

# Axepta Credit Card Form (payssl.aspx)



## Credit Card Payment Form (PaySSL)

The Credit Card Payment Form (PaySSL) is specialized for collecting the credit card data of your customer and is **hosted by Axepta**.

- [Credit card form](#)
- [How to call the Credit card form ?](#)
  - [Request parameters](#)
  - [Response](#)
- [Step by step : Create a 20 euros payment](#)
  - [Calculate the HMAC value](#)
  - [Calculate the DATA and Len values](#)
  - [Finalize the request](#)
- [Customize the checkout experience](#)
  - [Language](#)
  - [Integration and customization options](#)
  - [On the customer side](#)
- [Diagrams](#)
  - [Simplified Sequence Diagram](#)
  - [Extended Sequence Diagram](#)



## Notice about Cookie-/Session Handling

Please note that some browsers might block necessary cookies when returning to Your shop. [Here](#) you will find additional information and different solution approaches.

[Third-party-cookies](#) - [Browser cookies and session handling](#)

## Credit card form

When requesting card payments via hosted forms the complexity of 3-D Secure is completely removed from the merchant implementation.

From a merchant point of view the sequence itself does not differ between 3DS authenticated and non-authenticated payments though 3DS requires consideration of additional data elements in the request and response.



Sélectionner votre langue: Français

The screenshot shows a credit card payment form with a sidebar on the left and a main payment area on the right. The sidebar contains the following information:

- VOTRE COMMANDE**: 2018\_1234
- VOTRE PANIER**: Sport Shoes, size 45
- VOS COORDONNÉES**: CustomFields
- ADRESSE DE LIVRAISON**: CustomFields
- HEADER**: Custom Text
- MONTANT TOTAL**: 50 EUR
- [Annuler votre panier et revenir à la boutique](#)

The main payment area is titled "Veuillez saisir votre numéro de carte:" and contains the following fields:

- Numéro de carte
- Mois exp
- Année exp
- CVV
- Nom sur la carte

Below the fields, there is a "Transaction sécurisée par AXEPTA" logo and a "Payer maintenant" button. At the bottom, there are logos for "certification PCI DSS", "Verified by VISA", and "Mastercard SecureCode".

# How to call the Credit card form ?

To make payment requests via the credit card form, the merchant should send a request to the following URL via HTTP POST :



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

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

All details required for payment processing are forwarded as parameters.

## Request parameters

The following parameters are mandatory for all payment methods and have to be submitted Blowfish-encrypted within the Data parameter

Key	Format	CND	Description				
MerchantID	ans..30	M	MerchantID, assigned by Axepta. Additionally this parameter has to be passed in plain language too.				
MsgVer	ans..5	M	<div>Message version.</div> <div>Values accepted</div> <table><tr><th>Value</th><th>Description</th></tr><tr><td>2.0</td><td>With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.</td></tr></table> <div> <b>For all card transactions</b> (CB, Visa, Mastercard, AMEX)</div>	Value	Description	2.0	With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.
Value	Description						
2.0	With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.						
TransID	ans..64	M	Transaction identifier supplied by the merchant. Shall be unique for each payment				
RefNr	an..12	M recommended	<div>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 (CTSF) we cannot add the additional payment data.</div> <div>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.</div> <div>Notes:</div> <ul style="list-style-type: none"><li>• <b>Fixed length</b> of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, <b>no special characters</b> like whitespace, underscore...)</li><li>• If the number of characters entered is lower than 12, BNP will complete, starting from the left side, with "0" (Example : 000018279568)</li></ul> <div> <b>The format depends on the available paymethods for your MerchantId and this parameter is used for card payments reconciliation.</b> <b>Please choose your format in that way that all paymethods are covered.</b> We recommend to use the most restrictive format for this parameter (<b>AN12 - M</b>) and create <b>unique RefNr</b>. More details : <a href="#">Data reconciliation</a> : <a href="#">Key Data</a></div>				
Amount	n..10	M	Transaction amount in it smallest unit of the submission currency				
Currency	a3	M	ISO 4217 three-letter currency code - Ex : EUR				

Capture	ans..6	O	Determines the type and time of capture.								
			<table><tr><th>Capture Mode</th><th>Description</th></tr><tr><td>AUTO</td><td>Capturing immediately after authorisation (default value).</td></tr><tr><td>MANUAL</td><td>Capturing made by the merchant. Capture is normally initiated at time of delivery.</td></tr><tr><td>&lt;Number&gt;</td><td>Delay in hours until the capture (whole number; 1 to 696).</td></tr></table>	Capture Mode	Description	AUTO	Capturing immediately after authorisation (default value).	MANUAL	Capturing made by the merchant. Capture is normally initiated at time of delivery.	<Number>	Delay in hours until the capture (whole number; 1 to 696).
			Capture Mode	Description							
			AUTO	Capturing immediately after authorisation (default value).							
			MANUAL	Capturing made by the merchant. Capture is normally initiated at time of delivery.							
<Number>	Delay in hours until the capture (whole number; 1 to 696).										
Order Desc	ans..768	O	Order description								
AccVerify	a3	O	Indicator to request an account verification (aka zero value authorization). If an account verification is requested the submitted amount will be optional and ignored for the actual payment transaction (e.g. authorization).  Values accepted <ul style="list-style-type: none"><li>Yes</li></ul>								
three DSPolicy	JSON	O	Object specifying authentication policies and exemption handling strategies								
priorAuthenticationInfo	JSON	O	Prior Transaction Authentication Information contains optional information about a 3DS cardholder authentication that occurred prior to the current transaction								
accountInfo	JSON	O	The account information contains optional information about the customer account with the merchant								
billToCustomer	JSON	O	The customer that is getting billed for the goods and / or services. Required for EMV 3DS unless market or regional mandate restricts sending this information.								
shipToCustomer	JSON	O	The customer that the goods and / or services are sent to. Required if different from billToCustomer.								
billingAddress	JSON	O	Billing address. Required for EMV 3DS (if available) unless market or regional mandate restricts sending this information.								
shippingAddress	JSON	O	Shipping address. If different from billingAddress, required for EMV 3DS (if available) unless market or regional mandate restricts sending this information.								
credentialFile	JSON	C	Object specifying type and series of transactions using payment account credentials (e.g. account number or payment token) that is stored by a merchant to process future purchases for a customer. Required if applicable.								
merchantRiskIndicator	JSON	O	The Merchant Risk Indicator contains optional information about the specific purchase by the customer.  If no shippingAddress is present it is strongly recommended to populate the shippingAddressIndicator property with an appropriate value such as shipToBillingAddress, digitalGoods or noShipment.								
URLNotify	ans..256	M	A FQDN URL for redirection of the client in case the payment was processed successfully (HTTP POST).  Complete URL which Platform calls up in order to notify the shop about the payment result. The URL may be called up only via port 443. It may not contain parameters: Use the UserData parameter instead.  <div><div></div><div>Common notes:</div><div><ul style="list-style-type: none"><li>We recommend to use parameter "response=encrypted" to get an encrypted response by Platform</li><li>However, fraudster may just copy the encrypted DATA-element which are sent to URLFailure and send the DATA to URLSuccess/URLNotify. Therefore ensure to check the "code"-value which indicates success/failure of the action. Only a result of "code=00000000" should be considered successful.</li></ul></div></div>								

<b>URLSuccess</b>	ans..256	M	<p>A FQDN URL for redirection of the client in case the payment was processed successfully (HTTP POST).</p> <p>Complete URL which calls up Platform if payment has been successful. The URL may be called up only via port 443. This URL may not contain parameters: In order to exchange values between Platform and shop, please use the parameter <a href="#">UserData</a>.</p> <p><b>i Common notes:</b></p> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by Platform</li> <li>However, fraudster may just copy the encrypted DATA-element which are sent to URLFailure and send the DATA to URLSuccess. Therefore ensure to check the "code"-value which indicates success/failure of the action. Only a result of "code=00000000" should be considered successful.</li> </ul>
<b>URLFailure</b>	ans..256	M	<p>A FQDN URL for redirection of the client in case the payment was processed successfully (HTTP POST).</p> <p>Complete URL which calls up Platform if payment has been unsuccessful. The URL may be called up only via port 443. This URL may not contain parameters: In order to exchange values between Platform and shop, please use the parameter <a href="#">UserData</a>.</p> <p><b>i Common notes:</b></p> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by Platform</li> <li>However, fraudster may just copy the encrypted DATA-element which are sent to URLFailure and send the DATA to URLSuccess/URLNotify. Therefore ensure to check the "code"-value which indicates success/failure of the action. Only a result of "code=00000000" should be considered successful.</li> </ul>
<b>UserData</b>	ans..1024	O	If specified at request, forwards the parameter with the payment result to the shop
<b>MAC</b>	an64	M	<p>Hash Message Authentication Code (HMAC) with SHA-256 algorithm</p> <p><a href="#">HMAC Authentication (Request)</a></p> <p><a href="#">HMAC Authentication (Notify)</a></p>
<b>Response</b>	a7	O	Status response sent by Platform to <a href="#">URLSuccess</a> and <a href="#">URLFailure</a> , should be encrypted. For this purpose, transmit <a href="#">Response=encrypted</a> parameter.
<b>ReqID</b>	ans..32	O	To avoid double payments / actions, enter an alphanumeric value which identifies your transaction and may be assigned only once. If the transaction / action is submitted again with the same ReqID, Axepta Platform will not carry out the payment or new action, but will just return the status of the original transaction / action. Please note that the Axepta Platform must have a finalized transaction status for the first initial action. Submissions with identical ReqID for an open status will be processed regularly.
<b>Plain</b>	ans..50	O	A value to be set by the merchant to return some information unencrypted, e.g. the MID
<b>Custom</b>	ans..1024	O	<p>"Custom"-parameter is added to the request data before encryption and is part of encrypted "Data" in Axepta Platform request. By this they are protected against manipulation by a consumer.</p> <p>The Custom-value is added to the Axepta Platform response in plain text and the " " is replaced by a "&amp;". By this you can put a single value into Custom-parameter and get multiple key-value-pairs back in response for your own purpose.</p> <p>Custom=session=123 id=456 will change in the answer to Session=123&amp;id=456</p>
<b>expirationTime</b>	ans..19	O	<p>timestamp for the end time of the transaction processing, specified in UTC.</p> <p>Format: YYYY-MM-ddTHH:mm:ss</p>
<b>CustomField[n]</b>	ans..50	O	Field that can be used individually by the merchant. Presently 14 fields from CustomField1 to CustomField14 are supported.

## Response

When the payment is completed AXEPTA will send a notification to the merchant server (i.e. **URLNotify**) and redirect the browser to the **URLSuccess** respectively to the **URLFailure**.

The blowfish encrypted data elements as listed in the following table are transferred via **HTTP POST** request method to the URLNotify and URLSuccess/URLFailure.



**Notice:** Please note that the call of URLSuccess or URLFailure takes place with a GET in case of fallback to 3-D Secure 1.0. Therefore your systems should be able to **receive parameters both via GET and via POST**.

The following table describes the payment response parameters :

Key	Format	CND	Description
<b>MID</b>	ans..30	M	MerchantID, assigned by

MsgVer	ans..5	M	<div>Message version.</div> <div>Accepted values:</div> <div><ul style="list-style-type: none"><li>2.0</li></ul></div> <table><tr><th>Value</th><th>Description</th></tr><tr><td>2.0</td><td>With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.</td></tr></table>	Value	Description	2.0	With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.
Value	Description						
2.0	With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.						
<a href="#">PayID</a>	an32	M	ID assigned by for the payment, e.g. for referencing in batch files as well as for capture or credit request.				
<a href="#">XID</a>	an32	M	ID for all single transactions (authorisation, capture, credit note) for one payment assigned by				
<a href="#">TransID</a>	ans..64	M	TransactionID provided by you which should be unique for each payment				
schemeReferencelID	ans..64	C	Card scheme specific transaction ID required for subsequent credential-on-file payments, delayed authorizations and resubmssions.				
Status	a..20	M	<div>Staus of the transaction.</div> <div>Values accepted:</div> <div><ul style="list-style-type: none"><li>Authorized</li><li>OK (Sale)</li><li>FAILED</li></ul></div> <div>In case of <i>Authentication-only</i> the <i>Status</i> will be either <b>OK</b> or <b>FAILED</b>.</div>				
<a href="#">Description</a>	ans..1024	M	Further details in the event that payment is rejected. Please <b>do not</b> use the <b>Description</b> but the <a href="#">Code</a> parameter for the transaction status analysis!				
<a href="#">Code</a>	n8	M	Error code according to Response Codes ( <a href="#">A4 Response codes</a> )				
card	JSON	M	Card data				
ipInfo	JSON	C	Object containing IP information. Presence depends on the configuration for the merchant.				
threeDSData	JSON	M	Authentication data				
resultsResponse	JSON	C	In case the authentication process included a cardholder challenge additional information about the challenge result will be provided				
<a href="#">UserData</a>	ans..1024	O	If specified at request, forwards the parameter with the payment result to the shop.				
<a href="#">MAC</a>	an64	M	<div>Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here:</div> <div><ul style="list-style-type: none"><li><a href="#">HMAC Authentication (Request)</a></li><li><a href="#">HMAC Authentication (Notify)</a></li></ul></div>				

Key	Format	CND	Description	
MsgVer	ans..5	M	Message version.	
			Accepted values: <ul style="list-style-type: none"><li>• 2.0</li></ul>	
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>2.0</td><td>With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.</td></tr></table>	Value
Value	Description			
2.0	With 3-D Secure 2.x a lot of additional data were required (e.g. browser-information, billing/shipping-address, account-info, ...) to improve authentication processing. To handle these information the <a href="#">JSON-objects</a> have been put in place to handle such data. To indicate that these data are used the MsgVer has been implemented.			

Key	Format	CND	Description
<a href="#">PayID</a>	an32	M	ID assigned by for the payment, e.g. for referencing in batch files as well as for capture or credit request.

Key	Format	CND	Description
<a href="#">XID</a>	an32	M	ID for all single transactions (authorisation, capture, credit note) for one payment assigned by

Key	Format	CND	Description
<a href="#">TransID</a>	ans..64	M	TransactionID provided by you which should be unique for each payment

Key	Format	CND	Description
schemeReference ID	ans..64	C	Card scheme specific transaction ID required for subsequent credential-on-file payments, delayed authorizations and resubmissions.
Status	a..20	M	<p>Status of the transaction.</p> <p>Values accepted:</p> <ul style="list-style-type: none"> <li>• <b>Authorized</b></li> <li>• <b>OK</b> (Sale)</li> <li>• <b>FAILED</b></li> </ul> <p>In case of <i>Authentication-only</i> the <i>Status</i> will be either <b>OK</b> or <b>FAILED</b>.</p>

Key	Format	CND	Description
<a href="#">Description</a>	ans..1024	M	Further details in the event that payment is rejected. Please <b>do not</b> use the <b>Description</b> but the <a href="#">Code</a> parameter for the transaction status analysis!


Key	Format	CND	Description
<a href="#">Code</a>	n8	M	Error code according to Response Codes ( <a href="#">A4 Response codes</a> )


Key	Format	CND	Description
card	JSON	M	Card data
ipInfo	JSON	C	Object containing IP information. Presence depends on the configuration for the merchant.
threeDSData	JSON	M	Authentication data
resultsResponse	JSON	C	In case the authentication process included a cardholder challenge additional information about the challenge result will be provided

Key	Format	CND	Description
<a href="#">UserData</a>	ans..1024	O	If specified at request, forwards the parameter with the payment result to the shop.

Key	Format	CND	Description
<a href="#">MAC</a>	an64	M	<p>Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here:</p> <ul style="list-style-type: none"> <li>• <a href="#">HMAC Authentication (Request)</a></li> <li>• <a href="#">HMAC Authentication (Notify)</a></li> </ul>

The following table gives the result parameters which Axepta Platform transmits to **URLSuccess** or **URLFailure** and **URLNotify**. If you have specified the **Response=encrypt** parameter, the following parameters are sent Blowfish encrypted to your system:

 pls. be prepared to receive additional parameters at any time and do not check the order of parameters

 the key (e.g. MerchantId, RefNr) should not be checked case-sensitive

Key	Format	CND	Description
<a href="#">MID</a>	ans..30	M	MerchantID, assigned by BNP

RefNr	an12	M	<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"> <li>• <b>Fixed length</b> of 12 characters (only characters (A..Z, a..z) and digits (0..9) are allowed, <b>no special characters</b> like whitespace, underscore...)</li> <li>• <b>For AMEX</b> : RefNr is <b>mandatory</b></li> <li>• If the number of characters entered is lower than 12, BNP will complete, starting from the left side, with "0" (Example : 000018279568)</li> </ul>
PayID	an32	M	ID assigned by Platform for the payment, e.g. for referencing in batch files as well as for capture or credit request.
XID	an32	M	ID for all single transactions (authorisation, capture, credit note) for one payment assigned by Platform
Code	an8	M	Error code according to Platform Response Codes ( <a href="#">A4 Error codes</a> )
Description	ans..1024	M	Further details in the event that payment is rejected. Please <b>do not</b> use the <b>Description</b> but the <b>Code</b> parameter for the transaction status analysis!
TransID	ans..64	M	<p>TransactionID which should be unique for each payment</p> <p>Please note for some connections the different formats that are given within the specific parameters.</p>
Status	a..50	M	OK or AUTHORIZED (URLSuccess) as well as FAILED (URLFailure)
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <a href="#">HashMAC-Authentication</a> .
UserData	ans..1024	O	If specified at request, Platform forwards the parameter with the payment result to the shop.
MaskedPan	an..19	OC	Masked card number 6X4. If you want to receive the parameter MaskedPan, please contact <a href="#">Axepta Helpdesk</a> , which can activate the return.
TransID	ans..64	M	<p>TransactionID which should be unique for each payment</p> <p>Please note for some connections the different formats that are given within the specific parameters.</p>
CAVV	ans..40	OC	In the case of 3-D Secure with Authentication Hosting (only 3-D request without authorisation): Cardholder Authentication Validation Value: Contains the digital signature for authentication with the ACS of the card issuing bank.
Plain	ans..50	O	A value to be set by the merchant to return some information unencrypted, e.g. the MID
Custom	ans..1024	O	<p>The merchant can submit several values separated by   which are returned unencrypted and separated by &amp;.</p> <p>Custom=session=123 id=456 will change in the answer to Session=123&amp;id=456</p>
CustomField[n]	ans..50	O	Field that can be used individually by the merchant. Presently 14 fields from CustomField1 to CustomField14 are supported.
ECI	n2	OC	For 3D Secure: ACS E-Commerce indicator: defines the security level of a card payment via different communication paths: MOTO, SSL, Verified by Visa etc.
DDD	a1	C	<p>for 3D Secure Authentication Hosting:</p> <p>Y - fully authenticated (complete authentication done)</p> <p>N - not enrolled (checked, but Issuer does not participate)</p> <p>U - uneledgeble (technical error)</p> <p>A – attempt (card does not participate)</p> <p>B – bypass (bypass, only for Cardinal Commerce)</p>

## Step by step : Create a 20 euros payment

This example is based on the test shop [BNP\\_DEMO\\_AXEPTA](#), only credit card payments are setup on this shop.

### Calculate the HMAC value

The HMAC value is obtained by ciphering the string PayID\*TransID\*MerchantID\*Status\*Code with the HMAC key of your shop.

Example with [BNP\\_DEMO\\_AXEPTA](#)

- PayID\*TransID\*MerchantID\*Amount\*Currency \*1\*BNP\_DEMO\_AXEPTA\*2000\*EUR
- HMAC value 529c65ce765e684d42a29ca255ad99ae40b78715abc8ee958bfdbafd2597d30a



For a Payment request, the PayID (unique ID generated by Axepta) is not know yet, so the first data should be left empty.  
So the HMAC will start with \*.

## Calculate the DATA and Len values

The DATA parameter is obtained by ciphering all the parameters required for the payment with the blowfish key of your shop.

All parameters are assembled in a character string and separated by the character &.

At least, a request payment should contain the following parameters :

```
MerchantID=value&MsgVer=value&TransID=value&RefNr&Amount=value&Currency=value&URLNotify=value&URLSuccess=value&URLFailure=v  
alue&MAC=value&OrderDesc=value
```

Example with [BNP\\_DEMO\\_AXEPTA](#)

- Required parameters with the values
  - MerchantID=BNP\_DEMO\_AXEPTA&MsgVer=2.0&TransID=1&RefNr=0000000AB123&Amount=2000&Currency=EUR&URLNotify=<https://axepta.bnpparibas/>&URLSuccess=<https://axepta.bnpparibas/>&URLFailure=<https://group.bnpparibas/>&MAC=529c65ce765e684d42a29ca255ad99ae40b78715abc8ee958bfdbafd2597d30a&OrderDesc=Test:0000
    - If you use BNP\_DEMO\_AXEPTA you have to use "OrderDesc=Test:0000" but this is not mandatory with your own MID
- Encryption with the BNP\_DEMO\_AXEPTA blowfish key
  - DATA =  
43ad07f58ff6a5f9ebbdd42e361d2c85ce4ad41fcd63c697c9ca59076fb5cb782237a2e862a97bb24d949911bb701d698dfed6901f1bc  
b92404f53b8f5336525167ac5b8a9b89c5fb88d79967366e99e59d95f3f0c37126a52495115e28f938e76748a5dc703f7ccbda6ccb4f  
c253b255c06e0df990fd94f4313ec2b94142f9978adb9d1079a36a9dbb83e9638e3e58a124d532ece1b7bc175fa340bd0c73c33d4f7  
8374420091e90735bb014a5163d86bfe38795decacf0358075a85c0fbf80c5535046e7f8df64d204c7a4755e07700d4d17c9ef0bdc6e8  
bbd9c377e3ee0493a0ad2d3a9a624d693d04fe0bdfb3ebb2ef5badb63291ab8d7ad29b4f19b2b0f87dbc0bdb38f282816fe694ac2d51  
2ba741d76a830b2083232246763aa006472661aeb2acf126
  - LEN = 291

## Finalize the request

A correct parameter character string for Platform contains three basic parameters: **MerchantID**, **Len** and **Data**.

The parameters **MerchantID** and **Len** are unencrypted. Only the **Data** parameter is Blowfish-encrypted such as :

```
MerchantID=YourMerchantID&Len=67&Data=0A67FE96a65d384350F50FF1
```

They are added to the endpoint to create the GET request

```
https://paymentpage.axepta.bnpparibas/payssl.aspx?MerchantID=YourMerchantID&Len=67&Data=0A67FE96a65d384350F50FF1
```

The **Data** parameter contains the sensitive payment details such as amount and currency. The encrypted bytes are Hex-encoded and completed to two characters from the left with a zero. Encryption is via Blowfish ECB and is available to you as source-code and components.

The **Len** parameter is very important for encryption because it contains the length of the unencrypted(!) character string in the **Data** parameter. Since the data quantity to be encrypted is increased by a multiple of 8 in the case of the Blowfish encryption, the correct length of the character string must be known for decryption. Otherwise accidental characters emerge at the end of the character string.

The parameters are transmitted via HTTPS POST or HTTPS GET. The recommended transmit method is HTTPS POST because the parameter character string in the case of GET is attached to the URL, which is limited to 2048 bytes depending on the browser.



**Notice:** Please note that the maximum length of a payment request is limited to 5120 characters. If you require longer strings please contact [Axepta Helpdesk](#).

Example with [BNP DEMO AXEPTA](#)

[https://paymentpage.axepta.bnpparibas/payssl.aspx?MerchantID=BNP\\_DEMO\\_AXEPTA&Len=291&DATA=43ad07f58ff6a5f9ebbdd42e361d2c85ce4ad41fcd63c697c9ca59076fb5cb782237a2e862a97bb24d949911bb701d698dfed6901f1bcb92404f53b8f5336525167ac5b8a9b89c5fb88d79967366e99e59d95f3f0c37126a52495115e28f938e76748a5dc703f7ccbd46ccb4fc253b255c06e0df990fdd94f4313ec2b94142f9978adb9d1079a36a9dbb83e9638e3e58a124d532ece1b7bc175fa340bd0c73c33d4f78374420091e90735bb014a5163d86bfe38795decacf0358075a85c0fbf80c5535046e7f8df64d204c7a4755e07700d4d17c9ef0bdc6e8bbd9c377e3ee0493a0ad2d3a9a624d693d04fe0bdfb3ebbb2ef5badb63291ab8d7ad29b4f19b2b0f87dbc0bdb38f282816fe694ac2d512ba741d76a830b2083232246763aa006472661aeb2acf126](https://paymentpage.axepta.bnpparibas/payssl.aspx?MerchantID=BNP_DEMO_AXEPTA&Len=291&DATA=43ad07f58ff6a5f9ebbdd42e361d2c85ce4ad41fcd63c697c9ca59076fb5cb782237a2e862a97bb24d949911bb701d698dfed6901f1bcb92404f53b8f5336525167ac5b8a9b89c5fb88d79967366e99e59d95f3f0c37126a52495115e28f938e76748a5dc703f7ccbd46ccb4fc253b255c06e0df990fdd94f4313ec2b94142f9978adb9d1079a36a9dbb83e9638e3e58a124d532ece1b7bc175fa340bd0c73c33d4f78374420091e90735bb014a5163d86bfe38795decacf0358075a85c0fbf80c5535046e7f8df64d204c7a4755e07700d4d17c9ef0bdc6e8bbd9c377e3ee0493a0ad2d3a9a624d693d04fe0bdfb3ebbb2ef5badb63291ab8d7ad29b4f19b2b0f87dbc0bdb38f282816fe694ac2d512ba741d76a830b2083232246763aa006472661aeb2acf126)



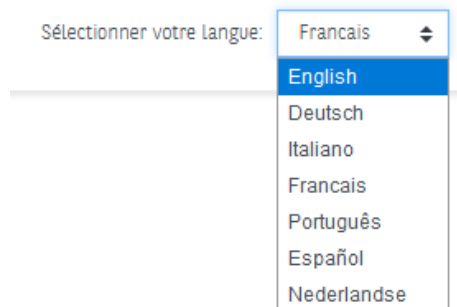
For additional technical information, please refer to [Programming basics : Technical implementation](#) and [Create an API call and samples to play](#)

## Customize the checkout experience

### Language

The standard AXEPTA credit card form is available in several languages such as french, english, german, spanish, portuguese, italian and dutch.

By default, the language of the payment page will match the language used previously by the user, on the merchant's website. However, the user will have the possibility to change the language once he arrives on the payment page thanks to a scrolling menu, on the top right of the page (see below) :



#### Notice about Cookie-/Session Handling

Please note that some browsers might block necessary cookies when returning to Your shop. [Here](#) you will find additional information and different solution approaches.

### Integration and customization options

To adapt the layout of the SSL-page to your shop you can use the following **unencrypted** parameters to configure :

Key	Format	CND	Description
<a href="#">CustomField [n]</a>	ans..50	O	Field that can be used individually by the merchant. Presently 9 fields from CustomField1 to CustomField9 are supported.
Template	ans..20	O	Name of XSLT-file with your own layout for the pay form.
Language	a2 (enum)	O	Language code of the merchant's payment page : <de> German, <en> English, <fr> French, <it> Italian, <pt> Portuguese, <es> Spanish, <nl> Dutch No details mean the language is French.



All information related to integration and customization options are available here : [Customize checkout experience](#)

## On the customer side

AXEPTA Platform will return an HTML document in the response body representing the requested card form. The form may be used as a standalone page or included in the merchant checkout page (iframe).

Cardholder authentication and payment authorization will take place once the cardholder entered all required card details and submitted the form data to AXEPTA Platform

**Note:** In case you are using your own templates (Corporate Payment Page), please make sure you include Cardholder name on your custom template. Cardholder name is mapped to API parameter "CreditCardHolder". Cardholder name field must not contain any special characters and must have minimal length of 2 characters and maximum length of 45 characters.

### Page



#### Details for this page

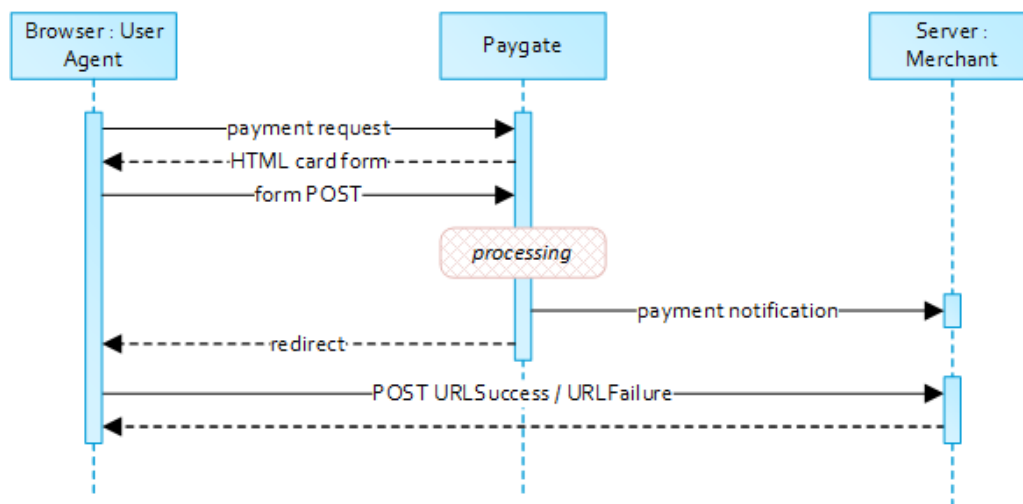
- ✓ provides automatic card type detection via card number
- ✓ your logo can be shown
- ✓ detailed order and customer information is displayed

How to:

- Your logo: CustomField3=<Logo-URL>
- Order and customer details: CustomField1..9

## Diagrams

### Simplified Sequence Diagram



Extended Sequence Diagram

