E-Payment

Service description
Specification for Baltic countries

Version 1.4

Table of contents

1 Overview..3

1.1 Advantages of E-Payment..3

1.2 Availability..3

1.3 Security..3

2 Service agreement, instructions and start-up..4

2.1 Service prerequisites..4

2.2 Service agreement..4

2.3 Instructions for the use of E-Payment..5

2.3.1 Name of payment method..5

2.3.2 Use of Nordea logo..5

2.3.3 Payment link on the service provider’s page..5

2.3.4 Implementation of E-Payment in the service provider’s service.........5

2.3.5 Links to Nordea on merchant’s pages..6

2.3.6 Start-up..6

3 E-Payment message descriptions..7

3.1 Payment request..7

3.2 Payment request field descriptions..8

3.3 Forming the MAC for the payment request..10

3.4 Return message verification..11

3.5 Returning to Service provider system..13

4 E-Payment query..14

4.1 Introduction..14

4.2 Using the e-payment query from the merchant’s service............................14

5 E-Payment query message descriptions..15

5.1 Query request..15

5.2 Query response message format in different situations..............................16

5.3 Query response codes..17

6 Testing..18

6.1 E-Payment request test message:..18

6.2 E-Payment query request test message..20

7 Contact information..22

1 Overview

E-Payment is an electronic payment method in which a buyer selects purchases and pays them within a single Internet session.

The seller, i.e. the service provider, is notified of an executed payment by the E-Payment identifier. The service provider also has query function at its disposal. With the query function the service provider can check that an e-payment was made successfully.

1.1 Advantages of E-Payment

The service provider need not send a separate invoice to the service user or deliver goods C.O.D. This reduces invoicing and packaging costs.

The service provider receives the payment immediately to its account, and can also verify it immediately.

The service provider need not acquire new software for E-Payment, because the payment service is based on the same Internet technology that the service provider uses in its services.

E-Payment provides the seller with a secure invoicing method for its electronic services.

1.2 Availability

The E-Payment service is available 24 hours a day, seven days a week, excluding cut-off times caused by maintenance, updating, etc.

1.3 Security

The service uses SSL encryption protocol in the communication between the parties. A third party cannot see or change the data. The service provider's server software must support 128-bit SSL encryption. However, the key length used in the communication is determined by the properties of the browser used by the customer. The integrity of the data in the payment request and the return message is secured by a MAC, so the customer who directs the transfer of the payment data cannot change the data without the service provider and Nordea noticing it.

Each party is responsible for the protection, security and correctness of the data they store.

When using E-Payment, the service user's account cannot be accessed by an outsider, because Nordea reliably identifies the service user by his/her Netbank codes (customer number and a session-specific password) or digital certificate. The service user also confirms each E-Payment with a specific confirmation code or digital signature.

2 Service agreement, instructions and start-up

2.1 Service prerequisites

The service provider’s invoicing system must be able to form an invoice for the service user by using Internet technology. In addition to normal invoice data, the invoice presents the E-Payment data. Once the service user has accepted the invoice, the data has to be transmitted to the service provider’s invoicing and order processing systems. The E-Payment service does not require any specific Internet server software.

In order to monitor service users’ payments, the service provider needs to use Nordea’s electronic banking services to get a transaction statement, an account statement or reference transactions. For example, via the banking program and Netbank, the above data can be retrieved from the file transfer service. The downloaded files can be further processed using ledger software.

2.2 Service agreement

The service provider and Nordea draw up a written service agreement. The service provider information is registered at the bank, and the service provider is also given a customer ID. The bank requires the service provider to use a verifier for its incoming E-Payments, and also provides it with a MAC.

The service provider notifies the branch of any changes in its services or information. When necessary, the branch will amend the agreement with the changed information.

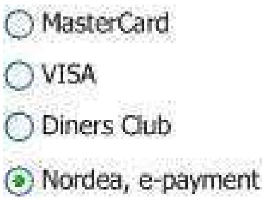
2.3 Instructions for the use of E-Payment

2.3.1 Name of payment method

Nordea’s Internet payment service is called E-Payment. Other names may not be used.

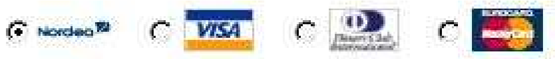
2.3.2 Use of Nordea logo

The service provider must show its use of e-payment by displaying the Nordea logo or the text “Nordea, E-Payment” on its web pages so that it is clearly visible. The Nordea logo is also used as the button functioning as the payment link. The logo is then referred to as the Nordea symbol.



○ MasterCard
○ VISA
○ Diners Club
● Nordea, e-payment

Picture 1. Nordea E-Payment displayed as text.



Picture 2. Nordea E-Payment displayed by the logo.

With the signing of the service agreement the service provider undertakes to use the Nordea logo as specified by Nordea. The trademark cannot be handed over or used for purposes other than those stated in the agreement. The service provider is not entitled to produce the Nordea logo by itself or to alter it. The company must copy the trademark over to its server from Nordea’s server.

2.3.3 Payment link on the service provider’s page

The agreement requires the service provider to use for its incoming payments the Nordea logo and a bank transfer form, by which the service user recognises the payment function. This promotes business, as the service user is already familiar with a similar form on paper and on the payment ATM display. The form is easy to read and creates confidence in the service user. The bank transfer form must carry the Nordea logo.

2.3.4 Implementation of E-Payment in the service provider’s service

E-Payment should be implemented in the merchant’s Internet service as simply and straightforwardly as possible. Use of frames/framesets is not allowed, as a payment may fail due to the service user’s hardware and browser or its versions or settings.

If ‘windowing’ is used, these matters should be paid attention to. If the service provider needs to use windowing, the E-Payment form presented in this description as well as the service provider’s receipt of an accepted payment must be shown in the created window.

It is possible to combine E-Payment with electronic invoicing, e.g. e-mail. However, the actual E-Payment (the form data group of E-Payment) may not be transmitted by e-mail or similar means. In these methods the transmitted data must always be a link, or equivalent, to the invoicer's/service provider's service in which the final E-Payment is created for the customer.

2.3.5 Links to Nordea on merchant's pages

If the service provider wants to give the service user information about E-Payment in its service, it must create a link to the E-Payment document located on Nordea's home page (http://www.nordea.ee). This way the service provider always has up-to-date information about E-Payment on its pages.

It is also advisable for the service provider to create a link to the Netbank services on Nordea's home page (http://www.nordea.ee/Teenused+eraisikule/Nordea+Internetipank/65682.html). The page is particularly useful to those customers who do not yet have the Netbank codes needed for E-Payment.

2.3.6 Start-up

The start-up day for the service is set when the agreement is made.

3 E-Payment message descriptions

3.1 Payment request

The payment request data are behind Nordea’s icon in the FORM data group as latent variables.

The data group structure is in HTML:
<FORM METHOD=”POST”
ACTION=”**https://netbank.nordea.com/pnbepay/epayn.jsp**”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
</FORM>

Form data group					
F#	**Data name**	**Field name**	**Value**	**Data type**	**Mandatory/ Optional**
1.	Payment version	SOLOPMT_VERSION	Constants, “0002”, “0003”, “0004”	AN 4	M
2.	Payment specifier	SOLOPMT_STAMP	Code specifying the payment	N 20	M
3.	Service provider’s ID	SOLOPMT_RCV_ID	Customer Legal ID	AN 15	M
4.	Service provider’s account	SOLOPMT_RCV_ACCOUNT	Other than the default account, must be registered in Nordea in IBAN format	AN 21	O
5.	Service provider’s name	SOLOPMT_RCV_NAME	Other than the default name	AN 30	O
6.	Payment language	SOLOPMT_LANGUAGE	3 = English 4 = Estonian 6 = Latvian 7 = Lithuanian	N 1	M
7.	Payment amount	SOLOPMT_AMOUNT	E.g. 990.00	AN 19	M
8.	Payment reference	SOLOPMT_REF	Standard reference number	AN 16	M
9.	Tax code	SOLOPMT_TAX_CODE	Tax code (for Lithuania)	AN 28	O Mandatory in version “0004”
10.	Payment due date	SOLOPMT_DATE	“EXPRESS” or current date “DD.MM.YYYY”	AN 10	M
11.	Payment message	SOLOPMT_MSG	Service user’s message	AN 210	M
12.	Return link	SOLOPMT_RETURN	Return address following payment	AN 256	M
13.	Cancel link	SOLOPMT_CANCEL	Return address if payment is cancelled	AN 256	M

14.	Reject link	SOLOPMT_REJECT	Return address for rejected payment	AN 256	M
15.	Payment MAC	SOLOPMT_MAC	Message authentication code	AN 32	M
16.	Payment confirmation	SOLOPMT_CONFIRM	Constants, “YES” or “NO”	A 3	O
17.	MAC key version	SOLOPMT_KEYVERS	MAC key version	N 4	M
18.	Currency code	SOLOPMT_CUR	Local currency (EUR, LTL)	A 3	M

Explanations

A/N=Alphanumeric, i.e. data content is either letters or numbers. The length shows the field’s maximum length.

M=Mandatory data, O=Optional data

For E-Payment Nordea's system supports ISO-8859-1 alphabets. This means, that all the fields must be in this encoding. Also the MAC key must be calculated with the field values in ISO-8859-1. This rule applies only for VERSION: 0002 and 0003. For VERSION 0004 calculated data must be in UTF-8.

In version 0003 the field names may also be sent without the prefix SOLOPMT_. For example, the name VERSION may be used instead of SOLOPMT_VERSION. This also applies to return data.

3.2 Payment request field descriptions

1. The Payment version number specifies the presentation form of the payment data. We accept versions 0002, 0003 and 0004.

2. The Payment specifier is a unique code, given by the service provider, which prevents the payment from being generated twice, for example due to a reload function. The specifier may be a reference number or a combination of date, time and a running code. We recommend to fill this field with timestamp, with additional numbers: “yyyymmddhhmmssxxxx”, where “xxxx” is random number.

3. The Service provider ID is a code given to the service provider by Nordea or legal Id of a service provider. The ID is used to retrieve the beneficiary’s name and account number from the bank’s register for the payment. The ID is stated in the agreement.

4. Destination account number, registered in Nordea. Not mandatory, should be used only if differs from default destination account.

5. Service provider’s name.

6. E-Payment user interface language.

7. Payment amount.

8. Payment reference number. Since e-payment uses a MAC, the reference number must be presented without the grouping and spaces used in the standard reference number presentation form.
   The reference number can be formed from the payment specifier, for example 123456, by calculating a check digit, i.e. the last digit of the reference number, by using multipliers 7-3-1. The specifier's digits are multiplied from right to left, and the products are added up. The sum is then subtracted from the next highest ten, and the remainder is the check digit added to the specifier.

Specifier	1	2	3	4	5	6	
Multiplier	1	3	7	1	3	7	
Product	1	6	21	4	15	42	Sum = 89
Check digit						90	90-89 = **1**

   The reference number is **1234561**

9. Payment tax code, used for Lithuanian payments. Tax code is mandatory if version (value of the field SOLOPMT_VERSION) 0004 is used.

10. Payment due date. If the due date is indicated as 'EXPRESS', the transfer from the service user to the service provider is effective immediately after the service user has accepted the payment. If the due date is later than the current date, the payment is entered into the bank's system and will be paid on the indicated due date. If the due date is not a banking day, the bank's system will affect the payment on the next banking day following the due date.

11. The Payment message must be comprised of maximum 210 characters.

12. Return address is a checkpoint in the service provider's service. The data must comprise the complete URL (uniform recourse locator) address in HTML (hypertext markup language) format, to which the service provider may attach a so-called query-string or parameter data. For example: VALUE=http://product.company.com/order/thankyou.htm OR
    VALUE=http://product.company.com/cgi-in/thankyou?orderno=1234

13. Cancel address is a checkpoint in the service provider's service if the service user wishes to cancel E-Payment. The data must comprise the complete URL address in HTML format, for example:
    VALUE=http://product.company.com/order/invoice.htm

14. Reject address is a checkpoint in the service provider's service if Nordea rejects E-Payment for technical reasons. The data must comprise the complete URL address in HTML format, for example:
    VALUE=http://product.company.com/order/error.htm

15. The MAC calculated from the encrypted data of the identification request and the service provider's MAC key with MD5 or SHA-1 algorithm. The receiver

uses the MAC to confirm the sender and the integrity of the request.

16. If the value is “YES”, the service provider receives information on the payment processing through all return links (payment OK, cancelled, rejected).

17. The key version used for the calculation of the MAC.

18. Three letter uppercase currency code.

3.3 Forming the MAC for the payment request

The payment MAC is calculated as follows:

1. A character string is generated out of the following fields:

   SOLOPMT_VERSION&SOLOPMT_STAMP&SOLOPMT_RCV_ID&↵
   SOLOPMT_AMOUNT&SOLOPMT_REF&SOLOPMT_DATE&↵
   SOLOPMT_CUR&**Service provider’s MAC key**&

   In case of version 0004 Tax code must be included:

   SOLOPMT_VERSION&SOLOPMT_STAMP&SOLOPMT_RCV_ID&↵
   SOLOPMT_AMOUNT&SOLOPMT_REF&
   SOLOPMT_TAX_CODE&SOLOPMT_DATE&↵
   SOLOPMT_CUR&**Service provider’s MAC key**&

2. The character string contains no spaces; the & characters must be included. The data is given in one line. "↵" character indicates line feed in this document.

   Note! The e-payment version is 0003 or 0002 and the data must be presented in the order stated above. Example:
   0003&1998052212254471&12345678&570.00&55&EXPRESS&EUR&LEHTI&

3. Using the MD5 or SHA-1 algorithm, a hash value is calculated from the above character string and converted into a hexadecimal presentation form in which values A–F are given in capital letters, the maximum length of which is 32 characters. The result of the calculation with the above values, using MD5 algorithm, is: **8D6577764DFB36A163EBC5BA6CD73CFB**
   The result of the calculation with the above values, using SHA-1 algorithm, is: **94EE2644B815EFC3BA75B1E4D181D6726A82BCF1**

4. The resulting hash value is entered in the payment MAC field.

The service provider’s MAC is a key provided by the Bank. It is 32 digits long and service provider-specific, and it is delivered by mail after the agreement is made.

3.4 Return message verification

When using the MAC in E-Payment, the service provider can request for additional information on the payment, and a control code for the return message. Thus the service provider’s Internet site can confirm that the returned message resulted from a successful, rejected or cancelled E-Payment.

PLEASE NOTE: The final payment and money transfer still have to be confirmed from the account statement.

If the service provider has asked for additional information on the return link and a control code by giving the value "YES" in the E-Payment field "SOLOPMT_CONFIRM", the E-Payment system inserts the following parameter information in query-string format at the end of the return message (note! field names are written with underline characters):

SOLOPMT_RETURN_VERSION = 0003
SOLOPMT_RETURN_STAMP = code specifying the payment
SOLOPMT_RETURN_REF = payment’s reference number
SOLOPMT_RETURN_PAID = payment code at the bank’s system (new information)
SOLOPMT_RETURN_MAC = return MAC

For version 0004 following fields are used:

SOLOPMT_RETURN_VERSION = 0004
SOLOPMT_RETURN_STAMP = code specifying the payment
SOLOPMT_RETURN_REF = reference number
SOLOPMT_RETURN_PAYER_NAME = payer name
SOLOPMT_RETURN_PAYER_ACCOUNT = payer account
SOLOPMT_RETURN_TAX_CODE = tax code
SOLOPMT_RETURN_MSG = payment details
SOLOPMT_RETURN_PAID = payment code at the bank’s system (new information)
SOLOPMT_RETURN_MAC = return MAC

The return data format (and content) corresponds to the fields in the original payment.

SOLOPMT_RETURN_PAID is new return data for express payments. Its maximum length is 24 digits. For rejected or cancelled payments, the data is not included in the return message.

SOLOPMT_RETURN_MAC is calculated in the same way as in the original E-Payment by generating a character string from the following fields in the return message:

In case of version 0004 following fields must be encoded as UTF-8: PAYER_NAME, PAYER_ACCOUNT, TAX_CODE and MSG.

Example:

```
String PAYER_NAME = "Pärt-Jörpa Mõngastu";
String PAYER_ACCOUNT = "EE291700017000111222";
String TAX_CODE = "123";
String MSG = "Tellimus";
```

```
encodedName = URLEncoder.encode(PAYER_NAME, "UTF-8");
encodedTaxCode = URLEncoder.encode(TAX_CODE, "UTF-8");
encodedMsg = URLEncoder.encode(MSG, "UTF-8");
encodedPayerAccount = URLEncoder.encode(PAYER_ACCOUNT, "UTF-8");
```

Result of this example:

```
encodedName = P%C3%A4rt-J%C3%B6rpa+M%C3%B5ngastu
encodedTaxCode = 123
encodedMsg = Tellimus
encodedPayerAccount = EE291700017000111222
```

SOLOPMT_RETURN_VERSION&↵
SOLOPMT_RETURN_STAMP&SOLOPMT_RETURN_REF&
SOLOPMT_RETURN_PAYER_NAME&SOLOPMT_RETURN_PAYER_ACCOU
NT&SOLOPMT_RETURN_TAX_CODE&SOLOPMT_RETURN_MSG&↵
SOLOPMT_RETURN_PAID&Service provider’s MAC&

The character string contains no spaces; the & characters must be included. The data is given in one line. "↵" character indicates line feed in this document.

Using the MD5 or SHA-1 algorithm (as stated in agreement), a hash value is calculated and converted into a hexadecimal presentation form in which values A–F are given in capital letters, the maximum length of which is 32 characters. This is returned to the service provider in the return parameter SOLOPMT_RETURN_MAC.

Example of the use of the return message and MAC:

0004&201401089876&1232&P%C3%A4rt-
J%C3%B6rpa+M%C3%B5ngastu&EE291700017000111222&123&Tellimus&PEP
M20140108123456789000&partner_key&

Result of previous calculation:

429E5A19BB56FD319F7C1C85773CA72B

Original return link: **http://product.company.com/cgi-bin/thankyou?orderno=1234**

On return to the service provider, the return URL is as follows:
http://product.company.com/cgi-bin/thankyou?orderno=1234&SOLOPMT_RETURN_VERSION=0003&SOLOPMT_RETURN_STAMP=123456&SOLOPMT_RETURN_REF=57834465&SOLOPMT_RETURN_PAID=PEPM960531258874B85991&SOLOPMT_RETURN_MAC=D8DA15F682C56D8BE3C85B7127F83787

3.5 Returning to Service provider system

Service provider and Nordea agree in the way how the data is sent back from Nordea site to Service provider's system.

There are two options:

1. Returning using customer's browser.

   In this case data is being sent on return link provided in field SOLOPMT_RETURN by using browser's form POST method.

2. Returning using server-to-server connection.

   In this case between Nordea system and Service provider's system URL connection is established. Data is being sent on return link provided in field SOLOPMT_RETURN.

   NB! Service provider should be able to handle request from Nordea, when customer after successful payment confirmation clicks in his/her browser on button "Back to partner", because data is being sent back exactly on the same address with the same set of parameters. If Service provider cannot handle such situation, it is possible to provide the additional return link where customer will be redirected. This additional return link will not contain the set of return parameters.

4 E-Payment query

4.1 Introduction

With the E-Payment query function merchants using E-Payment can check that a payment has been accepted and that an express payment has been paid if the situation was unclear.

PS! E-Payment Query must not be used as a tool to decide, wether to provide or not to the customer services and/or products. For that merchant must use return verification message (See § 3.4)

4.2 Using the e-payment query from the merchant's service

The E-Payment query is designed as an automatic, program-based function through which a merchant can make a query of all its payments or of open payments. The merchant's Internet server can, for example, browse orders to which the server has not received normal payment acknowledgements. When there is an order lacking acknowledgement, the server forms a query transaction, which includes the merchant's ID and the payment code and which has been protected for identification and against alteration with a MAC. The query is sent to the bank's server as form in http language using an encrypted SSL connection, and the bank's server will respond in a similar manner. The bank's response will include specific payment identification data in the desired form, if the original buyer has accepted the payment. For express payments the response will also include the identification data of the actual payment.

The response has been formed in such a manner that the merchant's server can handle the response automatically and update the order data.

Since the use of an automatic SSL (https) connection can be inconvenient and troublesome in some situations, these new features of E-Payment can be used with the browser also "manually". This means that the merchant's Internet server has, for example, a service program with which the user of the browser can retrieve the next open order to his browser in the format described above, and the query can be sent to Nordea's server by using the SSL features of the browser (like actual E-Payments). When the user sends the E-Payment query formed by its server to Nordea's server, the response to the E-Payment query will come to the user's browser. It includes a hidden form and a button with which the user can send the response to the Nordea E-Payment query to another server program, which is now able to update the order data. This response also shows the data on the payment in question.

5 E-Payment query message descriptions

5.1 Query request

The payment query request data are in the FORM data group as latent variables.

The data group structure is in HTML:
<FORM METHOD=”POST”
ACTION=”**https://netbank.nordea.com/pnbepay/query.jsp**”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
</FORM>

Form data group					
F#	**Data name**	**Field name**	**Value**	**Data type**	**Mandatory/ Optional**
1.	Payment version	SOLOPMT_VERSION	0001	AN 4	M
2.	Time of query	SOLOPMT_TIMESTMP	in format ”YYYYMMDDHHMMSSnnnn” where nnnn is the ordinal number, if needed	N 18	M
3.	Seller’s ID	SOLOPMT_RCV_ID	Customer legal ID	AN 15	M
4.	Language code	SOLOPMT_LANGUAGE	3= English 4= Estonian 6= Latvian 7=Lithuanian	N 1	M
5.	Response type	SOLOPMT_RESPTYPE	Constants "html" => Response returned in html format "xml" => Response returned in xml format	A 4	M
6.	Additional data for the response	SOLOPMT_RESPDATA	html: If the response should include a form data group, enter the full action address of the form data group here. If the field is empty, no form data group will be linked to the response. xml: If you want another mime type than "text/html" for a response in xml format, specify it in this field.	AN 120	O
7.	Displaying of program-form data	SOLOPMT_RESPDETL	" ": no program-form data to the visible html "Y": program-form data is displayed	A 1	O
8.	Code specifying the original e-payment, which is queried (either stamp or ref obligatory)	SOLOPMT_STAMP	Code of the original payment given by the merchant	N 20	M
9.	Reference specifying the original	SOLOPMT_REF	Standard reference number	AN 20	O

	e-payment, which is queried (either stamp or ref obligatory)				
10.	MAC key version	SOLOPMT_KEYVERS	e.g. 0001	N 4	M
11.	Algorithm	SOLOPMT_ALG	"01"	N 2	M
12.	Payment MAC	SOLOPMT_MAC	The authentication code of the query, SOLOPMT_MAC, is formed from the data in the query.	AN 32	M

An example of MAC calculation:

0001&19991116102459000 1&12345678&4&html&http://158.233.9.9/hsmok.htm&Y&501&0001&01&LEHTI&

NB! Different from E-Payment MAC calculation: If a field is left out (SOLOPMT_REF), the field in question is and the & character are excluded from the MAC calculation.

Result of the calculation, using MD5 algorithm:
2DF7A4A92C0D9D3D13E6C4B1167C5C11

5.2 Query response message format in different situations

If the query does not pass the MAC or other security checks, the response will be an http error message, response status 404, http error 404 URL not found.

If the payment cannot be found or several payments have been made under the same reference, the payment data will not be returned. Instead, an error message “Payment not found” is delivered as a response. The query data will be shown in the program form part (upon request).

Html responses (SOLOPMT_RESPTYPE=”html”):

Plain html response: SOLOPMT_RESPDATA not included.

Plain payment base: SOLOPMT_RESPDETL not included.

Payment base and program form data: SOLO_RESPDETL=”Y”.

Button (”Register”) for transmitting payment data automatically:

SOLO_RESPDATA included.

5.3 Query response codes

- **OK** - Means that payment was found and processed
- **Notfound** - Means that payment was not found
- **Queued** - Means that payments is in the queue and waiting for processing
- **Error -** Other error or payment with given STAMP was not found

6 Testing

The service provider can test the service in production environment even before the agreement is made by using Nordea’s test ID. If the service provider wants to test the service and/or the functionality of the agreement with its own Netbank codes, it must make an agreement that allows direct access to production. However, this agreement can only allow a test address of the service provider during the test period.

Test services,
E-Payment: https://netbank.nordea.com/pnbepaytest/epayn.jsp
E-Payment query: https://netbank.nordea.com/pnbepaytest/query.jsp

Service provider: MAC key: LEHTI

Netbank codes used by the customer in the payment test:

Customer number: 111111

Password: 9999

The service provider’s customer ID (RCV_ID) is 12345678 and the MAC key: LEHTI. The test account is empty.

A test service provider can receive test payments only from a test service user. This means that the payment is not remitted, but the actual process can be simulated.

6.1 E-Payment request test message:

Note: Version 0003 is used, field names are without SOLOPMT_ prefix. MAC is calculated using MAC key „LEHTI“.

Payment request – test message **Form data group**	
Field	**Value**
VERSION	0003
STAMP	1233059715344
RCV_ID	12345678
LANGUAGE	4
AMOUNT	123.45
CUR	EUR
REF	1232
DATE	EXPRESS
MSG	Some message
RETURN	http://test/hep3OK.htm?TESTID=1233059715344
CANCEL	http://test/hep3err.htm
REJECT	http://test/hep3err.htm
CONFIRM	YES
KEYVERS	0001

MAC	A181847555828624E630B3521C215FCC

Following data is returned when test payment shown above is inputted:

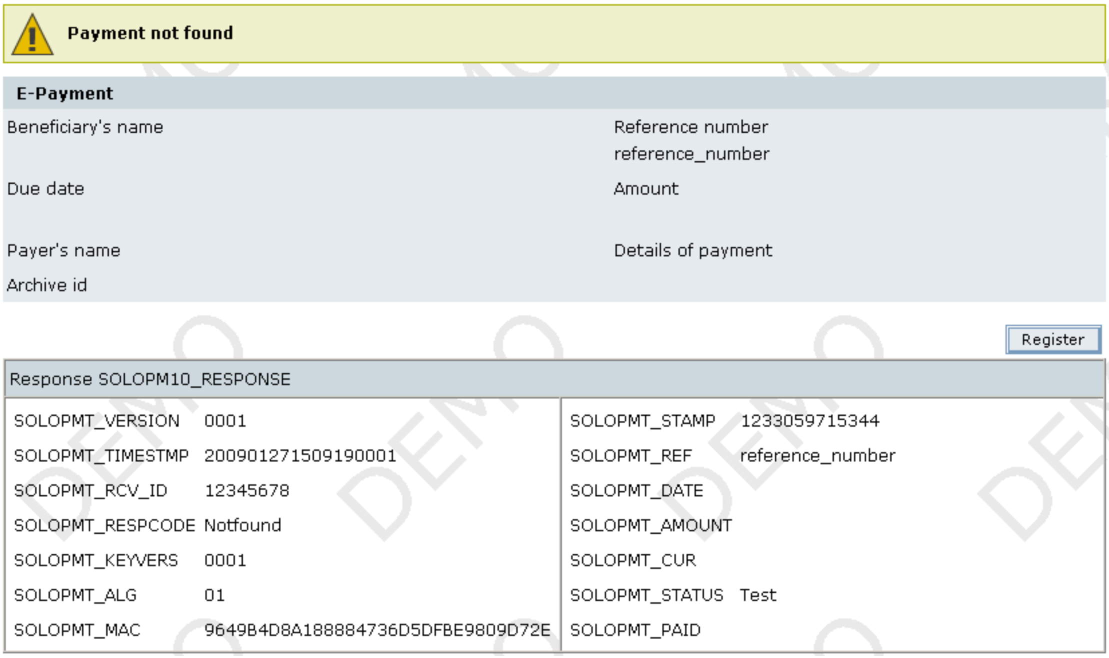
Payment return – test message **Form data group**	
Field	**Value**
RETURN_VERSION	0003
RETURN_STAMP	1233059715344
RETURN_REF	1232
RETURN_PAID	EPM1234567890
RETURN_MAC	2750EC903828892CEAE0F03A35017C02

6.2 E-Payment query request test message

Payment query request – test message **Form data group**	
Field	**Value**
SOLOPMT_VERSION	0001
SOLOPMT_TIMESTMP	200901271459010001
SOLOPMT_RCV_ID	12345678
SOLOPMT_LANGUAGE	4
SOLOPMT_RESPTYPE	xml
SOLOPMT_STAMP	1233059715344
SOLOPMT_REF	1232
SOLOPMT_KEYVERS	0001
SOLOPMT_ALG	01
SOLOPMT_MAC	8A67485B81389C6FF7A63E9A84BF48E7

As test payments are not remitted, returned documents does not contain payment data.

HTML:



Payment not found

E-Payment

Beneficiary's name	Reference number reference_number
Due date	Amount
Payer's name	Details of payment
Archive id	

Response SOLOPM10_RESPONSE

SOLOPMT_VERSION	0001	SOLOPMT_STAMP	1233059715344
SOLOPMT_TIMESTMP	200901271509190001	SOLOPMT_REF	reference_number
SOLOPMT_RCV_ID	12345678	SOLOPMT_DATE	
SOLOPMT_RESPCODE	Notfound	SOLOPMT_AMOUNT	
SOLOPMT_KEYVERS	0001	SOLOPMT_CUR	
SOLOPMT_ALG	01	SOLOPMT_STATUS	Test
SOLOPMT_MAC	9649B4D8A188884736D5DFBE9809D72E	SOLOPMT_PAID	

XML:

```
<SOLOPM10_RESPONSE>
  <SOLOPMT_VERSION>0001</SOLOPMT_VERSION>
  <SOLOPMT_TIMESTMP>200901271503580001</SOLOPMT_TIMESTMP>
  <SOLOPMT_RCV_ID>12345678</SOLOPMT_RCV_ID>
  <SOLOPMT_RESPCODE>Error</SOLOPMT_RESPCODE>
  <SOLOPMT_STAMP>1233059715344</SOLOPMT_STAMP>
  <SOLOPMT_RCV_ACCOUNT />
  <SOLOPMT_REF>1232</SOLOPMT_REF>
  <SOLOPMT_DATE />
  <SOLOPMT_AMOUNT />
  <SOLOPMT_CUR />
  <SOLOPMT_PAID>null</SOLOPMT_PAID>
  <SOLOPMT_STATUS>Prod</SOLOPMT_STATUS>
  <SOLOPMT_KEYVERS>0001</SOLOPMT_KEYVERS>
  <SOLOPMT_ALG>01</SOLOPMT_ALG>
  <SOLOPMT_MAC />
  <RESPONSE_INFO>
     <RESPONSE_TIME>27.01.2009 15:03:53 EEST</RESPONSE_TIME>
  </RESPONSE_INFO>
</SOLOPM10_RESPONSE>
```

7 Contact information

In problem situations call the e-banking help desk for corporate customers on banking days between 8.00 and 17.00:

Estonia: (+372) 6283 260
Latvia: (+371) 6 709 6096
Lithuania: (+370) 5 236 1341