

Card payment integration

Contents

- [Card payments integration](#)
 - General information about card payments
 - Payment page form & card's data are hosted by BNP Paribas ([payssl.aspx](#))
 - Chart of process flow
 - Process of a transaction with 3D Secure
 - Payment request
 - Payment page form is hosted by the merchant & card's data are hosted by BNP Paribas ([paynow.aspx](#))
 - Payment page form & card's data are hosted by the merchant (Server-to-Server)
 - Chart of process flow via Server-to-Server
 - Process of a transaction with 3D Secure via Server-to-Server connection
 - Call of interface: general parameters
 - Payment via batch
- [Card payments management](#)
 - Capture
 - Cancellation
 - Refunds

Card payments integration

General information about card payments

Axepta BNP Paribas's payment platform processes **all major cards** and **currencies worldwide**. Card data is protected against unauthorized access by **TLS encryption**. Additional security functions are integrated fraud prevention and risk management. Our standardized settlement files guarantee a straightforward reconciliation processes in your accounting.

Verified by Visa and MasterCard SecureCode secure your payment claim by password validation if a customer disputes the payment later. American Express SafeKey also uses the 3D-Secure technology, which means that the card holder must confirm their identity with an authentication feature.

Transaction processing can be made via

- Payment platform forms
- Server-to-server connection
- Batch transfer

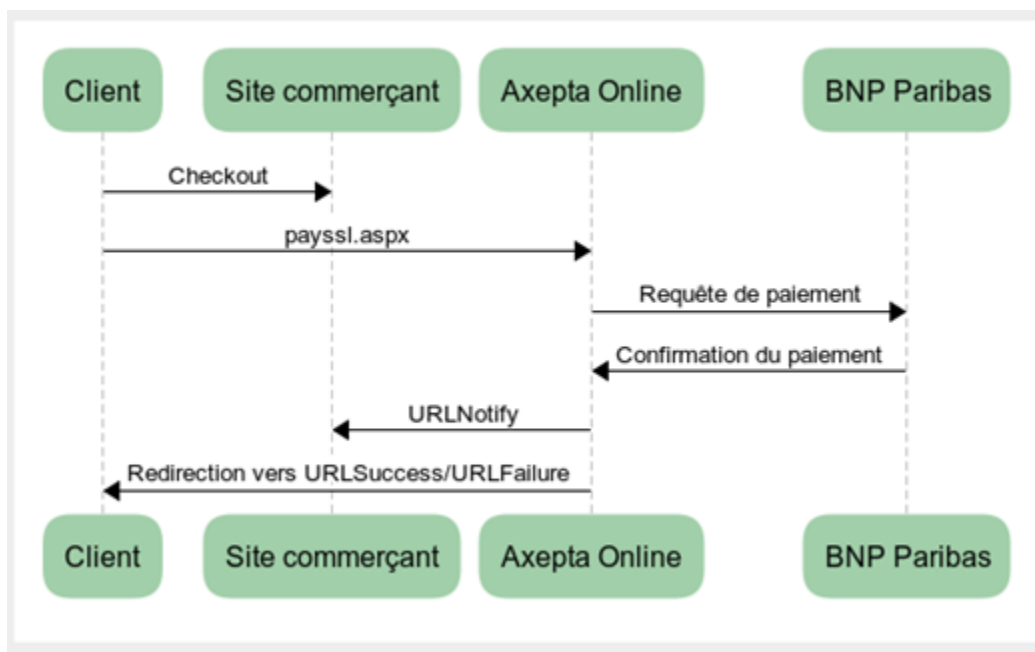
Merchants benefit from authentication with 3D Secure because the card schemes provide a **liability shift**.

From a technical perspective 3D Secure is an authentication process which precedes the payment: Once the card data has been entered, the payment platform checks the identity of the card holder and does not process the payment until the authentication is done.

For further steps it is important to know if the card connection is made via form interface or via Server-to-Server connection. In the first case the payment platform form assumes the further authentication process, with Server-to-Server connection the merchant has to manage the authentication through a separate interface.

Payment page form & card's data are hosted by BNP Paribas ([payssl.aspx](#))

Chart of process flow



Process of a transaction with 3D Secure

- The customer selects the card payment method in the shop and enters the card information.
- The payment platform receives the data and checks, via a connection to the scheme (Visa, MasterCard, Diners, JCB or American Express) whether this card is registered for Verified, SecureCode, Diners ProtectBuy, JCB-Card J/Secure or SafeKey. If the card is not registered a card payment is carried out with TLS.
- With that the transaction gets a flag which identifies payments with 3D Secure. This marking tells the Acquiring Bank that the transaction is using 3DS authentication and a secured payment claim is obtained based on the Liability Shift in case the card holder disputes the payment.
- The payment platform opens a new browser window which connects the customer to its bank. In this window the customer enters the password received by his bank.

The screenshot shows the BNP Paribas 3D Secure authentication interface. At the top, there are logos for BNP PARIBAS, Identification, and VISA. The main content area is titled 'Résumé de la transaction' (Transaction Summary) and includes the following details:

- Marchand:** Preview Merchant
- Montant:** 289,00 €
- Date:** 2017-10-18T17:11:00+02:00
- N° de carte:** xxxxxxxxxx0132
- N° de téléphone:** +3362750XXXX

Below the summary, there is a message: 'BNP Paribas a choisi la solution Visa Secure pour sécuriser vos achats en ligne chez les marchands référencés.' (BNP Paribas has chosen the Visa Secure solution to secure your online purchases at the referenced merchants.)

The next step is to enter the SMS code: 'Pour vous identifier, saisissez votre code d'accès reçu par SMS:' (To identify yourself, enter your access code received by SMS:). There is a text input field and a 'Valider' (Validate) button.

At the bottom, there is a link: 'En cas de problème, consultez l'aide en ligne en cliquant sur le lien ci-dessous.' (In case of a problem, consult the online help by clicking on the link below.)

The footer contains two buttons: 'Annuler' (Cancel) and 'Aide' (Help).

If the password is correct, the payment platform obtains a confirmation (as signature). Only after confirmation does the payment platform start the payment and send the transaction with the signature to BNP Paribas.

Notice: Please notice that in case of Fallback to 3-D Secure 1.0 the URLSuccess or URLFailure is called with GET. Therefore your systems should be able to receive parameters both via GET and via POST.

Payment request

In order to make a card payment via the payment platform form, go to the following URL:

<https://paymentpage.axepta.bnpparibas/payssl.aspx>

This section explains the parameters which are the same for each connection. The second table explains all response parameters which are also the same for all card connections.

Notice: For security reasons, the payment platform rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.



All information about payssl integration are available in the section [Axepta Credit Card Form \(payssl.aspx\)](#)

To adapt the layout of the SSL-page to your shop you can use unencrypted parameters, all details available in the section [Customize checkout experience](#)

Payment page form is hosted by the merchant & card's data are hosted by BNP Paribas (paynow.aspx)

Same 3DS Process as for payssl.aspx.

Silent order post links the benefits of the payment platform forms and Server-to-Server connections: AS opposed to the payment platform form, where the form is loaded from the payment platform server by calling **payssl.aspx**, the Silent order post form has to be provided by the merchant's system. The form uses the same parameters as described here below.

In contrast to the payment platform form, the parameters are not forwarded as URL parameters as is the case when calling the payssl.aspx, but as form input parameters.

Payssl.aspx	Paynow.aspx
payssl.aspx?MerchantID=[mid]&Len=[len]&Data=[data]	<pre><form action=paynow.aspx> <input type="hidden" name="MerchantID" value=[mid]> <input type="hidden" name="Len" value=[len]> <input type="hidden" name="Data" value=[data]> : </form></pre>

The card data must be transmitted to paynow.aspx with the following parameters:

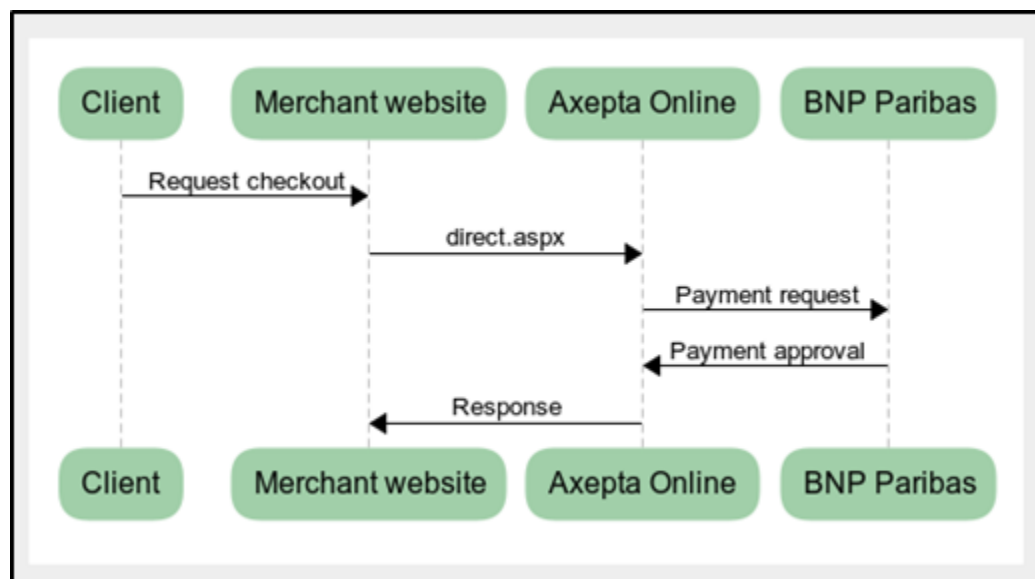
Parameter	Format	CND	Description
CCNr	n..16	M	card number at least 12-digit, numerical without spaces
CCCVC	n3	O	Card verification number: The last 3 digits on the signature strip of the card
CCEpiry	n6	M	Expiry date of the card in the format YYYYMM, e.g. 201807
CCBrand	a..22	M	Designation of card brand. Please note the spelling! According to table of card brands

After the customer has entered his card data, the payment data is forwarded to the Silent order post page, where the further payment processing takes place via 3D-Secure. The form details must be directly forwarded to the Silent order post page and may not be transmitted to the merchant's system! Also, no PCI-relevant data may be transmitted to the Silent order post page as additional input parameters!

Notice: Please note, that automatic retry attempts at the payment platform must be deactivated when using the Paynow.aspx. The background is that at a retry attempt, the payment platform cannot send back the customer to the previously used special shop form. Please contact the BNP Paribas Support to deactivate the retry attempts.

Payment page form & card's data are hosted by the merchant (Server-to-Server)

Chart of process flow via Server-to-Server



Process of a transaction with 3D Secure via Server-to-Server connection

To carry out authentication, the payment platform connects the card holder to his bank, which confirms the identity. A payment process with Verified by Visa or MasterCard SecureCode, Diners ProtectBuy, JCB-Card J/Secure or American Express SafeKey comprises two steps: authentication and payment.

In the next steps, there are two different cases in which the payment platform responds:

- **Case 1: card registered for a 3D Secure system with a pop-up payment page**

If the card is registered for Verified or SecureCode, ProtectBuy, J/Secure or SafeKey, the payment platform returns the socket-connection HTML source code with a JavaScript function. This JavaScript function creates the connection to the bank with which the customer is authenticated by entering its password into a popup-window. The HTML source code with the JavaScript function `Initiate3DSec()` which the payment platform sends to the shop must be embedded in the response page which the shop displays in the customer's browser.

Notice: Please note that the use of a popup window can lead to problems with popup blockers in the customer's browser. Therefore case 2 describes an alternative in the form of an iFrame variant.

The following example shows a response page in which the HTML code is embedded:

```

<HTML>

<HEAD>

<META http-equiv=Content-Type content="text/html; charset=unicode">

    <SCRIPT language="javascript">

<!--

<Response excerpt from request: HTML with JavaScript>

    //-->

    </script>

    </HEAD>");

    <BODY onload="javascript:Initiate3DSec();">

<table><tr>

<td align="center"><font face="Verdana" size="-1"><b>Please identify yourself with 3D Secure!</b></font></td>

</tr></table>");

</BODY>

</HTML>

```

Notice: You can also use this code if you only want to verify the identity of the card holder without making a card payment. Our Support team can set your account in a way that the payment platform can carry out just the authentication with Verified or SecureCode, ProtectBuy, J/Secure or SafeKey without payment (Authentication Hosting).

After the customer has been authenticated with its bank, the bank's Access Control Server (ACS) requests the TermURL in the shop. In the case of this Request the ACS transfers the following parameters via GET (QueryString) to the TermURL of the shop: MID, PayID and TransID. The PARES parameter is transferred via POST.

Notice: The PAResponse parameter must be URL encoded but not Blowfish-encrypted since the content can include special characters.

The parameter must be transferred via POST to the following URL:

<https://paymentpage.axepta.bnpparibas/direct3d.aspx>

Notice: If you forward the PARES and MID of the ACS parameters please use the specified parameter name MerchantID, PAResponse for the direct3d.aspx page.

- **Case 2: card registered for a 3D Secure system with an iFramed payment page**

Alternatively to the popup window, the card holder can also carry out authentication with the bank in an iFrame variant; this avoids difficulties with popup blockers in the customer's browser. Provided the card is registered on the Directory Server, the payment platform returns the following parameters via the socket connection.

If the card is registered with the server (Directory Server), the payment platform returns following parameters via socket connection.

Parameter	Format	CND	Description
ACSURL	ans..	C	Only in the case of registered cards: URL of the Access Control Server of the card issuer with attached request parameters (not URL-encoded!)
PaReq	ans..	M	Payer Authentication Request, which must be URL-encoded.
MD		M	Merchant Data is an empty value, which must be transferred for compatibility reasons
TermURL	ans..	M	Shop return address

Example of correct using of the ACSURL and TermURL :

acsurl=a?b=c&d=e&pareq=f&termurl=g?PayID=h&TransID=i&MID=j

ACSURL: a?b=c&d=e

TermURL: g?PayID=h&TransID=i&MID=j

Notice: Please note in this process that data must sometimes be transferred directly from the bank network. Therefore e.g. the ACSURL parameter is not URL-encoded, although the payment platform uses other URL-encoded data.

These parameters should be included as HIDDEN fields in an HTML page which posts itself to the ACS-URL. The following listing shows one such HTML page, in which the return parameters are embedded:

```
<HTML>

<HEAD>

<META http-equiv=Content-Type content="text/html; charset=unicode">

<A content="MSHTML 6.00.2800.1106" name=GENERATOR>

</HEAD>

<BODY onload="sendpareq.submit();">

<FORM action="[ACSURL]" method="POST" name="sendpareq">

<input type="hidden" name="MD" value="">

<input type="hidden" name="PaReq" value="[PaReq]">

<input type="hidden" name="TermUrl" value="[TermUrl]">

</FORM>

</BODY>

</HTML>
```

Notice: You can also use this code if you only want to verify the identity of the card holder without immediately making a card payment (Authentication Hosting). BNP Paribas Support can configure your checkout so that the payment platform can carry out Verified by Visa or SecureCode without payment.

After the customer has been authenticated with its bank, the bank's Access Control Server (ACS) requests the TermURL in the shop. In the case of this Request the ACS transfers the following parameters via GET (QueryString) to the TermURL of the shop: MID, PayID and TransID (unencrypted). The PARES parameter is transferred unencrypted via POST.

Notice: The PAResponse parameter must be URL encoded but not Blowfish-encrypted since the content can include special characters.


The parameter must be transferred in whole via POST to the following URL:

```
https://paymentpage.axepta.bnpparibas/direct3d.aspx
```

Notice: If you forward the PARES and MID of the ACS parameters please use the specified parameter name MerchantID, PAResponse for the direct3d.aspx page.

Call of interface: general parameters

Notice: For card payments with 3D Secure, please note the different cases as explained separately in the previous chapter. If the card is registered for Verified or SecureCode or SafeKey, the next phase is divided into two steps of authentication and payment. However, it always begins in the same way via the direct.aspx interface. The first response is the receipt of Javascript code or other parameters in order to carry out a second call up of the direct3d.aspx interface. Only after that, you receive the listed parameter as a response.

 Credit card still must be valid at time of capture / refund. Therefore BNP accepts credit cards when the card is at least 1 week valid before expire (e.g.: CC expire: 2020-03 authorizations possible until 2020-03-24, 23:59:59).

To carry out a TLS card payment via a Server-to-Server connection, call the following URL:

```
https://paymentpage.axepta.bnpparibas/direct.aspx
```

Notice: For security reasons, the payment platform rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.



All information about payssl integration are available in the section [Server-2-Server - MIT payments - direct.aspx](#)

Payment via batch

This section describes the parameters that must be transferred within the data set (Record) for executing a card payment and which information can be found within the response file about the payment status.

The structure for a card payment within a Batch file to be submitted is the following:

```
HEAD,<MerchantID>,<Date>,<Version>

CC,Authorize,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>]

CC,Capture,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,<FinishAuth>,<textfeld1>,<textfeld2>,<approvalcode>]

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>]

CC,Credit,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,<FinishAuth>,<textfeld1>,<textfeld2>]

CC,CreditEx,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,[<CCCVC>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>]

CC,Reverse,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>

FOOT,<CountRecords>,<SumAmount>
```

Example for batch versions:

```
Version 1.2:

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<cardholder>,<transactionID>,<schemeReferenceID>

Version 1.21:

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<transactionID>,<schemeReferenceID>

Version 1.3:

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>,<textfeld1>,<textfeld2>,<transactionID>,<schemeReferenceID>

Version 1.5:

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>,<Zone>
```

The following table describes the individual fields and values used within the data set (record) in the batch file:

Parameter	Format	CND	Description
RefNr	an12	OC	<p>Merchant's unique reference number, which serves as payout reference in the acquirer EPA file. Please note, without the own shop reference delivery you cannot read out the EPA transaction and regarding the additional settlement file we cannot add the additional payment data.</p> <p>Notes:</p> <ul style="list-style-type: none">• Fixed length of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, no special characters like whitespace, underscore...)• For AMEX : RefNr is mandatory• If the number of characters entered is lower than 12, BNP will complete, starting from the left side, with "0" (Example : 000018279568)

Type	a..11	M	HEAD for Header, FOOT for Footer, CC for card
Action	a..20	M	The parameter Action defines the type of transaction: Authorize (authorisation) Capture Sale Credit CreditEx (credit note without previous capture; please agree this with Support beforehand) Reverse (cancellation)
Amount	n..10	M	Amount in the smallest currency unit (e.g. EUR Cent). Please contact the helpdesk, if you want to capture amounts < 100 (smallest currency unit).
Currency	a3	M	Currency code, three digits DIN / ISO 4217
TransID	ans..64	M	TransactionID which should be unique for each payment
PayID	an32	M	ID for this transaction given by the payment platform
OrderDesc	ans..127	O	Description of purchased goods, unit prices etc.
CCBrand	a..22	C	Card brand. Please note the spelling! According to table of card brands!
CCNr	n..16	C	Card number at least 12-digit, numerical without spaces. You can optionally transmit also a pseudo card number (PCN)
PCNr	n..16	O	You can optionally transmit also a pseudo card number (PCN) instead of the real card number
CCCVC	n..4	O	Card verification number in Version 1.3: In the case of Visa and MasterCard the last 3 numbers on the signature strip of the card. 4 numbers in the case of American Express.
CCEpiry	n6	O	Expiry date of the card in the format YYYYMM, e.g. 201707.
FinishAuth	ans1	O	Version=1.4: If using the authorisation renewal, cancel repeat with the value Y in the field FinishAuth in the case of Capture or Credit. Example: You capture a partial delivery. The rest of the order cannot be supplied. You therefore enter Y in the FinishAuth field for Part-capture so that the payment platform does not authorise the remaining amount. Please note for this also the following section about Cancel authorisation renewals.

The record area within the response file for Batch transactions looks as follows:

```

HEAD,<MerchantID>,<Date>,<Version>

CC,Authorize,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>[
<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>],<Status>,<Code>

CC,Capture,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>[<textfeld1>,<textfeld2>,<approvalcode>],<Status>,<Code>

CC,AuthSplit,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,FAILED,<Code>,<Description>,<PCNr>

CC,Renewal,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,FAILED,<Code>,<Description>,<PCNr>

CC,Sale,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>[<textfeld1>,<textfeld2>,<RTF>,<approvalcode>,<cardholder>,<Zone>,<transactionID>,<schemeReferenceID>],<Status>,<Code>

CC,Credit,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>[,<FinishAuth>,<textfeld1>,<textfeld2>],<Status>,<Code>

CC,CreditEx,<Amount>,<Currency>,<TransID>,<RefNr>,<CCBrand>,<CCNr|PCNr>,<CCCVC>,<CCEpiry>,<OrderDesc>[<textfeld1>,<textfeld2>],<Status>,<Code>

CC,Reverse,<Amount>,<Currency>,<TransID>,<RefNr>,<PayID>,<Status>,<Code>

FOOT,<CountRecords>,<SumAmount>

```

Example for batch versions:

Version 1.2:

CC, Sale, <Amount>, <Currency>, <TransID>, (<RefNr>), <CCBrand>, <CCNr|PCNr>, <CCEpiry>, <OrderDesc>, <Status>, <Code>

CC, Sale, <Amount>, <Currency>, <TransID>, (<RefNr>), <CCBrand>, <CCNr|PCNr>, <CCEpiry>, <OrderDesc>, <textfield1>, <textfield2>, <RTF>, <cardholder>, <transactionID>, <schemeReferenceID>, <Status>, <Code>

Version 1.21:

CC, Sale, <Amount>, <Currency>, <TransID>, (<RefNr>), <CCBrand>, <CCNr|PCNr>, <CCEpiry>, <OrderDesc>, <textfield1>, <textfield2>, <RTF>, <approvalcode>, <cardholder>, <transactionID>, <schemeReferenceID>, <Status>, <Code>

Version 1.3:

CC, Sale, <Amount>, <Currency>, <TransID>, (<RefNr>), <CCBrand>, <CCNr|PCNr>, <CCCVC>, <CCEpiry>, <OrderDesc>, <textfield1>, <textfield2>, <transactionID>, <schemeReferenceID>, <Status>, <Code>

Version 1.5:

CC, Sale, <Amount>, <Currency>, <TransID>, (<RefNr>), <CCBrand>, <CCNr|PCNr>, <CCCVC>, <CCEpiry>, <OrderDesc>, <Zone>, <Status>, <Code>

The following table describes the response parameters which the batch Manager saves in the "Record" area for each transaction (standard parameters not explained here, such as <TransID> or <RefNr> and request parameters are returned unchanged and correspond to the call as specified before):

Parameter	Format	CND	Description
Action	a..20	M	The parameter Action defines the type of transaction like capture or credit – see above.
PayID	an32	M	ID for this transaction given by the payment platform
Status	a..50	M	OK or FAILED
Code	n8	M	Error code according to the payment platform Response Codes Excel file
PCNr	n..16	C	The Pseudo Card Number is only returned in the case of transaction types Authorize or Sale & CreditEx. It starts with 0 and the last 3 digits correspond to those of the real card number.

Card payments management

Capture

The merchant can choose one of these different options of capture:

- **Manual** capture
- **Automatic** capture
- **Automatic** capture with **customized delay** (number from 1 to 696)

When choosing the **manual** mode, it's necessary for the merchant to validate manually each transaction. A transaction must be validated before 7 days. Captures are possible via a Server-to-Server connection. To perform captures via a Server-to-Server connection please use the following URL:

<https://paymentpage.axepta.bnpparibas/capture.aspx>


When choosing the **automatic**, capture is made every day at the end of the day.

When choosing the **automatic** mode **with customized delay**, the merchant sets a delay in hours (from 1 to 696) that corresponds to the frequency of capture

Notice: For security reasons, the payment platform rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.

The following table describes the encrypted payment request parameters:

Parameter	Format	CND	Description
-----------	--------	-----	-------------

RefNr	an12	OC	<p>Merchant's unique reference number, which serves as payout reference in the acquirer EPA file. Please note, without the own shop reference delivery you cannot read out the EPA transaction and regarding the additional settlement file we cannot add the additional payment data.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Fixed length of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, no special characters like whitespace, underscore...) • For AMEX : RefNr is mandatory • If the number of characters entered is lower than 12, BNP will complete, starting from the left side, with "0" (Example : 000018279568) <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> In cas of manual capture, the RefNr should be the same for authorization (payment creation) and capture.</p> <p>If values are different, the financial reconciliation will not work.</p> </div>
MerchantID	ans..30	M	Merchant ID, assigned by BNP
PayID	an32	M	ID assigned by the payment platform for the payment
TransID	ans..64	M	TransactionID which should be unique for each payment
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm
Amount	n..10	M	<p>Amount in the smallest currency unit (e.g. EUR Cent).</p> <p>Please contact the helpdesk, if you want to capture amounts < 100 (smallest currency unit).</p>
Currency	a3	M	Currency, three digits DIN / ISO 4217
ReqID	ans..32	O	To avoid double payments, enter an alphanumeric value which identifies your transaction and may be assigned only once. If the transaction is submitted again with the same ReqID, the payment platform will not carry out the payment, but will just return the status of the original transaction. Please note that the payment platform must have a finalized transaction status for the first initial action. Submissions with identical ReqID for an open status will be processed regularly.
FinishAuth	a1	C	Only with ETM: Transmit value <Y> in order to stop the renewal of guaranteed authorisations and rest amounts after partial captures. Please use this parameter only if you are using the additional function ETM (Extended Transactions Management).
Textfeld1	ans..30	O	Card holder information: Name
Textfeld2	ans..30	O	Card holder information: City

The following table describes the payment platform's response parameters:

Parameter	Format	CND	Description
MID	ans..30	M	MerchantID
RefNr	an12	OC	<p>Merchant's unique reference number, which serves as payout reference in the acquirer EPA file. Please note, without the own shop reference delivery you cannot read out the EPA transaction and regarding the additional settlement file we cannot add the additional payment data.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Fixed length of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, no special characters like underscore, minus...) • For AMEX : RefNr is mandatory
PayID	an32	M	ID assigned by the payment platform for the payment, e.g. for referencing in batch files
XID	an32	M	ID for all single transactions (authorisation, capture, refund) for one payment assigned by the payment platform
TransID	ans..64	M	Merchant's transaction number
Status	a..50	M	OK or FAILED
Description	ans..1024	M	Further details in the event that payment is rejected. Please do not use the Description but the Code parameter for the transaction status analysis!
Code	n8	M	Error code according to the payment platform Response Codes Excel file

Partial captures are also possible by setting the « Amount » parameter with the partial amount to capture in the payment request, or via the back office by visualizing the transaction details then setting the partial amount to capture.

Cancellation

Cancellation function allows to cancel a transaction before it gets captured.

BNP Paribas manages the cancellation requests by proceeding to 2 verifications:

- The amount: It's forbidden to cancel an amount that is superior to the initial amount of the transaction.
- Payment capture time: Once a payment is captured, it can't be cancelled anymore.

To make a cancellation, use the following URL:


<https://paymentpage.axepta.bnpparibas/reverse.aspx>

Notice: For security reasons, the payment platform rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.

Notice: Reverse.aspx does not only reverse authorizations, but any last transaction stage. If the last transaction was a capture, Reverse.aspx initiates the reverse, e.g. a refund. Therefore, the utmost caution is urged. Use is at your own risk. We recommend checking the transaction status with Inquire.aspx before using Reverse.aspx.

(Further information about inquire.aspx you can find within the documentation Status requests.)

The following table describes the encrypted payment request parameters:

Parameter	Format	CND	Description
MerchantID	ans..30	M	MerchantID
PayID	an32	M	the payment platform ID for the identification of a payment
TransID	ans..64	M	TransactionID which should be unique for each payment
Amount	n..10	M	Amount in the smallest currency unit (e.g. EUR Cent). Please contact the helpdesk, if you want to capture amounts < 100 (smallest currency unit). <div> The amount should be the same as the authorization. Partial reverse is not available</div>
Currency	a3	M	Currency code, three digits DIN / ISO 4217
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm
ReqID	ans..32	O	To avoid double payments, enter an alphanumeric value which identifies your transaction and may be assigned only once. If the transaction is submitted again with the same ReqID, the payment platform will not carry out the payment, but will just return the status of the original transaction. Please note that the payment platform must have a finalized transaction status for the first initial action. Submissions with identical ReqID for an open status will be processed regularly.

The following table describes the payment platform response parameters:

Paramater	Format	CND	Description
MID	ans..30	MC	MerchantID
PayID	an32	M	ID assigned by the payment platform for the payment, e.g. for referencing in batch files
XID	an32	M	ID for all single transactions (authorisation, capture, refund) for one payment assigned by the payment platform
TransID	ans..64	M	Merchant's transaction number
Status	a..50	M	OK or FAILED
Description	ans..1024	M	Further details in the event that payment is rejected. Please do not use the Description but the Code parameter for the transaction status analysis!
Code	n8	M	Error code according to the payment platform Response Codes Excel file

Refunds

Refunds allow to re-credit a customer who was previously debited (product not delivered, product damaged, product sent back...). The customer's bank account is credited with the exact amount as the debit amount of the merchant. The merchant can refund a customer until 12 months following the purchase.

Refunds are not permitted for unpaid transactions.

Refunds are possible via a Server-to-Server connection. The payment platform permits refunds which relate to a capture previously activated by the payment platform and allows merchants to carry out refunds without a reference transaction. This section describes the processing of refunds with reference transactions. If you refer to a capture for a refund, the amount of the refund is limited to the amount of the previous capture.

To carry out a refund with a reference transaction, please use the following URL:

<https://paymentpage.axepta.bnpparibas/credit.aspx>

Notice: For security reasons, the payment platform rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.

The following table describes the encrypted payment request parameters:

Parameter	Format	CND	Description
RefNr	an12	OC	Merchant's unique reference number, which serves as payout reference in the acquirer EPA file. Please note, without the own shop reference delivery you cannot read out the EPA transaction and regarding the additional settlement file we cannot add the additional payment data. Notes: <ul style="list-style-type: none"> • Fixed length of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, no special characters like underscore, minus...) • For AMEX : RefNr is mandatory
MerchantID	ans..30	M	Merchant ID, assigned by BNP
PayID	an32	M	ID assigned by the payment platform for the payment
TransID	ans..64	M	TransactionID which should be unique for each payment
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm
Amount	n..10	M	Amount in the smallest currency unit (e.g. EUR Cent). Please contact the helpdesk, if you want to capture amounts < 100 (smallest currency unit).
Currency	a3	M	Currency, three digits DIN / ISO 4217
OrderDesc	ans..768	O	Merchant's reference number
ReqID	ans..32	O	To avoid double payments, enter an alphanumeric value which identifies your transaction and may be assigned only once. If the transaction is submitted again with the same ReqID, the payment platform will not carry out the payment, but will just return the status of the original transaction. Please note that the payment platform must have a finalized transaction status for the first initial action. Submissions with identical ReqID for an open status will be processed regularly.
Textfield1	ans..30	O	Card holder information: Name
Textfield2	ans..30	O	Card holder information: City

The following table describes the payment platform response parameters:

Parameter	Format	CND	Description
RefNr	an12	OC	Merchant's unique reference number, which serves as payout reference in the acquirer EPA file. Please note, without the own shop reference delivery you cannot read out the EPA transaction and regarding the additional settlement file we cannot add the additional payment data. Notes: <ul style="list-style-type: none"> • Fixed length of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, no special characters like underscore, minus...) • For AMEX : RefNr is mandatory
MID	ans..30	M	MerchantID
PayID	an32	M	ID assigned by the payment platform for the payment, e.g. for referencing in batch files
XID	an32	M	ID for all single transactions (authorization, capture, refund) for one payment assigned by the payment platform
TransID	ans..64	M	Merchant's transaction number
Status	a..50	M	OK or FAILED

Description	ans..1024	M	Further details in the event that payment is rejected. Please do not use the Description but the Code parameter for the transaction status analysis!
Code	n8	M	Error code according to the payment platform Response Codes Excel file