Nordea

E-payment

Technical manual – Version 1902

(2019-02-15)

Table of contents

Index of tables

This manual is published by Nordea Bank Abp, filial i Sverige. Revisions or other changes due to mistyping can be made by Nordea at any point and without notice. These changes will be incorporated in new versions of the manual. This manual should not be seen as a warranty from Nordea that systems described in the manual shall perform to any certain functionality of quality.

Nordea holds the responsibility to support definitions and user interfaces in accordance to this manual. Prior to changes in user interface or definitions, Nordea is responsible for informing merchants in advance. Nordea cannot be held responsible for further technical developments that are not described in this manual and therefore not supported by Nordea but still implemented by merchants.

1. Introduction

E-payment via Nordea is an electronic payment service for securing payments made on-line. The service is developed for companies, organizations and members of the public sector who wish to sell goods and services via the Internet to private individuals and companies in Sweden.

1.1 E-payment via Nordea, Version 1.1

In the updated version 1.1 of the service we offer “Pay direct”. In addition, e-payment via Nordea also includes services known as “Payment check” and “Repayment” which enables vendor companies to check whether payments have been received by the bank and to repay complete or parts of a “Pay direct” payment.

This installation manual comprises an updated version 1.1 of e-payment via Nordea.

”Pay direct” means that the transaction is carried out directly. The purchase sum is deducted from the account of the purchaser and credited to the account of the vendor company. Transfer is handled by Nordea’s payment system.

”Payment check” means that the vendor company is able to check at a later stage whether individual payments have been received, processed and concluded correctly in the payment service.

”Repayment” means that the vendor company is able to repay the complete payment or a part of the payment to the purchaser. The original payment has to been performed by e-payments “Pay direct” service, and the repayment is a reverse transfer of the accounts involved in the original payment.

1.2 Getting started

1.2.1 Implementation

The vendor company installs a link to Nordea from the vendor company’s web shop. It is required of the vendor company that a reference number for payments is generated for each purchase order. In addition, it is required that the vendor company implements a routine generating a checksum according to a special algorithm, HMAC. See chapter 3 Tamper protection for a more detailed description of HMAC.

The vendor company gets a secret key from Nordea that must be installed and kept secure and a key verification value (KVV).

1.2.2 Technical support

Support is provided by Internet support team concerning e-payment via Nordea, weekdays from 08.00 to 18.00, telephone-number 0771-776991.

1.3 Technical description of thepayments

Shown below is a technical description, in point form, of what takes places in connection with “Pay direct”.

The purchaser has put together an order in the vendor company's web shop and wishes to pay using e-payment via Nordea. Necessary information on the purchase is gathered in an electronic payment form, the format of which is specified by Nordea. This payment form constitutes the vendor company’s interface to the payment service. In order to make sure that the information is not changed, the vendor company works out a check sum bases on the content of the form. In this manner, any changes made to the form on route to the vendor and payment service will be detected. The exact procedure that occurs when the purchaser performs transactions with the vendor company and how the payment pages are designed are matters for the vendor to decide. What is most essential is that the information in the payment form is correctly formatted.

The only requirement that Nordea has on the web shop is that the purchaser is not directed to the e-payment service inside the web shop's frames or that the web shop acts as some kind of director for the purchaser under the purchaser's session with the e-payment service. The web shop has to direct the purchaser to the e-payment service by submitting a form.

- The purchaser is requested, via the log-on procedure, to establish a secure connection (https/TLS) with payment service prior to sending the payment form. The secure connection means above all that:
  - Information exchanged between the purchaser and payment services are coded.
  - The purchaser may rest assured that he/she has in reality contacted Nordea’s Payment Service and not another server. This is because the Payment Service provides a so-called server certificate, a form of electronic ID card used by the purchaser to identify Nordea.
- The payment form is now sent to the Payment Service at Nordea, where a checksum is calculated and compared with the checksum calculated by the vendor. The Payment Service also checks to ensure that the information sent in the form has the correct format.

- The purchaser knows that the Payment Service is Nordea, but the contrary is not the case, i.e., Nordea does not know who the purchaser is. The purchaser must therefore identifyhimself/herself.
- The purchaser identifies himself/herself according to the instructions given by Nordea. The identity of the purchaser is sent to the payment services.

- Nordea receives log-on and presents payment information together with the purchaser’s account details. The information on the payment, or alternatively, the payment instruction and purchaser/vendor is presented on a page where checking is done. Nordea requests that the purchaser sign the payment.

- The buyer checks that the payment details are correct and confirms the payment by putting signature to the payment details, signing is done by using the routines approved by Nordea.

- Payment, or alternatively, the payment instruction is accomplished if the signature is correct.

- The Payment Service presents confirmation to the purchaser that the payment is completed, or alternatively, that the payment instruction has been entered. The purchaser will automatic be linked back to the vendor company where a confirmation of the purchase is presented. If the connection to the vendor company is interrupted, the vendor company is nevertheless able to verify whether the payment or payment instruction has been received via a "payment check".

The vendor is able to check whether a payment has been accomplished via e.g.:

- Statement of account (for PlusGiro and Nordea accounts)
- Corporate bank services via Internet (for Nordea accounts)
- Corporate Netbank (for PlusGiro and Nordea accounts)
- ePlusGiro Företag (for PlusGiro accounts)
- Girovision (for PlusGiro accounts)

When the vendor company uses a PlusGiro account to receive e-payments the paper statement of account, the statement of account in ePlusGiro Företag and Girovision will only show 13 characters. When the vendor company uses a Nordea account 25 characters will be shown.

1.4 Technical description of payment check and repayment

Shown below is a technical description, in point form, of what takes places in connection with “Payment Check” and “Repayment”. The description applies to both services since they have the same procedure and flow.

- The web shop provides a webpage on which a user appointed by the vendor company is able to manually feed in values that are requested for a payment check or repayment in a form. The webpage has to calculate a checksum on the values that are fed to guarantee that the values do not change on their way to the payment service. The values and the checksum constitute the webshop's interface towards the payment check and repayment services. The exact look and design of the form is a matter for the vendor company to decide. What is most essential is that the information sent in the form is correctly formatted.

- The vendor company is requested to establish a secure connection (https/TLS1.2) with the Payment Service prior to sending the form. Nordea uses TLS version 1.2 with allowed cypher suites TLS1.2-ECDHE-RSA-

AES256-GCM-SHA384, TLS1.2-ECDHE-RSA-AES128-GCM-SHA256, TLS1-ECDHE-RSA-AES256-SHA, TLS1-ECDHE-RSA-AES128-SHA. Nordea can use extensions to the TLS such as Server Name Indication, SNI without any further notice. So, an implementer must cater for their implementation support SNI. The secure connection means above all that:

a) Information exchanged between the webshop and payment services are coded.
b) The webshop may rest assured that he/she has in reality contacted Nordea's Payment Service and not another server. This is because the Payment Service provides a so-called server certificate, a form of electronic ID card used by the purchaser to identify Nordea.
c) The payment form is now sent to the Payment Service at Nordea, where a checksum is calculated and compared with the checksum calculated by the vendor. The Payment Service also checks to ensure that the information sent in the form has the correct format.

- The webshop knows that the Payment Service is Nordea, but the contrary is not the case, i.e., Nordea does not know who the user submitted the request is. However, it is not necessary for the payment service to know whom the submitting user is to do a payment check or repayment. The payment service is only interested in which vendor company is submitting the request, and to be sure that the published vendor company actually is the one submitting the request. This is secured by the checksum that is used on the information sent by the webshop. The checksum is calculated by the certain algorithm HMAC and a special secret key that only the vendor company has knowledge about.

- If the checksum (MAC) is correct, information about the original payment is fetched or if a repayment is requested the total amount of repayments is checked that it does not exceed the original amount before the repayment is performed. Repayment means that the original payment is reversed, the repayment amount is drawn from the vendor company's account and transferred to the purchasers account.

- The Payment Service presents a confirmation to the user including information about the requested payment or repayment. The information is presented in clear text in a table where the status, amount and currency for the requested payment or repayment are displayed. There is also a button with a link to the webshop presented to the user under the table, where the user can choose to send the confirmation to the webshop. The confirmation that can be sent to the webshop contains information about the requested payment or repayment, to be saved or handled by the webshop to register in its enterprise solution.

The vendor company is also able to verify whether a repayment has been accomplished via f ex:

- Statement of account (for PlusGiro and Nordea accounts)
- Corporate bank services via Internet (for Nordea accounts)
- Corporate Netbank (for PlusGiro and Nordea accounts)
- ePlusGiro Företag (for PlusGiro accounts)
- Girovision (for PlusGiro accounts)

When the vendor company uses a PlusGiro account to receive e-payments the paper statement of account, the statement of account in ePlusGiro Företag and Girovision will only show 13 characters. When the vendor company uses a Nordea account 25 characters will be shown.

The course of events above is described for a manual use of the payment check and repayment where a user appointed by the vendor company manually feeds in the information requested by a payment check and a repayment. The vendor company can also choose to have the course of events to be more automatically performed by their webshop or some other enterprise solution software that supports Internet communication.

The webshop then collects and sends the information to the payment service instead for a user that manually edits the values for the information to be sent to the payment service. The webshop also reads and parses the information in the confirmation returned by the payment service.

The course of events above still applies and is the same for the more automatically service but with the only difference that the user mentioned above is represented by the webshop instead.

2. Information flow between the vendor and Nordea

The following text describes the flow of information that takes place between the vendor company and Nordea for the services that included in e-payment via Nordea concept:

- ”Pay direct”
- ”Payment check”
- ”Repayment”

In the text below the word *shop* refers to the vendor company’s web shop.

2.1 ”Pay direct”

2.1.1 Transaction details to payment service from the shop

The shop sends the following transaction details to the Payment Service via HTTP method POST:

#	Space name	Data description	Value	Format	Usage
1.	NB_VERSION	Payment version	0002	N4	Mandatory
2	NB_RCV_ID	Shop’s ID	Agreement no.	AN9	Mandatory
3.	NB STAMP	Payment ID	Free text	AN20	Mandatory
4a.	NB_DB_AMOUNT	Payment amount	Ex: 990,00	AN19	Mandatory
4b.	NB_DB_CUR	Currency	Ex: SEK	AN3	Mandatory
4c.	NB_DB_REF	Reference number for payment	Free number without leading zeroes	N25	Mandatory
5.	NB_RETURN	Return address if “OK” from the bank	URL	AN240	Mandatory
6.	NB_CANCEL	Return address if “Cancel” from the bank	URL	AN240	Mandatory
7.	NB_REJECT	Return address if “Reject” from the bank	URL	AN240	Mandatory
8.	NB_HMAC	Control amount for purchase order	MAC value	AN32	Mandatory
9.	NB_KVV	Key verification value	KVV value	AN32	Mandatory

Table 1 ”Pay direct”, Interface from payment service to vendor company

<u>Description of the contents of the space:</u>

1 The Payment Service’s version number 0002.

2 Identity of vendor in Nordea’s systems.

3 Payment’s ID is the vendor company’s signature on the payment, which individualises the payment at the shop. The shop’s ID is unique for each payment and is used by the shop as a means of linking together an order and a payment instruction. Among other things, it is used in order to prevent double invoicing. The signature may be of optional format, a reference or a combination of date, time of day and serial number.

4a Sum of payment, separated with decimal point (,).

4b Type of currency for the payment amount indicated. Only SEK or EUR is applicable for the timebeing.

4c Payment’s reference or invoice number indicated by the shop. The reference number is used as a means of linking the payment with an order. It is seen as a transaction text on the statement of account of the purchaser and the shop. Note that the number is not allowed to have any leading zeroes.

5 The shop’s return link for successful transactions. Payment information is attached in return to the URL link.

The return link must be a complete URL address and be in reference to a specific page.

6 The shop’s return link for a discontinued payment transaction, if it is the user who breaks off the transaction. No payment information is attached in the return to the URL link. (In order to determine exactly which payment has been discontinued, use of a so-called Query String after the URL link is suggested, for example "http://www.nb.se/cancel.html?NB_STAMP=12345".) The return link must be a complete URL-address and be in reference to a specific page.

7 The shop’s return link for an unsuccessful payment transaction. No payment information is attached in return to the URL link. (In order to determine exactly which payment has been discontinued, use of a so-called Query String after the URL link is suggested, for example "http://www.nb.se/cancel.html?NB_STAMP=12345".) The return link must be a complete URL-address and be in reference to a specific page.

8 HMAC hashed value of the transaction details in spaces 2, 3, 4a-c as well as a special secret key that the shop has received in connection with the agreement on utilisation of e-payment via Nordea. Please see section 3 Tamper protection for more information about how to produce the hashed value.

9 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

2.1.2 Returning transaction details from the payment service to the shop

When the bank returns confirmation as acknowledgement to the shop, the following information is delivered via the HTTP method POST:

#	Space name	Data description	Value	Form	Usage
1.	NB_RETURN_STAMP	Same payment ID as came from the shop	Free text	AN20	Mandatory
2a.	NB_RETURN_DB_AMOUNT	Transaction's amount	Ex:990,00	AN19	Mandatory
2b.	NB_RETURN_DB_CUR	Transaction's currency	Ex: SEK	AN3	Mandatory
2c.	NB_RETURN_DB_REF	Same reference number as came from the shop	Free number	N25	Mandatory
3.	NB_PAID	Nordea's confirmation ID for direct payment	Transaction's time stamp	AN26	Mandatory
4.	NB_HMAC	Check sum for confirmation	MAC value	AN32	Mandatory
5.	NB_KVV	Key verification value	KVV value	AN32	Mandatory

Table 2 "Pay direct", Interface from payment service to vendor company.

Description of the contents of the space:

1 The payment signature that came from the shop together with payment information.

2a The amount of the transaction. The format on the amount may have been changed for the format on the amount that the shop sent to the Payment Service.

2b The currency in question. The format on the currency may have been changed for the currency format on the currency that the shop sent in to the Payment Service.

3 The ID number that the bank has assigned to the transaction.

4 HMAC hashed value of the transaction details in spaces 1, 2a-c, 3 as well as a special secret key that is shown in the agreement on e-payment via Nordea. Please see section 3 Tamper protection for more information about how to produce the hashed value.

5 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

2.1.3 Example of communication between shop and direct payment

An example of how communication between shop and the Payment Service may appear for requesting a direct payment via account transfer:

- The purchaser is directed by a link in the vendor company's web shop to the web page https://gfs.nordea.se/e-betalning/direktbetalning by submitting a form that contains these parameters:

```
<INPUT TYPE=HIDDEN NAME="NB_VERSION" VALUE="0002 ">
<INPUT TYPE=HIDDEN NAME="NB_RCV_ID" VALUE="55082">
<INPUT TYPE=HIDDEN NAME="NB_STAMP" VALUE="20090515001 ">
<INPUT TYPE=HIDDEN NAME="NB_DB_AMOUNT" VALUE="550,00">
<INPUT TYPE=HIDDEN NAME="NB_DB_CUR" VALUE="SEK">
<INPUT TYPE=HIDDEN NAME="NB_DB_REF" VALUE="001 ">
<INPUT TYPE=HIDDEN NAME="NB_RETURN"
VALUE="http://www.internetshoppen.se/return.asp">
```

```
<INPUT TYPE=HIDDEN NAME="NB_REJECT"
VALUE="http://www.internetshoppen.se/reject.asp?NB_STAMP=20090515001     ">
<INPUT TYPE=HIDDEN NAME="NB_CANCEL"
VALUE="http://www.internetshoppen.se/cancel.asp?NB_STAMP=20090515001     ">
<INPUT TYPE=HIDDEN NAME="NB_HMAC"
VALUE="12345678901234567891234567890 12">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV"
VALUE="12345678901234567891234567890 12">
```

- The purchaser completes the transfer in the Payment Service and returns automatic back to the web shop by the link that the web shop supplied in the parameter NB_RETURN in the form together with a form in the Payment Service containing these parameters:

```
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_AMOUNT"   VALUE="550,00">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_STAMP"   VALUE="20090515001">
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE=" SEK">
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE="001">
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE="2009-05-15 13.22.41.155864">
<INPUT TYPE=HIDDEN NAME="NB_HMAC"
VALUE="12345678901234567891234567890 12">
<INPUT TYPE=HIDDEN NAME="NB_KVV"
VALUE="12345678901234567891234567890 12">
```

- The purchaser is directed back to the web shop by the link that the web shop supplied in the parameter NB_ CANCEL in the form if the purchaser chooses to cancel the payment and not complete the transfer in the Payment Service. The purchaser is directed without submitting any form and no additional information is sent back to the shop. The web shop can still see which payment that was cancelled by using a so-called query string in the form that were submitted in the web shop by the purchaser.
- Please note that there are no guarantees that the purchaser actually returns by using the link back to the web shop.
- The purchaser is directed back to the web shop by the link that the web shop supplied in the parameter NB_REJECT in the form if the purchaser is unable to complete the transfer for some reason in the Payment Service. The purchaser is directed without submitting any form and no additional information is sent back to the shop. The web shop can still see which payment that was rejected by using a so-called query string in the form that were submitted in the web shop by the purchaser.
- If the purchaser chooses to close down the window when linked to the payment services and the purchaser has not begun the payment session no answer will be directed back to the web shop.

2.2 ”Payment check”

The shop is able to check that a payment has been accomplished by conducting a payment check. Described below is the information that the shop and the Payment Service exchange when doing a payment check.

If the checksum of payment is incorrect and it cannot be verified, payment service will respond with "Not Found". If on the other hand some other error occurs in the payment service, it will respond in the same way as in the normal payment check, but with other parameters. A parameter shows that an error occurred and the parameter describes the error.

2.2.1 Payment details to the payment service for a payment check

The shop submits the following transaction details to the Payment Service via the HTTP method POST (Note: Nordea requires that the HTTP POST request contains Content-Type and User-Agent headers):

#	Space name	Data description	Value	Format	Usage
1.	NB_VERSION	Payment check version	0002	AN4	Mandatory
2.	NB_RCV_ID	Shop’s ID	Agreement number	AN9	Mandatory
3.	NBSTAMP	PaymentID	Freetext	AN20	Mandatory
4.	NB_RETURN	Return address if "OK" from the bank	URL	AN240	Optional
5.	NB_HMAC	Checksum of payment Check	MAC value	AN 32	Mandatory
6.	NB_KVV	Key verification value	KVV value	AN 32	Mandatory

Table 3 Interface to payment check from the vendor company

Description of the contents of the space:

1 Payment check’s version number.

2 Shop’s identity on Nordea’s systems.

3 Payment’s ID is the shop’s signature on the payment, which individualises the payment at the shop. Payment’s ID is unique for each payment and is used by the shop as a link between the order and the payment instruction. Among other things, it is used to prevent double invoicing. The signature may be of optional format, a reference or a combination of date, time of day and serial number.

Please observe that the payment ID (NB_STAMP) must be exactly concordant with the payment ID (NB_STAMP) of the payment that the payment check is referring to.

4 The shop’s return link for the answer from payment check. Information on the payment is attached in the return to the URL link. The return link must be a complete URL-address and be in reference to a specific page.

5 HMAC hashed value with a special secret key as well as the transaction details in spaces 2 and 3. Please see section 3 Tamper protection for more information about how to produce the hashed value.

6 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

2.2.2 Returning details from payment check

When the shop has requested a payment check page, payment service returns the following information on the requested page as parameters to a form:

#	Space name	Data description	Value	Format	Usage
1.	NB_VERIFIED	Payment status	YES/NO/ERR	AN3	Mandatory
2.	NB_RETURN_STAMP	Same Payment ID as the one from the shop	Free text	AN20	Mandatory
3a.	NB_RETURN_DB_AMOUNT	Transfer amount	Ex: 990,00	AN19	Optional
3b.	NB_RETURN_DB_CUR	Transfer currency	Ex: SEK	AN3	Optional
3c.	NB_RETURN_DB_REF	Transfer's reference number	Free number	N25	Optional
4.	NB_RETURN_BB_R	F1 (- 8) Same reference number as came from the shop for payment 1-8.	Free text	AN25	Optional
5.	NB_PAID	Nordea's confirmation ID for the payment	Transaction's time stamp	AN26	Optional
6.	NB_HMAC	Hash value of receipt	MAC value	AN32	Mandatory
7.	NB_KVV	Key verification value	KVV value	AN32	Mandatory
8.	NB_ERROR_DESCR	Error description	Free text	AN50	Optional

Table 4 Interface from payment check to vendor company.

Description of the contents of the space:

1 Return value for payment's status
"YES"" if the payment has been completed
"NO" if the payment cannot be found in Nordea's Central Data Systems
"ERR" when an error occurs and correct answer cannot be given.
In case of "YES " and "NO " the parameters 3a-c, 4 and 5 are returned. Parameter 7 is missing in the answer. In case of "ERR" parameter 7 is returned. Parameters 3a-c, 4 and 5 missing in the answer, also parameter 6 does not return any checksum since the error can depend on having problem calculating the checksum.

2 Same payment signature for monitored payment that came from the shop.

3a Transferred amount in the case of direct payment. The parameter is used only in case where a payment containing account transfer is carried out.

3b Transferred currency in the case of direct payment. The parameter is used only in case where a payment containing account transfer is carried out.

3c Reference number for direct payment. The parameter is used only in case where a payment containing account transfer is carried out.

4 Reference value for payments 1-8. The parameter is used only in case where a payment containing payment monitoring is carried out.

5 The bank's identification of the transaction.

6 HMAC hashed value. The following parameters are base for calculating the hashed value if parameter 1, return value for payment's status, has the one of these values:

"YES": spaces 1, 2, 3a-c, 4, 5

"NO": spaces 1, 2
"ERR": no hashed value is calculated

These parameters as well as a special secret key that the shop received in connection with the agreement of utilisation of e-payment via Nordea are used to calculate the hashed value. Please see section 3 Tamper protection for more information about how to produce the hashed value.

7 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

8 Description of possible error in payment checking. The parameter is used only in case an error occurs in payment checking.

The information given on the checking page is obtained as answer and comprises a table that shows the returned values with descriptive text. The returned values are also shown in HTML format as a hidden space in an HTML form, as a simple way of making it automatically readable for automated applications.

In the case of the shop indicated in a return link in space 4 (NB_RETURN) a button will be shown in connection with the table, and with a reference to the return link indicated. This link can be used to send parameters to the shop's web server in the same way as the return link that was presented for the purchaser in connection with confirmation of the payment.

2.2.3 Example of communication between shop and payment checking

An example of how communication between shop and the Payment Service may appear in connection with checking a payment via account transfer:

WebWeb shop requests page by issuing a HTTP POST request to gfs.nordea.se:

```
POST /e-betalning/betalningskontroll HTTP/1.1
Host: gfs.nordea.se
Content-Type: application/x-www-form-urlencoded
User-Agent: <user-agent>

NB_VERSION=0002&NB_
RCV_ID=999999&NB_STAMP=20081006001&NB_HMAC=123456789012
3456789123456789012&NB_KVV=1234567890123456789123456789012
```

The Payment Service answers in the page with a table that presents the answer as well as its hidden parameters when the request has been successful, and the requested payment has been found:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="YES">
<INPUT TYPE=HIDDEN NAME="NB _RETURN_STAMP" VALUE="20090515001 ">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_AMOUNT"   VALUE="550,00">
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE=" SEK">
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE="001 ">
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE="2009-05-15 13.22.41.155864">
<INPUT TYPE=HIDDEN NAME="NB_HMAC"
VALUE="12345678901234567890123456789012">
<INPUT TYPE=HIDDEN NAME="NB_KVV"
VALUE="12345678901234567890123456789012">
```

The Payment Service answers in the page with a table that presents the answer as well as its hidden parameters when the requested has been successful, but the requested payment cannot be found:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="NO">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_STAMP"   VALUE="20090515001 ">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_AMOUNT"  VALUE= "">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_CUR"  VALUE= "">
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE=" ">
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE=" ">
<INPUT TYPE=HIDDEN NAME="NB_HMAC"
VALUE="12345678901234567890123456789012">
<INPUT TYPE=HIDDEN NAME="NB_KVV"
VALUE="12345678901234567890123456789012">
```

The Payment Service answers in the page with a table that presents the answer as well as its hidden parameters when the requested has not been successful:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="ERR">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_STAMP"   VALUE="20090515001 ">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_AMOUNT"  VALUE= "">
<INPUT  TYPE=HIDDEN  NAME="NB_RETURN_DB_CUR"  VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE=" ">
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE=" ">

<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE= "">
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE= "">

<INPUT TYPE=HIDDEN NAME="NB_ERR_DESCR" VALUE=" Technical problem,
please try again later ">
```

2.3 ”Repayment”

The shop is able to repay the complete or parts of a payment that is performed by a direct payment through a repayment. Described below is the information that the shop and repayment service exchange when doing a repayment.

If the checksum of repayment is incorrect and it cannot be verified, the Payment Service will respond with "Not Found". If on the other hand some other error occurs in the Payment Service, it will respond in the same way as in the normal repayment answer, but with other parameters. A parameter shows that an error occurred and the parameter describes the error.

The procedure and flow for repayment is the same as for payment check and only differs by the information that is exchanged by the web shop and the Payment Service. Please see section 2.3.3 for payment check above that has the same procedure and flow for an example of the communication between the two actors.

2.3.1 Payment details to the payment service for a repayment

The shop submits the following transaction details to the Payment Service via the HTTP method POST (Note: Nordea requires that the HTTP POST request contains Content-Type and User-Agent headers):

#	Space name	Data description	Value	Format	Usage
1.	NB_VERSION	Repayment version	0002	AN4	Mandatory
2.	NB_RCV_ID	Shop’s ID	Agreement number	AN9	Mandatory
3.	NB_STAMP	Payment ID	Free text	AN20	Mandatory
4.	NB_DB_REF	Reference number for original payment	Free number	N25	Mandatory
5.	NB_PAID	Nordea’s confirmation ID	Transaction’s time stamp	AN26	Mandatory
6.	NB_REPAY_AMOUNT	Repayment amount	Ex: 999,00	AN19	Mandatory
7.	NB_REPAY_CUR	Repayment currency	Ex: SEK	AN3	Mandatory
8.	NB_RETURN	Return address if “OK” from the bank	URL	AN240	Optional
9.	NB_HMAC	Checksum of repayment	MAC value	AN32	Mandatory
10.	NB_KVV	Key verification value	KVV value	AN32	Mandatory

Table 5 Interface to repayment from the vendor company

<u>Description of the contents of the space:</u>

1 Repayment Service's version number.

2 Identity of vendor in Nordea's systems.

3 Payment's ID is the vendor company's signature on the payment, which individualises the payment at the shop. The shop's ID is unique for each payment, and is used by the shop as a means of linking together an order and a payment instruction. Among other things, it is used in order to prevent double invoicing. The signature may be of optional format, a reference or a combination of date, time of day and serial number.

- *Please observe that the payment ID (NB_STAMP) must be exactly concordant with the payment ID (NB_STAMP) of the payment that the repayment is referring to.*

4 Original payment's reference or invoice number indicated by the shop. The reference number is used as a means of linking the payment with an order. It is seen as a transaction text on the statement of account of the purchaser and the shop.

5 The ID number that the bank has assigned to the transaction and was send to the web shop in the confirmation from the Payment Service.

6 Sum of repayment. The total amount to be repaid to the purchaser cannot exceed the original payment amount.

7 Type of currency for the repayment amount indicated. Note! The currency for the repayment amount has to be the same as the currency for the original payment.

8 The shop's return link for successful transactions. Payment information is attached in return to the URL link.

- The return link must be a complete URL address and be in reference to a specific page.

9 HMAC hashed value of the transaction details in spaces 2, 3, 4, 5, 6 and 7 as well as a special secret key that the shop has received in connection with the agreement on utilisation of e-payment via Nordea. Please see section 3 Tamper protection for more information about how to produce the hashed value.

10 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

2.3.2 Returning details from repayment

When the shop has requested a repayment page, the payment service returns the following information on the requested page as parameters to a form:

#	Space name	Data description	Value	Format	Usage
1.	NB_VERIFIED	Payment status	YES/ERR	AN3	Mandatory
2.	NB_RETURN_STAMP	Same payment ID as the one from the shop	Free text	AN20	Mandatory
3.	NB_RETURN_DB_REF	Transfer's reference number	Free number	N25	Mandatory
4a.	NB_RETURN_REPAY_AMOUNT	Repayment amount	Ex: 990,00	AN19	Mandatory
4b.	NB_RETURN_REPAY_CUR	Repayment currency	Ex: SEK	AN3	Mandatory
5a.	NB_WITHDRAWAL_AMOUNT	Withdrawal amount from vendor's account	Ex: 999,00	AN19	Optional
5b.	NB_WITHDRAWAL_CUR	Withdrawal currency	Ex: SEK	AN3	Optional
5c.	NB_WITHDRAWAL_DATE	Date for withdrawal	Ex: 2009-05-15	AN10	Optional
5d.	NB_DEPOSIT_DATE	Date for deposit on purchaser's account	Ex:2009-05-16	AN10	Optional
5e.	NB_RATE	Exchange rate	Ex: 1,0	AN12	Optional
6.	NB_PAID	Nordea's confirmation ID for the payment	Transaction's time stamp	AN26	Mandatory
7.	NB_MAC	Hash value of receipt	MAC value	AN32	Mandatory
9.	NB_KVV	Key verification value	KVV value	AN32	Mandatory
10.	NB_ERROR_DESCR	Error description	Free text	AN120	Optional

Table 6 Interface from repayment to vendor company

<u>Description of the contents of the space:</u>

1 Return value for repayment's status; is "YES" if the repayment has been completed and "ERR" if an error occurs and correct answer cannot be given.
In case of "ERR " parameter 8 is returned with the error described in clear text, else parameter 8 is missing in the answer. Also parameter 6 does not return any checksum on error since the error can depend on having problem calculating the checksum.

2 Same payment signature for monitored payment that came from the shop.

3 The reference number for the payment that came from the shop together with the repayment information.

4a The amount of the repayment. The format on the amount may have been changed for the format on the amount that the shop sent to repayment service.

4b The currency in question. The format on the currency may have been changed for the currency format on the currency that the shop sent in to repayment service.

5a The withdrawal amount from the vendor company's account. The parameter is used only in case currency change has been done.

5b The withdrawal amount's currency from the vendor company's account. The parameter is used only in case currency change has been done.

5c The withdrawals date from the vendor company's account. The parameter is used only in case currency change has been done.

5d The deposits date for the purchaser's account. The parameter is used only in case currency change has been done.

5e The rates for a currency change. The parameter is used only in case currency change has been done.

6 The bank’s identification of the transaction, not the same value as that the web shop submitted in the request to the Repayment Service and was returned in the confirmation for the original payment but a new value. This new value for the identification of the transaction is now used to connect a payment from a web shop to a transaction in the bank, to be used for example in a additional request for repayment. It is also used to prevent double invoicing of a repayment.

7 HMAC hashed value of the transaction details in spaces 1, 2, 3, 4a-b, 5a-e (only used in case of currency change), 6 as well as the special secret key indicated in the agreement on e-payment via Nordea. Please see section 3 Tamper protection for more information about how to produce the hashed value.

Note! If parameter 1, return value for repayment’s status, has the value "ERR" then no checksum will be returned since the error can depend on having problem calculating the checksum.

8 Key verification value calculated as a seal for the secret key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

9 Description of possible error in repayment. The parameter is used only in case an error occurs in repayment.

The information given on the repayment page is obtained as answer and comprises a table that shows the returned values with descriptive text. The returned values are also shown in HTML format as a hidden space in an HTML form, as a simple way of making it automatically readable for automated applications.

In the case of the shop indicated in a return link in space 9 (NB_RETURN) a button will be shown in connection with the table, and with a reference to the return link indicated. This link can be used to send parameters to the shop's web server in the same way as the return link that was presented for the purchaser in connection with confirmation of the payment.

3. Tamper protection

There is different methods for calculate seal. For e-payment, Nordea is using a method called HMAC-SHA156-128. In principle, the method of tamper protection means that the data to be sent to Nordea is run through an algorithm (256-bit secure hash algorithm, SHA256) that calculate a cryptographic checksum on the data, a hash-based method authentication code (MAC).

The method is public and the security is built on that part of the base of calculation is secret, the seal key.

3.1 HMAC-SHA256-128

In order to protect the information transmitted it is essential that the vendor company implements a routine that will generate a check (hash value) according to a special algorithm.
In all the Payment Services HMAC is used in order to:

1) Calculate the checksum in the purchase order going from the shop to Nordea.
2) Check the checksum in the confirmation that Nordea sends to the shop.

More information on HMAC-SHA256-128 can be found in the following documents:
FIPS-180-3 (Describes HMAC)
FIPS-198-1 (Describes SHA256)
RFC4868 (Describes HMAC-SHA256-128 and how the hash value is truncated)

The MAC value itself is worked out by forming a long data string of the parameters that are included in the MAC calculation, separated with an ampersand (&). This result in the MAC value for “Pay direct” forming a data string put together in the following way:
shopidentification&paymentsidentification&amount&currency&reference.
This results in a string that, for example, may have the following appearance:
"999999&12345&899,00&SEK&123450".

Any optional parameter that is not used in the information for the request or confirmation is not used in the string and is not separated by any ampersands.

By using this data string in combination with the secret key in the algorithm a value is given back where the first 32 characters constitute the MAC value.

Please note that the values in the confirmation from the Payment Service can be of a different format than used by the web shop in the request. Therefore it is important to always build the string using the exact values that are sent by the Payment Service in the confirmation, otherwise there is a risk that the hashed values are different.

3.2 Secret key

In order to calculate the check sum with HMAC the shop must have its own secret key. The secret key is distributed by Nordea and must be kept in safe custody.

The standard uses a secret key that is 128 bits long (32 characters) to generate a MAC that is also 128 bits long. Note that the MAC should be truncated to 128 bits since SHA256 normally generates a 256-bit value. It is the first 128 bits that should be used as the MAC.

A secret key is valid until a new key is requested, which is then delivered in a sealed key envelope. The key is secret to all outsiders and only those assigned, and consequently entrusted, to handle the key shall have knowledge of it.

3.2.1 Period of validity

The secret key has a certain period of validity and is changed at regular intervals in connection with the transition between two dates. In order to ensure that the payment system operates with perfect functionality the right key must be used in accordance to its period of validity. There is no tolerance time, during which both keys are valid, within the e-payment system for Nordea

Time: - - 23.59.59	(Key for period X is valid)
Time: 00.00.00 - -	(Key for period X+1 is valid)

A none valid key will lead to an error which is shown as “Sigillfel”. In that case please contact Nordea to resolve the problem.

3.3 KVV – Key verification value

There is a key verification value (KVV) for each key. This KVV need not to be secret in the same way as a key and can be used to verify that the key value is correct without disclosing the key value.

To check the entry, the KVV belonging to each key can be used. The KVV can be stored in the system for comparison with the KVV obtained for the entered key value.

4. Verifying information flow

In order to facilitate the development of transaction details, the payment form provides the possibility to verify these against a special test page, without any payment being discharged. Nordea indeed recommends that the vendor company thoroughly test the information flow against this test page before the Payment Service in the shop is opened for live customers.

4.1 Differences in information flow

In contrast to normal payments, a buyer in the normal sense of the word is not a necessity in order to test the information flow. The vendor company acts as an anonymous buyer when the test pages area being run.

Apart from the fact that the payment form must be sent to another address (see section 7 Payments service information) the transaction details are the same for sharp payments with one exception – the check sum. The vendor company must *not* calculate the check sum with the help of the secret key. Instead, the following key must be used in connection with verification:

Key:
- 1234 5678 90AB CDEF 1234 5678 90AB CDEF

KVV:
- FF36 5893 D899 291C 3BF5 05FB 3175 E880

4.2 Verifying transaction details

The test page does not resemble the pages that the buyer arrives at in a connection with a sharp payment. On the test page, for example, no log-on is required. Instead, what is presented here is a table containing transaction details submitted where each row corresponds to a row in the payment form. For each row/space the following information is presented:

- Space name.
- Space value.
- Length of space value.
- Status. If the space value could be verified without error ”OK” is shown here. If verification is not successful an error message is shown instead.

4.3 Simulated return flow

On the test page a number of options simulating the various payment flows are then given:

- Successful payment. This flow corresponds to a situation in which a buyer carries out a successful payment and then returns to the shop with a receipt, i.e., ”OK” from the bank. This flow can only be selected if it was possible to verify the entire payment form without finding any errors.
- Discontinued payment, ”cancel”. This flow corresponds to when the buyer

stops thepayment.

- Rejected payment, ”reject”. This flow corresponds to a buyer’s attempted payment being rejected for some reason.

5. Payment service information

Shown below are links and information applicable to the various e-payment via Nordea services.

5.1 ”Pay direct”

For this version of the Payment Service ”Pay direct” the version number ”0002” must be entered.

- The address to which the purchaser must be referred for ”Pay direct” is: https://gfs.nordea.se/e-betalning/direktbetalning
- For verification/test the following address is used: https://gfs.nordea.se/e-betalning/test_direktbetalning

5.2 ”Payment checking”

For this version of payment checking the version number ”0002” must be used..

- The address for payment checking is: https://gfs.nordea.se/e-betalning/betalningskontroll

5.3 ”Repayment”

For this version of repayment the version number ”0002” must be used.

- The address for repayment is: https://gfs.nordea.se/e-betalning/aterbetalning
- For verification/test the following address is used: https://gfs.nordea.se/e-betalning/test_aterbetalning