Danske Bank´s Web Payment Service

Manual for Service Providers

1.3.2021

Danske Bank A/S, Suomen sivuliike
Rekisteröity toimipaikka ja osoite Helsinki,
Televisiokatu 1, 00075 DANSKE BANK.
Y-tunnus 1078693-2

Danske Bank A/S, Kööpenhamina
Tanskan kauppa- ja yhtiörekisteri
Rek. nro 61 12 62 28

Danske Bank A/S, Finland filial
Registrerad verksamhetsort och adress Helsingfors,
Televisionsgatan 1, 00075 DANSKE BANK
FO-nummer 1078693-2

Danske Bank A/S, Köpenhamn
Dansk handels- och företagsregister
Reg. nr 61 12 62 28

Danske Bank A/S, Finland Branch
Registered domicile and address: Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Table of Contents

1 Service description

1.1 General description

The Web Payment Service is an easy way for Danske Bank's business clients to receive payment for products sold over the internet.

Products that customers add to their shopping baskets are paid for immediately as an account transfer upon confirmation of the orders. Customers do not need to disclose their account information to the online store when paying for their purchases.

Once a customer has paid for his or her purchase by means of a web payment, the service provider can deliver the product ordered by the customer without risk, as the customer pays for the product immediately when ordering.

In addition, the service provider receives information about the payment immediately once the customer has confirmed the payment and returned to the service provider's website. The service provider can also monitor payment details from the Web Payment Service server (see Section 6: Payment enquiry as a separate function), or other banking software, as well as from the account transactions on eBanking and from the account statement.

The Web Payment Service requires a Web Payment Service Agreement between the service provider and Danske Bank. The Web Payment Service also requires that the service provider has an online store on the internet selling products, as well as a District agreement. Furthermore, the system used by the service provider must be able to produce an itemised invoiced for the ordered products using internet technology. Danske Bank's Web Payment Service does not require the use of any specific server software by the service provider.

1.2 Benefits for service providers

- Customers consider web payments to be a safe and easy way form of payment
- Payment details are transferred directly to the service provider
- Eliminates the costs of sending paper invoices
- No credit risk
- Affordable pricing

1.3 Security of the service

The transfer of payment details between the service provider and the Bank, as well as between the payer and the bank, is safe and protected. The Bank can identify both the payer and the service provider. In addition, payment details are protected using SSL encryption.

Each party is responsible for the protection and security of their own services, as well as for the accuracy of the information they store. Both the customer and the service provider are responsible for ensuring that Danske Bank's identification and authentication tools are not transferred to third parties.

It is important for the Bank that the online store complies with the obligations stipulated in the terms of the Web Payment Service Agreement. The online store must also comply with all relevant laws and guidelines, including the obligation to inform customers about their right to cancel their purchases.

If the service provider serves as a payment intermediary for other merchants, it is important to remember that the Bank has no responsibility for the transfer of funds from the intermediary to the merchant.

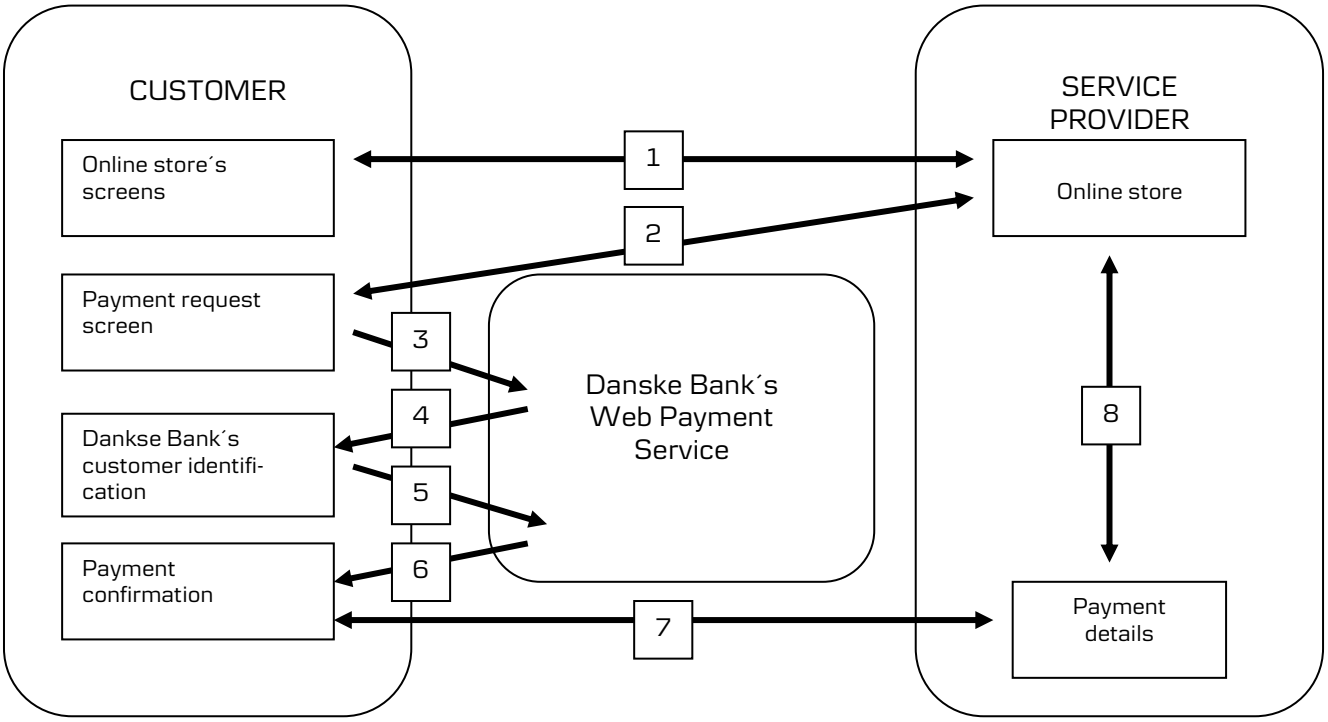
Danske Bank's Web Payment button must be included in the service provider's own service. The Web Payment button or a link to the Web Payment button cannot be included in an e-mail message or shared in any other way.

The Web Payment Service's screens must open in their own window on the online store's website. Frames are not permitted.

1.4 Changes to encrypted key

The encrypted key used to protect the Web Payment Service's messages (payment request and payment enquiry messages) is changed regularly for security reasons. The Bank shall supply the customer with new encrypted keys, which must then be activated by the deadline notified by the Bank.

2 Functional description of the service



Explanation of the steps:

1. The customer visits the online store and selects which products to buy by adding them to the shopping basket. The customer then confirms the contents of the shopping basket and clicks to pay for the purchase.

2. The service provider sends the customer a payment request that includes itemised information about the transaction. The customer checks the information in the payment request. The customer may at this point cancel the payment and return to the online store.

3. The customer selects Danske Bank's Web Payment as the payment method by clicking on the Danske Bank logo. The payment request sent to Danske Bank includes the information required by the Web Payment Service about the service provider and the payment transaction. The Bank checks the integrity of

the payment request, the correctness of the information and the Web Payment Service Agreement of the service provider.

4. If the payment request from the service provider is faultless, Danske Bank sends the payment request to the customer.

5. The customer types in his/her customer number, user ID and one-time password. If the customer identification fails, Danske Bank notifies the customer and the customer returns to the service provider's service.

6. After the customer identification and authentication, Danske Bank formulates the invoice. The customer is shown the name of the payee (service provider), the name of the payer, the reference number for the payment, the amount to be paid and the currency. The customer is also shown a list of debit accounts to choose from, if more than one. The customer then confirms the payment, after which Danske Bank notifies the customer that the payment was successful. If the service provider serves as a payment intermediary for other merchants, the Bank displays a message to the paying customer about the transfer of funds to the intermediary. The Bank has no responsibility for the transfer of funds from the intermediary to the merchant.

7. The customer and payment details (protected with authentication) are then transferred to the return address provided by the service provider in the payment request. The customer can also cancel the transaction and return to the service provider's online store, in which case the customer is transferred to the cancellation address provided by the service provider in the payment request.

8. The service provider confirms the integrity of the information received by means of SHA256 authentication. The service provider adds the payment to the customer's order and delivers the ordered products to the customer.

3 Service agreement and introducing the service

3.1 Agreement

The service provider must first agree to begin using the service with Danske Bank. The Web Payment Service requires a Web Payment Service Agreement, and the service provider must be a business client of Danske Bank with a payment account and a District agreement.

When making the agreement, the service provider must notify the Bank whether it serves as an intermediary for online merchants.

Once the agreement has been made, Danske Bank supplies the service provider with a service provider ID and encrypted key required by the service.

The service provider must notify the Bank about any changes to the information in the agreement.

The service provider must use Version 4 of the Web Payment Service.

3.2 Service requirements

The system used by the service provider must be able to produce a payment request using internet technology and that includes a unique reference number.

The Web Payment Service does not require the use of any specific server software by the service provider.

The service supports the most common browsers and their latest versions.

3.3 Payment transfers to the service provider

The basic function of the Web Payment Service is an account transfer from the customer's account to the service provider's account. This account transfer occurs immediately and appears without delay in the service provider's account transactions. The order and payment are connected to each other by a reference number that the service provider has given for the payment. Each payment must have its own, unique reference number so that orders and payments can be connected to each other.

3.4 Refund of Web payments

The merchant can return a payment made online to the buyer using the Web Payment Refund functionality on District. Refunds may be made, for example, if the product cannot be delivered or if the amount paid does not correspond to the final price of the product. The refund is made as a new payment transaction for either a portion of the value or the entire value. The original credit account will be debited in the refund transaction. The re-fund is always credited to the debit account of the original web payment transaction.

Refunds may be made, for example, if the product cannot be delivered or if the amount paid does not correspond to the final price of the product. The refund is made as a new payment transaction. The original credit account will be debited in the refund transaction. The refund is always credited to the debit account of the original web payment transaction.

Restrictions on the refund functionality

- The refund can be smaller or no more than the same as the original payment.
- The original credit account is debited in the refund transaction.
- The refund is always credited to the debit account of the original web payment transaction.
- Multiple refunds can be made for each payment until there is nothing to be refunded and the total amount is 0 EUR.

3.5 Refund of web payments through the service provider´s portal

The refund functionality from the service provider's portal is a functionality provided for the service provider for making refund payments to their customers (buyers). The features and the process of the refund of the web payments remain the same as they are currently on District with the exception of the initiation of the refund transaction. In the process the initiation (request) for a refund is made from the service provider's portal.

Refunds can be made in part or full, and the total refund amount is restricted only to the payment amount corresponding to the original transaction. Refunds may be made, for example, if the product cannot be delivered or if the amount paid does not correspond to the final price of the product. The refund is made as a new payment transaction. The original credit account will be debited in the refund transaction. The refund is always credited to the debit account of the original web payment transaction. The limitations of the refund functionality are the same as stated in Section 3.4.

Benefits of the refund process:

- With the refund process, the service provider can refund web payments to buyers from their own portal.
- Service providers do not require logging in to District every time to make the refund.
- This simplifies the process and reduces time consumption for making the refunds.

4 Messages and their data

4.1 Payment request

The payment request data comprise hidden values in the FORM data field behind the Danske Bank logo.

The Danske Bank logo can be downloaded from:
https://danskebank.fi/verkkomaksupainike

The HTML structure of the FORM data field is:

```
<FORM METHOD="POST"ACTION="https://verkkopankki.danskebank.fi/SP/vemaha/VemahaApp">
<INPUT NAME="KNRO" TYPE="HIDDEN" VALUE="000000000000">
<INPUT NAME="SUMMA" TYPE="HIDDEN" VALUE="100,00">
<INPUT NAME="VIITE" TYPE="HIDDEN" VALUE="9861156">
<INPUT NAME="VALUUTTA" TYPE="HIDDEN" VALUE="EUR">
<INPUT NAME="VERSIO" TYPE="HIDDEN" VALUE="4">
<INPUT NAME="ERAPAIVA" TYPE="HIDDEN" VALUE="pp.kk.vvvv">
<INPUT NAME="OKURL" TYPE="HIDDEN" VALUE="https://www.kauppa.fi/okpaluu">
<INPUT NAME="VIRHEURL" TYPE="HIDDEN" VALUE="https://www.kauppa.fi/virhepaluu">
<INPUT NAME="TARKISTE" TYPE="HIDDEN"
VALUE="648afba5b9193d9a6a5caf89b452d2d22a8a1b79ebc064b1f2dcba7e121fe44f">
<INPUT NAME="lng" TYPE="HIDDEN" VALUE="3">
<INPUT NAME="ALG" TYPE="HIDDEN" VALUE="03">
<INPUT TYPE="IMAGE"
 SRC="https://danskebank.fi/verkkomaksupainike"
BORDER=0></FORM>
```

PAYMENT REQUEST MESSAGE FORM DATA FIELD				
Field and data	**Data name**	**Form**	**Obligatory = C Optional = V**	**Description**
1. Sum	SUMMA	AN 19	C	
2. Reference number	VIITE	N 20	C	
3. Service provider's ID	KNRO	N 12	C	
4. Currency	VALUUTTA	A 3	C	EUR
5. Version of message	VERSIO	N 1	C	4
6. Due date	ERAPAIVA	AN10	C	dd.mm.yyyy
7. Return address	OKURL	AN 199	C	
8. Cancellation address	VIRHEURL	AN 199	C	
9. Verification code	TARKISTE	AN 64	C	
10. Language	lng	N1	V	
11. Algorithm	ALG	N3	C	03 = SHA256

Field explanations:

All fields are hidden on the form and they cannot contain spaces. The field names are in block capitals.

Field 1
The sum of the payment does not contain spaces. Use comma as a divider, e.g. 101, 10. If there are no cents in the sum, the sum can be presented without decimals, e.g. 100. If there are cents in the sum, the sum must be presented with two decimals.

Field 2
The invoice's reference number. This field provides the only individualising data of the payment. The reference number must be unique with a specific service provider ID. The minimum length of the reference number is 4 digits (3 + verification) and the maximum length 20 digits (19 + verification). The figure chosen for the basic reference data (e.g. customer number or invoice number) are written from right to left 7, 3, 1, 7, 3, 1

Field 3
The service provider's customer number, i.e., ID, which Danske Bank has delivered to the service provider after concluding the agreement. Danske Bank identifies the service provider on the basis of this number. Moreover, on the basis of this number, the name of the service provider found in Danske Bank's register is shown to the customer at the time of payment.

Field 4
Currency, only EUR is accepted.

Field 5
The number of the version of the Web Payment; currently the value is 4.

Field 6
The due date is obligatory for the payment request message. The due date can be either the current date or a date in the future. This field cannot be left empty, and the date cannot be a previous date. If the due date is a date in the future, the web payment shall be debited from the payer-customer's account on the due date provided that the customer's account his sufficient funds. It is important to note that a web payment that is falling due cannot be removed.

Field 7
Complete URL address to which the Bank directs the customer after the web payment. The euro symbol (€) cannot be used in the address, and the address must begin with http:// or https://. Danske Bank recommends using an addressing that begins with https://.

Field 8
Complete URL address to which the Bank directs the customer if the customer cancels the transaction. The euro symbol (€) cannot be used in the address, and the address must begin with http:// or https://. Danske Bank recommends using an addressing that begins with https://.

Field 9
The payment request is protected with a verification code connected to the message. The verification code is calculated from the payment request FORM data field using an encrypted key given to the service provider by Danske Bank and with the help of an SHA256 algorithm. Danske Bank uses the verification code to check the integrity and sender of the payment request.

The encrypted key is a code (64 characters) sent by the Bank to the service provider. This code is not sent to the Bank along with the form; it is a part of the calculated verification code.

The verification code is calculated by connecting the fields of the form with the encrypted key in the order mentioned below. Only values and &-marks are included in the verification code. The code is calculated by generating a character string using SHA256 algorithm.

VERIFICATION CODE = SHA256(MAC+'&'+SUMMA+'&'+VIITE+'&'+KNRO+'&'+↵
VERSIO+'&'+VALUUTTA+'&'+OKURL+'&'+VIRHEURL+'&'+ ERAPAIVA+'&')

The data is in a single line and the "↵" symbol represents a line break in the document.

The calculated hash value is converted into a hexadecimal, 64-character long presentation form, in which the letters A...F are in small letters. The hexadecimal value is transferred to Field 9 as the verification code.

The calculation of the verification code in the example form is made as follows if the ENCRYPTED KEY = jumCLB4T2ceZWGJ9ztjuhn5FaeZnTm5HpfDXWU2APRqfDcsrBs8mqkFARzm7uXKd

SHA256(jumCLB4T2ceZWGJ9ztjuhn5FaeZnTm5HpfDXWU2APRqfDcsrBs8mqkFARz↵
m7uXKd&100,00&9861156&000000000000&4&EUR&http://www.kauppa.fi/okpaluu&http↵
://www.kauppa.fi/virhepaluu&12.04.2013&)

The value of the verification code thus calculated is:
6c2ce421fdbaad582cd938d5719ff305702a971ecf950b65ab5416d33dda18f7

The data is in a single line and the "↵" symbol represents a line break in the document.

Field 10
It is also possible to send a code for preferred language with the form. When this language code is used, the Web Payment Service opens with this preferred language.

The parameter is lng (small letteres). The possible values of the parameter are:
lng=1 - Finnish
lng=2 – Swedish
lng=3 – English

Example:
<INPUT NAME="lng" TYPE="HIDDEN" VALUE="1">

Alternatively, the parameter can be attached after the URL using the & symbol.

The language code is not calculated with the payment's verification code and is not obligatory.

Field 11
With the algorithm the service provider can secure the payment request message. The algorithm is SHA256. The use of the MD5 algorithm was discontinued on 31 December 2013.

The value of the ALG parameter is ALG = 03 (SHA256).

4.2 Payment request reply message

Danske Bank adds the reply message's data to the OK return link in query-string format.

https://OKURL?&KNRO&VALUUTTA&VIITE&ERAPAIVA&SUMMA&VERSIO↵
& STATUS&TARKISTE&MTAPA&

The data is in a single line and the "↵" symbol represents a line break in the document.

The reply message is sent using the GET method.

Danske Bank calculates the verification code of the reply message using the service provider's unique encrypted key. With the encrypted key the service provider can ensure that the payment data has been formed within Danske Bank and that the payment data has not changed.

REPLY MESSAGE			
Field and data	**Data name**	**Form**	**Description**
1. Service provider's ID	KNRO	N 12	
2. Currency	VALUUTTA	A 3	
3. Reference number	VIITE	N 20	
4. Sum	SUMMA	AN 19	
5. Version of message	VERSIO	N 1	4
6. Status	STATUS	N 1	0 (zero)
7. Verification code	TARKISTE	AN 64	
8. Payment method	MTAPA	N 1	1 = account transfer
9. Due date	ERAPAIVA	AN10	Due date for the payment.

Field explanations

Field 1
The service provider's customer number, i.e., ID, which Danske Bank has delivered to the service provider after concluding the agreement.

Field 2
Currency, only EUR is accepted. The currency is taken from Field 4 of the payment request message (CURRENCY).

Field 3
The invoice's reference number, which is taken from Field 2 of the payment request message (REFERENCE).

Field 4
The sum of the payment, which is taken from Field 1 of the payment request message (SUM). The sum is present with decimals using a comma.
Example 1: The sum 100.00 in the payment request message is converted in the reply message to 100,00.
Example 2: The sum 100 in the payment request message is converted in the reply message to 100,00.

Field 5
The number of the version of the Web Payment; currently the value is 4. Support for versions 2 and 3 expired on 1 January 2014.

Field 6
The payment status, which is 0 (zero).

Field 7
The verification code is calculated from the reply message's data field and the service provider's encrypted key using an SHA256 algorithm.

The encrypted key is a code (64 characters) sent by the Bank to the service provider that must be kept confidential. This code is not sent to the Bank along with the form; it is a part of the calculated verification code.

The verification code is calculated by connecting the fields of the form with the encrypted key in the order mentioned below. Only values and &-marks are included in the verification code. The code is calculated by generating a character string using SHA256 algorithm. In the formula below the "+" symbols are not included.

VERIFICATION CODE = SHA256(MAC+'&'+VIITE +'&'+SUMMA+'&'+ STATUS+ '&'+↲
KNRO+ '&'+VERSIO+'&'+VALUUTTA+'&'+ERAPAIVA+'&')

The data is in a single line and the "↲" symbol represents a line break in the document.

The calculated hash value is converted into a hexadecimal, 64-character long presentation form, in which the letters A...F are in capital letters. The hexadecimal value is transferred to Field 7 as the verification code.

Field 8
The payment method, i.e. which of the payment methods offered by the Web Payment Service has been used. The payment options are:

1 = account transfer

The payment method data is not included in the verification code.

Field 9
The due date for the payment in the format dd.mm.yyyy.

4.3 Exceptional situations

The service provider must prepare for exceptional situations, for example:

1. The customer cancels the payment
   The customer may cancel the transaction while making the payment. In this case the customer is directed to the cancellation address (VIRHEURL), which is in Field 8 of the payment request form.

2. The customer's payment is unsuccessful
   The customer's payment may fail due to a lack of funds in the account, for example. In this case the customer is directed to the cancellation address (VIRHEURL), which is in Field 8 of the payment request form.

3. Danske Bank identifies an error in the payment request message
   Danske Bank may identify an error in the payment request message after the customer has logged on. In this case the customer is directed to the cancellation address (VIRHEURL), which is in Field 8 of the payment request form.

4. The service provider identifies an error in the payment request message
   The service provider may identify an error when checking the payment request message, which could be due to an error in the content of the message.

5. The service provider receives payments using the same reference number
   The Bank can provide a service whereby it checks that multiple payments cannot be made on the online store using the same reference number. Reference numbers are checked for the past 13 months.

5 Viewing web payment transactions and refunding payments via District

District features a simple and easy-to-use administration service for web payment transactions. The service provider can list and view all web payment transactions as a separate function on District.

All users listed in the service provider's eBanking agreement may list and view incoming payments.

Web payments can be searched for by date, amount, reference number of status. When viewing payments, the service provider can see the name of the payer.

District also has a refund function for returning web payments. All persons who are authorised to make payments using District are also authorised to return web payments. Web payments may be returned in full or in part. The payment is returned to the payer as a new payment transaction. The refund is always credited to the debit account of the original web payment transaction.

5.1 Request for refund from service providers and data

The service provider can submit the refund request for the payment transaction by using the original payment's reference number. The refund transaction is a server-to-server transaction and can be integrated in the web-server application of the service provider's online store.

The service provider's refund request is sent as follows:

Code	Description
<FORM METHOD="POST" ... >	Method = POST
ACTION="https://netbank.danskebank.dk/HB"	URL address
<INPUT TYPE="HIDDEN" NAME="..." VALUE= "...">	Parameters and values. See description below.
</FORM>	

The HTML structure of the data field reads as follows:

```
<FORM NAME="Form1" ACTION="https://netbank.danskebank.dk/HB" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="gsSprog" VALUE="FI">
<INPUT TYPE="HIDDEN" NAME="gsProdukt" VALUE="IBV">
<INPUT TYPE="HIDDEN" NAME="gsNextObj" VALUE="InetPayV">
<INPUT TYPE="HIDDEN" NAME="gsNextAkt" VALUE="InetPayCan">
<input type="HIDDEN" name="gsResp" value="S">
```

<input type="HIDDEN" name="gsShopId" value="012345679800">
<input type="HIDDEN" name="gsVersion" value="0001">
<input type="HIDDEN" name="gsRefno" value="1234">
<input type="HIDDEN" name="gsAlogv" value="03">
<input type="HIDDEN" name="gsCurrency" value="EUR">
<input type="HIDDEN" name="gsAmount" value="500">
<input type="HIDDEN" name="gsAmountCh" value="500">
<input type="HIDDEN" name="gsNewrefno" value=" 5678">
<input type="HIDDEN" name="gsSpltext" value="WP Refund">
<input type="HIDDEN" name="gsMacVl" value="
f0bfa9ca26cb91203e9acac654e84a194bc96d127df153bd85ca9051a50a3257">
</FORM>

REFUND REQUEST MESSAGE FORM DATA FIELD				
Field and data	**Data name**	**Form**	**C/V**	**Example**
1. Sum	gsAmount	N (13)	C	500
2. Reference number	gsRefno	AN (4-20)	C	1234
3. Service provider's ID	gsShopId	N (12)	C	012345679800
4. Currency	gsCurrency	A (3)	C	Always EUR
5. Version of message	gsVersion	Vakio	C	0001
6. Product code	gsProdukt	Vakio	C	IBV
7. Subsystem	gsNextObj	Vakio	C	InetPayV
8. Action ID	gsNextAkt	Vakio	C	InetPayCan
9. Verification code	gsMacVl	AN 64	C	f0bfa9ca26cb912 03e9acac654e84 a194bc96d127df 153bd85ca9051a 50a3257
10. Language	gsSprog	A (2)	C	FI, EN
11. Algorithm	gsAlogv	A (2)	C	03 =(SHA256)
12. Response type	gsResp	Vakio	C	S
13. New reference number	gsNewrefno	AN (4-20)	C	5678
14. Special text	gsSpltext	AN (4-50)	V	Comments by SP
15. Sum	gsAmountCh	N (13)	C	500

C=obligatory, V=optional, A=alphabetical/N=numerical, n = length (... = max. length n)

Field 1

The sum of the payment does not contain spaces. Use a comma as a divider, e.g. 100,00. If there are no cents in the sum, the sum can be presented without decimals, e.g. 100. If there are cents in the sum, the sum must be presented with two decimals.

Field 2

The invoice's reference number. This field provides the only individualising data of the payment. The reference number must be unique with a certain service provider ID.

Field 3
The service provider's customer number, i.e., ID, which Danske Bank has delivered to the service provider after concluding the agreement. Danske Bank identifies the service provider on the basis of this number. Moreover, on the basis of this number, the name of the service provider found in Danske Bank's register is shown to the customer at the time of payment.

Field 4
Currency, only EUR is accepted.

Field 5
The number of the version of the Web Payment; currently the value is 0001.

Field 6
This field is a product code which refers to an application. This application acts as a gateway to the incoming re-fund requests. The product code is represented by 'IBV' and is a constant value.

Field 7
This field refers to a subsystem under the product code, IBV. The subsystem is represented by 'InetPayV' which is a constant value.

Field 8
This field refers to an action ID which triggers the refund process. This field is represented by 'InetPayCan' and is a constant value.

Field 9
Verification code calculated from MAC Key. The verification code is calculated with the help of SHA256 algorithm on the basis of the information in the refund data and the service provider MAC.

The service provider MAC is a code (64 characters) sent by the bank to the service provider. This code is not sent to the bank along with the form; it is a part of the calculated verification code.

The verification code is calculated by connecting the fields of the form with the service provider MAC in the or-der mentioned below. Values and &-marks are included in the verification code. The code is calculated by generating a character string using SHA256 algorithm. In the form below, the "+"-signs are not included in the calculation.

Field 10
It is also possible to send a code for preferred language with the form. When this language code is being used, Web Payment service opens with this preferred language.

Field 11
The algorithm is SHA256
Parameter is gsAlogv Possible value is: ALG = 03 - SHA256.

Field 12
Response type. It is always 'S'.

Field 13
The service provider's new reference number for the repayment. This is a mandatory field. The value is sent back to the service provider in the reply message.

Field 14
Service providers can send a text message for repayment. This is an optional field. Danske Bank does not store the value of this field. The value is sent back to service provider in the reply message.

Field 15
This is the duplicate of Field 1 used for calculating the MAC value.
Please find the rule for assignment of this field:

self.document.Form1.gsAmount.value = self.document.Form1.iAmount.value;
self.document.Form1.gsAmountCh.value = self.document.Form1.iAmount.value;

Verification Code

The status request is protected with an attached verification code. With the help of SHA256 algorithm, the code is calculated from the MAC Key provided by the bank, the service provider ID and the reference number. The verification code enables Danske Bank to check the integrity and sender of the payment request.

The verification code is counted by connecting the fields of the form with the service provider MAC in the order mentioned below. Only the values are included in the verification code. The code is calculated by generating a character string using SHA256 algorithm.

VERIFICATION CODE = SHA256(MAC KEY+'&' +SUM+'&+REFERENCE NUMBER + '&'+Service Provider ID+'&' + CURRENCY + '&' + VERSION OF MESSAGE + '&' + NEW REFRENCE NUMBER + '&' + ALGORITHM + '&')

The calculated hash value is converted into a hexadecimal, 64-sign long presentation form, in which the letters A...F are in small letters.

Reply Refund message

Return response from the refund-transaction contains the following:

Parameter name	Description	Example
ReturnCode	Return code. 000 = OK 001 = Reference number not found 002 = Web payment already returned 003 = Refund transaction cannot be processed.	000
ReturnText	Return text, which describes the return code. Will be OK if return code is 000, otherwise not.	OK
Refno	Reference number	1234
SPNewRefno	Service Provider New reference number	5678
SPSpecialText	Service Provider special text	Refund for Danske Bank
Amount	Amount	500,00
MerchantID	Service provider's ID	001234567800
Currency	Currency code	EUR
Verification Code	Verification code calculated from MAC Key (SHA256 algorithm)	f0bfa9ca26cb91203e9ac ac654e84a194bc96d127 df153bd85ca9051a50a3257
TransactionBalance	Balance of the transaction remaining after this refund.	1,00

Example:
ReturnCode=000&ReturnText=OK(Refnoexists)&Refno=1234&SPNewRefno=5678&
SPSpecialText=Refund for Danske Bank& Amount=500,00&MerchantID=0123456789800
&Currency=EUR&VerificationCode= f0bfa9ca26cb91203e9acac654e84a194bc96d127df15
3bd85ca9051a50a3257&TransactionBalance=1,00

6 Payment enquiry as a separate function

Danske Bank's Web Payment Service also offers a separate service whereby the service provider can check whether the customer has paid for an order by means of a web payment.

This service is required if the customer, having made the payment, does not return to the service provider's website, for example due to a problem with the network connection (i.e. reply message is not sent to the service provider).

Payment requests can be made by reference number.

6.1 Payment enquiry by reference number

The service provider can enquire about the status of individual payments by reference number. Enquiries can only be made using individual reference numbers.

By means of a payment enquiry, the service provider can confirm whether a payment made with a specific reference number (Refno) has been processed or not. The reply message of the payment enquiry also includes the sum of the transaction.

The payment enquiry is a server-to-server transaction and can be integrated in the web-server application of the service provider's online store.

The service provider's payment enquiry is sent as follows:

Code	Description
<FORM METHOD="POST" ... >	Metodi = POST
ACTION="https://netbank.danskebank.dk/HB"	URL osoite
<INPUT TYPE="HIDDEN" NAME="..." VALUE= "...">	Parameteres and values. See description below.
</FORM>	

Parameters:

Parameter name	Description	Format	P/V	Example
Refno	Unique reference number given by the merchant individualising the payment.	AN (4-20)	C	Use only numbers. The verification code is calculating using the 7-3-1 method. The minimum length of the reference is 3+1.
MerchantID	Service provider's ID that individualises the merchant.	N (12)	C	00123456800
gsAftInr	District agreement number	N/AN (6)	C	1AB456
gsSprog	Language code	A (2)	C	FI or EN

gsProdukt	Product code	Standard	C	IBV
gsNextObj	Object that processes the enquiry.	Standard	C	InetPayV
gsNextAkt	Action that processes the enquiry.	Standard	C	InetPaySt
Version	Version	Standard	C	0001
gsResp	Reply type	Standard	C	S
VerifyCode	SHA256-algorithm	AN 64	C	b4a88dec5d2d6b14e79491e9c5289967af39b329abc9a9c4e4bc0b764e9ed1f8
algorithm	Algorithm type	N2	C	03 = SHA256

C=obligatory, V=optional, A=alphabetical/N=numerical, n = length (... = max. length n)

Verification code

The payment enquiry is secured by means of a verification code. The verification code is calculated using the SHA256 algorithm. The values used for calculating the verification code are: the encrypted key delivered by the Bank, the service provider's ID and the reference number. Danske Bank uses the verification code to ensure that the payment enquiry has not been changed and the sender.

The verification code is calculated by connecting the fields of the form with the encrypted key in the order mentioned below. Only values and &-marks are included in the verification code. The code is calculated by generating a character string using SHA256 algorithm.

TARKISTE = SHA 256 (SALAINEN AVAIN+'&'+KAUPPIASNUMERO+'&'+VIITENUMERO+'&')

Support for the MD5 algorithm was discontinued as of 1 January 2014.

The calculated hash value is converted into a hexadecimal, 64-character long presentation form, in which the letters A...F are in small letters. The hexadecimal value is transferred to the field "VerifyCode" as the verification code.

The HTML structure of the payment enquiry reads as follows

```
<FORM NAME="Form1" ACTION="https://netbank.danskebank.dk/HB" METHOD="POST">
<INPUT TYPE="HIDDEN" NAME="gsSprog" VALUE="FI">
<INPUT TYPE="HIDDEN" NAME="gsProdukt" VALUE="IBV">
<INPUT TYPE="HIDDEN" NAME="gsNextObj" VALUE="InetPayV">
<INPUT TYPE="HIDDEN" NAME="gsNextAkt" VALUE="InetPaySt">
<input type="HIDDEN" name="gsResp" value="S">
<input type="HIDDEN" name="gsAftlnr" value="123123">
<input type="HIDDEN" name="MerchantID" value="012345679800">
<input type="HIDDEN" name="Version" value="0001">
<input type="HIDDEN" name="Refno" value="123">
<input type="HIDDEN" name="VerifyCode" value="
b4a88dec5d2d6b14e79491e9c5289967af39b329abc9a9c4e4bc0b764e9ed1f8">
<input type="HIDDEN" name="algorithm" value="03">
</FORM>
```

The ASP structure of the payment enquiry reads as follows

```
<!-- #include file="asptearinclude.asp" -->
<%
strRefno = "9999"
Set xobj = CreateObject("SOFTWING.ASPtear")
xObj.ForceReload = True
xObj.UserAgent = "Mozilla/4.0 (compatible; MSIE 5.0b2; Windows NT)"
xObj.ConnectionTimeout = 45
strURL="https://netbank.danskebank.dk/HB"
strPayload =
        "Refno=" & strRefno & "&" &
        "MerchantID=012345679800&" &
        "gsAftlnr=123123&" &
        "gsSprog=FI&" &
        "gsProdukt=IBV&" &
        "gsNextObj=InetPayV&" &
        "gsNextAkt=InetPaySt&" &
        "Version=0001&" &
        " VerifyCode= b4a88dec5d2d6b14e79491e9c5289967↵
        af39b329abc9a9c4e4bc0b764e9ed1f8" &" &"
        “algorithm=03"
strResult = xobj.Retrieve(strUrl, Request_POST, strPayload, "", "")
Response.Write "Result: " & strResult
if inStr(strResult, "ReturnCode=000") > 0 then
Response.Write "<br><br><b>Maksu on suoritettu OK.”
<<Päivitä tilaus, jos käytetään automaattista maksukyselyä>>
<<tai vahvista että tilaus on loppuun käsitelty. >>
lopeta jos
%>
```

The data is in a single line and the ”↵” symbol represents a line break in the document.

Reply (Method = POST)

The reply message of the payment enquirty is sent as follows:

Parameter name	Description	Example
ReturnCode	Return code. 000 = OK (Reference number exists) 001 = Reference number does not exist 002 = Reference number has not been filled in 003 = Service provider’s ID has not been filled in 004 = Service provider’s ID does not exist 006 = Agreement does not exist 009 = Character set error 010 = Reference number is not unique.	000
ReturnText	Return text which notifies the return code. OK if the return code is 000, otherwise not.	OK
Refno	Reference number	123
MerchantID	Service provider’s ID	Test Shop

Amount	Amount	456,23
Currency	Currency	EUR
Total	Total can be less than the Amount if payment refunds have been made using the same reference number.	456,23
PayType	Payment type is always KT. Account transfer	KT
PayStatus	Payment status.	Settled

Example:
ReturnCode=000&ReturnText=OK&Refno=123&MerchantID=Test Shop 000024&Amount=456,23&Currency=EUR&Total=456,23&PayType=KT&PayStatus=Settled

7 Testing the service

Service provider can test the Web Payment Service in the production environment before signing the agreement by using the Service provider's test codes (Service provider's ID and encrypted key). The test takes place in a production-like environment with the same security demands as the actual production environment.

Test form:
A test can be performed either by creating a payment request yourself or by filling in the test form at the following address:

http://business.danskebank.fi/businesssbfi/WebpaymentProdtoCustomers_SHA256.htm

Your own customer codes must be used for the test. When using a test service provider, account transfers are not made and service fees are not charged.

Service provider's test codes:
Service provider's ID: 000000000000
Encrypted key: jumCLB4T2ceZWGJ9ztjuhn5FaeZnTm5HpfDXWU2APRqfDcsrBs8mqkFARzm7uXKd

Payment request data:
URL for Web Payment Service:
https://verkkopankki.danskebank.fi/SP/vemaha/VemahaApp

PAYMENT REQUEST – TEST MESSAGE		
Field and data	**Data name**	**Description**
1. Sum	SUMMA	See section 4.1.
2. Reference number	VIITE	See section 4.1.
3. Service provider's ID	KNRO	000000000000
4. Currency	VALUUTTA	See section 4.1.
5. Version of message	VERSIO	4
6. Return address	OKURL	See section 4.1.
7. Cancellation address	VIRHEURL	See section 4.1.
8. Verification code	TARKISTE	ed0ea6eed912bea06bc84944f7079acf4df9210db0a7ce1ae02ae86e2ec31e64

REPLY MESSAGE		
Field and data	**Data name**	**Description**
1. Service provider's ID	KNRO	000000000000
2. Currency	VALUUTTA	Currency according to payment request
3. Reference number	VIITE	Reference number according to payment request
4. Sum	SUMMA	Sum according to payment request
5. Version of message	VERSIO	4
6. Status	STATUS	0
7. Verification code	TARKISTE	ed0ea6eed912bea06bc84944f7079acf4df9210db0a7ce1ae02ae86e2ec31e64
8. Payment method	MTAPA	1 = account transfer

7.1 Testing Refund of payment

Service provider can test refund of Web Payment Service by using Service provider's test codes (Service provider's ID and encrypted key). The test takes place in a production-like environment with the same security demands as in the actual production environment.

Testing:
Service Provider performs test by creating a refund request from its own system.
When using a test service provider, account transfers are not made and service fees are not charged..

Service provider´s test codes:
Service provider´s ID: 000000000000
Encrypted key: jumCLB4T2ceZWGJ9ztjuhn5FaeZnTm5HpfDXWU2APRqfDcsrBs8mqkFARzm7uXKd

Refund request data:
URL for Web Payment Service:
https://netbank.danskebank.dk/HB

REFUND REQUEST MESSAGE FORM DATA FIELD				
Field and data	**Data name**	**Form**	**C/V**	**Example**
1. Sum	gsAmount	N (13)	C	500
2. Reference number	gsRefno	AN (4-20)	C	1232
3. Service provider's ID	gsShopId	N (12)	C	000000000000
4. Currency	gsCurrency	A (3)	C	Aina EUR
5. Version of message	gsVersion	Constant	C	0001
6. Product code	gsProdukt	Constant	C	IBV
7. Subsystem	gsNextObj	Constant	C	InetPayV
8. Action ID	gsNextAkt	Constant	C	InetPayCan
9. Verification code	gsMacVI	AN 64	C	ea6094c08ba67d702825e5b350e5271d6da2ad315d22552e04ceef660626ee37
10. Language	gsSprog	A (2)	C	FI, EN
11. Algorithm	gsAlogv	A (2)	C	03 =(SHA256)
12. Response type	gsResp	Constant	C	S
13. New reference number	gsNewrefno	AN (4-20)	C	4578

14. Special text	gsSpltext	AN (4-50)	V	Comments by SP
15. Sum	gsAmountCh	N (13)	C	500

C=obligatory, V=optional, A=alphabetical/N=numerical, n = length (... = max. length n)

Reply refund message		
Parameter name	**Description**	**Example**
ReturnCode	Return code. 000 = OK 001 = Reference number not found 002 = Web payment already returned 003 = Refund transaction cannot be processed.	000
ReturnText	Return text, which describes the return code. Will be OK if return code is 000, otherwise not.	OK
Refno	Reference number	1232
SPNewRefno	Service Provider New reference number	4578
SPSpecialText	Service Provider special text	Refund for Danske Bank
Amount	Amount	500,00
MerchantID	Service provider's ID	000000000000
Currency	Currency code	EUR
Verification Code	Verification code calculated from MAC Key (SHA256 algorithm)	5aa52ce23f9305c85842f01b55a4e092aada4fecbb1aa068de6312ab9d3b9df2
TransactionBalance	Verification code calculated from MAC Key (SHA256 algorithm)	1,00

8 Customer support and technical assistance

- Danske Bank branches during opening hours.
- Danske Bank Business Services, tel. 0100 2580 Mon-Fri 8am-6pm (local network charge/mobile call charge)

Corporate customers can send a message to Customer support through the Web bank in protected environment.