Issued by: Nexi SPA Version: 16.0 Issued on: 01/04/2020

Technical Specifications for Integration with the XPay Payment Gateway

TABLE OF CONTENTS

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	18/09/2017	Nexi	Addition link of GitHub example
11.3	24/10/2017	Nexi	Rebranding
11.4	08/03/2018	Nexi	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

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
- Blog at https://ecommerce.nexi.it
- Download Section (documents, specifications and brand repository)

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

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/web-mobile/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.

Codebase

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

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.

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 # character**. 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. If the MyBank service is activated, the only special characters that can be used are: / -: (). , + With Klarna you must not exceed 27 characters and the special characters accepted are: +, -.
url	Return url, directing back to the site upon completion of the transaction and transferring, using the GET method, the response parameters which show the transaction result.	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). 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.

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
urlpost	Url to which XPay sends the result of the transaction, transferring, in server-to-server mode using the POST method, the response parameters which show the transaction result. For detailed information on the parameters received, please refer to the Notification section.	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 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. 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	AN MAX 4000 CHAR.

	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.	
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 MAX 25 CHAR.
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 manages this function, it provides shipping information	AN

	in response. Valued with N does not return shipping data in response, if not present or valued with any other value, information is returned	
paypalCustom	additional field that remains in the detail of paypal order	AN
paypalInvoiceID	Identifies the invoice of the trader. for paypal is a unique one so the operator can not pass the same value for more than one order	AN
tipo_richiesta	"VC" (Card Verification) is used to perform a card verification, amount 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.	AN MAX 2 CHAR.

3D Secure 2.0

To use this service see **3D Secure 2.0**

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)

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.

Payment Notification Message: required fields

The merchant receives payment notification directly from the Nexi server through a POST call. The notification is sent to the address indicated in the "urlpost" parameter of the Payment Initiation Message.

WARNING:
To confirm receipt of the notification, the message returned from the call must be a "http 200".

No action must be taken on the transaction until the outcome (HTTP 200) has been returned in response to the notification.

The table below shows the parameters that are returned in the notification 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	Operation result	AN MAX 7 CHAR.
data	Transaction date	yyyymmdd
orario	Transaction time	HHmmss
codiceEsito	Transaction result. The possible values are shown in the table here.	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 the last 4 digits showing.	AN MAX 100 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, this will return a description of the card type used for payment (e.g. consumer).	AN MAX 200 CHAR.
Name	Name of the person who made the payment.	AN MAX 150 CHAR.
cogName	Surname of the person who made the payment.	AN MAX 150 CHAR.

Payment Notification Message: optional fields

This table indicates optional fields which may be present depending on the merchant configuration.

Name	Description	Format
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.	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 **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	MAX 700 CHAR.

	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 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 17–19 CHAR.
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

Payment Notification 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

Payment Notification Message: additional fields for Klarna

This table indicates the fields provided in response to Klarna payments

Name	Description	Format

klarnaID	Id defined by Klarna for this transaction	AN

Payment Notification Message: additional fields for Google Pay

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

Name	Descrizione	Formato
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

Payment Notification Message: addictional fields for WeChatPay and AliPay

This table shows fields submitted in reply for WechatPay and AliPay.

Name	Description	Format
codTransAPM	Transaction code given by partner	AN

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:

- Reaching out to technical support you can configure max 3 tentatives for payment with the same transaction cose. You can also choose, in case of more than one tentative, to leave users in XPay to retry payments or redirect to merchant site.
- Notification is sent for all payment tentative, if you have set more than one tentative for each transaction user will receive more notifications for the same order.

Payment Result Message

Once the payment has been completed, the customer is redirected to the merchant site at the address indicated in the payment initiation message ("url" field). The user then returns to the merchant's site, bringing the parameters that attest to the conclusion of the transaction.
The parameters are the same ones which we have already seen in the section regarding notifications, except that in this case they will be received using the GET method rather than the POST method. It is the responsibility of the merchant site to display a positive or negative message, based on the value of the "result" parameter received.
In the activation stage, merchants can also configure up to a maximum of 3 email addresses to receive a detailed message for every single transaction. In addition, they will also receive a daily summary email of all transactions undertaken on their virtual POS.

The merchant will receive the result of the payment in the following ways:

- By mail> The merchant will receive a message with the details of the transactions at the email address communicated during the configuration phase
- Online> Once the payment is completed, the user is redirected directly to the merchant's website, to the address indicated in the payment initiation message (field name "url"). The user then returns to the merchant's site, taking with him the parameters that attest to the conclusion of the transaction

Payment Result Message: required fields

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 # character. 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. If the MyBank service is activated, the only special characters that can be used are: / -: (). , + With Klarna you must not exceed 27 characters and the 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	AN MAX 7 CHAR.
data	Transaction date	yyyymmdd
orario	Transaction time	HHmmss
codiceEsito	Transaction result. The possible values are shown in the table here.	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 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.

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.
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	AN MAX 2000 CHAR.

	OUTPUT, otherwise the field will be null.		
tipoProdotto	If enabled, this will return a description of the card type used for payment (e.g. consumer).	AN MAX 200 CHAR.	
Name	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.
dati_gestione_consegna	Xml containing shipping information		MAX 700 CHAR.

Field name	Req.	Descriptio
WalletAddress		
BillingAddress		
City	YES	City
Country	YES	Country
CountrySubdivision	YES	
Line1	YES	address
Line2	NO	address
Line3	NO	address
PostalCode	YES	postal code

BillingAddress			
ShippingAddress			
	City	YES	City
	Country	YES	Country
	CountrySubdivision	YES	
	Line1	YES	address
	Line2	NO	address
	Line3	NO	address
	PostalCode	YES	postal code
	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</RecipientPh
oneNumber>
</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 17–19 CHAR.
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")	AN
BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

Payment Result Message: additional fields for Klarna

Name	Description	Format
klarnaID	Id defined by Klarna for this transaction	AN

Payment Result Message: additional fields for Amazon Pay

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	AN

Payment Result Message: additional fields for Google Pay

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

Name	Descrizione	Formato
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

Payment Notification Message: addictional fields for WeChatPay and AliPay

This table shows fields submitted in reply for WechatPay and AliPay.

Name	Description	Format
codTransAPM	Transaction code given by partner	AN

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>)

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/web-mobile/pagamento-semplice/pagamento-in-un-click

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.

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”.	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	AN 2 CHAR.
gruppo	The “gruppo” value is 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.

"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	The “gruppo” value is 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 17–19 CHAR.
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	N

	accepts otherwise with "0")	
BILLINGAGREEMENTID	Token that PayPal associates with the Nexi contract number	AN

3D Secure 2.0

To use this service see **3D Secure 2.0**

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 (subsequent payment)	AN 2 CHAR.
gruppo	The “gruppo” value is 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.

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.

"First Payment" initiation Message: required fields

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

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	The “gruppo” value is assigned by Nexi during activation.	AN MIN 4 MAX 10
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 # character. 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). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.
url	Return url, directing back to the site upon completion of the transaction and transferring, using the GET method, the response parameters which show the transaction result.	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).	AN MAX 200

	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

"First Payment" initiation Message: optional fields

The table below indicates optional fields that can be used to the discretion of the merchant.

Name	Description	Format
urlpost	Url to which XPay sends the result of the transaction, transferring, in server-to-server mode using the POST method, the response parameters which show the transaction result. For detailed information on the parameters received, please refer to the Notifi	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 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 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 MAX 25
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 MAX 20
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 manages this function, it provides shipping information in response. Valued with N does not return	AN

	shipping data in response, if not present or valued with any other value, information is returned	
paypalCustom	additional field that remains in the detail of paypal order	AN
paypalInvoiceID	Identifies the invoice of the trader. for paypal is a unique one so the operator can not pass the same value for more than one order	AN

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, $NAME, $COGNAME, EMAIL

3D Secure 2.0

To use this service see **3D Secure 2.0**

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>)

Do not forget

- 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.

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.

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 # character. 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). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.
esito	Result of the operation (Possible Values OK, KO, ANNULLO, ERRORE)	AN MAX 7

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

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_multi”.	AN MAX 30
gruppo	The value of the “gruppo” (group) is assigned during activation by Nexi	AN MIN 4 MAX 10
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 # character. The code must be unique for	AN MIN 2 MAX 30 (character # is forbitten). If the

	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	MyBank service is activated, the only special characters that can be used are: / -: (). , + 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.	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 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	AN MAX 7

	default language defined during the service configuration process.	
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

Payment result message: optional fields

You can receive the same optional data from the "CodeBase" solution in response with the addition of the specific parameters found below.

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.
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

Nome	Name of the person who made the payment.	AN MAX 150
tipoProdotto	If enabled, this will return a description of the card type used for payment (e.g. consumer).	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

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: required fields

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_multi”.	AN MAX 30
gruppo	The value of the “gruppo” (group) is assigned during activation by Nexi	AN MIN 4 MAX 10
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 # character. 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). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + 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.	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 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, this will return a description of the card type used for payment (e.g. consumer).	AN MAX 200
Nome	Name of the person who made the payment.	AN MAX 150

Payment notification message: optional fields

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.
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

- **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

Integrating recurring payments allows merchants to store credit card or PayPal account details, and use them to make subsequent payments. This service differs from the One Click Payment service, as it is the merchant who requests the recurring payment, rather than the end customer.
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/web-mobile/pagamento-semplice/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.

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) used for first paymens - RC (card renewal) used for update a card already associated with a contract	AN 2 CHAR.
gruppo	The "gruppo" value is 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.

"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	The "gruppo" value is 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 17–19 CHAR.
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 2.0

To use this service see **3D Secure 2.0**

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

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.

Github XPay sample code: **https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click/pagamento-successivo**

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

Download trace

Multi-Currency Payment (DCC)

This feature allows customers who have credit cards in currencies other than Euro to make a payment in their reference currency.
See supported currencies.

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 2.0

To use this service see **3D Secure 2.0**

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	AN 20 CHAR.

	space characters are added on the left until 20 characters are reached.	
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 Methods

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

Integration of these features is very simple and there are two options. As always, it starts by implementing the "Codebase" module:

1. The user chooses an alternative payment method in the Nexi environment after check out from the merchant's e-commerce site.
2. The user chooses an alternative payment method from the merchant's e-commerce site. In this case, the "selectedcard" parameter must be sent in order to direct the user to the correct page in relation to the payment method chosen.

Payment methods	Description	Activation mode
Visa Single and recurring payments	Visa is a payment card circuit recognized worldwide. It is currently one of the most popular.	Automatically activated with Nexi contract.
MasterCard Single and recurring payments	Mastercard is a payment card circuit recognized worldwide. It is currently one of the most popular.	Automatically activated with Nexi contract.
Maestro Single and recurring payments	Maestro is the debit card circuit of Mastercard's group.	Automatically activated with Nexi contract.
Masterpass Single and recurring payments	It allows you to create a free account on the bank channel.	Automatically activated with Nexi contract.
Google Pay Single and recurring payments	Google Pay allows you to pay quickly and easily using the credentials of your Google account.	Automatically activated with Nexi contract.

		XPay back office activation required.
Apple Pay Single and recurring payments	Linked to Apple devices, it allows you to pay quickly and securely.	Automatically activated with Nexi contract. XPay back office activation required.
JCB Single payments	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 Single payments	International payment card circuit based in China.	Can be activated on request with Nexi contract
American Express Single and recurring payments	American Express is an international credit card circuit.	Can be activated by contract with American Express.
Diners Single and recurring payments	Diners is an international credit card circuit.	Can be activated by contract with Diners.
Alipay Single payments	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 Single payments	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 Single payments	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 Single payments	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 Single payments	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 Single payments	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 inside the XPay back office.
Przelewy24 Single payments	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.
Amazon Pay Single and recurring payments	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.
PayPal Single and recurring payments	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 Single payments	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.

Google Pay

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

Activation

To make this payment method available on the cash page, you must activate it in the Nexi backoffice. No registration is required for Google.

It is possible to integrate Google Pay through the "Simple Payment" method or through API integrator

Simple Payment

Payment initiation does not change with respect to BaseCode.

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

Recurring Payments

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

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

Per integrare Google Pay in una pagina web tramite frame o XPay Build è necessario solamente abilitare il metodo di pagamento come indicato nella sezione precedente di "Attivazione".

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: a browser compatible with Google Pay must be used.

- webview: Chrome Custom Tabs must be used.
- frame in webview: Chrome Custom Tabs must be used.
- native: direct integration with Google Pay is required. The payment API is presented on the API integration page.

API Integration

In this case, Nexi will only take care of the authorization of the payment, the data concerning Google Pay will be collected by the Merchant website or app, which will forward the JSON received from Google to Nexi through the API described below.

URI
ecomm/api/paga/googlePay

METHODO
Post

ACCEPT
Application/json

Payment Initiation Message: required fields

Nome	Descrizione	Formato
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

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	Formato
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
informazioniContratto	Object whose structure is shown in the tables below.	Object

informazioniContratto

Nome	Descrizione	Formato
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used	AN MIN 5 MAX 30
codiceGruppo	Group assigned by Nexi	AN MIN 4 MAX 10
scadenzaContratto	Contract expiration date	DATE dd/mm/yyyy
rinnovoCarta	Indicates if a card renewal operation is taking place. Possible values: "true" or "false".	

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>)

Payment Result Message

Nome	Descrizione	Formato
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
ppo	Wallet payment (Apple Pay, Masterpass, ecc...)	AN MIN 2 - MAX 30 CRT
brand	Type of card used by the user to make paymen	AN MAX 100 CRT
tipoProdotto	Credit card type if qualified (eg.: consumer)	AN MAX 200 CRT
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*>)

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

You can accept payments via Apple Pay by activating the payment method from the Nexi back office. No registration is required for Apple.

It is possible to integrate the Apple Pay through the "Simple Payment" method or through AP integration.

Simple Payment

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

Payment initiation does not change with respect to BaseCode.

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

Recurring Payments

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

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 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.

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	Formato
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	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,

	following table an example of parameters	$EMAIL, $NOME, $COGNOME, EMAIL
informazioniContratto	Object whose structure is shown in the tables below.	Object

informazioniContratto

Nome	Descrizione	Formato
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used	AN MIN 5 MAX 30
codiceGruppo	Group assigned by Nexi	AN MIN 4 MAX 10
scadenzaContratto	Contract expiration date	DATE dd/mm/yyyy
rinnovoCarta	Indicates if a card renewal operation is taking place. Possible values: "true" or "false".	

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
ppo	Payment with wallet (Apple Pay, Masterpass, ecc...)	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
tipoProdotto	Method by which the payment was made, if the e-commerce used 3D-Secure, SSL, or MOTO.	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.

Recurring Payments

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

Diners

Activation

To make this card circuit available on the cashier page, you must contact Diners 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 Diners Commercial Service on 800 864 064 (from Monday to Friday from 09.00 to 20.00).

Once Diners informs you of the activation code, forward it by email by contacting support.ecommerce@nexi.it

It is possible to integrate Diners through the "Simple 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 Diners using the parameter “selectedcard” enhanced “DINERS” during initiation payment phase.

Recurring Payments

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

AliPay

Activation

To make this payment method available on the cash page, you must activate it in the Nexi backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to AliPay using the parameter “selectedcard” enhanced “ALIPAY” during initiation payment phase.

Backoffice 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 backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to WeChat Pay using the parameter “selectedcard” enhanced “WECHATPAY” during initiation payment phase.

Backoffice 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 backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to Giropay using the parameter “selectedcard” enhanced “GIROPAY” during initiation payment phase.

Backoffice 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."

iDEAL

Activation

To make this payment method available on the cash page, you must activate it in the Nexi backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to iDEAL using the parameter “selectedcard” enhanced “IDEAL” during initiation payment phase.

Backoffice 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."

Bancontact

Activation

To make this payment method available on the cash page, you must activate it in the Nexi backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to Bancontact using the parameter “selectedcard” enhanced “Bancontact” during initiation payment phase.

Backoffice 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 backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to EPS using the parameter “selectedcard” enhanced “EPS” during initiation payment phase.

Backoffice 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 backoffice entering the ID received by nexi partner

Payment

Payment initiation does not change with respect to BaseCode.
It is possible to redirect users directly to Przelewy24 using the parameter “selectedcard” enhanced “P24” during initiation payment phase.

Backoffice 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."

Amazon Pay

Activation

To set Amazon Pay service you have to select the “Amazon Pay” option into the backoffice.
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 backoffice.
To allow the payments, besides the XPay configurations, you have to enter into Amazon Pay portal, generate the MWS token and set:

- Field "URL restituiti consentiti"
  with https://ecommerce.nexi.it/ecomm/cassa/AmazonPayRedirect.jsp
- Field "Istant notification Integrator URL" with
  https://ecommerce.nexi.it/ecomm/amazonpay/Notification

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.

NOTES:

- In the case of Amazon Pay transactions, the "codAut" parameter is set to "AMAZON"

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 backoffice

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

Integrated Payments

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	Group assigned by Nexi (only for Recurring Payments)	AN MIN 4 MAX 10
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	To manage payment retry, following an error code 96, it is necessary to enhance this field with 'S', in other cases it is possible not to enhance it or not to include it in the object	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, Masterpass, 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, this will return a description of the card type used for payment (e.g. consumer).	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:	JSON

	codice -> error code, see table Restful API Error Codes Table messaggio -> error details	
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 # character. 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 Escluso carattere #. In caso di attivazione del servizio MyBank, i soli caratteri speciali utilizzabili sono: / - : ( ) . , +
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 # character. 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 backoffice Nexi in the “PayPal” Tab 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

You should register in the **sandbox area of PayPal**, in order to perform some test to verify these changes and receive your business account and buyer test account.

These information should be added in the test area of the Nexi backoffice

NOTE:

- If you want to enable “recurring” transactions you must contact the customer service of Paypal. If the PayPal recurring service is NOT active, the transactions will still be successful, but the contract will not be enabled.
  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.

Klarna Pay Now (Sofort)

Klarna is one of the main european payment suppliers. Klarna Pay Now (Sofort) is a solution that allows you to receive swiftly and safely credit transfers. It offers a quick shopping experience without the classical complications of the standard credit transfers.

Activation Set up

The merchant can configure his profile to use Klarna Pay Now (Sofort) through the "Sofort" backoffice section. In this section you will enter the project id, the customer number, the api key and the buyer protection obtained from registration done on the **Sofort portal**. You can also choose whether to receive notifications of order status changes sent from Sofort to Xpay sw and enable / disable the use of the payment method from the cash page

Payment

The process of requesting a payment does not change with respect to the base code. In the case of a valid call, XPay will display the "Klarna Pay Now" logo, if configured and enabled, within the selection page in the "Other payments" section. XPay will not display the logo, even if correctly configured, if:

- the request has the field "service_type" filled with "pay_multi", "paga_oc3d". this is done to avoid the creation of a contract with the possibility of recurring transaction
- the amount of the request is less than 10 cents, this is done to avoid the negative response from Klarna for too low amount

  The merchant will be able to redirect directly its customers to the Klarna cash page by filling the "selectedcard" parameter with "KLARNA" value in the payment initiation phase.
  NB: With the use of the "selectedcard" option, if the previous describe checks made by XPay fail, an error will be returned.
  .

Warning:

- In the case of Klarna transactions, the "codTrans" parameter can have a maximum length of 27 characters and the special characters accepted are:,. + -
- The cancellation of the payments in the event of a failed urlpost notification is NOT managed, in other word if the notification fails the Klarna order is NOT canceled.

Back office operation

The merchant can not perform reversal or refund transactions from the back office.
The merchant has the opportunity to flag in Xpay back office if a transaction not tracked by Klarna has been correctly accounted or has failed, in this way the merchant can verify the updated status at subsequent access without having to login in the merchant's bank portal the portal

Notice

In the event that the merchant has an agreement with klarna he can receive notifications regarding any changes in the status of payments.

In order to enable this option in the back office the merchant must activate the receipt of the notifications and in every request of new payment it must indicate in the "urlpost" parameter, the value of the link to which the notifications will be made..

Pending status

This notification is forwarded when a payment is generated.
The "status" parameter is changed to "pending".

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 (character # is forbitten). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + **With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.**
klarnaID	Id defined by Klarna for this transaction	AN
status	The status of the transaction	AN
data	Transaction date	DATA dd/mm/yyyy

orario	Hour of transaction	AN hh:mm:ss
sender_holder		AN
sender_account		AN
sender_bank_code		AN
sender_bank_name		AN
sender_bic		AN
sender_iban		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 reply message, the string to sign must contain the following fields:

- codTrans
- klarnaID
- status
- data
- orario
- chiaveSegreta <secret key>

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>klarnaID=<val>status=<val>data=<val>orario=<val><chiaveSegreta>

Loss

This notification is forwarded when a payment is rejected.
The "status" parameter is changed to "loss".

Name	Description	Format

numeroMerchant	Terminal assigned to the merchant by Nexi	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 (character # is forbitten). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + **With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.**
klarnaID	Id defined by Klarna for this transaction	AN
status	The status of the transaction	AN
data	Transaction date	DATA dd/mm/yyyy
orario	Hour of transaction	AN hh:mm:ss
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
- klarnaID
- status
- data
- orario
- chiaveSegreta< secret key>

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>klarnaID=<val>status=<val>data=<val>orario=<val><chiaveSegreta>

Receive

This notification is forwarded when a payment is authorized and complete.
The "status" parameter is changed to "receive".

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 (character # is forbitten). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + **With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.**
klarnaID	Id defined by Klarna for this transaction	AN
status	The status of the transaction	AN
data	Transaction date	DATA dd/mm/yyyy
orario	Hour of transaction	AN hh:mm:ss
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
- klarnaID
- status
- data
- orario
- chiaveSegreta< secret key>

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>klarnaID=<val>status=<val>data=<val>orario=<val><chiaveSegreta>

Untraceable

This notification is forwarded when a payment is not done on the Klarna bank .
The "status" parameter is changed to "Untreaceable".

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 (character # is forbitten). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + **With Klarna you must not exceed 27 characters and the special characters accepted are only : +, -.**
klarnaID	Id defined by Klarna for this transaction	AN
status	The status of the transaction	AN
data	Transaction date	DATA dd/mm/yyyy
orario	Hour of transaction	AN hh:mm:ss
sender_holder		AN
sender_account		AN
sender_bank_code		AN
sender_bank_name		AN
sender_bic		AN

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

- codTrans
- klarnaID
- status
- data
- orario
- chiaveSegreta< secret key>

SAMPLE STRING
MAC = HASH SHA1(codTrans=<val>klarnaID=<val>status=<val>data=<val>orario=<val><chiaveSegreta>

Refunded

The "status" parameter is changed to "refunded”.

Name	Description	Format
numeroMerchant	Terminal assigned to the merchant by Nexi	AN MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 (character # is forbitten). If the MyBank service is activated, the only special characters that can be used are: / -: (). , + **With Klarna you must not exceed 27 characters and the special characters**

		accepted are only : +, -.
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
klarnaID	Id defined by Klarna for this transaction	AN
status	The status of the transaction	AN
data	Transaction date	DATA dd/mm/yyyy
orario	Hour of transaction	AN hh:mm:ss
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
- importo
- divisa
- klarnaID
- status
- data
- orario
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(codTrans=<val>importo=<val>divisa=<val>klarnaID=<val>status=<val>data=<val>orario=<val><chiaveSegreta>)

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.

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 backoffice.
- 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 5 days (3 for PayPal). 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.

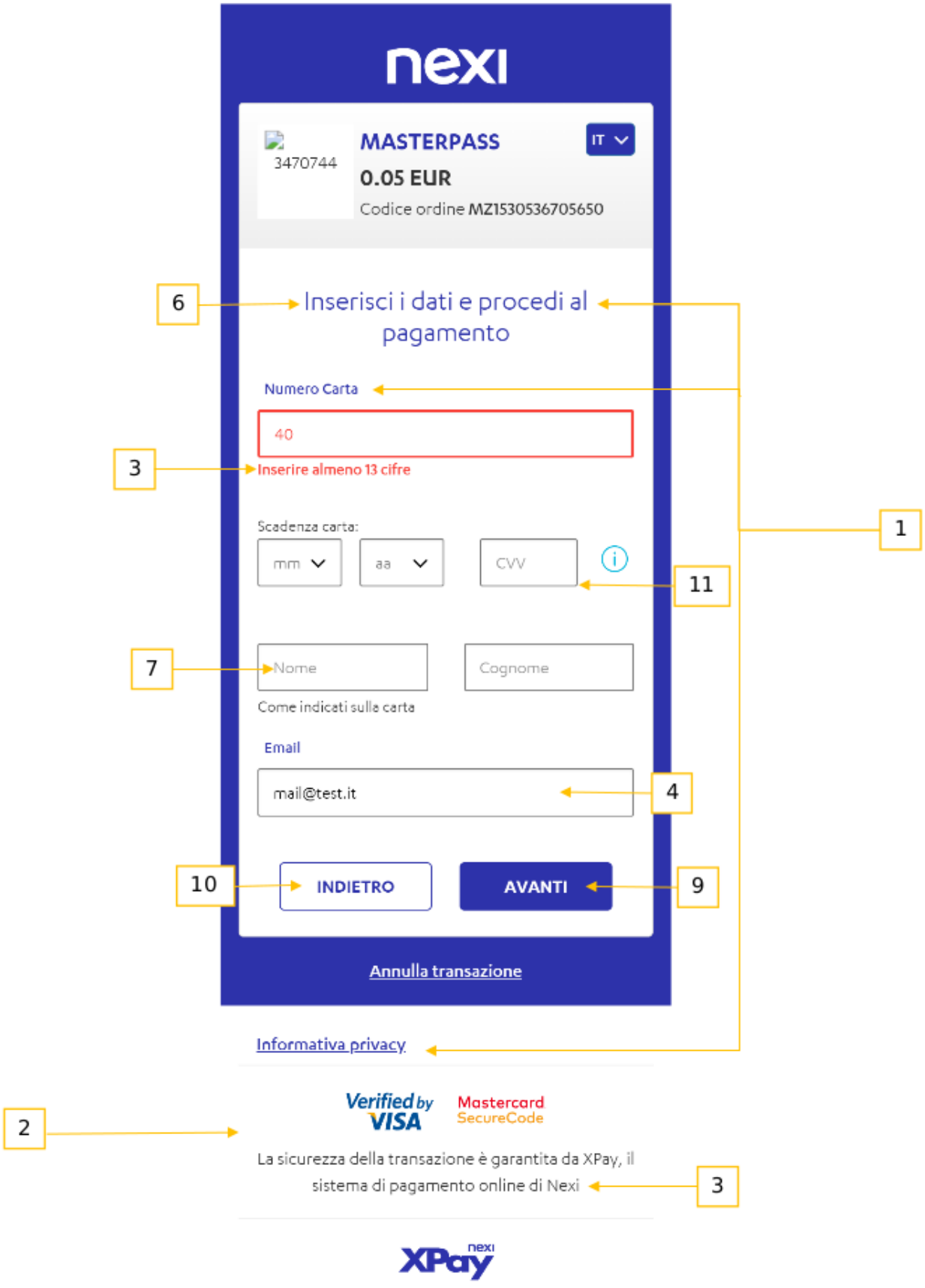
Personalization

Merchants can modify the syle of cash page sending additional paramenters that define page properties.
These parameters must be added to the address used to redirect their customers during the initiation phase of the payment.
The parameters that manage the cash page style can also be sent only once, Nexi will keep the configuration sent until it is overwritten with a more recent one or returned to the default one.

Below is the table containing the modifiable properties.

Name	Description	Format
primary-color	Change the color of the texts Item 1	Format Hexadecimal format color MAX 7
sfondo-footer	Change the color of footer background Item 2	Format Hexadecimal format color MAX 7
color-footer-text	Change the color of footer background Item 3	Format Hexadecimal format color MAX 7
sfondo-input	Change the color of input background Item 4	Format Hexadecimal format color MAX 7

color-error-msg	Change the color of errore message and of input Item 5	Format Hexadecimal format color MAX 7
font-Title-Heigth	Change height of page title Item 6	Format 10px o 10%
color-input-text	Change the color of text entered by users (input fields of form) Item 7	Format Hexadecimal format color MAX 7
font-Heigth	Change height of text except Item 8	Format 10px o 10%
font	Change font of the page	Existing font
button-color	Change botton color Item 9	Format Hexadecimal format color MAX 7
input-radius	Defines the radius of the input angles Item 10	Value in px
button-radius	Define the radius of the corners of the button Item 11	Value in px
back-To-Default	If it is enhanced, it restores the default configuration	


nexi
3470744
MASTERPASS
IT
0.05 EUR
Codice ordine MZ1530536705650
6
Inserisci i dati e procedi al pagamento
Numero Carta
40
3
Inserire almeno 13 cifre
Scadenza carta:
mm
aa
CVV
11
1
7
Nome
Cognome
Come indicati sulla carta
Email
mail@test.it
4
10
INDIETRO
AVANTI
9
Annulla transazione
Informativa privacy
Verified by VISA
Mastercard SecureCode
2
La sicurezza della transazione è garantita da XPay, il sistema di pagamento online di Nexi
3
nexi XPay

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, Masterpass, 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)

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, Masterpass, 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

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

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 'payXpayNonce' to make the payment with the xpayNonce provided by the SDK.

Environment comfiguration

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

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

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

Object paymentParams

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 # and _ 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.	

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 2.0

If you want to manage the 3D Secure 2.0 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

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

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.
Exaple:

```
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

```
// 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.MASTERPASS
- 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)

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 PayPal and ApplePay payment

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 (MasterPass, 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.createXpayNonce("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.

NOTES:

In response to the json together with the xpayNonce the card detail is shown as in the example below

"dettaglioCarta": {
"brand": "MASTERCARD",
"tipoProdotto": "PROPRIETARY ATM - DEBIT - N",
"prepagata": "N",

"pan": "525599******9992",
"scadenza": "202012",
"regione": "",
"nazionalita": "USA"
}

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, this will return a description of the card type used for payment (e.g. consumer).	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
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.

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 payXpayNonce 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.

URI
ecomm/api/hostedPayments/pagaNonce

METHODO
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 35
timeStamp	Timestamp in millisecond format	N 13 CHAR
tipo_contratto	- 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 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	Credit card type if qualified (eg.: consumer)	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
ppo	Payment with Masterpass wallet	AN MIN 2 MAX 30 only MasterPass

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 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 case of KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

Recurring Payment

First payment

Integrating recurring payments allows merchants to store credit card or PayPal account details, and use them to make subsequent payments.

Create a contract through a valid xpayNonce. 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: required fileds

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 35
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	Group assigned by Nexi	AN MIN 4 MAX 10

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. 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, $NAME, $COGNAME, EMAIL
tipo_contratto	- 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.	

Name	Description	Format

mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
Name	Name of the person who made the payment.	AN MAX 150
cogName	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 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.

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	Credit card type if qualified (eg.: consumer)	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
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 MAX 30 solo MasterPass

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>)

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:

URL AMBIENTE DI TEST
https://int-ecommerce.nexi.it

URL AMBIENTE DI PRODUZIONE
https://ecommerce.nexi.it

URI
ecomm/api/recurring/pagamentoRicorrente

METHODO
POST

ACCEPT
application/json

Subsequential payment initiation message: required fields

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 characters, excluding the # and _ characters. The code must be unique for each authorization request.	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	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
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. 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.

Name	Description	Format
mail	Buyer's email address to which the payment result will be sent.	AN MAX 150
Name	Name of the person who made the payment.	AN MAX 150
cogName	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 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>)

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, this will return a description of the card type used for payment (e.g. consumer).	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
ppo	Payment with Masterpass wallet	AN MIN 2 MAX 30 only MasterPass
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
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." "BACKOFFICE"	AN

	"PAGAMENTO" "CIRCUITI"	
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 ": {}

- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

OneClick Payment

First 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.

Create a contract through a valid xpayNonce. 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: required fileds

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 35
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	Group assigned by Nexi	AN MIN 4 MAX 10

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. 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, $NAME, $COGNAME, EMAIL
tipo_contratto	- S forza un primo pagamento di tipo MIT SCHEDULED - U forza un primo pagamento di tipo MIT UNSCHEDULED E' necessario passare questo parametro all'interno dell'oggetto "parametriAggiuntivi" e all'interno del calcolo del MAC come parametro prima del timestamp.	

Name	Description	Format
mail	Buyer’s email address to which the payment result will be sent.	AN MAX 150
Name	Name of the person who made the payment.	AN MAX 150

cogName	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 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.

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	Credit card type if qualified (eg.: consumer)	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
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 MAX 30 solo MasterPass

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>)

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 "contract_number" and "group" parameters in the "customParams" object, enhancing them with the appropriate contract number and group assigned
- add the "serviceType" field with value "paga_oc3d" in the config object
- add the "requestType" field with "PR" value in the config object

Payment

The payment does not change compared to the basic payment.

3D-secure Management

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 2.0

The 3D Secure 2.0 service is managed through the enhancement of the JSON information Security object whose content is considered in the 3DSecure 2.0 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: {
                threeDSRequestorChallengeIndicator: "01",
        },
        language : XPay.LANGUAGE.ITA,
        serviceType: "paga_rico",
        requestType: "PP",
        }

//Inizializzazione del pagamento
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.threeDSRequestorChallengeIndicator = "01";
```

```
// Creazione del xpayNonce e assegnazione dell'handler di gestione della
        XPay.createXpayNonce("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.createXpayNonce () call.

```
        var payForm = document.getElementById('payment-form');
        payForm.elements['pagaBtn'].addEventListener("click", function () {
                this.disabled = true;

                var infoSicurezza = {};
                infoSicurezza.threeDSRequestorChallengeIndicator = "01";
                XPay.setInformazioniSicurezza(infoSicurezza);

// Creazione del xpayNonce e assegnazione dell'handler di gestione della
                XPay.createXpayNonce("payment-form", card);
        });
});
```

APM Lightbox

The default of payments through alternative payment methods (except Paypal, ApplePay and GooglePay) involves a redirect of the user's browser to the payment page of the chosen method.
It is possible to request to manage payment methods in non-fullredirect mode by specifying the "fullRedirect" parameter in false in the payment configuration json:

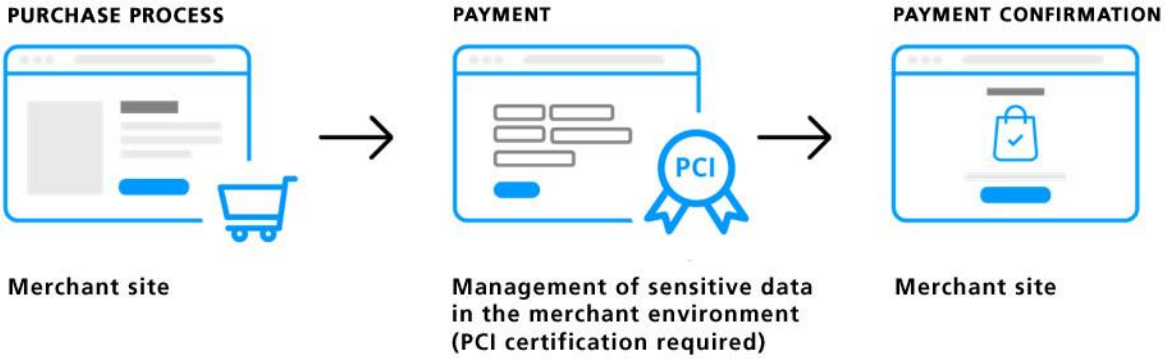
```
    var config = {
        baseConfig: {
            apiKey: ${requestScope.alias},
            enviroment: XPay.Environments.INTEG,
            fullRedirect: false
        },
paymentParams : {
    amount : ${requestScope.importo},
    transactionId : ${requestScope.codTrans},
    currency : ${requestScope.divisa},
```

XPay will open a new browser window in popup with the appearance of a lightbox where the user can make the payment. Once payment has been completed, the outcome of the transaction will be communicated to the merchant page via the XPay_Payment_Result event, as is the case for the Paypal, ApplePay and GooglePay methods.

As the outcome of the payment is communicated through the event the url and urlBack parameters of the paymentParams object are not considered by XPay if specified.

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/web-mobile/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

This service carries out 3D-Secure payment transactions and provides duplicate APIs: one for 3D-Secure verification and one for payment.
In the first step, the API responds with a JSON containing the html code provided by the MPI, which is to be included with the details being used by 3D-Secure. It is the receiver's responsibility to print the html received onto the user's browser. After authentication by the user, the API communicates the result to the response address specified in the request. Once the XpayNonce has been received in response, the next step is to recall the second API for carrying out the actual 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/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 idOperazione	AN MAX 500 CHAR.

	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 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 service to work	JSON

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>)

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.
html	HTML code to be printed on the user's browser for 3D-Secure authentication.	
errore	Only present when the result is ko. It is an object containing: codice -> codice errore, see table messaggio -> dettaglio errore	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
- operationId
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(esito=<val>operationId=<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.

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 35 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.
tipoProdotto	If enabled, this will return a description of the card type used for payment (e.g. consumer).	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.

Payment Result Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass

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 transaction code and passing as parameter "softDecline" valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

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/web-mobile/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.
Name	Name of the person who made the payment.	AN MAX 150 CHAR.
cogName	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, this will return a description of the card type used for payment (e.g. consumer).	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.

Payment Result Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass

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 ": {}

Card verification

The following API performs a card verification not aimed at tokenization, but for the sole purpose of verifying whether a card is valid.
This service requires the merchant to achieve PCI DSS certification.

URI
ecomm/api/recurring/verificaCartaSSL

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.
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.
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 5 - MAX 30 CHAR.
verificaCarta	Valued with "true"	boolean
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
codiceGruppo	Code assigned by Nexi during activation.	AN MIN 4 - MAX 10 CHAR.
tipo_contratto	- 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
- pan
- scadenza
- cvv
- timeStamp
- secretKey

SAMPLE STRING
MAC= HASH SHA1(apiKey=<val> pan=<val>scadenza=<val>cvv=<val> timeStamp=<val><SecretKey>)

Payment 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, 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

MAC CALCULATION RESULT MESSAGE
MAC= HASH SHA(esito=<val>idOperazione=<val>timeStamp=<val>SecretKey)

NOTES:

- Fill (only PCI compliant) the pan, the maturity and the CVV (optional) without enhancing numeroContratto to verify the validity of the card.
- fill the numeroContratto, without evaluating the card data, to verify that the card associated with the contract is still valid. N.B. In this case, since the card data is not present, the calculation of the mac changes by entering the Contract number in place of the card data.

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.

URI
ecomm/api/paga/pagaMPI

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.
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.

Payment Initiation Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass
threeDSServerTransID	Contains the potential 3DS Server Transaction ID, generated in case of 3DSECURE 2.0	AN
mitFramework	Object needed to handle Merchant Initiated Transaction (MIT) transactions. The composition is described in the following table.	JSON

Oggetto mitFramework

Name	Description	Format
operazione	compliant values are described in the table MIT Framework parameters	AN
networkData		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: required fields

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.

Payment Result Message: optional fields

Il campo opzionale threeDSServerTransID contiene l'eventuale 3DS Server Transaction Id generato in caso di 3DSECURE 2.0.

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass
threeDSServerTransID	Contains the potential 3DS Server Transaction ID, generated in case of 3DSECURE 2.0	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:
As this is a synchronous payment, POST notifications are not performed.

Recurring Payment - One Click Payment

Integrating Recurring and OneClickPay services allows end customers to store their credit card details on the Nexi systems and use them to make subsequent purchases with just one click, or for merchants to send recurring payments (for example, in subscription or invoicing services). At a technical level, management of these services is divided into 2 main stages:

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

Github XPay sample code: https://github.com/NexiPayments/XPay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click

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. The first transaction can be an actual payment, or just a card verification with no charge to the user.

If the first transaction is an actual payment, the API sequence used is as follows:

- To manage 3D-Secure authentication -> creaNonce
- To manage the payment -> primoPagamento3DS

If the first transaction is registration with card verification only, the API sequence used is as follows:

- To manage 3D-Secure authentication -> creaNonceVerificaCarta
- To manage verification of card validity -> verificaCarta3DS

Management of subsequent payments

Management of subsequent OneClick and recurring payments is similar at the technical level. In practice, the merchant application/site must use the API:

recurringPayment

3D-Secure Card Verification

This service carries out card verification transactions, with no charge to the customer, using the 3D-Secure method. This service provides duplicate APIs: one for 3D-Secure verification and one for payment.
The API responds with a JSON containing the html code provided by XPay, which is to be included with the details being used by 3D-Secure. It is the receiver's responsibility to print the html received onto the user's browser. After authentication by the user, the API communicates the result.

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 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 fields

Name	Description	Format
informazioniSicurezza	JSON object whose structure is described in the 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 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>)

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.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 35 CHAR.
html	HTML code to be printed on the user's browser for 3D-Secure authentication.	
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 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:
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 35 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	- 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 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

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. This service provides duplicate APIs: one for 3D-Secure verification and one for payment.
The API responds with a JSON containing the html code provided by XPay, which is to be included with the details being used by 3D-Secure. It is the receiver's responsibility to print

the html received onto the user's browser. After authentication by the user, the API communicates the result.

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/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 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 service to work	JSON

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.
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 35 CHAR.

html	HTML code to be printed on the user's browser for 3D-Secure authentication.	
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 if a xpayNonce is received

For the result message if a xpayNonce is received, the string to sign must contain the following fields:

- esito
- idOperazione
- xpayNonce
- timeStamp
- secretKey

SAMPLE STRING

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

MAC calculation if html or errors are received

For the result message if html or errors are received, 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 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 35 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. For MyBank: AN MAX 140 CRT you can use just these special characters/ - : ( ) . , For PAYPAL: AN MAX 127 CHAR
scadenzaContratto	Scadenza del contratto creato	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	- 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 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 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.

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, this will return a description of the card type used for payment (e.g. consumer).	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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass

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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

3D-Secure Subsequent Payment

When you need to charge a previously registered contract, your system must send a call with contract data previously registered with the first payment or verification 3D-Secure or SSL card. This type of call will require the inclusion of the 3D-Secure code also on recurring payments.

3D-Secure Authentication

It permits to create a xpayNonce to be used to make a payment. If the call requires the 3DSecure (3DSecure card and merchant enabled for the function) to be performed, a json containing the html code will be returned to perform the 3DSecure and then the xpayNonce only if the authentication has been successful. The xpayNonce will be returned to the address urlResponse, which is a mandatory parameter if you want to perform the 3DSecure. The expiration field of the incoming json is the expiration of the card, useful in case you need to update it.

URI

ecomm/api/recurring/creaNonceRico3DS

METHOD

Post

ACCEPT
Application/json

Payment Initiation Message: required fields

Nome	Descrizione	Formato
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	Formato
scadenza	Credit card expiry date	DATA aaaamm
informazioniSicurezza	JSON object whose structure is described in the 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 service to work	JSON

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>)

Payment Result Message

Nome	Descrizione	Formato
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	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 outcome message, the string to be signed must contain the following fields:

- esito
- idOperazione
- html
- timeStamp
- chiaveSegreta

SAMPLE STRING

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

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	Formato
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 35
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	Formato

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 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 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	Formato
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, this will return a description of the card type used for payment (e.g. consumer).	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
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass
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
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." "BACKOFFICE" "PAGAMENTO" "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 caso di esito KO con codice di errore 96, è possibile ritentare il pagamento riutilizzando lo stesso codice transazione e passando come parametro "softDecline" valorizzato a "S" nella creaNonce. Si riceverà in risposta il codice html che forzerà la SCA, in modo da ottenere un nuovo nonce da utilizzare nell'api pagaNonce.
- E' possibile effettuare pagamenti OneClick utilizzando numeri contratto creati da transazioni MIT scheduled e unscheduled.

Subsequent Payment (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, this will return a description of the card type used for payment (e.g. consumer).	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
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass
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
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." "BACKOFFICE" "PAGAMENTO" "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": {}

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/web-mobile/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. For AMEX cards only, it is a four-digit code and is found on the front of cards.	N MAX 4 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. 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	- 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.

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, this will return a description of the card type used for payment (e.g. consumer).	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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass

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, this will return a description of the card type used for payment (e.g. consumer).	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
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass
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
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." "BACKOFFICE" "PAGAMENTO" "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 ": {}

DCC

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 38 currencies.
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.

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/web-mobile/server-to-server/pagamento-dcc

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:	AN MAX 500 CHAR.

	esito 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 fileds

Nome	Descrizione	Formato
informazioniSicurezza	JSON object whose structure is described in the 3DSecure 2.0 section. It is necessary for the 3DSecure 2.0 service to work	JSON

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 35 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, this will return a description of the card type used for payment (e.g. consumer).	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
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

AN EXAMPLE OF THIS STRING MAY BE

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

AN EXAMPLE OF THIS STRING MAY BE

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 35 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-	N MAX 4 CHAR.

	digit code and is found on the front of cards.	
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, this will return a description of the card type used for payment (e.g. consumer).	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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR. only Masterpass

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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

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.

Notes

This solution is compatible only with payment cards.

Payment Management

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

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:

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

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 required fields

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 # character. 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

Oggetto paymentParams optional fields

Name	Description	Format
urlPost	URL to which XPay sends the transaction result passing, in server-to-server mode with POST method, the response parameters with the outcome of the transaction.	AN MAX 500

3D Secure 2.0

To manage 2.0 3D-Secure protocols, you have to call this function:

XPay.setInformazioniSicurezza({});

passing as paramater the JSON object which content is described in 3DSecure 2.0 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 of the payment and other details.

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

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 tokenise the customer's card data, so that he can make recurrences for subscriptions or other services.

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.

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:

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	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 4 MAX 10

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.

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.

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.

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	Unique code assigned by the merchant for matching with the archive containing sensitive credit card data	AN MIN 4 MAX 10

NOTES:

- In the first payment phase, if the amount "0" (zero) is used, XPay will send a verification request to the circuit with tokenization.

Recurring Subsequent Payment

To make subsequent payments follow the instructions in the section 3D-Secure Subsequent Payment

SDK FOR APP
Integrate Nexi in your APP

IOS SDK

Getting Started

Nexi provides the SDK for the iOS platform on the public CocoaPods repository. By connecting to it, you can download the SDK directly from your development environment in the most appropriate version for your application.

NOTA: 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.

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: We advise not to include the secret key within your app, but to have it available via a back end runtime request.

MAC configuration

Below is a list of methods for customising the MAC Calculation configuration:

```
XPay._MacConfig.IsOnlyValues = false // false if the MAC expects both keys and values, or true if it only expects values
XPay._MacConfig.ExternalSeparator = “” // Defines the separator between key-value pair
XPay._MacConfig.InternalSeparator = “=” // Defines the separator between key and value
XPay._MacConfig.Algorithm = .SHA1 // Defines the algorithm for MAC hashing
XPay._MacConfig.IsUppercase = false // false if the MAC uses lowercase characters, or true if it uses uppercase characters
XPay._MacConfig.IsUrlEncode = false // false if the MAC does not use Url encoding, or true if it does
XPay._MacConfig.IsBase64Encode = false // false if the MAC does not use Base64 encoding, or true if it does
```

NOTES: Any changes to MAC settings can be agreed with Nexi.

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._BackOffice.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:

- BackOffice
- 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", transCode: "NUMBER_ORDER", currency: CurrencyUtilsQP.EUR, amount: 1000)

Below is an example of how to use the XPay payment page, with the previously created request:

```
xPay._FrontOffice.pagaQP(apiFrontOfficeQPRequest, parentController: self) { (response) in
  if response.IsValid {
        if response.IsCanceled {
              print("Il pagamento è stato annullato dall'utente")
        }
        else {
              print("Il pagamento si è concluso correttamente, codice transazione: " + response.CodTrans)
        }
  }
  else {
        print("La risposta non è valida ") THIS INDICATES A SECURITY ERROR
  }
```

If the response is valid, the IsValid property in the response will be true. Alternatively, if it is false, the response is not valid, and it will contain error messages with their corresponding codes. In order to confirm that the payment was cancelled by the user, it will be necessary to check whether the IsCanceled variable is in the true state. If it is set to true, then the user cancelled the payment, otherwise it would have been brought to completion correctly.

The specifications for this methodology are as follows:

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 specifications for this methodology are as follows:

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 # character.** 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 # character.** 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	N MAX 9 CHAR.

	numbers to the right represent the euro cents.	
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".

Easy Payment with Contract Registration

To manage an initial payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

Name	Description	Format
tipo_servizio	The field must be set to: “paga_oc3d”.	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 paymens	AN 2 CHAR.

	- PR (subsequent payment) used in subsequent payments - RC (card renewal) used for update a card already associated with a contract

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.

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”.

Native Form

To facilitate the native integration by the developers, a specific control was created that can be used 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 "createXpayNonce" 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 can be disabled by setting the "enableKeyboard" property to false (also from 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).

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 "createXpayNonce" method. Below is an example of a code:

```
do {
try cardForm.createXpayNonce(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
createXpayNonce

METHOD
contabilizza

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 # character**. 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,	AN MIN 2 MAX 30 NO #. If MyBank you canuse only: / - : ( ) . , +

	the merchant may choose to decrease this to less than 3 attempts.	
handler	The function that listens to the API call	AN

RESPONSE

CLASS
ApiCreaNonceResponse

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 35

PAYMENT

Once the nonce is received, payment can be made via the pagaNonce API.

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 BackOffice. 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:

- As already mentioned, it is necessary 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

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	Credit card nation	AN MIN 2 MAX 30
codTrans	Payment identification code consisting of alphanumeric characters, excluding the # character. 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 #. If the MyBank service is activated, the only special characters that can be used are: / -: (). , +
SelectedEnvironment	Execution enviroment	AN
ShippingFields	Shipping address	AN
BillingFields	Billing address	AN

RESPONSE

CLASS
ApiApplePayResponse

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
ppo	Wallet payment (Apple pay, Masterpass, ecc...)	AN MIN 2 MAX 30
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")
}
```

ANDROID SDK

Getting Started

Nexi provides the Android platform SDK on the public JCenter repository. By connecting to it, you can download the SDK directly from your development environment in the most appropriate version for your application.

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.

Begin by importing the AAR library into the app project, following 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:
We advise not to include the secret key within your app, but to have it available via a back end runtime request.

MAC configuration

Below is a list of methods for customising the MAC Calculation configuration:

XPay.macConfig.setOnlyValues(false); // false if the MAC expects both keys and values, or true if it only expects values
XPay.macConfig.setExternalSeparator(“”); // Defines the separator between key-value pair
XPay.macConfig.setInternalSeparator(“=”); // Defines the separator between key and value
XPay.macConfig.setAlgorithm(“SHA1”); // Defines the algorithm for MAC hashing
XPay.macConfig.setUppercase(false); // false if the MAC only uses lowercase characters, or true if it uses uppercase characters
XPay.macConfig.setUrlEncode(false); // Set to false if the MAC does not use Url encoding, or true if it does
XPay.macConfig.setBase64Encode(false); // false if the MAC does not use Base64 encoding, or true if it does

NOTES:
Any changes to MAC settings can be agreed with Nexi.

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:

- BackOffice
- 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;
```

Easy Payment

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();
}
```

In this case, you will need to capture the triggered exceptions.

- MacException: Exception generated if a MAC control error or calculation error occurs.

Below is an example of how to use the XPay payment page, with the previously created request:

```
xPay.FrontOffice.pay(
        apiFrontOfficeQPRequest,
        new FrontOfficeQPCallback() {
            @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 specifications for this methodology are as follows:

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 # character.** 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 # character.** 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.

Easy Payment with Contract Registration

To manage an initial payment from the FrontOffice WebView, you need to pass the following additional parameters using the addExtraKeys() method:

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 paymens - PR (subsequent payment) used in subsequent payments - RC (card renewal) used for update a card already associated with a contract	AN 2 CHAR.

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.

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”.

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 "createXpayNonce" 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 "createXpayNonce" method. Here is an example of code:

```
try {
cardFormMultiline.createXpayNonce(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
createXpayNonce

Nome	Descrizione	Formato
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 # character.** 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

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 35

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

Nome	Descrizione	Formato
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 # character.** 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 Escluso carattere #. In caso di attivazione del servizio MyBank, i soli caratteri speciali utilizzabili sono: / - : ( ) . , +
amount	Amount expressed in euro cents without separators	N MAX 9
currency	978 per Euro	AN MAX 3

RESPONSE

CLASS
ApiFrontOfficeQPResponse

Nome	Descrizione	Formato
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 # character.** 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

Nome	Descrizione	Formato
extraParameters	Optional extra parameters	AN

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:

- If you have not already done so, 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
}
});
```

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());
}
```

SERVICES AVAILABLE ON ANDROID AND IOS SDKS

Backoffice 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 # character**. 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 # character**. 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
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 # character**. 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 # character**. 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.
nOrder	Search by order	AN
codTrans	Payment identification code consisting of alphanumeric characters, **excluding the # character**. 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.

	choose to decrease this to less than 3 attempts.

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 # character**. 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 # character**. 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 # character**. 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	AN MAX 500

	response parameters with the result of the transaction

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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
taxCode	User CF Codice fiscale	AN MAX 16
expire	Card expiry date	DATA
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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
nMerchant	Terminal assigned by Nexi to the merchant	AN MAX 30
taxCode	User CF Codice fiscale	AN MAX 16
expire	Card expiry date	DATA
status	Order Status	AN
hashPan	hashPan where you want to verify association	
dRegistration	Operation data	DATA

Contract Management

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

Name	Description	Format

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 the SCT format but is truncated to the 140th character	AN MAX 2000 For MyBank: AN MAX 140 CRT and you can use only: / - : ( ) . , + For PAYPAL: AN MAX 127 CHAR
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

Name	Description	Format
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

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
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 # character**. 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 # character**. 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 35

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 # character**. The code must be unique for each authorisation request. If, and only if,	AN MIN 2 - MAX 30 CHAR.

	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.	
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 # character**. 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	OBJ

	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.	
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 # character**. 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 Escluso carattere #. In caso di attivazione del servizio MyBank, i soli caratteri speciali utilizzabili sono: / - : ( ) . , +
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
ppo	Wallet Payment (Apple pay, Masterpass, ecc...)	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:

- creaNoncePrimoPagamento3DS - to manage 3D-Secure authentication
- primoPagamento3DS - to manage payment and contract registration

No 3D-Secure:

- primoPagamentoSSL - 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
ApiPrimoPagamentoSSLRequest

METHOD
primoPagamentoSSL

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 # character**. 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
ApiPrimoPagamentoSSLResponse

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.

Optional parameters

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	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.

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	OBJ

	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.

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 35 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 35 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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

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
ApiCreaNoncePrimoPagamento3DSRequest

METHOD
creaNoncePrimoPagamento3DS

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

Name	Description	Format
codTrans	Payment identification code consisting of alphanumeric characters, **excluding the # character**. 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
ApiCreaNoncePrimoPagamento3DSResponse

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 35 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 ApiCreaNoncePrimoPagamento3DSResponse will be returned after this has been completed.

Payment and contract registration

REQUEST

CLASS
ApiPrimoPagamento3DSRequest

METHOD
primoPagamento3DS

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 # character**. 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 35 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
ApiPrimoPagamento3DSResponse

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.
- In case of KO outcome with error code 96, it is possible to retry the payment by reusing the same transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce.

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
ApiPrimoPagamentoMOTORequest

METHOD
primoPagamentoMOTO

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 # character**. 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

Nome	Descrizione	Formato
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
ApiPrimoPagamentoMOTOResponse

Nome	Descrizione	Formato
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
ppo	Wallet Payment (Apple pay, Masterpass, ecc...)	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.

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
ApiPagamentoRicorrenteRequest

METHOD
pagamentoRicorrente

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 # character**. 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
ApiPagamentoRicorrenteResponse

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.

Optional parameters

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	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

ApiPagamentoRicorrenteMOTORequest

METHOD
pagamentoRicorrenteMOTO

Nome	Descrizione	Formato
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 # character**. 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
ApiPagamentoRicorrenteMOTOResponse

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
ppo	Wallet payment (Apple pay, Masterpass, ecc...)	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
ApiCreaNoncePagamentoRicorrente3DSRequest

METHODO
creaNoncePagamentoRicorrente3DS

Nome	Descrizione	Formato
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 # character**. 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 Escluso carattere #. In caso di attivazione del servizio MyBank, i soli caratteri speciali utilizzabili sono: / - : ( ) . , +
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
ApiCreaNoncePagamentoRicorrente3DSResponse

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 35

Payment

REQUEST

CLASSE
ApiPagamentoRicorrente3DSRequest

METHODO
pagamentoRicorrente3DS

Nome	Descrizione	Formato
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 # character**. 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 Escluso carattere #. In caso di attivazione del servizio MyBank, i soli caratteri speciali utilizzabili sono: / - : ( ) . , +
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 35

RESPONSE

CLASSE

ApiPagamentoRicorrente3DSResponse

Nome	Descrizione	Formato
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
ppo	Wallet Payment (Apple pay, Masterpass, ecc...)	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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce

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). 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.
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 # character**. 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 35 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.

Optional parameters

Name	Description	Format
ppo	Wallet payment (Apple pay, Masterpass, etc ...)	AN MIN 2 - MAX 30 CHAR.

ELECTRONIC INVOICING

XPay allows you to issue electronic invoices quickly and easily using the Get Your Bill service.

The service guarantees numerous advantages:

- Allows you to quickly manage invoice issuing and reduce operations
- It is easy to use and integrated into the back office of the XPay gateway
- Allows you to quickly archive and search all invoices
- It is sufficient to switch to XPay the Get Your Bill code or the VAT number or the customer's fiscal code and all the personal data are recovered directly from the system

Backoffice operations

In the back office the GYB section has been added from where the merchant can perform:

- Search for invoices
- Creating an invoice without payment
- The cancellation of an invoice issued
- Creating a P @ ymail link with invoice issue

The creation of an invoice and the cancellation are operations accessible only to the users of the back office device, while the search is accessible to all users.

XpayNonce Fattura Creation

URI
ecomm/api/fattura/creaNonceFattura

METHOD
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
numeroFattura	Contains the document number (just incremental part)	AN
numeroFatturaCompleto	Contains the document number, including any prefixes / suffixes	AN
tipoFattura	Invoice type (1 = traditional, 61 = electronic)	N
cliente	JSON object whose structure is described in the following table	JSON
carrello	Array of objects that describe the article whose structure is described in the table below	Array
iva	Describes section/field including taxable amount. Array of objects whose structure is described in the table below	Array
sconto	It represents the applied head discount expressed in hundredths	N MAX 9
note	Possible invoice notes	AN MAX 400
timeStamp	Timestamp in millisecond format.	N 13
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40

CLIENTE OBJECT

Name	Description	Format
codiceGYB	GYB USER CODE	AN
partitaIVA	USER VAT CODE	AN
codiceFiscale	User CF	AN

ARTICOLO OBJECT: required fields

Name	Description	Format
codice	Iterm code	AN MAX 20
importoTotale	Total amount expressed in cents	N MAX 9
quantita	Number of items	N
importoUnitario	Unitary amount of the item expressed in cents	N MAX 9
descrizione	Item description	AN MAX 500
importoIVA	VAT amount for the item	N MAX 9
codiceIVA	VAT code for the item. Possible values VAT codes	AN MAX 20

ARTICOLO OBJECT: optional fields

Name	Description	Format
codiceTipo	To be used for fuel product types	AN MAX 20
codiceValore	To be used for fuel product types	AN MAX 20
targa	Licence plate	AN MAX 50
numeroddt	Ddt number	AN MAX 100
dataddt	ddt date	DATE dd/mm/yyyy hh:mi:ss
numeroScontrino	Ticket number to which the invoice refers	AN MAX 100

dataScontrino	Ticket date to which the invoice refers	DATA dd/mm/yyyy hh:mi:ss
unitaMisura	Unit of measure of the row	AN MAX 100
sconto	It represents the applied head discount expressed in hundredths	N MAX 9

VAT OBJECT

Name	Description	Format
aliquotaIVA	Applied rate VAT	N es. 10.00
imponibileIVA	taxable amount of the various VAT invoices	N
importoIVA	VAT amount for the item	N MAX 9
importoLordo	Total current VAT caption expressed in hundredths	N MAX 9
codiceIVA	VAT code for the item. Possible values VAT codes	AN MAX 20

MAC Calculation

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

- apiKey
- codiceTransazione
- importo
- articolo<codice_0>=<importo_0>
- articolo<codice_1>=<importo_1>
- articolo<codice_n>=<importo_n>
- sconto
- timeStamp
- chiaveSegreta

In the string used in the calculation of the MAC all the articles must be specified in the order in which they are present in the "cart" array in the form: "article <code_i> = <import_i>".

SAMPLE STRING

MAC = HASH SHA1 (apiKey=<val>codiceTransazione=<val>importo=<val>articolo<val_codice_0>=<val_importo_0>articolo<val_codice_1>=<val_importo_1>timeStamp=<val><chiaveSegreta>)

Notification 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
xpayNonce	Code assigned by XPay for use in the payment request.	AN MAX 35
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
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
- xpayNonce
- timeStamp
- chiaveSegreta

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

L’api crea un nuovo xpayNonce se le seguenti verifiche hanno esito positivo:
• Active service enabled on the merchant

• Merchant with GYB service configured and enabled
• Valued transaction code that complies with the XPay standard
• At least one of the valued customer parameters is present
• The complete invoice number and the invoice number are evaluated
• The invoice type is a valid value
• The cart contains at least one element and each element has the mandatory fields valued and with formally valid values
• The vat amount contains at least one element and a maximum of 5. Each with the required mandatory fields and with formally valid values
• The total is congruent with what is obtained by summing up the various items: it is verified that (∑ cart.importTotal) - (∑ cart.discount) - discount = amount and what amount = (∑ VAT VAT) - discount.

Obtained a positive outcome from the API with the xpayNonce, the merchant can call the Cash page by adding the enhanced billing parameter Y to indicate the invoice request and the billing_xpayNonce parameter set to the value of the xpayNonce obtained from previous API.

Invoice Report

It allows you to query XPay to get a list of invoices, applying different filter conditions. It is mandatory to enter the search date period.
The response report will contain 1 to n json objects, one per invoice found.

URI
Ecomm/api/fattura/reportFatture

METODO
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
numeroFattura	Contains the document number (just incremental part)	AN
numeroFatturaCompleto	Contains the document number, including any prefixes / suffixes	AN
codiceRecupero	Valued with the recovery code obtained from GYB in the event of a positive outcome	AN
ricercaDal	Search by date from	DATA dd/mm/yyyy
ricercaAl	Search by date to	DATA dd/mm/yyyy
cliente	JSON object whose structure is described in the following table	JSON
timeStamp	Timestamp in millisecond format	N 13
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40

CLIENTE OBJECT

Name	Description	Format
codiceGYB	GYB USER CODE	AN
partitaIVA	USER VAT CODE	AN
codiceFiscale	User CF	AN

MAC Calculation

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

- apiKey
- ricercaDal
- ricercaAl
- timestamp
- chiaveSegreta

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

Result 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
report	Contains one or more objects whose structure is shown in the following table	Array
timeStamp	Timestamp in millisecond format	N 13
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CRT

REPORT OBJECT

Nome	Descrizione	Formato
stato	Inovoice status. Possible values Invoice Status Codes	AN
Stato ordine	Status Description	AN
codiceTransazione	Transaction identifier assigned by the merchant.	AN MIN 2 MAX 30
numeroFattura	Contains the document number (just incremental part)	AN
dataEmissione	Invoice issue date	DATA dd/mm/yyyy

codiceRecupero	Valued with the recovery code obtained from GYB in the event of a positive outcome	AN
annullabile	Indicates if the transaction is cancelable	true/false
cliente	JSON object whose structure is described in the following table	JSON

CLIENTE OBJECT

Name	Description	Format
codiceGYB	GYB USER CODE	AN
partitaIVA	USER VAT CODE	AN
codiceFiscale	User CF	AN

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>)

Invoice Call Off

It allows you to cancel the invoice associated with the indicated transaction and recovery code.

URI

ecomm/api/fattura/annullaFattura

METODO
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
codiceRecupero	Valued with the recovery code obtained from GYB in the event of a positive outcome	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

MAC Calculation

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

- apikey
- codiceTransazione
- codiceRecupero
- timeStamp
- chiaveSegreta

SAMPLE STRING

MAC = HASH SHA1(apikey=<val>codiceTransazione=<val>codiceRecupero=<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

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>)

3D SECURE 2.0

The new 3D Secure 2.0 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.

3DSecure 2.0 management via API

The structure of the "informazioniSicurezza" JSON object required for 3DSecure 2.0 service is described below:

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

Name	Description	Format

email	Buyer Mail	AN MIN 1 MAX 254
msisdn	Mobile number	AN MIN 1 MAX 16
homePhone	Home Phone	AN MIN 1 MAX 16
workPhone	Work Phone	AN MIN 1 MAX 16
account	Cardholder’s ID Account	AN MIN 1 MAX 64

Shipping address, "destinationAddress" element

Name	Description	Format
city	City	AN MIN 1 MAX 40
countryCode	Country code	AN 3 CHA
street	Street	AN MIN 1 MAX 50
street2	Address first detail	AN MIN 1 MAX 50
street3	Address second detail	AN MIN 1 MAX 50
postalCode	Postal Code	AN MIN 1 MAX 8
stateCode	Province abbreviation	AN 2 CHA

Billing address, "billingAddress" element

Name	Description	Format
city	City	AN MIN 1 MAX 8
countryCode	Country code	AN 3 CHA

street	Street	AN MIN 1 MAX 50
street2	Address first detail	AN MIN 1 MAX 50
street3	Address second detail	AN MIN 1 MAX 50
postalCode	Postal Code	AN MIN 1 MAX 8
stateCode	Province abbreviation	AN 2CHA

Cardholder account information, "cardHolderAcctInfo" element

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 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 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

Name	Description	Format
deliveryEmail	Delivery email address for intangible purchases	AN MIN 1 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)	JSON
giftCardCount	Number of gift or prepaid cards used	N MAX 2 CHA

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

3DSecure 2.0 management through redirection

The following are the parameters necessary for the 3DSecure 2.0 service to function:

Buyer Information

Name	Description	Format
Buyer_email	Cardholder’s email	AN
Buyer_homePhone	Buyer’s home phone	AN
Buyer_workPhone	Buyer’s work phone	AN
Buyer_msisdn	Mobile phone	AN
Buyer_account	Buyer account on merchant site	AN

Shipping address information

Name	Description	Format
Dest_city	City of destination of the shipment	AN
Dest_country	Country code (ISO3166-1) numeric of 3 digits	AN
Dest_street	Delivery address	AN
Dest_street2	Second delivery address row	AN
Dest_street3	Third delivery address row	AN
Dest_cap	Postal code	AN
Dest_state	Province code	AN

Billing address information

Name	Description	Format
Bill_city	Billing city	AN
Bill_country	Country code (ISO3166-1) numeric of 3 digits	AN
Bill_street	Billing Address	AN
Bill_street2	Third billing address row	AN
Bill_street3	Second billing address row	AN
Bill_cap	Postal code	AN
Bill_state	Province code	AN

Buyer account information

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 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	N

	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	

Information concerning the reliability of the merchant:

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.	N
gca_curr	Currency code of the gift or prepaid card used for the transaction (ISO 4217)	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.	N

	02 = Goods already purchased previously.	
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

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-backoffice/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	The field is only present when depositing a PayPal transaction and is required for managing reversals.	

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-backoffice/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
TipoPagamento	Method by which the payment was made, if the e-commerce used 3D-Secure, SSL, or MOTO, with Klarna PayNow(Sofort) Bonifico diretto	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	Credit card type	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
dataOperazione	Operation date	dd/mm/yyyy
tipoServizio	Type of service used for the transaction.	AN
Name	Customer name	AN MIN 2 - MAX 30 CHAR.
cogName	Customer surname	AN MIN 2 - MAX 30 CHAR.
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
Name	Customer name	AN MIN 2 - MAX 30 CHAR.
cogName	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.
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.
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 status:

- Autorizzato: the payment has been authorized, not yet accounted for. The accounting is normally done automatically by NEXI, at midnight on the same day
- Negato: The payment was not authorized. It will therefore not be accounted.
- Annullato: the payment was authorized but then canceled, either due to an error in notification, or due to the explicit action of the merchant (via back office, or via API)
- Contabilizzato: payment has been accounted.
- Rimborsato: the payment, previously accounted for, was completely reimbursed to the user.
- Non Creato: the payment did not reach the authorization, there was a problem on the previous phases (eg: interruption of the 3DSecure by the user)
- Contabilizzato Parz.: on payment a partial payment of the authorized amount has been made.

- Rimborsato Parz.: a partial repayment of the amount booked was made on the payment.

Order List

This allows to get a list of orders that meet the chosen filters in a request.

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

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.	DATE
	Possible values for channel: All MyBank CreditCard PayPal Sofort	AN
stato	Valorizzando questo parametro verranno restituiti solo gli ordini in un determinato stato (es. Annullato). E' possibile inserire in questo array più valori durante una ricerca (Autorizzato, Negato, Annullato).	AN

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

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

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.
tipoPagamento	Method by which the payment was made, if the e-commerce used 3D-Secure, SSL, or MOTO, with Klarna Pay Now (Sofort): bonifico diretto	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, this will return a description of the card type used for payment (e.g. consumer).	AN MAX 200 CHAR.
pan	Masked credit card number with only the first 6 and the last 4 digits showing.	AN MAX 19 CHAR.
parametri	Additional parameters	AN
stato	Order status	AN
dataTransazione	Transaction date	DATE dd/mm/yyyy
dataOperazione	Operation date	DATE dd/mm/yyyy
tipoServizio	Type of service used for the transaction.	AN
Name	Name of the person who made the payment.	AN MAX 150 CHAR.
cogName	Surname of the person who made the payment.	AN MAX 150 CHAR.
mail	Buyer's email address to which the payment result will be sent.	AN MAX 150 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:

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 status:
- Autorizzato
- Negato
- Annullato
- Incassato
- rimborsato
- nonCreato
- incParziale
- rimbParziale

Possible values per channel:
- All
- MyBank
- CartaCredito
- PayPal
- Sofort

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-backoffice/richiesta-link-Pay-by-Link

URI
ecomm/api/bo/richiestaPay-by-Link

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.
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.

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	AN 40 CHAR.

	details, see the end of this chapter: MAC Calculation.	
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
Pay-by-LinkUrl	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.

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 backoffice, in the "Report" section, inserting the type, filters, data and format of the report to be generated.

URI
ecomm/api/bo/elencoReport

METHODO
Post

ACCEPT
Application/json

Messaggio di Avvio

Nome	Descrizione	Formato
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

UN ESEMPIO DI TALE STRINGA POTREBBE ESSERE
MAC = HASH SHA1(apiKey<val> timeStamp=<val>chiaveSegreta>)

Messaggio di Esito

Nome	Descrizione	Formato
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

Nome	Descrizione	Formato
dataElaborazione	processing data	DATA dd/MM/yyyy HH:mi:ss
formato	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

UN ESEMPIO DI TALE STRINGA POTREBBE ESSERE
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

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.

URI
ecomm/api/bo/ReportPay-by-Link

METHOD
Post

ACCEPT
Application/json

Initiation Message: required fields

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

Initiation Message: optional fields

If not passed, the search is carried out on the previous week

Name	Description	Format
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

NOTA: 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).

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
Pay-by-Link	Array whose structure is described in the following table	Array
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

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"	N
statoEsteso	Status description. Possible values: - "Link P@ymail non utilizzato", - "Pagamento Effettuato Correttamente", - "Pagamento Non Riuscito"	AN

dataTransazione	Transaction 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

MAC Calculation

For the startup 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>)

ADDITIONAL SERVICES

The following RESTful APIs are available for merchants to manage the additional services available on XPay, in particular:
a) Creation of a Recurring Contract
b) Cancellation of Recurring/OneClickPay contracts
c) Cancellation of Tax Code/PAN pairing
d) Contract read-out
e) Blacklist management

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/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 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.
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. 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	AN

	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.	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 Management - 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 Management - 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 Management - 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 Management - 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 Management 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 Management - 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 (BACKOFFICE, 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)
- BACKOFFICE - Card Data manually edited via backoffice application
- PAGAMENTO - 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

METODO
POST

ACCEPT
application/json

Initiation Message: required fileds

Name	Description	Format
apiKey	Alias assigned to the merchant by Nexi.	AN 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
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
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
codiceTransazione	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
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." "BACKOFFICE" "PAGAMENTO" "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 - 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 or contract code.	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. 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>)

Control Management - 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>)

Control Management - 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. 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>)

Control Management - 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. 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>)

Control Management - 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	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.	

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>)

Control Management - 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	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.	

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.

Control Management - 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

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 transaction code and passing as a "softDecline" parameter valued at "S" in the creaNonce. You will receive in response the html code that will force the SCA, in order to obtain a new nonce to be used in the API pagaNonce
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: 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

Transaction Type Coding

transactionType	Description
NO_3DSECURE (*NO_3DSECURE _MASTERPASS)	The merchant is not enabled to use the Verified by Visa and Mastercard Identity Check security protocols, or the protocols could not be used.
VBV_FULL (*VBV_FULL _MASTERPASS)	The merchant is enabled to use the Verified by Visa protocol, and the cardholder is registered for the service and has been properly authenticated.
SC_FULL (*SC_FULL _MASTERPASS)	The merchant is enabled to use the Mastercard Identity Check protocol, and the cardholder is registered for the service and has been properly authenticated.
VBV_MERCHANT (*VBV_MERCHANT _MASTERPASS)	The merchant is enabled to use the Verified by Visa protocol, but the cardholder or credit card issuer do not use this service.
SC_MERCHANT (*SC_MERCHANT _MASTERPASS)	The merchant is enabled to use the Mastercard Identity Check protocol, but the cardholder or credit card issuer do not use this service.
M.O.T.O.	This value is used when it is not an e-commerce transaction (which involves buyers making purchases by using their own browsers). Instead, it is a Mail Order Telephone Order transaction, where credit card details are provided from the buyer to the merchant.

AMEX_FULL	The merchant is enabled to use the AMEX SafeKey protocol, and the cardholder is registered for the service and has been properly authenticated.
AMEX_MERCHANT	The merchant is enabled to use the AMEX SafeKey protocol, but the cardholder is not registered for the service.
EXPRESSCO	The transaction was made using a PayPal account.
Paga Ora	The transaction has been processed by Klarna
AMAZONPAY	The transaction has been processed by Amazon Pay
GOOGLEPAY	The transaction has been processed by GooglePay
APPLEPAY	The transaction has been processed by ApplePay
ALIPAY	The transaction has been processed by AliPay
WECHATPAY	The transaction has been processed by WeChatPay

*Transaction made using Masterpass Wallet.

Coding: message and resultDetails

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 3DSecure	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).

Card Type Coding

brand/cardType/selectedcard
VISA
MasterCard
Amex
Diners
Jcb
Maestro
MYBANK (only for brand)
SCT (only for selectedcard, allows payment by MyBank transfer only)
SDD (only for selectedcard)
CC (only for selectedcard, allows payment by credit cards only)
Masterpass (only for selectedcard, allows payment by Masterpass wallet only)
BANCOMAT
SOFORT (for brand and selectedcard)
PAYPAL (only for brand)
AMAZONPAY (for brand and selectedcard)
GOOGLEPAY (for selectedcard)
APPLEPAY (for selectedcard)
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)

Coding: resultCode and resultDescription

resultCode	resultDescription
0	Authorization granted
20	Order not present
101	incorrect or missing parameters
102	Incorrect PAN
103	Authorisation denied by card issuer
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	Check BLACKLIST (or check PAN, or check TC, or check TC/PAN combination) -> result only occurs when filters are being used

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
401	Expired card
402	Restricted card
403	Invalid merchant
404	Transaction not permitted
405	Not sufficient funds
406	Technical problem
407	Host not found

ECI, XID and CAVV Coding

VISA	Status	Eci	Cavv	Xid
VERes	N	30	NO	NO
VERes	U	20	NO	NO
PARes	Y	11	YES	YES
PARes	A	31	YES	YES
PARes	N	00	NO	NO
PARes	U	20	NO	NO

MASTERCARD/MAESTRO	Status	Eci	Cavv	Xid
VERes	N	30	NO	NO
VERes	U	20	NO	NO
PARes	Y	11	YES	YES
PARes	A	30	YES	YES
PARes	N	00	NO	NO
PARes	U	20	NO	NO

SSL Transactions	Eci	Cavv	Xid
	20	NO	NO

VERes/PARes result description:

3D Secure Mess.	VERes	Transaction
	N	Card not enrolled
	U	Unable to supply status / no response

3D Secure Mess.	VERes	Transaction
	Y	CH passed authentication
	A	Attempt
	N	CH Failed authentication
	U	Unable to authenticate CH/ no response
	N	Card not enrolled
	U	Unable to supply status / no response

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 backoffice

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
1.1.6	5	10.2
1.2.0	5.1	11.1
1.2.3	5.1.2	11.2.1

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 initiated by the merchant or unscheduled card holder. Save the networkData value returned by the API for subsequent recurring transactions.	No
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

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.

Codebase

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 # character**. 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, directing back to the site upon completion of the transaction and transferring, using the GET method, the response parameters which show the transaction result.	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. 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.
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 result of the transaction, transferring, in server-to-server mode using the POST method, the response parameters which show the transaction result.	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. 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	AN MAX 4000 CHAR.

	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.	
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 MAX 25 CHAR.
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>)

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>ID0000000000025486A</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=31376271324E6B684F3255447533507576470 6C56644F513D3
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, this will return a description of the card type used for payment (e.g. consumer).	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.	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	The “group” value is 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.
*PPO	Allowed values: Y or N. If present and set to Y, identifies a card from the MasterCard Masterpass wallet, therefore the CVV2 field becomes optional. If set to N, identifies a card acquired directly by the merchant.	AN MAX 4 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>T00000000000000000001</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.
*PPO	Allowed values: Y or N. If present and set to Y, identifies a card from the MasterCard Masterpass wallet, therefore the CVV2 field becomes optional. If set to N, identifies a card acquired directly by the merchant.	AN MAX 4 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.

Codebase

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 # character**. 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, directing back to the site upon completion of the transaction and transferring, using the GET method, the response parameters which show the transaction result.	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). The url will be called queuing the following parameters:	AN MAX 200 CHAR.

Field name	Description
Importo	Request amount
Divisa	EUR

	codTrans Esito NB: if result = ANNULLO, the merchant may choose to return the user to the payment page with the same transaction code.	payment identification code assigned by the merchant Possible values: ANNULLO or ERROR	
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 result of the transaction, transferring, in server-to-server mode using the POST method, the response parameters which show the transaction result.		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	AN MAX 2000 CHAR. For MyBank: AN MAX 140 CRT

	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.	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 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 MAX 25 CHAR.
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	AN 20 CHAR.

	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 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.	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 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, this will return a description of the card type used for payment (e.g. consumer).	AN MAX 200 CHAR.
Name	Name of the person who made the payment.	AN MAX 150 CHAR.
cogName	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.

<table>
<tr><th>Name</th><th>Description</th><th>Format</th></tr>
<tr><td>Parametri aggiuntivi</td><td>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.</td><td>AN MAX 4000 CHAR.</td></tr>
<tr><td>mail</td><td>Email address of the person who made the payment.</td><td>AN MAX 150 CHAR.</td></tr>
<tr><td>hash</td><td>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.</td><td>AN 28 CHAR.</td></tr>
<tr><td>infoc</td><td>Additional information about the individual payment. This information can be transmitted to the company on the basis of prior agreement with the same company.</td><td>AN MAX 35 CHAR.</td></tr>
<tr><td>infob</td><td>Additional information about the individual payment. This information can be transmitted to the bank on the basis of prior agreement with the same bank.</td><td>AN MAX 20 CHAR.</td></tr>
<tr><td>codiceConvenzione</td><td>Merchant code assigned by the acquirer. Where required.</td><td>AN MAX 15 CHAR.</td></tr>
<tr><td>dati_gestione_consegna</td><td>Xml containing shipping information
WalletAddress
BillingAddress
City — YES — City
Country — YES — Country
CountrySubdivision — YES
Line1 — YES — address
Line2 — NO — address
Line3 — NO — address
PostalCode — YES — postal cod
BillingAddress</td><td>MAX 700 CHAR.</td></tr>
</table>

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 17–19 CHAR.
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	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	The “gruppo” value is 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.	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>)

PLUGIN

Do you already have an e-commerce platform?

You can integrate Nexi with your e-commerce in just a few clicks.

Nexi solutions are compatible with the major e-commerce platforms on the market. Implementation is easy and fast. Just go to the marketplace, download the plugin, and integrate it.

PLUGIN for Prestashop

Payment module for the Nexi system dedicated to the CMS Prestashop.
Go to plugin

PLUGIN for WooCommerce

Module which allows Nexi XPay gateway to be used on WordPress/WooCommerce platforms.
Go to plugin

PLUGIN for VirtueMart

Module which allows Nexi XPay gateway to be integrated with the VirtueMart platform.
Go to plugin

PLUGIN for Zen Cart

Module dedicated to the open source e-commerce management software Zen Cart.
Go to plugin

PLUGIN for Magento Community

Module for integrating Nexi within Magento Community software.
Go to plugin

PLUGIN for Magento Enterprise

Module for integrating Nexi within Magento Enterprise software.
Go to plugin

PLUGIN for OS Commerce

Module for managing payments on the OS Commerce platform.
Go to plugin

PLUGIN for OpenCart

Payment module which can be integrated with the CMS platform OpenCart.
Go to plugin