Technical Specifications for Integration with the XPay Payment Gateway

TABLE OF CONTENTS

Web & Mobile8

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

GETTING STARTED

Welcome to the technical area

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, Hosted Fields, 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 Hosted Fields 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.cartasi.it
- Download Section (documents, specifications and brand repository)

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

Integrating Nexi in web and mobile environments

There are four tools available for integrating Nexi virtual POS in a way that it is optimised and accessible from all devices:

1. Easy Payment

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.

2. I-Frame - LightBox

Nexi provides the merchant with a customisable payment interface. During the transaction, the customer stays on the merchant's e-commerce site, while the sensitive data continues to be handled in the secure Nexi environment. This limits the impact on PCI certification, and SAQ A type questionnaires are suitable.

3. Hosted Fields

The merchant has full control over the payment interface. The only elements linked to Nexi are the data fields which are used for entering sensitive data. Even with this solution, the merchant does not need to handle any sensitive data. This limits the impact on PCI certification, and SAQ A-EP type questionnaires are suitable.

PURCHASE PROCESS — Merchant site

PAYMENT — Management of sensitive data in the merchant environment (PCI certification required)

PAYMENT CONFIRMATION — Merchant site

4. Server to Server

Sensitive data relating to the transaction is handled directly by the merchant's servers. This allows complete customisation of the payment experience, but requires PCI DSS security certification to be achieved with an SAQ D questionnaire.

PURCHASE PROCESS — Merchant site

PAYMENT — Integration of input fields in the merchant environment

PAYMENT CONFIRMATION — Merchant site
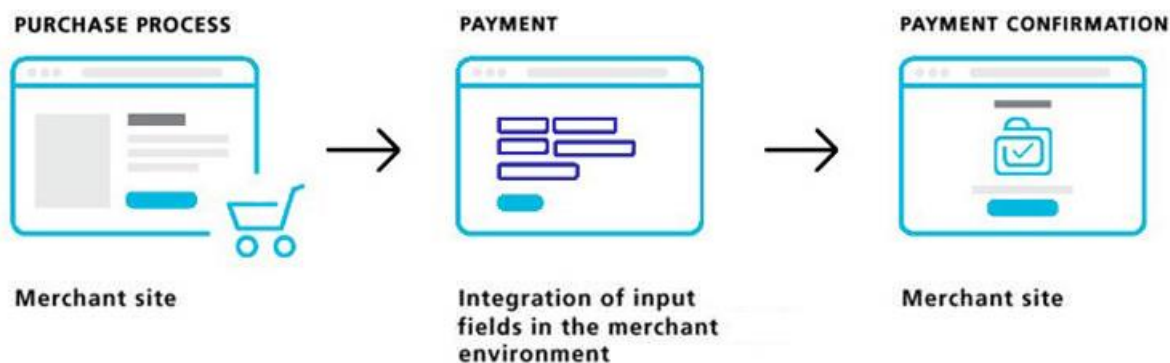
Easy Payment

The easiest way to enable an e-commerce site to receive payments, without having to worry about handling sensitive customer data.

GitHub XPay E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 Get request (redirect - link) or Post request (by sending a form with hidden fields), directing the customer's browser to the following URL. The request must be integrated with the parameters/values specific to the service that you want to implement, as found in the relevant section for each service below.

PRODUCTION ENVIRONMENT URL
https://ecommerce.cartasi.it/ecomm/ecomm/DispatcherServlet

TEST ENVIRONMENT URL
https://int-ecommerce.cartasi.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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/pagamento-semplice/codice-base

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 7 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (Euro).	AN 3 CHAR.
codeTrans	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). 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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. for MyBank: AN Max 140 CHAR.
session_id	Session identifier	AN Max 100 CHAR.
Note1	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	AN Max 200 CHAR.
Note2	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	AN Max 200 CHAR.
Note3	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	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,	AN Max 4000 CHAR.

	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.	
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). This data will also be included in the report queryable by the back office.	AN 16 CHAR.
selectedcard	If present, the payment page that is shown only allows the user to make payment using the network or payment method 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 [table here](#).	AN Max 25 CHAR.
TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to I (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.
modo_gestione_consegna	This field is only available for MySi wallet payments. Customer details are shown	AN Max 40 CHAR.

	in the result depending on the field value. Possible values: • no: no value returned • mail_tel: allows for the return of email, telephone and billing address • complete: allows for the return of email, telephone, billing address and shipping address	
shipping	if present and valued at N, paypal does not provide in reply shipping data if it is not present or valued with any value instead returns them and if the merchant does not ship to the address indicated by paypal is not guaranteed	AN
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

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(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
importo	Transaction amount retrieved from the payment initiation message.	N Max 7 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".

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 7 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 30 CHAR.
nome	Name of the person who made the payment.	AN Max 150 CHAR.
cognome	Surname of the person who made the payment.	AN Max 150 CHAR.
mail	Email address of the person who made the payment.	AN Max 150 CHAR.
session_id	Session identifier retrieved from the initiation message.	AN Max 200 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	AN Max 4000

	of the string must not exceed 4,000 characters in total, including all parameter names and values.	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.
modo_gestione_consegna	This field is only available for MySi wallet payments. Customer details are shown in the result depending on the field value. Possible values: • no: no value returned • mail_tel: allows for the return of email, telephone and billing address • complete: allows for the return of email, telephone, billing address and shipping address	AN Max 8 CHAR.
dati_gestione_consegna	Xml containing shipping information	Max 700 CHAR.

Field name	Req.	Descript
WalletAddress		
BillingAddress		
City	YES	City
Country	YES	Country
CountrySubdivision	YES	
Line1	YES	address
Line2	NO	address
Line3	NO	address
PostalCode	YES	postal co
BillingAddress		
ShippingAddress		
City	YES	City
Country	YES	Country
CountrySubdivision	YES	
Line1	YES	address
Line2	NO	address

	Line3	NO	address
	PostalCode	YES	postal co
	RecipientName	YES	Contact
	RecipientPhoneNumber	YES	Tel. no.
ShippingAddress			
WalletAddress			

Example:

```xml
<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</Recipient
PhoneNumber>
</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.

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.

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

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 Max 30 CHAR.
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 5 - Max 30 CHAR.

"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.
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 5 - Max 30 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.

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 synchronous call in server-to-server mode
- By redirecting the customer to the Nexi payment environment as in the first payment

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.

The environment endpoints are as follows:

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

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

URL
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.

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 Max 30 CHAR.
tipo_servizio	The field must be set to: "paga_multi".	AN Max 30 CHAR.
tipo_richiesta	PR (subsequent payment)	AN 2 CHAR.
gruppo	The "gruppo" value is assigned by Nexi during activation.	AN Min 5 - Max 30 CHAR.

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 Max 30 CHAR.
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 5 - Max 30 CHAR.

"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.
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 5 - Max 30 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.

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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.cartasi.it

PRODUCTION ENVIRONMENT URL
https://ecommerce.cartasi.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

Payment Result Message: additional fields for DCC

Name	Description	Format
dccRate	Exchange rate applied on the basis of exchange rates issued by Global Blue. Only present for the DCC service.	AN Max 15 CHAR.
dccAmount	Shows the value of the amount converted into the currency chosen by the payer for the transaction. The currency used is shown in the dccCurrency field. Blank space characters are added on the left until 20 characters are reached.	AN 20 CHAR.
dccCurrency	Code of the currency in which the dccAmount is expressed (e.g. 840=USD). Only present for the DCC service. For allowed values, see the table here.	AN 3 CHAR.
dccState	Shows if the transaction took place using DCC. The possible values are: 00 No DCC provided for the card used 02 DCC not accepted by cardholder 03 DCC accepted by cardholder	AN 2 CHAR.

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 "I" 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 ability to customise the Easy Payment service according to a range of features, depending on their individual needs.

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.
Send your logo to technical support so that it can be displayed on the check-out page. Maximum measurement: 180 X 80 pixel. Format: jpg, gif or png.
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.
Advise the support team which email address you wish to use for receiving communications about payment results.
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.

Additional Payment Methods

With XPay, merchants have the option of offering their e-commerce customers the ability to pay not only by credit card, but also via any of the following alternative payment methods:

- MySi - only easy payments
- Masterpass - only easy payments

- MyBank - only easy payments
- Pagobancomat web (only for authorised banks)
- PayPal - easy or recurring/OneClick/CardOnFile payments

IN PRACTICE

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, with the exception of PayPal, which can only be activated on the Nexi page mentioned in point 1.

I-Frame

Customising the layout of the check-out page

This section is designed to give you all the information you need to customise the check-out page by configuring the CSS and optimising it so that it can be selected within an iframe/lightbox.

Custom CSS Management

To customise the check-out page, the configuration parameters must be sent in the payment initiation message.

If the check-out page receives customisation parameters, it saves them to the page configuration and loads the page with the specified layout. The page stores the most recent configuration received in memory, so you only need to send customisation parameters the first time, and the page will continue to show the custom layout for subsequent requests.

If no configuration information is present, the standard Nexi layout will be used.

A message has also been programmed for restoring initial settings.

Editable Elements

In addition to CSS customisation, you can delete the page header and footer:
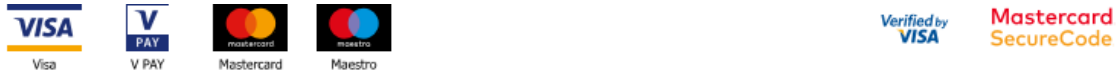
Parameter List

Variable Name	Accepted Values	Description	Element ID
primary-color	Colour in RGB format (#FF6E28)	Changes the background colour of the central part of the header (when shown), the top border of the box containing the form, the colour of the buttons, the colour of the help links, and the title colour.	1
sfondo-footer	Colour in RGB format (#FF6E28)	Changes the background colour of the footer.	2
color-footer-text	Colour in RGB format (#FF6E28)	Changes the colour of footer text.	3

box-background	Colour in RGB format (#FF6E28)	Changes the background colour of the box containing the payment data entry form.	4
color-error-msg	Colour in RGB format (#FF6E28)	Change the colour of error messages.	5
font-Title-Heigth	In 10px or 10% format	Changes title size on the page.	6
color-input-text	Colour in RGB format (#FF6E28)	Changes the colour of text entered by the user (form input fields).	7
color-label	Colour in RGB format (#FF6E28)	Changes label colour.	8
font-Heigth	In 10px or 10% format	Changes label height.	8
font	Existing font	Changes label font.	
back-To-Default	YES	If populated, resets the configuration to default settings.	

NB: Special parameters transferred using the GET method are url-encoded.

Hosted fields

Integrating Nexi with Hosted Fields

This method is available for integrating Nexi XPay, allowing you to fully customize your payment experience, with limited impact on PCI DSS requirements.

What will be covered in this section?

A description of the XPay payment process using hosted fields.
Hosted Fields is taken to mean a system in which the card data collection fields are hosted on the merchant's pages. Typically, this sort of approach requires merchants to collect, process and store card details on their own systems, meeting the appropriate security certifications (PCI with SAQ D questionnaire).

The Hosted Field approach allows to overcome this constraint, as card details are never transmitted to the merchant's server and are only collected on the merchant's own pages. The type of questionnaire for the required PCI certification is SAQ A-EP.

A further benefit of the hosted approach is the complete customisability of the check-out page and its perfect integration within the e-commerce site, thereby improving the user experience.

The above applies for web-based payments, as well as for Android and iOS mobile apps. In the latter case, the fields are hosted in the native form of the merchant's app. For specifics on this topic, please see the SDK section.

Are there any prerequisites?

Integration such as this requires the merchant page to be hosted on a secure url (https), given that card details are not transmitted to the merchant's server, but are only collected on the merchant's pages. Therefore, the level of PCI certification required is the one with questionnaire: SAQ A-EP, rather than SAQ-D as is the case of server to server.

Description

The following describes the architecture and payment process for the web version of hosted fields, which involves the use of a client JavaScript SDK.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/hosted-fields

Hosted payments consist of the following elements:

- Custom check-out page hosted on the merchant's certified domain (https)
- XPay unobtrusive JavaScript library hosted on the check-out page, which, after appropriate configuration, is able to insert itself in the data entry process
- Merchant back end, which receives the nonce (random code valid for a single transaction) and uses it for the server-to-server payment
- XPay pagaNonce API, which carries out the server-to-server payment
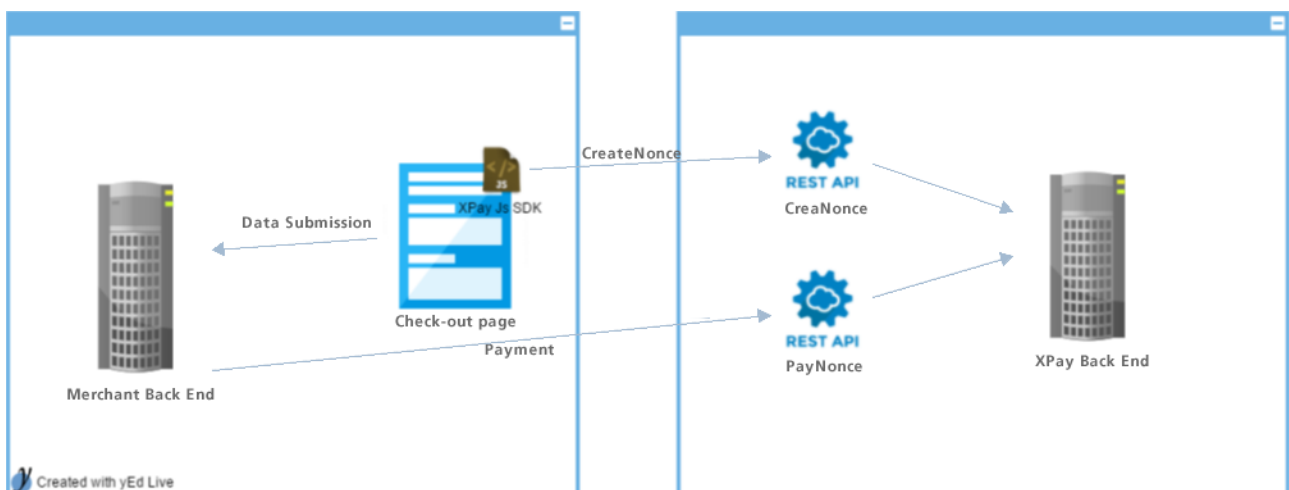
SDK configuration

The merchant's data collection page must include a dynamic JavaScript generated by a specific XPay Servlet and configured through appropriate identification parameters. The merchant can also avoid a prior jQuery download by using a specific Bundle. The JavaScript to be included in the page head is as follows:

Testing:

```
<script type="text/javascript" src="https://int-
ecommerce.cartasi.it/ecomm/hostedPayments/JavaScript/custom?bundle=HP_NO_JQ&ali
as=ALIAS_MERCHANT"></script>
```

Production:

```
<script type="text/javascript"
src="https://ecommerce.cartasi.it/ecomm/hostedPayments/JavaScript/custom?bundle=HP
_NO_JQ&alias=ALIAS_MERCHANT"></script>
```

The value of the *bundle* parameter will depend on whether jQuery and jQuery-UI are present on the merchant's page or not:

- Bundle = **HP_FULL** if the merchant does not use jQuery or jQuery-UI
- Bundle = **HP_NO_JQ** if the merchant only uses jQuery-UI, and does not use jQuery
- Bundle = **HP** if the merchant already uses jQuery and jQuery-UI

The alias parameter must be set to the merchant apiKey (or alias).

Below is a commented example of SDK configuration which is to be executed on page load:

```javascript
<script type="text/javascript">
        $(document).ready(function () {

                //1.1 SDK initialisation
                XPay.init();

                //1.2 Environment setting. Allowed values:
                // XPay.Environments.INTEG: local testing
                // XPay.Environments.PROD: production
                XPay.setEnvironment(XPay.Environments.PROD);

                //1.3 XPay SDK Configuration with merchant API Key
                XPay.setAPIKey('alias_merchant');

                // 2 Insertion of nonce calculation during the form submission process;
                // NB: Effective implementation depends on how the merchant manages the submit

                        var $form = $('#payment-form');
                        $form.find('#payBtn').click(function () {
                                //2.1 Disabling the click function for the form submit button
                                $(this).prop('disabled', true);

                                //2.2 Creating the nonce and assigning the Xpay response
                                management handler; the back-end form submission will be in
                                the handler, which must be implemented by the merchant
                                XPay.creaNonce("payment-form", xpayResponseHandler);
                        };
                };
</script>
```

Form for Collecting Card Details

Merchants can create their own page to collect card details, and there are no limitations from the user experience point of view. The page must contain a form which has the fields required for the transaction. Below is a sample form:

```
<form action="FakeMerchant" id="payment-form" method="POST">
    <input type="hidden" data-xpay-order="importo" name="importo" id="importo"
value="1000"/>
    <input type="hidden" data-xpay-order="timeStamp" name="timeStamp"
    id="timeStamp" value="1484929141412"/>
    <input type="hidden" data-xpay-order="divisa" name="divisa" id="divisa"
value="EUR" />
    <input type="hidden" data-xpay-order="mac" name="mac"
    value="c91292a7fe7c16cb6d3608746cafa4a6710276d1" id="mac" />
    <input type="hidden" data-xpay-order="codiceTransazione"
    name="codiceTransazione" value="MZ1484929141412" id="codiceTransazione" />
    <input type="hidden" name="alias" value="hostedPayment" id="alias"/>

    <h2>Dati Pagamento</h2>
    <br>
    <span class="payment-error" style="color: red;"></span>
    <br>
    <label for="_importo" >Importo:  </label>
    <label id="_importo" >1000</label>
    <br><br>
    <label for="_nOrdine" >Numero d'ordine:  </label>
    <label id="_nOrdine" > MZ1484929141412</label>
    <br><br>
    <label for="_email" >Indirizzo e-mail</label>
    <input id="_email" type="text" >
    <br><br>
    <label for="_nCarta" >N. Carta</label>
    <input id="_nCarta" type="text" Maxlength="20" data-xpay-card="pan"
    placeholder="Numero carta" >
    <br><br>
    <label><span>Scadenza (MM/YY)</span></label>
    <input type="text" size="5" data-xpay-card="scadenza">
    <br><br>
    <label for="cvv" >CVV</label>
    <input type="text" Maxlength="3" data-xpay-card="cvv" id="cvv">
    <br><br>
    <input type="button" value="Paga" id="pagaBtn" />
</form>
```

Required fields

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, i.e. 5000 represents € 50.00.	N Max 7 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
codiceTransazione	Transaction identifier assigned by the merchant.	AN Max 30 CHAR.
pan	Credit card number	AN Max 19 CHAR.
scadenza	Credit card expiry 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.	N Max 4 CHAR.
timeStamp	Timestamp in millisecond format.	AN 13 CHAR.

Optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	AN Min 2 - Max 30 CHAR.

The form's action is a merchant endpoint, towards which the POST of fields occurs. It can be noted that the form is divided into two sections:

- The "Payment Details" section, which is visible to the user and has all the classic fields required for payment (card number, card expiry date, cvv, email address). As a precaution, these fields do not include the html name attribute, which ensures that these fields are unable to reach the merchant server when the form is submitted to the back end. Instead, the browser will automatically exclude them.
- The section which is not visible to the user and contains the hidden fields to be sent to the merchant for completion of the purchase process, once card details have been correctly captured. Each of these fields has the name attribute expected by the back end. The merchant's back end pre-fills these fields with the details confirmed in the previous steps of the purchase process. It is the merchant's responsibility to handle the correct propagation of this data in the most appropriate manner. The use of hidden fields is given as an example only. For this section, merchants can choose their preferred strategy.

The MAC calculation must occur according to existing XPay rules, and when, after the completion of order details, the user moves to the page for capturing card details, it should have already taken place. This is because card details do not affect the MAC calculation, and more than anything else, it is a fundamental factor in the correct generation of a one-time nonce by XPay. The MAC for the creaNonce API must be generated on the basis of the following data:

- apiKey
- codiceTransazione
- divisa
- importo
- timeStamp
- secretString

A fundamental part of the XPay library configuration is the assignment of a custom attribute to the form fields:

- data-xpay-order: identifies a field relating to the order. Since this is not considered sensitive information from the point of view of PCI legislation, the name attribute can be included and the field sent to the merchant back end as standard. This is the attribute which is normally assigned to some of the hidden fields on the form (only those required for generation of the nonce)
- data-xpay-card: identifies a field relating to the card. Since this is considered sensitive information from the point of view of PCI legislation, the name attribute cannot be included and the field cannot be sent to the merchant back end. This is the attribute assigned to the visible fields of the form.

Each field which contributes to XPay's generation of the nonce will be populated with one of the special attributes.
In practice, the merchant must indicate which of the fields represents the order number, which field represents the card number, etc.

The attribute value must be one of those nominated by XPay for identifying input fields:

- alias
- codiceTransazione
- divisa
- importo
- timeStamp
- mac
- pan
- scadenza
- cvv

Nonce Generation

As seen above, the suggested approach is to disable the submit button (recommended or mandatory) on the form for capturing card details. Instead, when it is clicked, the creaNonce API will be run by XPay's SDK. Upon completion, this will invoke the JavaScript xpayResponseHandler callback as indicated by the merchant. XPay's JavaScript SDK will retrieve all the fields in the form which are marked with the data-xxx-xpay attribute. It will then populate them with the configuration parameters used for initialising the SDK itself, serialise them, and send them asynchronously to the XPay creaNonce API as specified for the indicated environment.

If the SDK detects that one of the fields tagged with the data-xpay-card attribute also has a name attribute, the nonce creation process will terminate immediately with an error. This will indicate that there is a risk of card details being passed to the merchant's server. Before invoking the API, the SDK performs a formal validation of PAN, CVV and expiry date fields. If the check process fails, the process is discontinued and the SDK instead invokes the handler specified by the merchant, with the following JSON object in the output:

```
{
        "esito": "KO",
        "errore": {
          "codice": 600,
          "messaggio": "<Messaggi di errore concatenati>"
        }

}
```

Once the call to XPay has been completed, the SDK will either handle the communication error or the success (including any application errors from the XPay side). In the event of success, control will be transferred to the *xpayResponseHandler* callback. This callback only expects one input parameter - the response. This parameter contains all the information necessary for interpreting the error or the nonce.

In the event of a communication error, the response handler is invoked with the following JSON:

```
{
        "esito": "KO",
        "errore": {
          "codice": 500,
          "messaggio": "<Messaggio di errore>"
         }
}
```

The callback must manage any errors (and display them on the page, according to the UX logic decided by the merchant) or, if the message is successful, perform the following steps:

- Retrieve the nonce from the response
- Attach it to the form as a new hidden field
- Submit the form to the action specified (merchant back end)

Below is a merchant callback example:

```javascript
function xpayResponseHandler(response) {

    // Retrieve the form
    var $form = $('#payment-form');

    if (response.result && response.result == "OK") { // nonce created
        // 3.A Retrieve the nonce and other properties in output. Insert as hidden fields
        //     in the form. The back end should validate the MAC of the response where
        //     appropriate
        $form.append($('<input type="hidden" name="xpagaNonce">').val(response.nonce));
        $form.append($('<input type="hidden" name="xpayIdOperazione">').val(response.idOperazione));
        $form.append($('<input type="hidden" name="xpayTimeStamp">').val(response.timeStamp));
        $form.append($('<input type="hidden" name="xpayEsito">').val(response.esito));
        $form.append($('<input type="hidden" name="xpayMac">').val(response.mac));

        // Submit the form
        $form.get(0).submit();
    }
    else {
        // 3.B Display the error and restore the form button
        $form.find('.payment-error').text("[" + response.errore.codice + "] " +
            response.errore.messaggio);
        $form.find('#pagaBtn').prop('disabled', false);
    }
};
```

Payment

The merchant back end receives the nonce along with the other fields of the form. After an optional validation of the MAC in the output, the merchant back end initiates payment with the RESTful pagaNonce API described below. It is noted that the order details sent by the merchant at this stage are those to be used for payment (importo, currency, order number); all details sent by the merchant in the nonce generation step are filed by XPay (together with the nonce itself), but are only used as a consistency check between the two stages. This is to ensure that any request for a new nonce and its use in the payment have been generated by the same entity and for the same purpose. However, it is critical for the merchant's back end to provide XPay with the correct details in the server-to-server stage.

Handling of the result (by parsing the response from the pagaNonce API) is entrusted to the merchant, as per the RESTful API payment procedures.

Below are the contact URI and the table indicating the parameters which must be included in the JSON request.

URI
ecomm/api/hostedPayments/pagaNonce

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 collected, expressed in euro cents with no separators.	N Max 9 CHAR.
divisa	978 for Euro	AN 3 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN 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.

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	Result of the request.	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 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer.	AN Min 2 - Max 30 CHAR.
data	Transaction date	dd/mm/yyyy
ora	Transaction time	hh:mm:ss
nazione	Credit card country	ISO 3166-1 alpha-3
regione	Credit card global region of origin	AN Min 2 - Max 30 CHAR.
tipoProdotto	Credit card type	AN Min 2 - Max 30 CHAR.
tipoTransazione	Indicates the payment method. See the table here for possible values.	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
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 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>)

NOTE:

This makes a payment using a valid nonce.

The transactionCode, importo, currency, and apiKey must be the same as the Nonce request, otherwise an invalid data error will be received. This error can also occur if more than 10 minutes have passed since the nonce was generated.

First recurring payment

Create a contract through a valid nonce. The xpayNonce field is the generated nonce with the creaNonce API. The transactionCode, importo, currency, and apiKey must be the same as the Nonce request, otherwise an invalid data error will be received. This error can also occur if more than 10 minutes have passed since the nonce 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

METODO
POST

ACCEPT
application/json

Payment Initiation Message: required fileds

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 collected, expressed in euro cents with no separators.	NUM Max 9 Char.
divisa	978 for Euro	AN 3 CHAR.
xpayNonce	Code assigned by XPay for use in the payment request.	AN 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.
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN MIN 2 MAX 30

Payment Initiation Message: optional fields

Name	Description	Format
codiceGruppo	Group assigned by Nexi.	AN MIN 2 MAX 30
scadenzaContratto	For recurring payments, indicates when the expiry date for the contract occurs.	DATA gg/mm/aaaa
mail	Email address of the person who made the payment.	AN MAX 150
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 Per MyBANK: AN MAX 140 CHAR.
codiceFiscale	User Tax Code. Optional.	AN MAX 16

MAC Calculation

For rhis 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: optional fields

Name	Description	Format
esito	Result of the request.	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 6 CHAR.
codiceConvenzione	Merchant code assigned by the acquirer.	AN Min 2 – Max 30 CHAR.
data	Transaction date	gg/mm/aaaa
ora	Transaction time	hh:mm:ss
nazione	Credit card country	ISO 3166-1 alpha-3
regione	Credit card global region of origin	AN Min 2 – Max 30 CHAR.
tipoProdotto	Credit card type	AN Min 2 – Max 30 CHAR.
tipoTransazione	Indicates the payment method. See the table here for possible values.	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
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 CHAR.

MAC Calculation

For rhis 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\>)

Management of Recurring Payments/Subsequent Payments

See the [Subsequent Payment](#) section for detailed information on the call and the response to handle.

3D-Secure Management

If 3D-Secure payment is enabled for the transaction, during creation of the nonce 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 nonce will be made available only upon completion of the credential capture process, which will be initiated automatically by the SDK in any case.

Remember

- The nonce can only be used only once and it has a 10-minute time limit. If these two conditions are not satisfied, the payment will return an error
- Payment retry management is delegated to the merchant. This means that if there is an error in the first payment attempt, but the merchant is authorised to make n attempts for each order number, it is the merchant's responsibility to refresh the form for capturing card details and request generation of a second nonce. This will re-engage a *de facto* new payment.
- The SDK carries out JavaScript calls in CORS mode (Cross Origin Resource Sharing). It is necessary to verify that the merchant's network infrastructure does not impede this in any fashion.

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server

The environment endpoints are as follows:

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

PRODUCTION ENVIRONMENT URL
https://ecommerce.cartasi.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 Nonce 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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 9 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 will return the result using the following parameters: esito	AN Max 500 CHAR.

	idOperazione xpayNonce timeStamp mac and, in the case of error, also codice and messaggio.	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	

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>)

NOTE:
This allows a nonce 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 nonce will only be returned if the authentication is successful. The nonce 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 7 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.

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

- apiKey

- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- 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 30 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	Payment with Masterpass wallet.	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>)

NOTE:

This carries out a payment transaction with 3D-SECURE.

The xpayNonce is the nonce obtained from the authentication3DS API, which takes care of saving card details and carrying out the 3D-Secure process.

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 7 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	Masked credit card number with only the first 6 and the last 4 digits showing.	AN Max 100 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the payment result will be sent.	AN Max 150 CHAR.
nome	Name of the person who made the payment.	AN Max 150 CHAR.
cognome	Surname of the person who made the payment.	AN Max 150 CHAR.
additional parameters	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values. The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.	AN Max 4000 CHAR.

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 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	AN 40 CHAR.

Payment Result Message: optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	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>)

NOTE:

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 ": {}

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 on their own site the function to request credit card payment authorisations without using 3D-Secure, where details are collected directly from the pages of the merchant's own site.

This service requires the merchant to achieve PCI DSS certification.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server/pagamento-ssl

URI
ecomm/api/paga/pagaSSL

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 7 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	Masked credit card number with only the first 6 and the last 4 digits showing.	AN Max 100 CHAR.
scadenza	Credit card expiry date	DATE yyyymm
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
mail	Buyer's email address to which the payment result will be sent.	AN Max 150 CHAR.
nome	Name of the person who made the payment.	AN Max 150 CHAR.
cognome	Surname of the person who made the payment.	AN Max 150 CHAR.
additional parameters	An n number of additional parameters can be specified, which will be returned in the result messages. There is no limit to the number of additional parameters, but the length of the string must not exceed 4,000 characters in total, including all parameter names and values. The following parameter names should be avoided as they are already in use by XPay: TRANSACTION_TYPE, return-ok, tid, INFO_PAGE, RECALL_PAGE, back_url, ERROR_URL, $EMAIL, $NAME, $SURNAME, EMAIL.	AN Max 4000 CHAR.

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 30 CHAR.
errore	Only present when the result is ko. It is an object containing:	AN

	code -> error code, <u>see table</u> message > error details	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Result Message: optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	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

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

NOTE:

This carries out an SSL payment transaction, and asynchronous POST notifications are not performed. The result is a JSON object containing the response parameters.
If you do not wish to append additional parameters, you can:

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

E.g.   " parametriAggiuntivi ": {}

Payments with External 3D-Secure MPI

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	Masked credit card number with only the first 6 and the last 4 digits showing.	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 7 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	Payment with Masterpass wallet.	AN Min 2 - Max 30 CHAR. only Masterpass

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 7 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

Name	Description	Format
ppo	Payment with Masterpass wallet.	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>)

NOTE:
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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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	Masked credit card number with only the first 6 and the last 4 digits showing.	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 will return the result 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.

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>)

NOTE:
This allows a nonce 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 nonce will only be returned if the 3D-Secure authentication is successful. The nonce 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 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.

Initiation Message: optional fields

Name	Description	Format
scadenzaContratto	For recurring payments, indicates when the expiry date for the option contract occurs.	DATE dd/mm/yyyy
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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank: AN Max 140 CHAR.
codiceFiscale	User Tax Code. Optional.	AN Max 16 CHAR.

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>)

SSL Card Verification

This service carries out a card verification transaction, with no charge to the customer, using the server-to-server SSL method, at the same time as the contract is registered for use in subsequent recurring or OneClickPay payments.

This service requires the merchant to achieve PCI DSS certification.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click/verifica-carta-ssl

URI
ecomm/api/recurring/verificaCartaSSL

METHOD
POST

ACCEPT
application/json

Initiation Message: required fields

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN Min 2 - 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.
numeroContratto	Code allowing Nexi to save a paired link between the user and the payment card used.	AN Min 2 - Max 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - Max 30 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Transaction signature field	AN 40 CHAR.

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	Description assigned to the contract.	AN Max 2000 CHAR.

		For MyBank: AN Max 140 CHAR.
codiceFiscale	User Tax Code	AN 16 CHAR.

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	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>)

NOTE:

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 ": {}

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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	Masked credit card number with only the first 6 and the last 4 digits showing.	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 will return the result using the following parameters: esito idOperazione	AN Max 500 CHAR.

	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.

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 nonce is received

For the result message if a nonce 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>)

NOTE:

This allows a nonce 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 nonce will only be returned if the authentication is successful. The nonce will be returned to the urlResponse address.

Otherwise, the API will return the nonce 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 2 - Max 30 CHAR.

codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - 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 7 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
scadenzaContratto	For recurring payments, indicates when the expiry date for the contract occurs.	dd/mm/yyyy
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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank AN Max 140 CHAR.
codiceFiscale	User Tax Code. Optional.	AN 16 CHAR.

MAC Calculation

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

- apiKey
- numeroContratto
- codiceTransazione
- importo
- divisa
- xpayNonce
- timeStamp
- 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 30 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	Payment with Masterpass wallet.	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>)

NOTE:

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 nonce generated with the creaNoncePrimo3DS API.

MOTO 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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 2 - Max 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - 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 7 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.

Name	Description	Format
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
scadenzaContratto	For recurring payments, indicates when the expiry date for the contract occurs.	dd/mm/yyyy
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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank AN Max 140 CHAR.
codiceFiscale	User Tax Code. Optional.	AN 16 CHAR.

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>)

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 30 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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	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>)

NOTE:
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 ": {}

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.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-pagamento-in-un-click/primo-pagamento-ssl

URI
ecomm/api/recurring/primoPagamentoSSL

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 2 - Max 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - 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 7 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	N Max 4 CHAR.

	only, it is a four-digit code and is found on the front of cards.	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

Payment Initiation Message: optional fields

Name	Description	Format
scadenzaContratto	For recurring payments, indicates when the expiry date for the contract occurs.	dd/mm/yyyy
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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank AN Max 140 CHAR.
codiceFiscale	User Tax Code. Optional.	AN 16 CHAR.

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>)

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 30 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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	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>)

NOTE:

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 Verification

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 nonce request and any 3D-Secure authentication, using the creaNonce API
3. Make the payment request with the nonce and exchange rate ticket obtained, using the pagaDCC API.

This service requires the merchant to achieve PCI DSS certification.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server/pagamento-dcc

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 7 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:	AN

	codice -> error code, see table messaggio > error details	
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.

MAC Calculation

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

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

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

NOTE:

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.

DCC Generate Nonce

After verification and once the customer has been allowed to choose whether to transact in own currency or in Euro, this API allows a nonce 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 nonce will only be returned if the authentication is successful. The nonce will be returned to the urlRisposta address.

Otherwise, the API will return the nonce directly for use with the payment.

The details for the Nonce request are as follows:

URI
ecomm/api/hostedPayments/creaNonce

METHOD
Post

ACCEPT
application/json

Initiation Message

Name	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN Max 30 CHAR.
pan	Masked credit card number with only the first 6 and the last 4 digits showing.	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 will return the result 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.

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 nonce is received

For the result message if a nonce is 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>)

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:

- result
- operationId
- timeStamp
- secretKey

SAMPLE STRING

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

DCC 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-digit code and is found on the front of cards.	N Max 4 CHAR.
scadenza	credit card expiry date	yyyymm

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 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.

Transaction Result Message: optional fields

Name	Description	Format
ppo	Payment with Masterpass wallet.	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>)

NOTE:

The xpagaNonce 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 nonce.

Management of Recurring Payments

Subsequent Payment (Recurring Payment and One Click 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/SSL card verification.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 2 - 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 7 CHAR.
divisa	978 for Euro	N 3 CHAR.
scadenza	Credit card expiry date	yyyymm
codiceGruppo	Code assigned by Nexi during activation.	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
mail	Buyer's email address to which the payment result will be sent.	AN Max 150 CHAR.
parametriAggiuntivi	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.

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 30 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	Payment with Masterpass wallet.	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>)

NOTE:

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

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/tree/master/web-mobile/server-to-server/pagamento-ricorrente-moto**

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 2 - 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 7 CHAR.
divisa	978 for Euro	N 3 CHAR.
scadenza	Credit card expiry date	yyyymm
codiceGruppo	Code assigned by Nexi during activation.	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
mail	Buyer's email address to which the payment result will be sent.	AN Max 150 CHAR.

parametriAggiuntivi	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.

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 30 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	Payment with Masterpass wallet.	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>)

NOTE:

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 ": {}

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 two-factor 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

Nexi provide two different kind of integration with Apple Pay:

- Button on the check out Page : it is possible to accept payment with Apple Pay enabling the visibility of "Apple Pay button" on the Xpay check out page . You should load in the back office of Xpay Nexi the certificate that has been requested directly to Apple and generated and provided directly in the Apple developers web portal
- Authorization via API: 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

   For this second solution 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

METODO
POST

ACCEPT
application/json

Initiation Message

Nsme	Description	Format
apikey	Alias assigned to the merchant by Nexi.	AN Max 30 CRT
codiceTransazione	Transaction identifier assigned by the merchant.	

importo	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.It must be equal to the amount that was sent to Apple for the token generation	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
applePay	JSON receive from the Apple call	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

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)

SEMPLE STRING

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

Reply Message

Nome	Descrizion	Format
esito	Result of the operation (Possible Values OK, KO, ANNULLO e 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 required.	AN Max 15 CRT
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 CRT

ppo	Payment with wallet (Apple Pay, Masterpass, ecc...)	AN Min 2 - Max 30 CRT
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 30 CRT
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 CRT
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 CRT

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

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/api-backoffice

The environment endpoints are as follows:

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

PRODUCTION ENVIRONMENT URL
https://ecommerce.cartasi.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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 7 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (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.

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 7 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (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.

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

- esito
- idOperazione
- timeStamp
- secretKey

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

NOTE:
The type of reversal depends on the processing status of the order:

- If it has been authorised-> Online Reversal (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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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.
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
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
ordini	Contains one or more objects whose structure is shown in the following table.	AN

Orders 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 9 CHAR.
divisa	978 for 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.	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 30 CHAR.
pan	Credit card number	AN Max 19 CHAR.
parametri	Additional parameters	AN
stato	Order status	AN
dataTransazione	Transaction date	dd/mm/yyyy
dataOperazione	Operation date	dd/mm/yyyy
tipoServizio	Type of service used for the transaction.	AN
nome	Customer name	AN Min 2 - Max 30 CHAR.
cognome	Customer surname	AN Min 2 - Max 30 CHAR.
mail	Customer email	AN Max 150 CHAR.
dettaglio	Contains an object whose structure is shown in the following table.	AN

Details element

Name	Description	Format

nome	Customer name	AN Min 2 - Max 30 CHAR.
cognome	Customer surname	AN Min 2 - Max 30 CHAR.
mail	Customer email	AN Max 150 CHAR.
importo	Transaction amount expressed in euro cents with no separator.	N Max 9 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 9 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

MAC Calculation

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

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

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

NOTE:

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.

Order List

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

GitHub XPay E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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.	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
canale	Possible values for channel: All MySi MyBank CreditCard PayPal	AN
stato	Order status	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 7 CHAR.
divisa	Code of the currency in which the amount is expressed, with the only acceptable value being: EUR (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.	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 30 CHAR.
pan	Masked credit card number with only the first 6 and the last 4 digits showing.	AN Max 100 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
nome	Name of the person who made the payment.	AN Max 150 CHAR.
cognome	Surname of the person who made the payment.	AN Max 150 CHAR.
mail	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>)

NOTE:

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

PayMail 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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/tree/master/api-backoffice/richiesta-link-paymail**

URI
ecomm/api/bo/richiestaPayMail

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 7 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

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>)

NOTE:

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.

SDK FOR APP

Integrate Nexi in your APP

SDK is available for iOS and Android environments in order to easily integrate Nexi gateway services within your APP.
APIs are divided into functional areas:

- BackOffice
- SecurityControls
- FrontOffice
- ContractManagement
- HostedPayments
- SynchronousPayments
- FirstPaymentsRecurring
- RecurringPayments

IOS SDK
Getting Started
To install the framework in a merchant app, follow the steps below:

- Open XCode (requires Xcode 8.2.1+) in the app project
- Select solution settings
- Navigate to General -> Embedded Frameworks and choose "+", selecting the XpaySDK.framework file
- Drag the CommonCrypto folder to your app project, accepting the default settings when merging:
  - Copy items if needed -> yes
  - Create groups -> yes
  - Add to targets: - select app

NOTE:
Check that the path contained in the module.map within the CommonCrypto directory points to the correct CommonCrypto.h path

- Navigate in the project to -> app -> Build Settings -> Swift Compiler - Search Paths -> Import Paths, and add "CommonCrypto"

To use creaNonce, derivatives and FrontOffice, a NavigationController will need to be used within your Storyboard to allow UIWebView to open. It relies on navigation controllers receiving in input the appropriate methods.

If you are using:

- SWIFT 3.0+: In the project's BuildSettings, choose "Use Legacy Swift LanguageVersion"
  -> YES
- Objective-C: In the project's BuildSettings, choose "Always Embed Swift Standard Libraries" -> YES

In order to be able to use an Endpoint with a Self-Signed Certificate, the following node will need to be added to the Info.plist file in the merchant app:

```
<key>NSAppTransportSecurity</key>
<dict>
  <key>NSAllowsArbitraryLoads</key>
  <true/>
</dict>
```

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
NOTE: 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

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

Practical Example

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 (default)

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

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.

NOTE: Each request can be coupled with additional parameters, where this has previously been agreed between the merchant and Nexi. Example:

apiReverseRequest.ExtraParameters[“ParameterName”] = “ParameterValue”

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.
To enable navigation in WebView, use the following instruction:

```
apiFrontOfficeQPRequest.NavigationEnabled = true
```

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.

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 numbers to the right represent the euro cents.	N Max 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
brand	Credit card network	AN Max 100 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	AN hh:mm:ss
isValid()	If this is true, the response is valid. If it is not true, the error parameter will be populated.	True/false
error	Element containing the error code and description: code -> error code, see table message -> error details	OBJ

Optional parameters

Name	Description	Format
extraParameters	Additional optional parameters	AN

NOTE:
All 3D-Secure and payment procedures are entrusted to the Front Office WebView.

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 2 - Max 30 CHAR.
tipo_richiesta	PP (first payment)	AN 2 CHAR.

IN PRACTICE

apiFrontOfficeQPRequest.addExtraKey("tipo_servizio","paga_multi");
apiFrontOfficeQPRequest.addExtraKey("num_contratto",""); // contract number to be associated with the card that the user will use for payment.
apiFrontOfficeQPRequest.addExtraKey("tipo_richiesta","PP");

Getting Started

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).
- Navigate to File -> New -> New Module -> Select 'Import .jar / .aar package', and select the file to import as a library. This will create a new module within the project, with the name of the imported library.
- Right-click the module where you want to use the library, and navigate to 'Open Module Settings' -> Modules (app) -> Navigate to the 'Dependencies' tab, and press '+' -> Module Dependency, and select the library module. At this point, you should be able to access the library from the project where it was imported.
- In the app's .gradle file, add dependencies to GSON and Volley in the following manner:

```
dependencies {
    compile 'com.android.volley:volley:1.0.0'
    compile 'com.google.code.gson:gson:2.8.0'
}
```

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

NOTE: 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

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

Practical Example

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 (default)

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

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.

NOTE: Each request can be coupled with additional parameters, where this has previously been agreed between the merchant and Nexi. Example:

apiAbilitaContrattoRequest.addExtraKey("ParameterName", "ParameterValue");

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

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();
        }
}
```

To enable navigation in WebView, use the following instruction:

apiFrontOfficeQPRequest.setNaviagationEnabled(true);

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.

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	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

NOTE:
All 3D-Secure and payment procedures are entrusted to the Front Office WebView.

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 2 - Max 30 CHAR.
tipo_richiesta	PP (first payment)	AN 2 CHAR.

IN PRACTICE

apiFrontOfficeQPRequest.addExtraKey("tipo_servizio","paga_multi");
apiFrontOfficeQPRequest.addExtraKey("num_contratto",""); // contract number to be associated with the card that the user will use for payment.
apiFrontOfficeQPRequest.addExtraKey("tipo_richiesta","PP");

Hosted Fields/Server-to-Server Payment

As described above, the hosted fields approach does not transmit card details to the merchant's server, but rather allows them to be only *collected* on the native form of the merchant's app.

This service requires the merchant to achieve PCI DSS certification.

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 nonce. Once the nonce has been received in response, the app notifies the back end, which proceeds to recall the second "PagaNonce" API for carrying out the actual payment.

Service details for the Nonce request are as follows:

REQUEST

CLASS
ApiCreaNonceRequest

METHOD
creaNonce

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
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.
codTrans	Payment identification code consisting of alphanumeric characters, **excluding the #**	AN Min 2 - Max 30 CHAR.

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.

RESPONSE

CLASS
ApiCreaNonceResponse

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

NOTE:
If the card needs to be authenticated using 3D-Secure, a WebView will open in order to complete the procedure. The response will be returned after this has been completed.

To manage the payment with the received Nonce, see the hosted field payment section.

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 cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N Max 9 CHAR.

currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.

RESPONSE

CLASS
ApiPagaSSLResponse

Name	Description	Format
result	Result of the request.	AN Max 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
convCode	Merchant code assigned by the acquirer.	AN Min 2 - Max 30 CHAR.
date	Transaction date	DATE dd/mm/yyyy
time	Transaction time	hh:mm:ss
country	Credit card country	AN Min 2 - Max 30 CHAR.
region	Credit card global region of origin	AN Min 2 - Max 30 CHAR.
productType	Credit card type	AN Min 2 - Max 30 CHAR.
transactionType	Indicates the payment method. See the table here for possible values.	AN Min 2 - Max 30 CHAR.

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, the authorisation request fails, then the merchant may repeat the same request with the same transCode twice more. In the configuration stage, the merchant may choose to decrease this to less than 3 attempts.	AN Min 2 - Max 30 CHAR.
card	Element containing payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ
amount	Amount to be authorised, expressed in euro cents with no separator. The first 2 numbers to the right represent the euro cents.	N Max 9 CHAR.
currency	Code of the currency in which the amount is expressed, with the only acceptable value being: 978 (Euro).	AN 3 CHAR.
eci	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.
xid	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.
cavv	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.

RESPONSE

CLASS
ApiPagaMPIResponse

Name	Description	Format
result	Result of the request.	AN Max 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	AN

timeStamp	Timestamp in millisecond format.	N 13 CHAR.
codTrans	Transaction identifier assigned by the merchant.	AN Min 2 - Max 30 CHAR.
authCode	Confirmation code issued by the card issuer.	AN 6 CHAR.
amount	Amount expressed in euro cents with no separators.	N Max 6 CHAR.
currency	978 for Euro	N 3 CHAR.
date	Transaction date	DATE dd/mm/yyyy
transactionType	Indicates the payment method. See the table here for possible values.	AN Min 2 - Max 30 CHAR.
eci	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.
xid	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.
cavv	3D-Secure data. See table	AN Min 2 - Max 30 CHAR.

Management: Recurring - Card on File - OneClickPay

Integrating Recurring, OneClickPay or Card on File 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

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 sequence of services used is as follows:

With 3D-Secure:

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

Without 3D-Secure:

- To manage payment and contract registration -> primoPagamentoSSL

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

With 3D-Secure:

- To manage 3D-Secure authentication -> creaNonceVerificaCarta
- To manage verification of card validity and register the contract -> verificaCarta3DS

Without 3D-Secure:

- To manage verification of card validity and register the contract -> verifcaCartaSSL

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

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 nonce. With the Nonce 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 nonce

REQUEST

CLASS
ApiCreaNonceVerificaCartaRequest

METHOD
creaNonceVerificaCarta

Name	Description	Format
alias	Merchant profile identification code (fixed value communicated by Nexi during the activation phase).	AN Max 30 CHAR.
card	Element containing payment card details: pan – credit card number month – credit card expiry month year – credit card expiry year cvc – three-digit code found on the back of VISA, MASTERCARD, MAESTRO, DINERS, and JCB branded credit cards. For AMEX cards only, it is a four-digit code and is found on the front of cards.	OBJ

RESPONSE

CLASS
ApiCreaNonceVerificaCartaResponse

Name	Description	Format
result	Result of the request.	AN Max 30 CHAR.
operationId	Transaction identifier assigned by Nexi.	ENUM ok/ko
timeStamp	Timestamp in millisecond format.	N 13 CHAR.
nonce	Code assigned by XPay for use in the payment request.	AN 35 CHAR.

NOTE:

This allows a nonce 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.
nonce	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 2 - 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.

![nexi CartaSi logo]

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 nonce. With the Nonce received in response, the APP proceeds to recall the second payment service.

This service requires the merchant to achieve PCI DSS certification.

Create nonce

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.

NOTE:

This allows a nonce 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 2 - 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.

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 2 - 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	Payment with Masterpass wallet.	AN Min 2 - Max 30 CHAR.

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 2 - 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.

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 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.
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	Payment with Masterpass wallet.	AN Min 2 - Max 30 CHAR.

Back Office Services - 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 #**	AN Min 2 - Max 30 CHAR.

	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 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.

Back Office Services - 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.

NOTE:

Once the order has been authorised, only a total transaction cancellation is possible.

Back Office Services - 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 - MySi - 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.

NOTE:
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

Back Office Services - 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
ApiDettaglioOrdineRequest

METHOD
dettaglioOrdine

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	AN Min 2 - Max 30 CHAR.

the configuration stage, the merchant may choose to decrease this to less than 3 attempts.

RESPONSE

CLASS
ApiDettaglioOrdineResponse

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

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	Payment with Masterpass wallet.	AN Min 2 - Max 30 CHAR.

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/tree/master/altri-servizi

The environment endpoints are as follows:

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

PRODUCTION ENVIRONMENT URL
https://ecommerce.cartasi.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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 2 - 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 7 CHAR.

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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank: AN Max 140 CHAR.
mail	Buyer's email address to which the payment result will be sent.	AN Max 150 CHAR.

MAC Calculation

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

- apiKey
- numeroContratto
- idPOSFisico
- codiceAutorizzazione
- stan
- importo
- descrizione
- mail
- timeStamp
- secretKey

SAMPLE STRING

MAC = HASH SHA1(apiKey=<val>numeroContratto=<val>idPOSFisico=<val>codiceAutorizzazione=<val>
stan=<val>importo=<val>descrizione=<val>mail=<val>timeStamp=<val><SecretKey>)

Result Message

Name	Description	Format
esito	Operation result	AN Max 7 CHAR.
idOperazione	Transaction identifier assigned by Nexi.	AN Min 2 - Max 30 CHAR.
errore	Only present when the result is ko. It is an object containing: code -> error code, the possible values are shown in the "RESTful API Error Codes" table in the TABLES AND CODINGS section message -> error details	AN
mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
timeStamp	Timestamp in millisecond format.	N 13 CHAR.

MAC Calculation

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

- esito
- idOperazione
- timeStamp
- secretKey

SAMPLE STRING

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

Contract 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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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 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.

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 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.

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 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.

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 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.
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

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 2 - Max 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - Max 30 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>)

NOTE:

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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 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.
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 2 - Max 30 CHAR.
codiceGruppo	Code assigned by Nexi during activation.	AN Min 2 - Max 30 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>)

NOTE:

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.

Control Management - Adding to Blacklist

This service adds Tax Codes or contract codes to the blacklist.

GitHub XPay E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank: AN Max 140 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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank: AN Max 140 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

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 E-Commerce Gateway integration code: **https://github.com/Nexi/X-Pay/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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. For MyBank: AN Max 140 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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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
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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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
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

NOTE:

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 E-Commerce Gateway integration code: https://github.com/Nexi/X-Pay/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

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>*)

NOTE:

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
19	Payment rejected

50	Unable to calculate the MAC. Either the alias is invalid, or the incoming JSON does not comply with requirements
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

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

Transaction Type Coding

transactionType	Description
NO_3DSECURE (*NO_3DSECURE_MASTERPASS)	The merchant is not enabled to use the Verified by Visa and Secure Code 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 Secure Code 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 Secure Code 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.

*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)
MYSI (only for selectedcard, allows payment by MySi wallet only)
CC (only for selectedcard, allows payment by credit cards only)
Masterpass (only for selectedcard, allows payment by Masterpass wallet only)
BANCOMAT

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

HTTP/XML API

Server to Server Payments

Payment

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.cartasi.it/ecomm/ecomm/ServletS2S

TEST ENVIRONMENT URL
https://int-ecommerce.cartasi.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

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 7 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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. for MyBank: AN Max 140 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,	AN Max 4000 CHAR.

	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). This data will also be included in the report queryable by the back office.	AN 16 CHAR.
selectedcard	If present, the payment page that is shown only allows the user to make payment using the network or payment method 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 table here.	AN Max 25 CHAR.
TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to I (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>ID000000000025486A</TRANSACTION_ID>
<HTML_CODE>
<![CDATA[
```

```html
<!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=31376271324E6B684F325544753350757664706C56644F513D3
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.cartasi.it:443/mdpaympi/MerchantServer?msgid=4766030">
<input type="hidden"
name="MD"
value="D6A7882ACB6D8D32645DA85B381FD3AD.ecdvas">
<!-- To support javascript unaware/disabled browsers -->
<noscript>
<center>Please click the submit button below.<br>
<input type="submit" name="submit" value="Submit"></center>
</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/3c63af6a33373131633430313633313313330333061373130/3ds/vereqauthid=33377337556F4D48656B7659417264576D4365473878355113D3D
"
method="POST">
<input type="hidden"
name="PaReq"
value="eJxVUttOAjEQ/RXCq5Hetu2WDE0QTOBBggiJ+mI23cZdlQW6RcGvt10W1KYPc+
bSOXOmsCycteMHa/bOarizdZ292k6ZD7qJFAIz1tUwHy7sTsOndXW5qTTp4R4FdIahyJki
q7yGzOxupjOdKMYxBtRCWFs3HWvcHi45FRJfJwzLFBMG6BSHKItbLUIKU8IBNQjMZl95
d9QsDe+dAezdhy683/YRAhQBoF8S83206lB8KHO9eptMlth+PS9oYRS5vyoen/xMjPz3+w
BQzIA881ZTTJrbIaLPcT8JtBo/ZOvYVd+uFp0weJzq5IBt7DM8ARIDfx0Q9HS2MketZBqYn

xHYw3ZT2ZARFLzYkNva6OkYXw7liVDDF8KoxDIRCWNYBUYxDdDvhKNJFN34IB9lQiilp
CRBUyK4Ys0GmljsWgbhwny8aRsBoFiN2uWidvXB+vclfgA8Gam7">

```
<input type="hidden"
name="TermUrl"
value="https://ecommerce.cartasi.it:443/mdpaympi/MerchantServer?msgid=4766033">
<input type="hidden"
name="MD"
value="4E7311C0EEF2F0C861D81963B419C637.ecdvas">
<!-- To support javascript unaware/disabled browsers -->
<noscript>
<center>Please click the submit button below.<br>
<input type="submit" name="submit" value="Submit"></center>
</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 7 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 30 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.

Name	Description	Format
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

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 Max 30 CHAR.
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 5 - Max 30 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.
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 5 - Max 30 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

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

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.cartasi.it/ecomm/ecomm/XPayServlet

TEST ENVIRONMENT URL
https://int-ecommerce.cartasi.it/ecomm/ecomm/XPayServlet

2. Recording the transaction result

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>T0000000000000000001</TRANSACTION_ID>
<REQUEST_TYPE>FA</REQUEST_TYPE>
<ACTION_CODE>VERI</ACTION_CODE>
<PAN>1234567890123456</PAN>
<EXPIRE_DATE>0605</EXPIRE_DATE>
<CVV2>123</CVV2>
<AMOUNT>000123056</AMOUNT>
<CURRENCY>978</CURRENCY>
<ECI>30</ECI>
<XID>20002232324ER2345678</XID>
<CAVV>12345655545454QWE1QWQWERDFSA</CAVV>
<VERSION_CODE>01.00</VERSION_CODE>
</AUTHONLYREQ>
<MAC>70C4F1F621A5DED95C7EE8C5507A9E1F2970BCFE</MAC>
</VPOSREQ>
```

MAC Calculation:

The fields used for the calculation of the MAC of this message are:

- TERMINAL_ID
- TRANSACTION_ID
- PAN
- EXPIRE_DATE
- CVV2
- AMOUNT
- CURRENCY
- ECI
- XID
- CAVV
- VERSION_CODE
- secretKey

SAMPLE STRING

mac= HASH SHA1(<TERMINAL_ID>< TRANSACTION_ID><PAN><EXPIRE_DATE>< CVV2><AMOUNT>< CURRENCY>< ECI>< XID>< CAVV>< VERSION_CODE><secretKey>)

Payment Result Message

This XML message is returned by the XPay platform in response to the AuthOnlyReq message. It uses the same connection on which the message was received, and contains the transaction result for the requested authorisation.

The following table lists the XPay parameters that are included in the message:

Name	Description	Format
TERMINAL_ID	Merchant identification code within XPay.	AN Max 30 CHAR.
TRANSACTION_ID	Unique code which identifies the merchant order.	AN Max 30 CHAR.
REQUEST_TYPE	Possible values: FA: First Attempt RA: Payment request retry	AN 2 CHAR.
RESPONSE	Result of the payment requested. For possible values see the table below.	AN Max 3 CHAR.
AUTH_CODE	This is the authorisation code obtained from the credit card issuer. If the payment result is negative, an empty string will be sent.	AN Min 2 - Max 6 CHAR.
AMOUNT	Amount of the payment requested. This is a string of 9 fixed numbers, where the last	AN Max 9 CHAR.

	two numbers represent the 2 decimal places, and no separator is used between whole numbers and decimal numbers.	
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 PayMail Links

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.cartasi.it/ecomm/ecomm/OffLineServlet

TEST ENVIRONMENT URL

https://int-ecommerce.cartasi.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

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 7 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	payment identification code assigned by the merchant
Esito	Possible values: ANNULLO or ERROR

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

mac	Message Authentication Code. Transaction signature field. For calculation details, see the end of this chapter: MAC Calculation.	AN 40 CHAR.
urlpost	Url to which XPay sends the 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. This field will also be shown in the text of the email sent to the cardholder. For the MyBank service, the field is transmitted to the bank for inclusion in the SCT instruction description, but is truncated to 140 characters.	AN Max 2000 CHAR. for MyBank: AN Max 140 CHAR.
session_id	Session identifier	AN Max 100 CHAR.
Note1	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	AN Max 200 CHAR.

Note2	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	AN Max 200 CHAR.
Note3	Field where the merchant can show information relating to the order. This data will also be included in the report queryable by the back office.	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). This data will also be included in the report queryable by the back office.	AN 16 CHAR.
selectedcard	If present, the payment page that is shown only allows the user to make payment using the network or payment method 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 table here.	AN Max 25 CHAR.
TCONTAB	This field identifies the merchant's chosen deposit method for each transaction. If set to I (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.
modo_gestione_consegna	This field is only available for MySi wallet payments. Customer details are shown in the result depending on the field value. Possible values: • no: no value returned • mail_tel: allows for the return of email, telephone and billing address • complete: allows for the return of email, telephone, billing address and shipping address	AN Max 40 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 7 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 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 30 CHAR.
nome	Name of the person who made the payment.	AN Max 150 CHAR.
cognome	Surname of the person who made the payment.	AN Max 150 CHAR.
mail	Email address of the person who made the payment.	AN Max 150 CHAR.
session_id	Session identifier retrieved from the initiation message.	AN Max 200 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.
modo_gestione_consegna	This field is only available for MySi wallet payments. Customer details are shown in the result depending on the field value. Possible values: • no: no value returned • mail_tel: allows for the return of email, telephone and billing address • complete: allows for the return of email, telephone, billing address and shipping address	AN Max 8 CHAR.
dati_gestione_consegna	Xml containing shipping information	Max 700 CHAR.

Field name	Req.	Descript
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</Recipient
PhoneNumber>
</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.

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>Secret Key>)

Recurring/Card on File Payment

Integrating recurring or CardOnFile payments using PayMail 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 Max 30 CHAR.
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 5 - Max 30 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.
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 5 - Max 30 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.

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

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.cartasi.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
<?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

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.cartasi.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
<?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>T0000000000000000001</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

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.cartasi.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 details, see the end of this chapter: MAC Calculation.	AN 40 CHAR. fixed

(*) 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
<?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
<?xml version="1.0" encoding="ISO-8859-15"?>
<VPOSRES>
     <alias>0000000050242004</alias>
     <REPRES>
     <AUTH NUMELM="1">
      <ELEMENT_AUTH>
          <transCode>T0000000000000000001</transCode>
          <resultCode>0</resultCode>
```

```xml
        <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 (available soon)

PLUGIN for OS Commerce

Module for managing payments on the OS Commerce platform.
Go to plugin version 2.2
Go to plugin version 2.3.4

PLUGIN for OpenCart

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