One-click payment

Description

Offer a simple checkout experience to your customers by allowing them to reuse their credit card data

Steps

Step 1 : Initial payment and Card registration

- A customer makes a purchase of € 20.00 on the merchant's site.
- He enters all the data necessary for payment (card number, expiration date, CVV, etc.).
- The merchant offers his customer to register his card.

Step 2 : Offer a One-click payment

- During his next purchase, the merchant offers the customer to reuse his card.
- The customer can be authenticated (CIT - Customer initiated transaction)
- The CVV is optionnal

Prerequisites

- You offer your customers payment by card
- Customers buy in your shop and you store the pseudo card number
- A strong authentication (SCA) is mandatory for the initial payment (card registration)

Implementation

Step 1 : Initial payment and Card registration

The first payment can be done with :

- Credit card form hosted by BNP Paribas - PaySSL.aspx
- Credit card form hosted by the merchant - PayNow.aspx - for merchants PCI-DSS certified

> Authentication with 3D Secure is mandatory for the first transaction initiated by the customer (CIT) / card registration

Request

The following table describes the **additional** encrypted parameters to add in the payment request :

Key	Format	CND	Description	Example

credentialOnFile	JSON	M	Object specifying type of transaction	<pre>{
				    "type": {
				        "unscheduled":
				"CIT"
				    },
				    "initialPayment": true,
				    "useCase": "cof"
				}</pre>

threeDSPolicy	JSON	M	Object specifying authentication policies and exemption handling strategies. Use : **Mandate challenge**	__

Response

JSON Object sent in the response of the initial payment, stored by the merchant and will be used for the next transactions

Key	Format	CND	Description
card	JSON	M	Card response data The object Card available in the response should be decrypted and stored. The object card used in the next request requires less parameters than the card object in the reponse. • card:request EN • card:response EN

Step 2 : One-click payment

One-Click payment can be initiated by the merchant through PayNow.aspx.

The merchant doesn't need to PCI-DSS certified because this feature requires the use of the PCNr (Pseudo Card Number not real PAN). This data is stored by the merchant.

Authentication with 3D Secure is not mandatory for these transactions, so exemptions can be requested.

CVV is optionnal for One-click payments.

Request with paynow.aspx

Mechant creates a **form** with the following fields :

- Number - Hidden field / filled with PCNr by the merchant
- securityCode - Empty or will be filled by the custmer (optionnal)
- expiryDate - Visible or Hidden field / filled with the expiryDate by the merchant
- brand - Visible or Hidden field / filled with the brand by the merchant
- cardholder - Visible or Hidden field / filled with the cardholder by the merchant

All details for integration are available here : Merchant Credit Card Form - Silent Order Post (PayNow.aspx)

The following table describes the **additional** encrypted parameters to add in the payment request :

Key	Format	CND	Description	Example

credentialOnFile	JSON	M	Object specifying type of transactions	<pre>{
				    "type": {
				
				"unscheduled": "CIT"
				    },
				
				"initialPayment": false,
				    "useCase": "cof"
				}</pre>

browserInfo	JSON	M	Accurate browser information are needed to deliver an optimized user experience. Required for 3DS 2.0 transactions.	--

Example with BNP_DEMO_AXEPTA

This example is based on the test shop ***BNP_DEMO_AXEPTA***, only credit card payments are setup on this shop.

Step 1 : Initial payment and Card registration

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 *111*BNP_DEMO_AXEPTA*20*EUR
- HMAC value 634AA4452E61434ECF87533ED31A99FB62CC2A43B466097A26DBF2129B2B82AA

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=value&MAC=value&OrderDesc=value
```

Example with BNP_DEMO_AXEPTA

- Encode JSON Object

Parameter	JSON Object	Base64 Encoding with Padding

credentialOnFile	<pre>{
	"type": {
	
	"unscheduled":
	"CIT"
	},
	
	"initialPayment":
	true
	}</pre>
		ew0KICAgICJ0eXBlIjogew0KICAgICAgICAidW5zY2hlZHVsZWQiOiAiQ0lUIg0KICAgIH0sDQogICAgImluaXRpYWxQYXltZW50IjogdHJ1ZQ0KfQ==

- Required parameters with the values
  - MerchantID=BNP_DEMO_AXEPTA&MsgVer=2.0&TransID=111&RefNr=0000000AB123&Amount=20&Currency=EUR&URLNotify=https://axepta.bnpparibas/&URLSuccess=https://axepta.bnpparibas/&URLFailure=https://group.bnpparibas&MAC=634AA4452E61434ECF87533ED31A99FB62CC2A43B466097A26DBF2129B2B82AA6&OrderDesc=Test:0000&credentialOnFile=ew0KICAgICJ0eXBlIjogew0KICAgICAgICAidW5zY2hlZHVsZWQiOiAiQ0lUIg0KICAgIH0sDQogICAgImluaXRpYWxQYXltZW50IjogdHJ1ZQ0KfQ==
- Encryption with the BNP_DEMO_AXEPTA blowfish key
  - DATA = 43AD07F58FF6A5F9EBBDD42E361D2C85CE4AD41FCD63C697C9CA59076FB5CB782237A2E862A97BB26AA9C827F3BACA3A64792BF0297DF7CE0A25DF836ACDDB100490D0FD09271A0C82F4567B75AE8F3E59D95F3F3F0C37126A52495115E28F938E76748A5DC703F7CCBDA6CCB4FC253B255C06E0DF990FDD94F4313EC2B94142F9978ADB9D1079A36A9DBB83E9638E3E58A124D532ECE1B7BC175FA340BD0C73C33D4F78374420091E90735BB014A5163D86BFE38795DECACF0358075A85C0FBF80C5535046E7F8DDCFFB39A3312AEC824579851424ED4426F4C9901FF06312B0E05479ABE1E935C85EBADFBA9A166631CEDFC90D9A672BF1607E3EAAEC81263AD8751DB1C714492BBDBBA108B82548D59B12FF6A18A80A651D20D91B8F0D8DD55000C257A9899BA214EE17E548B7454015489D127C0F3BCC3504993C36CBC37541F3F7A5961C88DB357AB1B378B492F6A9A8DF8D9B0F254449E35D4D89C02008B95253466EBEB6B218B1C9464B37B371F3D303ED6D7255758848F1CB40866D9A60FF54D872AB41AC55F50A39B7F79CAA19F83A0F3B1F3FD42CA37219D55D62C50C79F9E4571A0A4343FFCF03B977EF2
  - LEN = 425

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 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=425&DATA=43AD07F58FF6A5F9EBBDD42E361D2C85CE4AD41FCD63C697C9CA59076FB5CB782237
A2E862A97BB26AA9C827F3BACA3A64792BF0297DF7CE0A25DF836ACDDB100490D0FD09271A0C82F4567B75AE8F3E59D95F3F3F0C37126A
52495115E28F938E76748A5DC703F7CCBDA6CCB4FC253B255C06E0DF990FDD94F4313EC2B94142F9978ADB9D1079A36A9DBB83E9638E3E
58A124D532ECE1B7BC175FA340BD0C73C33D4F78374420091E90735BB014A5163D86BFE38795DECACF0358075A85C0FBF80C5535046E7F8
DDCFFB39A3312AEC824579851424ED4426F4C9901FF06312B0E05479ABE1E935C85EBADFBA9A166631CEDFC90D9A672BF1607E3EAAEC8
1263AD8751DB1C714492BBDBBA108B82548D59B12FF6A18A80A651D20D91B8F0D8DD55000C257A9899BA214EE17E548B7454015489D127C
0F3BCC3504993C36CBC37541F3F7A5961C88DB357AB1B378B492F6A9A8DF8D9B0F254449E35D4D89C02008B95253466EBEB6B218B1C9464
B37B371F3D303ED6D7255758848F1CB40866D9A60FF54D872AB41AC55F50A39B7F79CAA19F83A0F3B1F3FD42CA37219D55D62C50C79F9E
4571A0A4343FFCF03B977EF2

Step 2 : One-click Payment

Merchants can offer One-click payments to their customers with PayNow.aspx.

PCI DSS certification is not mandatory for this feature, the merchant will use the PCNr (Pseudo Card Number and not a real PAN). This data is stored by the merchant.

Le marchand n'a pas besoin d'être certifié PCI-DSS car cette fonctionnalité nécessite l'utilisation du PCNr (Pseudo Card Number et ps un vrai PAN). Cette donnée est stockée par le commerçant.

3D authentication is not mandatory for this kind of payment, an exemption can be requested by the merchant. Cf. Exemption & 'Frictionless' payments

CVV is optionnal for One-click payments

Request with paynow.aspx

The merchant creates a form with the following fields :

- Number - Hidden field / filled with PCNr by the merchant
- securityCode - Empty or will be filled by the custmer (optionnal)
- expiryDate - Visible or Hidden field / filled with the expiryDate by the merchant
- brand - Visible or Hidden field / filled with the brand by the merchant
- cardholder - Visible or Hidden field / filled with the cardholder by the merchant

More details : Merchant Credit Card Form - Silent Order Post (PayNow.aspx)

The masked PAN or the 4 last digits of the PCNr can be displayed to the customer so he can easily identify the card that will be used for the payment.

The masked PAN can be available in the payment response, please contact Axepta Support.

The following table describes the additional encrypted parameters added to the payment request for One-click :

Key	Format	CND	Description	Example

credentialOnFile	JSON	M	Type of transaction (One-click)	<pre>{
				    "type": {
				
				"unscheduled": "CIT"
				    },
				    "initialPayment": false,
				    "useCase": "cof"
				}</pre>

browserInfo	JSON	M	Browser information is required to provide an optimized user experience. Required for 3DS 2.0 transactions.	--