Web-shop integration manual

Table of Contents

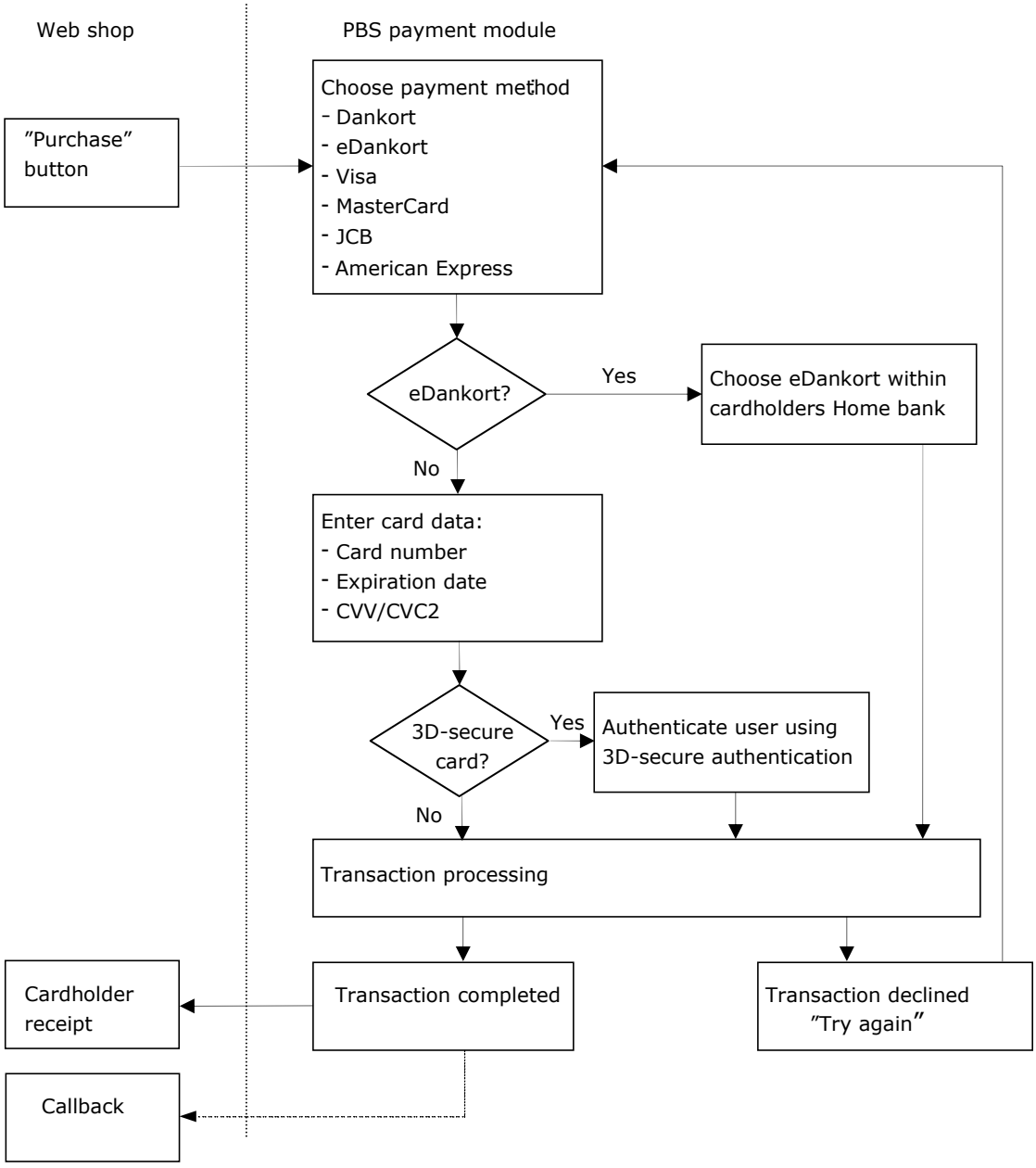
1. Document History

Revision	Date	Change
1	1st July 2005	Version 1
2	1st August 2006	Version 1.1
3	1st November 2006	Version 1.2
4	31st January 2007	Version 1.3
5	19st Februar 2007	Version 1.4 output parameter ordereid changed to orderID
6	20th August 2007	Version 1.5 added feature to enable preselection of the cardtype
7	16th June 2008	Version 1.6 added SHA-512 signature check (including examples), updated flow diagram to include eDankort and 3D-secure, removed callback url from the list of input parameters as well as within the examples, added note about SSL certificate usage of the store, elaborated the description regarding the usage of recurring orders, added Dutch (nl) to list of languages, added card type "Forbrugsforeningen".

2. Purpose

This document describes the integration of a web shop with PBS' payment module. Merchants using the payment module benefits from a simple way of integration where the merchants does not have to worry about compliance with the present PCI DSS requirements.

3. Illustration of the payment process



A user purchases goods or services at the merchant web shop. When the user clicks the ”purchase” button, a payment form is transmitted to an URL at the PBS payment server. A list of card types (payment methods) covered by the merchant’s merchant agreement(s) and approved for the currency in question is shown on the screen.

When the user has selected payment method, the user is redirected to a page where the necessary data must be entered. When the necessary data have been entered, a transaction is exchanged with the payment gateway. The result of the transaction is either “COMPLETED” or “DECLINED”. Some international issuers of payment cards require the user to be authenticated using 3D Secure. This technique requires the user for identification against the card issuer (typically accomplished by use of the home bank associated to the card holder). Currently VISA, MasterCard and JCB require the use of the 3D Secure (Verified by VISA, MasterCard SecureCode and JCB J/Secure). This is automatically handled by the PBS payment module.

If the transaction is declined, the user receives an error message and he/she may choose to return to the home page where another payment method may be selected.

When the transaction is completed, the user is redirected to merchant web shop page where the cardholder receipt is shown. At the same time, a direct server to server call is made; i.e. a call not involving the user’s browser, which the merchant may use in its bookkeeping. Note that the callback is only performed in the case the transaction is completed. The callback url is to be specified within the web administration interface located at https://pay.pbs-international.dk.

This is the first element of a transaction, the authorization. The amount to be captured is currently reserved on the cardholder account. The purpose of the authorization is to verify the validity of the card and the availability of the amount in the cardholder’s account with the card issuer. To complete a transaction a Capture needs to be made. This can be done in several ways – using the web administration interface, the web services or the PBS batch module. Please refer to the respective manuals for more information.

4. The payment window

The payment window is opened from the merchant’s web shop when the user is ready to pay for his/her purchase.

It is important that the payment window is not opened as a popup, but is read into the main window which is thus “taken over”. This is done by setting target ="_top" in the HTML form which is designed as shown below:

Design of payment form	
<form method=”POST”	Method=POST
target=”_top”	Opens in the full window

action=”https://pay.pbs-international.dk/pipay/pay”>	Server: https://pay.pbs-international.dk/.....
<input name=”...” type=”...” value=”...” />	Form parameters: name, type, value
</form>	End of form

The design of the payment module is by default standard. However, it is possible to change the design of the payment window using CSS layout. For more information on this contact PBS International.

5. Input parameters

Input parameters are the parameters which the payment form must contain. It is important that the parameter name is exactly as shown below, including the correct use of upper and lower case. If this is not the case, or if the format is not correct, the user will receive an error message.

Some parameters are not required, since they carry default values. I.e. if no specific data is indicated, the default values are used.

#	Meaning	Parameter name name=	Parameter value value=	Format	Required
1	Merchant-ID	merchantID	”mystore”	AN1..20	Yes
2	Order number	orderID	”DN03448423”	AN1..20	Yes
3	Amount	amount	”19995” (199,95 DKK)	N1..12	Yes
4	Currency	currencyCode	”DKK”	A3 (ISO 4217)	Yes
5	Server type	serverFlag	”P”	A1 (”T” or ”P”)	Yes
6	Return URL	acceptURL	”http://mystore.dk/receipt”	AN7..255	Yes
7	Cancel URL	cancelURL	”http://mystore.dk/shop”	AN7..255	Yes
8	Instant capture	instantCapture	”Y”	A1 (”Y” or ”N”)	No (default ”N”)
9	Recurring payment	recurring	”Y”	A1 (”Y” or ”N”)	No (default ”N”)
10	Internal reference	reference	”invoice 02-323”	AN1..255	No
11	Language of the payment window	language	"no" for Norwegian "da" for Danish "uk" for English	A2 (“no”, “da”, “uk”, “de”, “se” or “nl”)	No (default “da”)

			"de" for German "se" for Swedish "nl" for Dutch		
12	Perform pre-authorization	reauthorize	"Y"	A1 ("Y" or "N")	No (default "N")
13	Card type	cardType	"6" for preselect of the card type MasterCard	N1..20	No
14	Message Signature	signature	128 character hex signature string	AN128	No (Yes, if enabled for merchant account)

Additional explanations

AN = alphanumeric field, i.e. digits and letters (a-zA-Z0-9) may be used

A = only letters may be used (a-zA-Z)

N = only digits may be used (0-9)

Field 1: Merchant-ID is the identification allocated to the merchant by the payment module. The merchant-ID is the key to the merchant's data.

Field 2: Unique order number which unambiguously defines a specific order in the system. The order number must at any time be unique. If the merchant is only able to generate order numbers that are unique for a limited period of time, it may be necessary to add a time stamp to the field. The total data length does not exceed 20 characters.

Field 3: The amount that will be drawn on the cardholder's account.
IMPORTANT! The amount must be indicated in smallest currency unit, which is usually 1/100 of the main currency unit.

The ratio between the units depends on the currency as shown in the table below:

ISO 4217 Code	Currency	Ratio
DKK	Danish Kroner	1/100
EUR	Euro	1/100
USD	US Dollar	1/100

GBP	Great Britain Pound	1/100
SEK	Swedish Kroner	1/100
AUD	Australian Dollar	1/100
CAD	Canadian Dollar	1/100
ISK	Icelandic Kroner	1/100
JPY	Japanese Yen	1/1
NZD	New Zealand Dollar	1/100
NOK	Norwegian Kroner	1/100
PLN	Polish Zloty	1/100
CHF	Swiss Franc	1/100
CZK	Czech Koruny	1/100
HUF	Hungarian Forint	1/100

From the table appears that payments in yen must be indicated in the full Yen amount whereas amount in Euro must be indicated in cents.

Field 4: Currency is indicated in applicable ISO 4217 code consisting of 3 letters. The table above lists the currencies applicable at present. It is important that the currencies correspond with the card types accepted by the merchant (cf. the merchant agreement(s)). If a merchant wishes to accept Dankort only, it will not be able to accept payments in any currencies, except for DKK.

Field 5: During the process of designing and testing its web shop, the merchant will have the possibility of testing the payment process by indicating that the payment must be completed at the test server. This is done by indicating "T" in the payment form. When "T" is indicated, a simulated transaction is completed for testing purposes. When the test results are satisfactory, the merchant may shift to production mode by setting the flag at "P". NB: Switching the server type to production will only work when PBS International has confirmed the webshop integration conducted.

Field 6: When the payment has been completed, the user is redirected to a cardholder receipt at the merchant's server. The merchant must design and implement this page on basis of the parameters received for this purpose.

Refer to chapter 6 for detailed information.

Refer to chapter 11 for minimum requirements to the receipt.

Return URL must be indicated as an absolute URL (e.g. http://mystore.dk/shop.asp).

Note: As communication with PBS payment module is secure using a SSL certificate, some browsers might present a warning to the user when performing redirection to the receipt page in the web shop. This can be avoided implementing a SSL certificate on the web shops server and use HTTPS in the return URL.

Field 7: In cases where the user changes his mind and wishes to cancel before the payment has been completed, this may click back to the web shop.

Cancel URL must be indicated as an absolute URL. No parameters are included for this page.

Field 8: The merchant can choose whether capture should be made instantly. If the merchant wants to use this function, the support centre must be contacted in order to have the function activated. Please note that the capture may only be submitted when the goods/services are delivered/rendered.

Please also note that instant capture cannot be used when the goods/services are subject to an agreement regarding recurring payments or when reauthorization has been selected.

Note that when using instant capture the transaction is only completed when the given amount have been successfully captured, i.e. both an authorization and capture have succeeded. Otherwise the transaction will be declined.

Field 9: If the merchant sells goods or services that are subject to a subscription agreement; e.g. goods/services provided monthly, the payment may be completed as a recurring transaction, i.e. the user allows the merchant to draw amounts from his/her account on the terms agreed between those parties. Please note that the merchant agreement should be open to recurring payments before this function may be used. The merchant agreement stipulates the requirements to merchants providing goods or services on subscription.

Regarding recurring payments the payment window is only used to register the card data with a new subscription. Afterwards the subscription can be used to carry out subsequent transactions – using the web interface, the web services or the batch module. The orderID provided for the subscription registration acts as a token for subsequent uses of the registered card data. Upon registration the indicated amount is discarded.

Recurring payment cannot be used together with instant capture or reauthorization.

Field 10: The payment window allows the merchant to indicate its own reference value which is included in the data sent to the Return and Server Call URL's. This parameter is not required and the merchant may define the contents thereof.

Field 11: The payment window can be shown in different languages. Set the value to the preferred language. If no language is set, Danish is used. The payment window currently offers the following translations: English, Danish, Norwegian, Swedish, German and Dutch. Note that the language on some of the pages used through the eDankort and 3D Secure flow is located outside of the PBS payment module for which reason the language might differ from the specified language.

Field 12: If set to "Y" the transaction will be a pre-authorization which means it will be possible to perform one or more reauthorizations later. Preauthorisation should be used when it is not expected that a capture will be performed within 7 days from the authorization.

Field 13: IMPORTANT: This feature is only implemented as an intermediate solution. The current solution has a number of disadvantages, e.g. the flow is not compatible with the back button in the user's browser. However, it is indeed useable to perform payments. The next version of the payment window will remove the known disadvantages and will be compatible with the interface described here.

If set the initial step "Chose payment method" of the payment process can be avoided as a selection of the card type may have taken place prior to entering the payment window. The card type field can be set to any of the below card types to indicate that a preselection of the associated card type.

0 = Dankort
2 = eDankort
3 = Visa
5 = Visa Electron
6 = MasterCard
7 = JCB
9 = Maestro
15 = American Express
16 = Diners Club
17 = Forbrugsforeningen

Note that the Danish card type Visa/Dankort should be issued as the card type "Dankort" when issued from a Danish merchant. Merchants located outside of Denmark should issue this card as a regular VISA-card.

Field 14: A signature is a data integrity check and ensures that the posted form data is unchanged by malicious parties while transferred from the webshop to the payment window. **Usage of signature checking is highly recommended**.

The signature check should be enabled and a signature keyword should be set using the web administration system, before the payment window reacts on incoming requests with signatures. When the signature check is enabled the payment request of the user will be rejected in case the received parameter does not suit with the provided signature.

The signature includes integrity check for the following parameters

- merchantID (myMerchantID)
- orderID (myOrderID)
- amount (myAmount)
- currencyCode (myCurrency)
- serverFlag (myServerFlag)
- acceptURL (myAcceptURL)
- recurring (myRecurring)
- instantCapture (myInstantCapture)

The signature is basically a SHA-512 checksum of a concatenation of the chosen signature key (hash salt secret) and the eight parameters outlined above.

signature = SHA-512("mySaltmyMerchantIDmyOrderIDmyAmountmyCurrencymyServerFlagmyacceptURLmyRecurringmyInstantCapture")

An example:

Merchant PBStest with order TestOrder0001 on 1045 EUR which should be issued against the production gateway. The secret key is "HIDDENSECRET".

signature = SHA-512("HIDDENSECRETPBStestTestOrder0001104500EURPhttp://www.mystore.dk/accept.phpNN")

Important: The instantCapture parameter and the recurring parameter are mandatory parameters in the signature. I.e. in the case that your integration does not provide them as they are not required the default value should be used when generating the signature.

The result of the SHA-512 hash method is an ASCII encoded hex string with 128 characters. E.g. signature = 895BB403C6BCB3841ECC0672ACD7E6342FAFF4B74F576F636E2C270F101CAA80F2077E6E5577AE06806B785C1A66C01C327C793C06D7D3C38DB2BD10896ED8F9

The SHA-512 algorithm is available in many programming languages and environments like ASP, ASP.Net, C#, C/C++, Java, Perl, PHP4, PHP5, Python, and Ruby.

Important: Using the signature for parameter integrity check you need to make sure that the signature is calculated server side. Calculating the signature client side, e.g. using JavaScript will result in exposure of the secret signature keyword. This will lead to insignificant securing of the parameters.

6. Output parameters

Output parameters are the parameters which PBS' payment server includes when calling the merchant's Return and Server Callback URLs. The method "POST" is used.

A program/server script using these parameters should, however, not assume that these are the only ones possible. As the system is expanded, additional parameters may be added. Furthermore, the system does not distinguish whether a parameter is included or whether the value is empty ("").

Several of these parameters are echoes from the payment form and only included as a reference for the merchant.

#	Meaning	Parameter name name=	Parameter value value=	Format	Always included
1	Order number	ordered	"DN03448423"	AN1..20	Yes
2	Authorised amount	authAmount	"19995" (199,95 DKK)	N1..12	Yes
3	Currency	currencyCode	"DKK"	A3 (ISO 4217)	Yes
4	Server type	serverFlag	"P"	A1 ("T" or "P")	Yes
5	Instant capture	instantCapture	"N"	A1 ("Y" or "N")	Yes
6	Recurring payment	Recurring	"N"	A1 ("Y" or "N")	Yes
7	Internal	reference	"invoice 02-323"	AN1..255	No

	reference				
8	Partly approved	partlyApproved	”N”	A1 (”Y” or ”N”)	Yes
9	Return code authorisation	authActionCode	”000”	N3	Yes
10	Cardholder text authorisation	authCardholderText	”Approved”	AN1..255	Yes
11	Merchant text authorisation	authMerchantText	”Approved”	AN1..255	Yes
12	Return code capture	captActionCode	”000”	N3	No
13	Cardholder text capture	captCardholderText	”Approved”	AN1..255	No
14	Merchant text capture	captMerchantText	”Approved”	AN1..255	No
15	Expiration date	Exp	"MMYY"	N4	Yes
16	Card type	cardType	”6” indicating a MasterCard	N1..6	No
17	Card identification	cardID	"000000"	N6	Yes
18	Message Signature	Signature	128 character hex string	AN128	No (Yes if enabled for merchant)

Additional explanations

AN = alphanumeric field, i.e. digits and letters may be used (a-zA-Z0-9)

A = only letters may be used (a-zA-Z)

N = only digits may be used (0-9)

Field 1: The order number echoed from the payment form.

Field 2: The amount available in the account linked to the card. The amount is not necessarily the same as that of the payment form. If instant capture is selected, this is the amount transferred to the merchant. If there are not sufficient funds in the account to cover the amount for which authorisation was requested, the amount is lower. However, using instant capture, the capture and thereby the transaction will fail when the authorised amount is less than the initial amount.

Field 3: The currency code echoed from the payment form.

Field 4: The server indicated in the payment form.

Field 5: Instant capture echoed from the payment form. (If Instant capture was not indicated in the payment form, the field contains its default value = ”N”).

Field 6: Recurring payment echoed from the payment form. (If Recurring payment was not indicated in the payment form, the field contains its default value = ”N”).

Field 7: The merchant’s internal reference echoed from the payment window (if included).

Field 8: Partly approved occurs in situations where the full amount cannot be reserved in the user’s account. In those cases, field 2 will contain the amount that was reserved and field 8 will contain the value ”Y”.

Field 9: Return code is a 3-digit code generated by PBS’ payment gateway. Usually, the value will be 000 but other values may be indicated. Numerical values below 100 indicate that the transaction is completed.

Field 10: Cardholder text is a brief text which may be presented to the cardholder. The text is linked to the return code and in case of completed transactions it contains the value ”Approved”. If the merchant is able to translate the return code, the merchant will have a greater flexibility instead of just using the cardholder text.

Field 11: Merchant text contains a more detailed description of the return code than the cardholder text and may include sensitive data. Consequently, this text may not be presented to the cardholder but it provides the merchant with further information about the transaction.

Field 12: Same as field 9, but for the capture transaction. Is only included, if Instant capture is chosen.

Field 13: Same as field 10, but for the capture transaction. Is only included, if Instant capture is chosen.

Field 14: Same as field 11, but for the capture transaction. Is only included, if Instant capture is chosen.

Field 15: The expiration date of the card (MMYY).

Field 16: Card type presented as a numeric value:

0 = Dankort
2 = eDankort
3 = Visa
5 = Visa Electron
6 = MasterCard
7 = JCB
9 = Maestro
15 = American Express
16 = Diners Club
17 = Forbrugsforeningen

Field 17: Card identification presented as the first 6 digits of the card number.

Field 18: The signature variable is a data integrity check that ensures that the posted form data is unchanged by malicious parties while transferred from the payment module to the webshop. It is highly recommended to implement a signature check with in the webshop on both the payment receipt and when receiving the server callback. This way the webshop is able to ensure that the data is received from PBS payment module and that it has not been modified.

When the signature check has been enabled within the web administration interface, and a secret signature key provided, the payment module calculates and sends the SHA-512 checksum back to the webshop.

The signature includes integrity check for the following parameters

- orderID (myOrderID)
- authAmount (myAuthAmount)
- currencyCode (myCurrency)
- serverFlag (myServerFlag)
- recurring (myRecurring)
- instantCapture (myInstantCapture)
- authActionCode (authActionCode)
- captActionCode (captActionCode)
- cardType (cardType)
- cardID (cardID)

The signature is basically a SHA-512 checksum of a concatenation of the chosen signature key (hash salt secret) and the 10 parameters outlined above.

signature = SHA-512("mySaltmyOrderIDmyAuthAmountmyCurrencymyServerFlagmyRecurringmyInstantCaptureauthActionCode[captActionCode][cardType]cardID")

An example (continued from Input parameters, Field 14):

The payment has been performed successfully using a payment card with the prefix "457120", which is card type "0". No capture where performed as instantCapture was set to "N" in the input.

signature = SHA-512("HIDDENSECRET104500EURPNN0000457120")

Important: All the outlined parameters are mandatory when calculating the signature, except the optional parameters captActionCode and cardType. These two parameters must be included if and only if they are included in the output parameters.

The result of the SHA-512 hash method is a 128 character hex string e.g. signature= 5C9C84A4599B688A7A07150C8CAB0EB75BA88637E77838F34DDAEDB1C3C89837C1AD7EF2D350A162BBE647C0A845042866C1A437C16F9331AF6AF27E28006D12.

The SHA-512 algorithm is available in many programming languages and environments like ASP, ASP.Net, C#, C/C++, Java, Perl, PHP4, PHP5, Python, and Ruby.

Callback URL

As the user may not be redirected to the cardholder receipt in all cases (the user may e.g. close his browser before the cardholder receipt is shown), it is important that the merchant does not base its recording of payment status on the return URL. A server callback URL, which is called directly from the payment server when a payment is completed, should be configured.

The callback url is configured in the web administration interface and it is **highly recommended** to use a callback url, since this minimizes the risk of malicious usages.

Note that only HTTP urls can be used for the server callback urls.

7. Example of a Payment Form

Example of a payment form for the merchant "mystore". The amount is DKK 199.95.

```
<html>
<head><title>Example of payment form</title></head>
<body>
<form action="https://pay.pbs-international.dk/pipay/pay" method="POST" target="_top">
        <input type="hidden" name="merchantID" value="mystore" />
        <input type="hidden" name="orderID" value="DN03448423" />
        <input type="hidden" name="amount" value="19995" />
        <input type="hidden" name="currencyCode" value="DKK" />
        <input type="hidden" name="serverFlag" value="P" />
        <input type="hidden" name="acceptURL" value="http://mystore.dk/receipt" />
        <input type="hidden" name="cancelURL" value="http://mystore.dk/shop" />
        <input type="hidden" name="instantCapture" value="N" />
        <input type="hidden" name="recurring" value="N" />
        <input type="hidden" name="reference" value="faktura 02-323" />
        <input type="hidden" name="language" value="uk" />
        <input type="submit" value="Pay" />
</form>
</body>
</html>
```

8. Example of a Payment Form with Signature

Example of a payment form for the merchant "mystore". The amount is DKK 199.95 and "mySignatureKey" is used as the signature key for calculation of the signature.

```
<html>
<head><title>Example of payment form</title></head>
<body>
<form action="https://pay.pbs-international.dk/pipay/pay" method="POST" target="_top">
        <input type="hidden" name="merchantID" value="mystore" />
        <input type="hidden" name="orderID" value="DN03448423" />
        <input type="hidden" name="amount" value="19995" />
        <input type="hidden" name="currencyCode" value="DKK" />
        <input type="hidden" name="serverFlag" value="P" />
        <input type="hidden" name="acceptURL" value="http://mystore.dk/receipt" />
        <input type="hidden" name="cancelURL" value="http://mystore.dk/shop" />
        <input type="hidden" name="instantCapture" value="N" />
        <input type="hidden" name="recurring" value="N" />
        <input type="hidden" name="signature"
        value="0d0d936277aa0e60c1c18d6f94291cff12d85e1e18050174c44ea558546a6466fbc9
        ac6214cb937eb79c0920d1620b9d0dae923b834c3fcedda4698b848827f0" />
        <input type="hidden" name="reference" value="faktura 02-323" />
        <input type="hidden" name="language" value="uk" />
        <input type="submit" value="Pay" />
</form>
</body>
```

```
</html>
```

9. Example of a Payment Form with card type preselection

Example of a payment form for the merchant 'mystore'. The amount is DKK 199.95. The preselection specifies a MasterCard.

```
<html>
<head><title>Example of payment form</title></head>
<body>
<form action="https://pay.pbs-international.dk/pipay/pay" method="POST" target="_top">
        <input type="hidden" name="merchantID" value="mystore" />
        <input type="hidden" name="orderID" value="DN03448423" />
        <input type="hidden" name="amount" value="19995" />
        <input type="hidden" name="currencyCode" value="DKK" />
        <input type="hidden" name="serverFlag" value="P" />
        <input type="hidden" name="acceptURL" value="http://mystore.dk/receipt" />
        <input type="hidden" name="cancelURL" value="http://mystore.dk/shop" />
        <input type="hidden" name="instantCapture" value="N" />
        <input type="hidden" name="recurring" value="N" />
        <input type="hidden" name="reference" value="faktura 02-323" />
        <input type="hidden" name="language" value="uk" />
        <input type="hidden" name="cardType" value="6" />
        <input type="submit" value="Pay" />
</form>
</body>
</html>
```

Test cards

The following test card numbers may be used for testing purposes. The card number might either be approved or declined depending on the currently provided action code specified as the last digits of the card number. For the available action codes and meaning see Section 9. Any other card number may be either approved or declined in the test phase.

Authorization (and Capture) is approved.

The date of expiration of all cards is **date of expiry (mm/YY): 03/10** and **CVC/CVV: 741**

Card type	Card number
VISA	4111 0000 0000 0000
MasterCard	5111 0000 0000 0000
JCB	3528 0000 0000 0000
Dankort	5019 0000 0000 0000
VISA/Dankort	4571 0000 0000 0000
Diners Club	3614 000000 0000
American Express	3747 000000 00000

Authorization declined:

The date of expiration of all cards is **date of expiry (mm/YY): 03/10** and **CVC/CVV: 741**

xxx is filled in with the requested action code

Card type	Card number
VISA	4111 0000 0000 0xxx
MasterCard	5111 0000 0000 0xxx
JCB	3528 0000 0000 0xxx
Dankort	5019 0000 0000 0xxx
VISA/Dankort	4571 0000 0000 0xxx
Diners Club	3614 000000 0xxx
American Express	3747 000000 00xxx

Capture is declined (authorization is approved):

The date of expiration of all cards is **date of expiry (mm/YY): 03/10** and **CVC/CVV: 741 xxx** is filled in with the requested action code

Card type	Card number
VISA	4111 9000 0000 0xxx
MasterCard	5111 9000 0000 0xxx
JCB	3528 9000 0000 0xxx
Dankort	5019 9000 0000 0xxx
VISA/Dankort	4571 9000 0000 0xxx
Diners Club	3614 900000 0xxx
American Express	3747 900000 00xxx

10. Action Codes

Action Code	Merchant text	Action against cardholder
000	Approved	Approved
001	Honor with identification	Decline
002	Approved for partial amount	Partly Approved
060	Approved	Approved
061	Approved	Approved
063	Approved	Approved
100	Do not honor	Decline
101	Expired Card	Decline/Expired Card
102	Suspected Fraud	Decline
103	Card acceptor contact acquirer	Decline
104	Restricted card	Decline
105	Card Acceptor call Acquirers security department	Decline
106	Allowable pin tries exceeded	Decline
107	Refer to card issuer	Decline
108	Refer to card issuer special conditions	Decline
109	Invalid merchant	Decline
110	Invalid amount	Decline/Amount Error

111	Invalid card number	Decline
112	Pin data required	Decline
113	Unacceptable fee	Decline
114	No account of type requested	Decline
115	Requested function not supported	Decline
116	Not sufficient funds	Decline
117	incorrect pin	Decline
118	No card record	Decline
119	Transaction not permitted to cardholder	Decline/Invalid Transaction
120	Transaction not permitted to terminal	Decline/Invalid Transaction
121	Exceeds withdrawal amount limit	Decline
122	Security violation	Decline
123	Exceeds withdrawal frequency limit	Decline
124	Violation of law	Decline
125	Card not effective	Decline
126	Invalid pin block	Decline
127	Pin length error	Decline
128	Pin key synch error	Decline
129	Suspected counterfeit card	Decline
160	Invalid date	Decline
161	Allowable number of pin tries exceeded	Decline
162	Unable to locate previous message	Decline
164	Card entry found, below low range	Decline
165	Pan length not according to table	Decline
167	Match on previous transaction not allowed	Decline
200	Do not honor	Decline
201	Expired card	Decline/Expired Card
202	Suspected fraud	Decline
203	Card acceptor contact acquirer	Decline
204	Restricted card	Decline
205	Card acceptor call acquires security department	Decline
206	Allowable pin tries exceeded	Decline
207	Special conditions	Decline
208	Lost cards	Decline
209	Stolen card	Decline

210	Suspected counterfeit card	Decline
900	Advice acknowledged, no financial liability accepted.	Approved
901	Advice acknowledged, financial liability accepted.	Approved
902	Invalid transaction Decline/Invalid	Transaction
903	Re-enter transaction	Decline
904	Format error	Decline/ System Error
905	Acquirer not supported by switch	Decline/System Error
906	Cut over in process	No Reply
907	Card issuer or switch inoperative	No Reply
908	Transaction destination cannot find routing	Decline
909	System malfunction	Decline/ System Error
910	Card issuer signed off	No Reply
911	Card issuer timed out	No Reply
912	Card issuer unavailable	No Reply
913	Duplicate transmission	Decline/ System Error
914	Not able to trace back to original transaction	Decline
915	Reconciliation cut over or checkpoint error	No Reply
916	MAC incorrect	Decline/System Error
917	MAC key sync error	Decline/System Error
918	No communication keys available	Decline/System Error
919	Encryption key error	Decline/System Error
920	Security software/hardware error, try again	System Error
921	Security software/hardware error, no action	System Error
922	Message number out of sequence	System Error
923	Request in progress	System Error
940	Invalid date and time, local transaction	System Error
945	KIR (PBS host) timeout	No Reply
946	PGW error occurred, unspecified	No Reply
950	Violation of business arrangement	Decline/ System Error
984	No valid conversion for a field	Decline/ System Error

11. Requirements to Cardholder Receipt

When the transaction has been approved, the merchant must transmit a receipt to the cardholder's PC. The receipt must, as a minimum, include the following data (please refer to merchant agreement for further details):

1) The name of the merchant
2) The merchant's e-mail address
3) A description of the goods/services ordered
4) Order number (field 1 in Output parameters)/transaction number (e.g. merchant internal system transaction number)
5) Transaction date
6) Transaction currency (field 3 in Output parameters)
7) Transaction amount (field 2 in Output parameters)
8) Expected date of delivery