

# Merchant Credit Card Form - Silent Order Post (PayNow.aspx)



## Merchant Credit Card Form

Create and host your own credit card to collect credit card data of your customer. **PCI DSS Self-Assessment Questionnaire (SAQ) A-EP is mandatory.**

This approach is very similar to BNP hosted payment forms and leaves the merchant in full control of the checkout experience as all website elements are delivered from the merchant's server.

The 3DS authentication is handled by the Axepta Platform.

### Steps :

- The merchant creates and hosts a payment form. The form data is sent directly to Axepta using the "action" parameter of the HTML form which contains the URL of the Axepta server.
- Thus, sensitive data entered on the merchant's website is transmitted directly to the Axepta server and is not transmitted to the merchant's server (silent POST request).

- [Overview](#)
- [PayNow](#)
  - [Silent Mode for credit cards with SSL and 3-D Secure method](#)
- [Payment Request](#)
  - [Form Elements](#)
    - [Data](#)
  - [Sample HTML Form](#)
- [HTTP POST to URLSuccess / URLFailure / URLNotify](#)
  - [Diagram](#)

## Overview

A **Silent Order Post** or **Direct Post** is a transmission method where form data from a merchant website are getting directly posted to a third-party server. This is commonly achieved through the **form action attribute** that specifies the URL the data are sent to.



Sensitive data such as card details can be captured within a merchant's website without being processed by the merchant server as the POST is submitted silently. The URL endpoint in to receive Silent Order Post requests is referred to as **PayNow**.

```
<form action="../../../payNow.aspx" method="post">
```



### PCI-DSS Considerations

Merchants processing card transactions using the Silent Post model must submit the PCI DSS Self-Assessment Questionnaire (SAQ) A-EP. This SAQ is more comprehensive and thus might require more time and resources in comparison to SAQ A applicable to merchants that use hosted payment pages. However, merchants should always consult with their acquirer to evaluate the level of compliance required and refer to the [PCI DSS guidelines](#). This does not affect the use of pseudo card numbers which is possible without submitting the SAQ questionnaire.



### 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.

# PayNow

## Silent Mode for credit cards with SSL and 3-D Secure method

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

In contrast to the Platform form, the parameters are not forwarded as URL parameters as is the case when calling the payssl.aspx, but as form input parameters. By the way for calling the PayNow.aspx the same parameters can be used as for PaySSL.aspx.

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.

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

## Payment Request

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

Please POST the form data as outlined in table below to payNow.aspx.

### Form Elements

Data Element	Legacy Element	3DSV2 Element - Parameter from Card JSON Object	Description
MerchantID	--	--	Merchant identifier assigned by
Len	--	--	The length of the original encrypted with Blowfish
Data	--	--	Blowfish encrypted data
number	CCNr	number	Card number
securityCode	CCCVC	securityCode	Card security value
expiryDate	CCExpiry	expiryDate	Card expiry in format YYYYMM
brand	CCBrand	brand	Card network
cardholder	CreditCardHolder	cardholderName	Name of the cardholder as printed on the card

(- will continue to support the legacy form data fields that are currently in use. -)

### Data


Key	Format	CND	Description
MerchantID	ans..30	M	MerchantID, assigned by . Additionally this parameter has to be passed in plain language too.
TransID	ans..64	M	TransactionID provided by you which should be unique for each payment

MsgVersion	ans..5	M	<p>Message version.</p> <p>Accepted values:</p> <ul style="list-style-type: none"><li>2.0</li></ul>								
RefNr	an..12	M recommended	<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 (CTSF) 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>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><div></div><div><p><b>This parameter is mandatory for card payments reconciliation.</b></p><p>We recommend to use the most restrictive format for this parameter (<b>AN12 - M</b>) and create <b>unique RefNr</b>.</p><p>More details : <a href="#">Data reconciliation</a> : <a href="#">Key Data</a></p></div></div>								
Amount	n..10	M	Amount in the smallest currency unit (e.g. EUR Cent). Please contact the , if you want to capture amounts <100 (smallest currency unit).								
Currency	a3	M	Currency, three digits DIN / ISO 4217, e.g. EUR, USD, GBP. Please find an overview here: <a href="#">Currency table</a>								
Capture	an..6	O	<p>Determines the type and time of capture.</p> <table><thead><tr><th>Capture Mode</th><th>Description</th></tr></thead><tbody><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></tbody></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								
ReqId	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.								
AccountVerification	a3	O	<p>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).</p> <p>Values accepted:</p> <ul style="list-style-type: none"><li>Yes</li></ul>								
threeDSPolicy	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.								
browserInfo	JSON	M	Accurate browser information are needed to deliver an optimized user experience. Required for 3DS 2.0 transactions.								
accountInfo	JSON	O	The account information contains optional information about the customer account with the merchant.								
billToCustomer	JSON	C	The customer that is getting billed for the goods and / or services. Required unless market or regional mandate restricts sending this information.								
shipToCustomer	JSON	C	The customer that the goods and / or services are sent to. Required if different from billToCustomer.								

<a href="#">billingAddress</a>	JSON	C	Billing address. Required (if available) unless market or regional mandate restricts sending this information.
<a href="#">shippingAddress</a>	JSON	C	Shipping address. If different from billingAddress, required (if available) unless market or regional mandate restricts sending this information.
<a href="#">credentialFile</a>	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.
<a href="#">merchantRiskIndicator</a>	JSON	O	The Merchant Risk Indicator contains optional information about the specific purchase by the customer.  If no <a href="#">shippingAddress</a> is present it is strongly recommended to populate the <a href="#">shippingAddressIndicator</a> property with an appropriate value such as <a href="#">shipToBillingAddress</a> , <a href="#">digitalGoods</a> or <a href="#">noShipment</a> .
<a href="#">URLSuccess</a>	ans..256	M	Complete URL which calls up 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 and shop, please use the parameter <a href="#">UserData</a> .  <b>i Common notes:</b> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by</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>
<a href="#">URLFailure</a>	ans..256	M	Complete URL which calls up 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 and shop, please use the parameter <a href="#">UserData</a> .  <b>i Common notes:</b> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by</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>
<a href="#">URLNotify</a>	ans..256	M	Complete URL which 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 <a href="#">UserData</a> parameter instead.  <b>i Common notes:</b> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by</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>
<a href="#">MAC</a>	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> <li><a href="#">HMAC Authentication (Request)</a></li> <li><a href="#">HMAC Authentication (Notify)</a></li> </ul>
<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="#">TransID</a>	ans..64	M	TransactionID provided by you which should be unique for each payment

Key	Format	CND	Description	Beschreibung
<a href="#">MsgVer</a>	ans..5	M	Message version.  Accepted values: <ul style="list-style-type: none"> <li>2.0</li> </ul>	Message-Version.  Zulässige Werte: <ul style="list-style-type: none"> <li>2.0</li> </ul>

RefNr	an..12	M recomm ended	<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 (CTSF) 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>• 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 style="border: 1px solid green; padding: 10px; margin-top: 10px;">  <b>This parameter is mandatory for card payments reconciliation.</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 : Key Data</a> </div>	<p>Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird. Bitte beachten Sie, ohne die Übergabe einer eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das <b>The page DE:Wording was not found</b> -- Please check /update the page name used in the MultiExcerpt-Include macro Settlement File (CTSF) auch nicht zusätzlich angereichert werden.</p>
-------	--------	----------------------	--	---


Key	Format	CND	Description
Amount	n..10	M	Amount in the smallest currency unit (e.g. EUR Cent). Please contact the , if you want to capture amounts <100 (smallest currency unit).


Key	Format	CND	Description
Currency	a3	M	Currency, three digits DIN / ISO 4217, e.g. EUR, USD, GBP. Please find an overview here: <a href="#">Currency table</a>

Key	Format	CND	Description	
Capture	an..6	O	Determines the type and time of capture.	
			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).

Key	Format	CND	Description	Beschreibung
Order Desc	ans..768	O	Order description	Beschreibung der Bestellung
ReqId	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.	
AccVerify	a3	O	<p>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).</p> <p>Values accepted:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b></li> </ul>	<p>Indikator zur Anforderung einer Konto-Verifizierung (alias Nullwert-Autorisierung). Wenn eine Konto-Verifizierung angefordert wird, ist der übermittelte Betrag optional und wird für die tatsächliche Zahlungstransaktion (d.h. Autorisierung) ignoriert.</p> <p>Zulässige Werte:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b></li> </ul>
three DSPolicy	JSON	O	Object specifying authentication policies and exemption handling strategies	Objekt, dass die Authentisierungs-Richtlinien und Strategien zur Behandlung von Ausnahmen angibt

<a href="#">priorAuthenticationInfo</a>	JSON	O	Prior Transaction Authentication Information contains optional information about a 3DS cardholder authentication that occurred prior to the current transaction.	Das Objekt Prior Transaction Authentication Information enthält optionale Informationen über eine 3DS-Authentisierung eines Karteninhabers, die vor der aktuellen Transaktion erfolgt ist.
<a href="#">browserInfo</a>	JSON	M	Accurate browser information are needed to deliver an optimized user experience. Required for 3DS 2.0 transactions.	Exakte Browserinformationen sind nötig, um eine optimierte Nutzererfahrung zu liefern. Erforderlich für 3DS 2.0 Transaktionen.
<a href="#">accountInfo</a>	JSON	O	The account information contains optional information about the customer account with the merchant.	Die Kontoinformationen enthalten optionale Informationen über das Kundenkonto beim Händler.
<a href="#">billToCustomer</a>	JSON	C	The customer that is getting billed for the goods and / or services. Required unless market or regional mandate restricts sending this information.	Der Kunde, dem die Waren und / oder Dienstleistungen in Rechnung gestellt werden. Erforderlich, sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.
<a href="#">shippingCustomer</a>	JSON	C	The customer that the goods and / or services are sent to. Required if different from billToCustomer.	Der Kunde, an den die Waren und / oder Dienstleistungen gesendet werden. Erforderlich, falls von billToCustomer abweichend.
<a href="#">billingAddress</a>	JSON	C	Billing address. Required (if available) unless market or regional mandate restricts sending this information.	Rechnungsadresse. Erforderlich (falls verfügbar), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.
<a href="#">shippingAddress</a>	JSON	C	Shipping address. If different from billingAddress, required (if available) unless market or regional mandate restricts sending this information.	Lieferadresse. Falls abweichend von billingAddress, erforderlich (falls verfügbar), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.
<a href="#">credentialFile</a>	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.	Objekt, dass Art und Reihe der Transaktionen angibt, die unter Verwendung von beim Händler hinterlegten Zahlungsdaten (z.B. Kontonummer oder Zahlungs-Token) zur Verarbeitung künftiger Käufe eines Kunden erfolgen. Erforderlich, falls zutreffend.
<a href="#">merchantRiskIndicator</a>	JSON	O	The Merchant Risk Indicator contains optional information about the specific purchase by the customer.  If no <b>shippingAddress</b> is present it is strongly recommended to populate the <b>shippingAddressIndicator</b> property with an appropriate value such as <b>shipToBillingAddress</b> , <b>digitalGoods</b> or <b>noShipment</b> .	Der Händler-Risikoindikator enthält optionale Informationen über den bestimmten Einkauf des Kunden.  Falls keine <b>shippingAddress</b> vorhanden ist, ist es dringend empfohlen, die Eigenschaft <b>shippingAddressIndicator</b> mit einem entsprechenden Wert wie <b>shipToBillingAddress</b> , <b>digitalGoods</b> oder <b>noShipment</b> auszufüllen.

Key	Format	CND	Description
<a href="#">URLSuccess</a>	ans..256	M	Complete URL which calls up 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 and shop, please use the parameter <a href="#">UserData</a> .   <b>Common notes:</b> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by</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>

Key	Format	CND	Description
<a href="#">URLFailure</a>	ans..256	M	Complete URL which calls up 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 and shop, please use the parameter <a href="#">UserData</a> .   <b>Common notes:</b> <ul style="list-style-type: none"> <li>We recommend to use parameter "response=encrypted" to get an encrypted response by</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>

Key	Format	CND	Description
-----	--------	-----	-------------

<a href="#">URLNotify</a>	ans..256	M	<p>Complete URL which 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 <a href="#">UserData</a> parameter instead.</p> <p><b>Common notes:</b></p> <ul style="list-style-type: none"> <li>• We recommend to use parameter "response=encrypted" to get an encrypted response by</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>
---------------------------	----------	---	---

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>

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.

## Sample HTML Form

**i** BASEURL= <https://paymentpage.axepta.bnpparibas/>

```
<!DOCTYPE html>
<html>
  <head>
    <title>Merchant Checkout</title>
  </head>
  <body>
    <form name="card form" action="BASEURLpayNow.aspx" method="post">
      <input type="hidden" name="MerchantID" value="MerchantID">
      <input type="hidden" name="Len" value="Length of the Blowfish encrypted data">
      <input type="hidden" name="Data" value="Blowfish encrypted data">
      Cardholder:
      <input type="text" name="cardholder"><br>
      Card number:
      <input type="text" name="number"><br>
      Expiry date:
      <input type="text" name="expiryDate"><br>
      CVV2:
      <input type="text" name="securityCode"><br>
      Card brand:
      <input type="text" name="brand"><br>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>
```

When the payment is completed 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 receiver parameters both via GET and via POST.

## HTTP POST to URLSuccess / URLFailure / URLNotify

Key	Format	CND	Description
<a href="#">MID</a>	ans..30	M	MerchantID, assigned by
<b>MsgVer</b>	ans..5	M	Message version.  Accepted values: <ul style="list-style-type: none"> <li>• 2.0</li> </ul>
<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
<b>scheme Referenc eID</b>	ans..64	C	Card scheme specific transaction ID required for subsequent credential-on-file payments, delayed authorizations and resubmissions
<b>Status</b>	a..20	M	Status of the transaction.  Values accepted: <ul style="list-style-type: none"> <li>• <b>Authorized</b></li> <li>• <b>OK (Sale)</b></li> <li>• <b>FAILED</b></li> </ul> In case of <b>Authentication-only</b> the <b>Status</b> will be either <b>OK</b> or <b>FAILED</b> .
<b>Descripti on</b>	ans..1024	M	Textual description of the code
<a href="#">Code</a>	n8	M	Error code according to Response Codes ( <a href="#">A4 Response codes</a> )
<b>RefNr</b>	an12	M	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"> <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>
<a href="#">card</a>	JSON	M	Card response data
<a href="#">ipInfo</a>	JSON	C	Object containing IP information. Presence depends on the configuration for the merchant.
<a href="#">threeDS Data</a>	JSON	M	Authentication data
<a href="#">resultsR esponse</a>	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	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> <li>• <a href="#">HMAC Authentication (Request)</a></li> <li>• <a href="#">HMAC Authentication (Notify)</a></li> </ul>

Key	Format	CND	Description	Beschreibung
<b>MsgVer</b>	ans..5	M	Message version.  Accepted values: <ul style="list-style-type: none"> <li>• 2.0</li> </ul>	Message-Version.  Zulässige Werte: <ul style="list-style-type: none"> <li>• 2.0</li> </ul>

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	Beschreibung
<b>scheme Referen celID</b>	ans..64	C	Card scheme specific transaction ID required for subsequent credential-on-file payments, delayed authorizations and resubmissions	Kartensystemspezifische Transaktions-ID, die für nachfolgende Zahlungen mit hinterlegten Daten, verzögerte Autorisierungen und Wiedereinreichungen erforderlich ist
<b>Status</b>	a..20	M	Status of the transaction.  Values accepted: <ul style="list-style-type: none"> <li>• <b>Authorized</b></li> <li>• <b>OK (Sale)</b></li> <li>• <b>FAILED</b></li> </ul> In case of <b>Authentication-only</b> the <b>Status</b> will be either <b>OK</b> or <b>FAILED</b> .	Status der Transaktion.  Zulässige Werte: <ul style="list-style-type: none"> <li>• <b>Authorized</b></li> <li>• <b>OK (Sale)</b></li> <li>• <b>FAILED</b></li> </ul> Im Falle von <b>nur Authentisierung</b> ist der <b>Status</b> entweder <b>OK</b> oder <b>FAILED</b> .
<b>Descript ion</b>	ans..1024	M	Textual description of the code	Textliche Beschreibung des Codes

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	Beschreibung
<b>RefNr</b>	an12	M	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"> <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>	
<a href="#">card</a>	JSON	M	Card response data	Kartenantwortdaten
<a href="#">ipInfo</a>	JSON	C	Object containing IP information. Presence depends on the configuration for the merchant.	Objekt mit IP-Informationen. Das Vorhandensein hängt von der Konfiguration des Händlers ab.
<a href="#">three DSDData</a>	JSON	M	Authentication data	Authentisierungsdaten
<a href="#">result sResp onse</a>	JSON	C	In case the authentication process included a cardholder challenge additional information about the challenge result will be provided.	Falls der Authentisierungsprozess eine Challenge des Karteninhabers enthalten hat, werden zusätzliche Informationen über das Ergebnis der Challenge bereitgestellt

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

Diagram

