payment identification code assigned by the merchant Esito / Possible values: ANNULLO or ERROR NB: if result = ANNULLO, the merchant may choose to return the user to the Payment page with the same transaction code.	
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
urlpost	URL to which XPay sends the transaction outcome via server-to-server POST method, passing response parameters with the transaction outcome. The value of the field must start with "http://" or "https://" and must use the standard ports 80 or 443. The address specified in this field must have a public certificate, should not be protected by authentication, and must support the TLS 1.2 security protocol. The POST notification has the "application/x-www-form-urlencoded" format.To confirm the successful receipt of the notification, the message returned by the call must be an "HTTP 200" response.No actions can be taken on the transaction until the outcome (HTTP 200) is returned in response to the notification.	AN MAX 500 CHAR.
userid	User provided by Nexi.	N 11 CHAR
Password	Password provided by Nexi.	AN 8 CHAR.

Payment Initiation Message: optional fields

This table indicates optional fields which can be used for data-entry at the discretion of the merchant.

Name	Description	Format
mail	Buyer's email address to which the Payment result will be sent.	AN MAX 150 CHAR.
languageId	Language identifier for the language to be displayed on the check-out page. The available languages are shown in the table here. If this field is not specified or is left blank, the text displayed will be in the default language defined during the service configuration process.	AN MAX 7 CHAR.
descrizione	Field where the merchant can specify a description of the type of service offered. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters. For Paypal the value will be avaible in the Payment detail on paypal account.	AN MAX 2000 CHAR. Excluding the # ' " characters For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
Note1	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
Note2	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
Note3	Field where the merchant can show information relating to the order.	AN MAX 200 CHAR.
Parametri aggiuntivi	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values. The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.	AN MAX 4000 CHAR.
OPTION_CF	Field which the merchant uses to send the user's Tax Code to XPay. This is only required if checks validating the	AN 16 CHAR.

	Tax Code against associated PAN number are active (optional security control activated on request).	
selectedcard	If present, the Payment page that is shown only allows the user to make Payment using the networks or Payment methods indicated. This feature is useful for merchants who wish to enter the choice of Payment method on their own check-out page. The possible values are shown in the Card Type Coding. It is necessary to separate the values with a comma ",".	AN
TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to C (immediate), when the transaction is authorised the Payment is deposited without any further intervention on the part of the merchant and without considering the default profile set for the terminal. If set to D (deferred) or if the field is empty, when the transaction is authorised it will be handled as defined by the terminal profile.	AN 20 CHAR.
infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.
infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20 CHAR.

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards

MAC Calculation

For the transaction initiation message, the string to sign must contain the following fields:

- codTrans
- divisa
- importo
- secretKey

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>divisa=<val>importo=<val><SecretKey>)

Payment Result Message: required fields

The merchant may choose to configure the receipt/display of the Payment result in the following ways:

- Via e-mail: the merchant will receive a message with transaction details sent to the e-mail address indicated during configuration
- Online: once the Payment has been completed, the user is redirected straight to the merchant's site, at the address indicated in the Payment initiation message (field name: "url"). The user then returns to the merchant's site, bringing the parameters that attest to the conclusion of the transaction
- Online server to server: the merchant can receive the result directly from the Nexi server through a server-to-server call. The notification contains the same parameters as the previous method, and is carried out to the address indicated in the Payment initiation message (field name: "urlpost").

The table below shows the parameters that are returned in the result message.

Name	Description	Format
alias	Store identification code transferred in the Payment initiation message.	AN MAX 30 CHAR.
importo	Transaction amount retrieved from the Payment initiation message.	N MAX 8 CHAR.
divisa	Code of the currency in which the amount is expressed (EUR = Euro).	AN 3 CHAR.
codTrans	Code associated with the Payment retrieved from the Payment initiation message.	AN MIN 2 - MAX 30 CHAR.
brand	Type of card used by the user to make Payment. The possible values are shown in the table here.	AN MAX 100 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
esito	Payment result (OK or KO)	AN 2 CHAR.
data	Transaction date	yyyymmdd

orario	Transaction time	HHmmss
codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods	N MAX 3 CHAR.
codAut	Authorisation code assigned by the credit card issuer, only present when authorisation is granted.	AN MIN 2 - MAX 6 CHAR.
Pan	Masked credit card number with only the first 6 and/or the last 4 digits showing.	AN MAX 19 CHAR.
scadenza_pan	Credit card expiry date	yyyymm
regione	If enabled, this will return the global region associated with the card used for Payment (e.g. Europe).	AN MAX 30 CHAR.
nazionalita	Shows the country of the card used for making Payment.	AN 3 CHAR. ISO 3166-1 alpha-3 code
messaggio	Shows a brief description of the Payment result. The possible values are shown in the table here.	AN MAX 300 CHAR.
descrizione	If this information is provided during INPUT from the merchant, it will also be returned as OUTPUT, otherwise the field will be null.	AN MAX 2000 CHAR.
languageId	Value retrieved from the Payment initiation message.	AN MAX 7 CHAR.
TipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
tipoProdotto	If enabled, the description of the card type used for the Payment is returned. The composition of the parameter is described below: product description - type of use (CREDIT / DEBIT) - prepaid (S / N) Example: VISA CLASSIC - CREDIT - N	AN MAX 200 CHAR.
nome	Name of the person who made the Payment.	AN MAX 150 CHAR.
cognome	Surname of the person who made the Payment.	AN MAX 150 CHAR.

Payment Result Message: optional fields

This table indicates optional fields which may be present depending on the merchant configuration.

Name	Description	Format
Parametri aggiuntivi	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values.	AN MAX 4000 CHAR.
mail	Email address of the person who made the Payment.	AN MAX 150 CHAR.
hash	If expected under the merchant profile, this field will be populated and returned with the hash of the PAN of the card used for Payment.	AN 28 CHAR.
infoc	Additional information about the individual Payment. This information can be transmitted to the company on the basis of prior agreement with the same company.	AN MAX 35 CHAR.
infob	Additional information about the individual Payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.	AN MAX 20 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer. Where required.	AN MAX 15 CHAR.
dati_gestione_consegna	Xml containing shipping information	MAX 700 CHAR.

Field name	Req.	Descripti
WalletAddress		
BillingAddress		
City	YES	City
Country	YES	Country
CountrySubdivision	YES	
Line1	YES	address
Line2	NO	address
Line3	NO	address
PostalCode	YES	postal cod
BillingAddress		
ShippingAddress		
City	YES	City
Country	YES	Country
CountrySubdivision	YES	
Line1	YES	address
Line2	NO	address

	Line3	NO	address
	PostalCode	YES	postal cod
	RecipientName	YES	Contact
	RecipientPhoneNumber	YES	Tel. no.
ShippingAddress			
WalletAddress			

Example:

```
<WalletAddress>
        <BillingAddress>
                <City>Milan</City>
                <Country>ITA</Country>
                <CountrySubdivision>-</CountrySubdivision>
                <Line1>corso sempione 55</Line1>
                <Line2/>
                <Line3/>
                <PostalCode>20100</PostalCode>
        </BillingAddress>
        <ShippingAddress>
                <City>Milan</City>
                <Country>ITA</Country>
                <CountrySubdivision>-</CountrySubdivision>
                <Line1> corso sempione 55</Line1>
                <Line2/>
                <Line3/>
        <PostalCode>20100</PostalCode>
        <RecipientName>Luca Rossi</RecipientName>
        <RecipientPhoneNumber>0234111111</RecipientP
honeNumber>
</ShippingAddress>
</WalletAddress>
```

Payment Result Message: additional fields for PayPal

This table indicates the fields provided in response to PayPal Payments.

Name	Description	Format
PAYERID	Unique identifier of the user's PayPal account.	AN 13 CHAR.
PAYMENTINFO_0_TRANSACTIONID	Unique identifier of the Payment transaction.	AN

PAYMENTREQUEST_0_SHIPTONAME	Name and surname attached to the shipping address.	AN 128 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET	First shipping address field	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOSTREET2	Second shipping address field. Optional.	AN 100 CHAR.
PAYMENTREQUEST_0_SHIPTOCITY	Shipping address city	AN 40 CHAR.
PAYMENTREQUEST_0_SHIPTOSTATE	Shipping address country or province. The PayPal country code list can be found here.	AN 40 CHAR.
PAYMENTREQUEST_0_SHIPTOZIP	Postal Code	AN 20 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYCODE	Country Code	AN 2 CHAR.
PAYMENTREQUEST_0_SHIPTOCOUNTRYNAME	Country	AN 20 CHAR.
BILLINGAGREEMENTACCEPTEDSTATUS	Indicates whether the customer accepts recurring Payments (valued with "1" if he accepts otherwise with "0")	N
BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

Remember

- The values of the "url", "urlpost" and "url_back" fields must start with "http://" or https://
- The address indicated in "urlpost" must have a public certificate and must not be protected by authentication
- Standard ports 80 or 443 must be used
- For proper call management, remember to comply with RFC 2396 and RFC 3986 standards

MAC Calculation

For the transaction result message, the string to sign must contain the following fields:

- codTrans

- esito
- importo
- divisa
- data
- orario
- codAut
- secretKey

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>esito=<val>importo=<val>divisa=<val>data=<val>orario=<val>codaut=<val>SecretKey>)

Recurring/Card on File Payment

NOTES:

• These APIs are deprecated, remain available for existing users

Integrating recurring or CardOnFile Payments using Pay-by-Link for the first Payment allows merchants to store credit card details, and use them to make subsequent Payments. At a technical level, the operation involves 2 stages: a registration or first Payment stage, where the contract is registered and associated with a credit card, and a second stage, where subsequent Payment requests are forwarded for existing contracts.

1. First Payment
2. Management of recurring Payments/subsequent Payments

Activation and/or first Payment

During the first transaction, a contract code must be generated for use in subsequent Payments. This contract code allows Nexi to save a paired link between the user and the Payment card used.

IN PRACTICE

The "Codebase" module must be integrated and the following specific parameters added.

"First Payment" Initiation Message

Name	Description	Format
num_contratto	Unique code assigned by the merchant for pairing with the archive storing sensitive credit card details.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
tipo_richiesta	PP (first Payment)	AN 2 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Result Message: required fields

The same information found in the "Codebase" module is received in response, along with the following specific parameters.

Name	Description	Format
num_contratto	Contract number retrieved from the initiation message.	AN MIN 5 - MAX 30 CHAR. Except the “+” character and the quotes
tipo_servizio	The field must be set to: “paga_multi”.	AN MAX 30 CHAR.
gruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.

"First Payment" Result Message: optional fields

The same optional information found in the "Codebase" module can be received in response, along with the following specific parameter.

Name	Description	Format
Check	This is populated if one or more of the controls programmed under the merchant profile fail. The check to see if a card PAN exists against other contract codes will be set to: "PGP". Depending on the merchant profile, if the check fails the transaction can be blocked or a notification can be sent advising that the pan exists on another n_contract. If all checks are passed, the field will not be populated.	AN 3 CHAR.

Management of subsequent recurring/Card on File Payments

Each time registered users make subsequent purchases, the e-commerce provider must send a call to Nexi with the registered contract details.

IN PRACTICE

When you need to make a charge on a previously registered contract, two options are available: either through synchronous calls in server-to-server mode, or through batch file.

Synchronous call

In server-to-server mode, the services displayed by Nexi use http POST methods and a RESTful structure. Requests must be sent in JSON format and responses are formatted JSON objects. Alternatively, Non-Rest APIs are available, where communication is handled synchronously (using https calls accompanied by a series of parameters and values). The result message is an XML handled on the same connection.
See the Subsequent Payment section for detailed information on the call and the response to handle.

Batch file

The trace for managing recurring Payments through batch files can be found here.

Download trace

Back Office API

Deposit/Cancellation/Refund

NOTES:

• These APIs are deprecated, remain available for existing users

The merchant's application must send this message in order to make requests for processing, cancelling, or reversing transactions where Payments have previously been successfully made.

1. Requesting operation towards Nexi Payment endpoint

IN PRACTICE

The XML message containing the parameters/values shown below must be sent, using the post method, to this URL:

https://ecommerce.nexi.it/ecomm/ecomm/XPayBo

2. Recording the result of the requested operation

IN PRACTICE

The request result must always be managed in XML format, and on the same connection as used for the request (synchronous response).

Request message - ECREQ

This table indicates the mandatory fields that must be included in the request message, and their corresponding characteristics.

Name	Description	Format
alias	Merchant identification code within XPay.	AN MAX 30 CHAR.
codTrans	Payment order unique identification code.	AN MAX 30 CHAR.
request_type	Possible values: FA: First Attempt RA: Payment request retry	AN 2 CHAR. fixed
id_op	Unique identifier of the requested operation; single identifier for any type of operation.	N MAX 10 CHAR.

type_op	Type of operation requested. For possible values see the table below.	AN 1 CHAR.
importo	Amount for which Payment authorisation has previously been requested.	AN 9 CHAR. fixed
divisa	ISO code for the currency in which Payment authorisation has previously been requested.	AN 3 CHAR. fixed
codAut	Authorisation code received by the merchant in response to the Payment request.	AN MAX 10 CHAR.
importo_op	Amount that the merchant wants to use for the specified operation. Consequently, depending on the type of operation requested, it is the amount to be processed/cancelled/reversed.	AN 9 CHAR. fixed
*user	Merchant operator requesting the operation.	AN MAX 20 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR. fixed

*optional value

type_op: the types of operations managed by XPay are as follows:

type_op	Description
R	Cancellation or accounting reversal. Depending on the status of the transaction, this could be an authorisation and/or accounting reversal. NB: a partial reversal can only be done on operations that have already been processed. Authorised operations must be cancelled in full, or partially deposited.
P	Processing

Example:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
        <alias>0000000050242004</alias>
        <ECREQ>
                <codTrans>T0000000000000000001</codtrans>
                <request_type >FA</request_type>
                <id_op>0000000001</id_op>
                <type_op>C</type_op>
                <importo>000123056</importo>
                <divisa>978</divisa>
                <codAut>098765</codAut>
                <importo_op>000120056</importo_op>
        </ECREQ>
        <user>User001</user>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSREQ>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias
- codTrans
- id_op
- type_op
- importo
- divisa
- codAut
- importo_op
- user
- secretKey

SAMPLE STRING

MAC = HASH SHA1(<alias><codTrans><id_op><type_op><importo><divisa><codAut><importo_op><user><SecretKey>)

Response message - ECRES

This message is returned by XPay in response to the ECReq message. It uses the same connection on which the message was received, and contains the result for the requested operation.
The following table lists the parameters that are included in the result:

Name	Description	Format
alias	Merchant identification code within XPay.	AN MAX 30 CHAR.
codTrans	Value indicated in the relevant ECReq message.	AN MAX 30 CHAR.
request_type	Value indicated in the relevant ECReq message.	AN 2 CHAR. fixed
esitoRichiesta	Result of the requested operation. For possible values, see the table below.	AN MAX 3 CHAR.
id_op	Value indicated in the relevant ECReq message.	N MAX 10 CHAR.
type_op	Value indicated in the relevant ECReq message.	AN 1 CHAR.
importo_op	Value indicated in the relevant ECReq message.	AN 9 CHAR. fixed
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR. fixed

requestResult: result of the requested operation. This field can take on the following values:

Code	Description
0	Request executed correctly
1	Request error: incorrect message format or missing or incorrect field
3	Request error: duplicate id_op field ("FA" case) or id_op not found ("RA" case)
16	Request error: alias field unknown or not enabled
18	Request error: operation denied by credit card issuer
2	Request error: an unexpected error occurred while processing the request
8	Request error: incorrect MAC
21	Operation error: transCode field unknown
22	Operation error: non-executable operation (e.g. reversal greater than deposit)

Example of a positive result:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
```

```
<VPOSRES>
<alias>0000000050242004</alias>
<ECRES>
<codTrans>T0000000000000000001</codTrans>
<request_type>FA</request_type>
<esitoRichiesta>0</esitoRichiesta>
<id_op>0000000001</id_op>
<type_op>C</type_op>
<importo_op>000120056</importo_op>
</ECRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

Example of a negative result:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
<alias>0000000050242004</alias>
<ECRES>
<codTrans>T0000000000000000001</codTrans>
<request_type>FA</request_type>
<esitoRichiesta>32</esitoRichiesta>
<id_op>0000000001</id_op>
<type_op>C</type_op>
<importo_op>000120056</importo_op>
</ECRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias
- codTrans
- esitoRichiesta
- id_op
- type_op
- importo_op
- secretKey

THE MAC WILL BE CALCULATED AS FOLLOWS

mac= HASH SHA(<alias><codTrans><esitoRichiesta><id_op><type_op><importo_op><SecretKey>)

Order Query

NOTES:

• These APIs are deprecated, remain available for existing users

This message can be used by the merchant's application to ask XPay for the current status of an order, and the status of all associated operations.

1. Requesting query towards Nexi Payment endpoint

IN PRACTICE

The XML message containing the parameters/values shown below must be sent, using the post method, to this URL:

https://ecommerce.nexi.it/ecomm/ecomm/XPayBo

2. Recording transaction details

IN PRACTICE

The query result must always be managed in XML format, and on the same connection as used for the request (synchronous response).

Request message - INTREQ

This table indicates the fields that must be included in the request message, and their corresponding characteristics.

Name	Description	Format
alias	Merchant identification code within XPay.	AN MAX 30 CHAR.
codTrans	Unique identification code for the order being queried by the merchant.	AN MAX 30 CHAR.
id_op	Unique identifier of the requested query.	N MAX 10 CHAR.
type_op	Always set to V (Verify order status).	AN 1 CHAR.
*user	Merchant operator making the query.	AN MAX 20 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR. fixed

*optional value

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
        <alias>0000000050242004</alias>
```

```
        <INTREQ>
            <codTrans>T0000000000000000001</codTrans>
            <id_op>0000000001</id_op>
            <type_op>V</type_op>
        </INTREQ>
        <user>User001</user>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
    </VPOSREQ>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias
- codTrans
- id_op
- type_op
- user
- secretKey

THE MAC WILL BE CALCULATED AS FOLLOWS
mac= HASH SHA1(<alias><codTrans><id_op><type_op><user><SecretKey>)

Response message - INTRES

This table indicates the fields that must be included in the request message, and their corresponding characteristics.
This message is returned by XPay in response to the IntReq message. It uses the same connection on which the message was received, and contains a list of the operations requested for the specified order, along with their corresponding status.
The message consists of the following elements:

- An alias element (always included) containing the merchant identification code within XPay
- An INTRES element (always included) containing the general transaction details and a list of operations undertaken on the specified transaction. The list of operations is contained in the OPERATIONS_LIST type element (which is always included where a transCode exists), consisting of OPERATION type elements and a NUMELM attribute which indicates the number of OPERATION type elements that are present in the list, and which may be 0 if the search did not return any results. The structure of the OPERATION element is detailed below.
  The list contains an OPERATION type element for each of the operations requested in relation to the specified order. The list contains only those operations that were successful.

- A MAC element (always included) containing the message security code.

The following table contains a description of the elements that XPay will include in the message (except for the OPERATIONS_LIST element):

Name	Description	Format
codTrans	Value indicated in the relevant IntReq message.	AN MAX 30 CHAR.
esitoRichiesta	Result of the requested query. For possible values, see the table below.	AN MAX 3 CHAR.
tipoCarta	Type of card used for Payment.	AN MAX 15 CHAR.
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
importo	Payment request amount	AN 9 CHAR. fixed
divisa	ISO code for the Payment request currency.	AN 3 CHAR. fixed
codAut	Authorisation code for the Payment request.	AN MAX 10 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	40 CHAR. fixed

requestResult: result of the requested operation. This field can take on the following values:

Name	Description
0	Operation processed correctly
1	Search error: incorrect message format or missing or incorrect field
16	Search error: alias field unknown or not enabled
2	Search error: an unexpected error occurred while processing the request
8	Search error: incorrect MAC
21	Search error: transCode field unknown (no successful Payment associated with the order specified) Please note that in this case the cardType, transactionType, importo, currency, and authCode elements of the message will contain an empty string and the OPTION FIELDS elements will not be included.
3	Request error: duplicate id_op field
32	transCode expired due to timeout, the user did not complete the Payment within 30 minutes of the order being generated.

The structure of the OPERATION element is as follows:

Name	Description	Format
id_op	Value indicated in the ECReq message which initiated the operation, or empty string for operations not performed using ECReq.	N MAX 10 CHAR.
type_op	Operation type. For possible values, see the table below.	AN 1 CHAR.
importo_op	Operation amount	AN 9 CHAR. fixed
divisa	ISO code for the operation currency.	AN 3 CHAR. fixed
dataOra	Date the operation was carried out.	Format: dd/mm/yyyy hh.mm.ss
result	Operation status. For possible values, see the table below.	AN MAX 3 CHAR.
*user	Merchant operator requesting the operation.	AN MAX 20 CHAR.
codiceEsito	Transaction result. The possible values are shown in the table here. This parameter is always returned when paying by card, but is not returned for all alternative payment methods	N MAX 3 CHAR.
descrizioneEsito	Transaction result. The possible values are shown in the table here - only for type_op=A	AN MAX 2000 CHAR.
dettaglioEsito	Shows a brief description of the Payment result. The possible values are shown in the table here - only for type_op=A	AN MAX 200 CHAR.

*optional value

type_op: the types of operations managed by XPay are as follows:

type_op	Description
A	Payment authorisation
R	Cancellation
P	Processing
C	Accounting reversal

result: the types of operations managed by XPay are as follows:

result	Description
E	Executed: this is the status used for authorisation and authorisation reversal operations, which are executed immediately.
D	To be sent: this is the status used for accounting and accounting reversal operations. In fact, XPay takes responsibility for these operations and subsequently processes them by generating an accounting file to be sent to the credit card

	issuer. Operations have this status if they have not yet been entered into an accounting file.
I	Sent: this is the status used for accounting and accounting reversal operations. Operations have this status if they have already been entered into an accounting file.

Example of an XML with a successful result:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
        <alias>0000000050242004</alias>
        <INTRES>
                <codTrans>T0000000000000000001</codTrans>
                <esitoRichiesta>0</esitoRichiesta>
                <tipoCarta>VISA</ tipoCarta >
                <tipoTransazione>VBV_FULL</tipoTransazione>
                <importo>000123056</importo>
                <divisa>978</divisa>
                <codAut>098765</codAut>
                 <OPERATIONS_LIST NUMELM="3">
                        <OPERATION>
                                <id_op></id_op>
                                <type_op>A</type_op>
                                <importo_op>000123056</importo_op>
                                <divisa>978</divisa>
                                <dataOra>06/07/2005 16.55.56</dataOra>
                                <result>E</result>
                                <user>User001</user>
                                <codiceEsito>0</codiceEsito>
                                <descrizioneEsito>autorizzazione
        concessa</descrizioneEsito>
                                <dettaglioEsito>Message OK</dettaglioEsito>
                        </OPERATION>
                        <OPERATION>
                                <id_op></id_op>
                                <type_op>P</type_op>
                                <importo_op>000123056</importo_op>
                                <divisa>978</divisa>
                                <dataOra>06/07/2005 16.56.20</dataOra>
                                <result>E</result>
                                <user>User001</user>
                        </OPERATION>
                        <OPERATION>
                                <id_op>0000000001</id_op>
                                <type_op>C</type_op>
                                <importo_op>000120056</importo_op>
```

```
                        <divisa>978</divisa>
                        <dataOra>07/07/2005 16.56.20</dataOra>
                        <result>E</result>
                        <user>User001</user>
                    </OPERATION>
                </OPERATIONS_LIST>
        </INTRES>
        <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```


Example of an XML with an unsuccessful result:


```
<VPOSRES>
<alias>0000000050242004</alias>
        <INTRES>
                <codTrans>T00000000000000000001</codTrans>
                <esitoRichiesta>21</esitoRichiesta>
                <tipoCarta>VISA</tipoCarta>
                <tipoTransazione>VBV_FULL</tipoTransazione>
                <importo>000123056</importo>
                <divisa>978</divisa>
                <codAut></codAut>
                <codiceEsito>103</codiceEsito>
                <descrizioneEsito>aut. negata dall'emittente della
        carta</descrizioneEsito>
                <dettaglioEsito>Auth. Denied</dettaglioEsito>
        </INTRES>
<mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```


MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias field
- transCod field of the INTRES tag
- requestResult field of the INTRES tag
- importo field of the INTRES tag
- currency field of the INTRES tag
- authCod field of the INTRES tag
- NUMELM field of the OPERATIONS_LIST tag

For each OPERATION element for the OPERATIONS_LIST tag, the following fields are also considered:

- id_op field
- type_op field
- importo_op field
- currency field
- result field
- user field
- secretKey

OPERATION tags must be considered in the order they were listed in the VPOSRes message forwarded by XPay.

Order List

NOTES:

• These APIs are deprecated, remain available for existing users

This message can be used by the merchant's application to request a complete list of transactions filtered by appropriate parameters.

1. Requesting query towards Nexi Payment endpoint

IN PRACTICE

The XML message containing the parameters/values shown below must be sent, using the post method, to this URL:

https://ecommerce.nexi.it/ecomm/ecomm/XPayBo

2. Recording the transaction list

IN PRACTICE

The query result must always be managed in XML format, and on the same connection as used for the request (synchronous response).

Request message - REPREQ

This table indicates the fields that must be included in the request message, and their corresponding characteristics.

Name	Description	Format
alias	Merchant identification code within XPay.	AN MAX 30 CHAR.
id_op	Identifier of the requested query.	N MAX 10 CHAR.
type_op	Indicates the type of operation for which the report is requested. If populated, it takes on the following values: ▪ A = authorisation ▪ R = authorisation reversal ▪ P = deposit ▪ C = accounting reversal ▪ T = all operations	AN 1 CHAR.
user	Merchant operator making the query.	AN MAX 20 CHAR.
start_date (*)	Start date and time	Format: YYYY-MM-DDThh:mm:ss
finish_date(*)	Finish date and time	Format: YYYY-MM-DDThh:mm:ss
mac	Message Authentication Code. Transaction signature field. For calculation	AN 40 CHAR. fixed

	details, see the end of this chapter: MAC Calculation.

(*) The XPay Payment platform makes the last 12 months of data available to merchants. Because of this, the validity range for the requested date must not be greater than 31 days.

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSREQ>
    <alias>0000000050242004</alias>
    <REPREQ>
        <id_op>1010</id_op>
        <type_op>A</type_op>
        <start_date>2006-05-15T09:00:00</start_date>
        <finish_date>2006-05-25T18:00:00</finish_date>
    </REPREQ>
    <user>User001</user>
    <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSREQ>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias
- id_op
- type_op
- user
- start_date
- finish_date
- secretKey

SAMPLE STRING
MAC= HASH SHA1(<alias ><id_op><type_op><user><start_date><finish_date><SecretKey>)

Response message - REPRES

This message is returned by XPay in response to the RepReq message. It uses the same connection on which the message was received, and contains the details of the requested report.
The message consists of the following elements:

- An alias element (always included) containing the merchant identification code within XPay
- A REPRES element (always included) consisting of a list of elements where each one corresponds to a specific operation (AUTH, MOV, ANNULMENT_AUTH, ANNULMENT_MOV). Each of these elements contains an attribute which indicates the number of transactions present for the specified operation, and which may be 0 if the search did not return any results.
- Each ELEMENT_AUTH, ELEMENT_MOV, ELEMENT_ANNULMENT_AUTH, ELEMENT_ANNULMENT_MOV element repeated for NUMELEM contains details specific to an individual transaction.
- A MAC element (always included) containing the message security code.

The following table contains a description of the elements included in the message:

Name	Description	Format
alias	Merchant identification code within XPay.	AN MAX 30 CHAR.
esitoRichiesta	Result of the requested query. For possible values, see the table below.	AN MAX 3 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR. fixed

The structure of the ELEMENT_AUTH, ELEMENT_MOV, ELEMENT_ANNULMENT_AUTH and ELEMENT_ANNULMENT_MOV element is shown below:

Name	Description	Format
codTrans	Order identifier within XPay.	AN MAX 30 CHAR.
result	Status of the requested operation.	AN MAX 3 CHAR.
tipoCarta	Type of card used for Payment.	AN MAX 15 CHAR.
tipoTransazione	Transaction type, indicates the Payment method. See the table here for possible values. If the Payment result is negative, an empty string will be sent.	AN MAX 20 CHAR.
importo	Request amount	AN 9 CHAR. fixed
divisa	ISO code for the Payment request currency.	AN 3 CHAR. fixed
codAut	Authorisation code for the Payment request.	AN MAX 10 CHAR.
dataOra	Date the operation was carried out.	Format: dd/mm/yyyy hh.mm.ss
user	Merchant operator requesting the operation.	AN MAX 20 CHAR.

result: the types of operations managed by XPay are as follows:

result	Description
E	Executed: this is the status used for authorisation and authorisation reversal operations, which are executed immediately.
D	To be sent: this is the status used for accounting and accounting reversal operations. In fact, XPay takes responsibility for these operations and subsequently processes them by generating an accounting file to be sent to the credit card issuer. Operations have this status if they have not yet been entered into an accounting file.
I	Sent: this is the status used for accounting and accounting reversal operations. Operations have this status if they have already been entered into an accounting file.

requestResult: result of the requested operation. This field can take on the following values:

code	Description
0	Operation processed correctly
1	Search error: incorrect message format or missing or incorrect field
16	Search error: alias field unknown or not enabled
3	Request error: duplicate id_op field
2	Search error: an unexpected error occurred while processing the request
8	Search error: incorrect MAC
30	Number of results returned is too high. Unable to process the request (*)
32	transCode expired due to timeout, the user did not complete the Payment within 30 minutes of the order being generated.
31	Error in the start_date or finish_date field, due to format type or a range greater than a year

(*) In order to optimise response times, the XPay platform does not consider any request which returns a number of results (elements) greater than 5,000 to be valid. In this case, the merchant must repeat the request, amending the filters for start_date, finish_date and transactionType fields.

Example of an XML with a successful result for a request where the merchant wants a report of all the operations made. It is distinguished by the tags AUTH = Authorisations, MOV = Movements, ANNULMENT_AUTH = Authorisation reversals, ANNULMENT_MOV = Accounting reversals.

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
        <alias>0000000050242004</alias>
        <REPRES>
        <AUTH NUMELM="1">
          <ELEMENT_AUTH>
                <transCode>T0000000000000000001</transCode>
                <resultCode>0</resultCode>
```

```
        <result>E</result>
        <cardType>VISA</cardType>
        <transactionType>VBV_FULL</transactionType>
        <importo>000023056</importo>
        <currency>978</currency>
        <authCode>098765</authCode>
        <dateTime>06/07/2005 16.55.56</dateTime>
        <user>User001</user>
    </ELEMENT_AUTH>
</AUTH>
<MOV NUMELM="1">
    <ELEMENT_MOV>
        <transCode>T0000000000000000001</transCode>
        <resultCode>0</resultCode>
        <result>E</result>
        <cardType>VISA</cardType>
        <transactionType>VBV_FULL</transactionType>
        <importo>000023056</importo>
        <currency>978</currency>
        <authCode>098765</authCode>
        <dateTime>06/07/2005 16.55.56</dateTime>
        <user>User001</user>
    </ELEMENT_MOV>
</MOV>
<ANNULMENT_AUTH NUMELM="1">
    <ELEMENT__ANNULMENT_AUTH>
        <transCode>T0000000000000000001</transCode>
        <resultCode>0</resultCode>
        <result>E</result>
        <cardType>VISA</cardType>
        <transactionType>VBV_FULL</transactionType>
        <importo>000023056</importo>
        <currency>978</currency>
        <authCode>098765</authCode>
        <dateTime>06/07/2005 16.55.56</dateTime>
        <user>User001</user>
    </ELEMENT_ANNULMENT_AUTH>
</ANNULMENT_AUTH>
<ANNULMENT_MOV NUMELM="1">
    <ELEMENT__ANNULMENT_MOV>
        <transCode>T0000000000000000001</transCode>
        <resultCode>0</resultCode>
        <result>E</result>
        <cardType>VISA</cardType>
        <transactionType>VBV_FULL</transactionType>
        <importo>000023056</importo>
        <currency>978</currency>
        <authCode>098765</authCode>
        <dateTime>06/07/2005 16.55.56</dateTime>
        <user>User001</user>
    </ELEMENT_ANNULMENT_MOV>
```

```
        </ANNULMENT_MOV>
    </REPRES>
    <requestResult>0</requestResult>
    <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

Example of an XML with an unsuccessful result for a request where the data requested by the merchant exceeds the allowable limit.

```
<VPOSRES>
    <alias>0000000050242004</alias>
    <REPRES/>
    <requestResult>30</requestResult>
    <mac>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</mac>
</VPOSRES>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- alias
- esitoRichiesta
- secretKey

SAMPLE STRING
MAC = HASH SHA1(<alias><esitoRichiesta><SecretKey>)