Nordea

E-Identification

Service description
Specification for Baltic countries

Version 1.3

Table of contents

E-Identification

In Nordea's e-identification a service provider uses Nordea's electronic identification solutions to reliably identify its customers on the Internet. In the service Nordea identifies the customer on behalf of the service provider. If so agreed between a customer and the service provider, the identification data transferred in the service can also be used to form a digital signature.

Nordea's e-identification is based on the Tupas standard of the Finnish Bankers' Association. Together with similar services of other Finnish banks the service provider can reach several million Finnish private persons on the Internet and increase its clientele. More information on the standard is documented on the Internet pages of the Finnish Bankers' Association at www.pankkiyhdistys.fi.

1 Overview

1.1 Advantages of E-Identification

Users of Internet services want the services to be user-friendly. One thing that adds user-friendliness is the possibility to use familiar identification methods. With Nordea's E-Identification, a service provider can make use of the same identification solutions that are used in Nordea's Netbank services. E-identification makes all Nordea's Netbank customers potential customers to the service provider.

With E-Identification the service provider can reliably identify its customers without separate customer numbers and passwords. This brings considerable savings to development and maintenance costs.

A service provider and its customer can agree that E-Identification is used in the creation of the customer's digital signature to conclude a legal transaction between them. This allows the customer to send applications to and make agreements with the service provider on the Internet. In a legal transaction, the bank's responsibility in the e-identification is the identification of the customer. The service provider must take care of other issues required in a digital signature, such as the supervision of transmitted information, recording of a return message and immutability of its service.

E-Identification can be used side by side with various PKI certificates. However, e-identification allows Internet services to be customised quite quickly to serve a large clientele, and so companies need not wait for the introduction and adoption by the general public of smart cards for electronic identification.

E-identification increases the safety in online business. For example, with E-Identification the service provider and the customer can agree on a method for making orders and for invoicing. In addition, E-Identification increases the safety of E-payment, because the use of due dated payments is more risk-free if the orderer's identity is confirmed and the order is dated.

1.2 General description of E-Identification

The starting point of the service is a customer who wants to identify him- or herself on the Internet. It is the customer who directs the transfer of his or her information between Nordea and the service provider. Nordea and the service provider are not in direct contact during the service.

The identification given by Nordea is unique. It is traceable to both the service transaction at the service provider's end and to the customer. When a service provider needs to identify a customer, it sends an identification request to him or her. To perform the identification, the customer moves to Nordea's E-Identification service by clicking Nordea's icon. The click transfers the service provider's identification request from the customer to Nordea, who identifies the customer and sends a return message back to him or her.

The customer checks the information in the returned message, accepts it and returns to the service provider's service and continues with its functions. The customer can cancel or reject the identification either before making it or after checking the return message. If the identification is cancelled or rejected, the customer's information is not transmitted to the service provider.

The option to use the identification data in creation of digital signatures is based on a mutual agreement between the customer and the service provider allowing the identification data to be used as part of the digital signature in a legal transaction between them. The use of E-Identification in a digital signature is also supported by the terms and conditions of Nordea's Netbank agreement, the time stamps of the return message and Nordea's log file. If the parties wish to use the service to make agreements or applications, the service provider must take care of other issues required in a digital signature, such as the supervision of transmitted information, recording of a return message and immutability of its service. Nordea is not responsible for the content or the validity of an agreement or other legal transaction between the service provider and the identifying customer.

1.3 Functions of E-Identification

The E-Identification service has different functions and alternative uses depending on the kind of return message that is defined into the service agreement. The return message always includes the name of the customer. Any other transmitted data can be in plain text or encrypted.

If the return message is in plain text, Nordea transmits the customer's complete Personal Identity Number (PIN), or only its control sign, or Business Identity Code (BIC), depending on what has been agreed in the service agreement. A plain text PIN is only transmitted to a service provider who has the right to process it.

If the return message is encrypted, Nordea transmits a Message Authentication Code (MAC) formed of the customer's PIN or BIC to the service provider. The PIN or BIC is not transmitted in the return message. The service provider must have the customer's PIN or BIC so that it can compare it to the data in the return message and establish correct identification. If the service provider doesn't have the customer's PIN or BIC, it must request it before sending an identification request. In other words, this function is suitable for confirming the information given by the customer from the bank.

Functions where the customer's PIN is used are suitable for customer identification, service log-in, and making of binding agreements, among other uses. The control sign of a PIN can be used, for example, in log-in after having registered to a service.

1.4 Usability

The E-Identification service is mainly applicable for Internet services directed at consumers in Baltic countries and Finland. Although the service allows the transfer of company information, the applicability of the service for identification in b-to-b transactions is limited. However, it is applicable for intra-company use.

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

1.5 Security

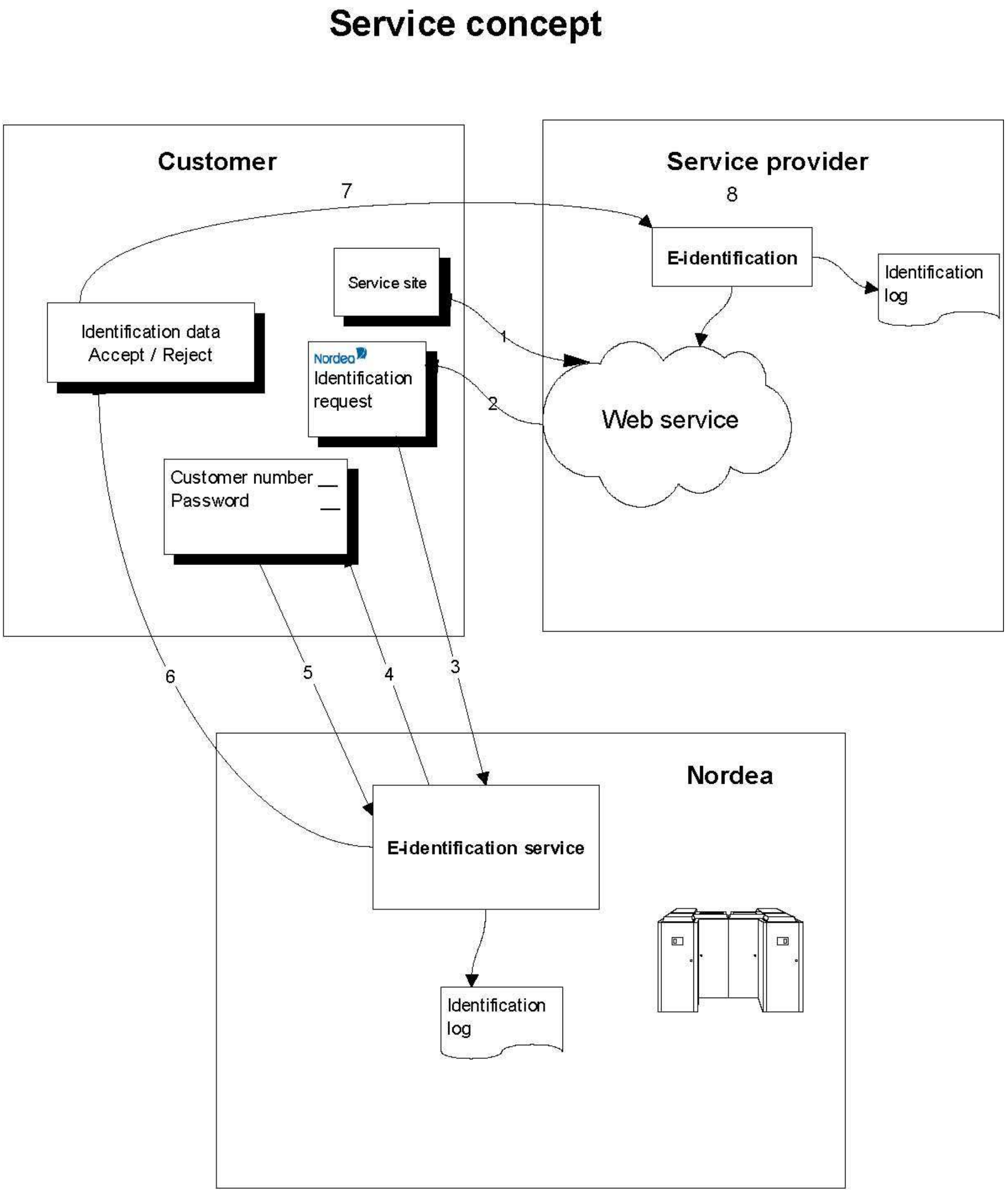
The service uses SSL encryption protocol in the communication between the parties. A third party cannot see or change the data. The service provider’s server software must support 128-bit SSL encryption. However, the key length used in the communication is determined by the properties of the browser used by the customer. The integrity of the data in the identification request and the return message is secured by a MAC, so the customer who directs the transfer of the identification 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. The identifying customer is responsible for safeguarding codes or other identification tools given by Nordea from a third party.

The customer is also responsible for keeping his or her Netbank codes out of reach of outsiders and must ensure that the codes are only given to a computer running Nordea’s identification service. The customer also recognises the service provider from the identification data returned by Nordea and accepts the transfer of the E-Identification.

2 Functional description

2.1 Operational chart



1. An identifying customer contacts the service provider's site. The communication between the customer and the service provider must be SSL encrypted when the customer begins entering his or her data for the identification service. During the stages 2–7 the communication is always SSL encrypted.

2. The service provider sends the customer an identification request with data that specifies the transaction. The service provider's identification request sets Nordea's icon and a cancellation button on the customer's display.

3. The customer clicks the icon, which leads the customer to Nordea's identification service. The identification request transmitted to Nordea includes the data on the service provider and the transaction. Nordea confirms the integrity of the request and the accuracy of the data.

4. If the service provider's identification request is accurate, Nordea sends it on to the customer. If Nordea detects errors in the request, it gives the customer an error message.

5. The customer identifies him- or herself to Nordea. If the identification fails, Nordea gives the customer an error message.

6. After a successful identification Nordea forms a return message. Nordea's service sets acceptance and cancellation buttons for the customer, and sends the return message to the customer's browser.

7. The customer confirms the identification data and accepts the transfer of the identification to the service provider. Or, the customer can reject the identification by clicking the cancellation button and return to the service provider's service.

8. The service provider confirms the integrity and inimitability of the return message. The service provider links the identification to the customer's transaction and stores it for as long as the other service information. The identifications cannot be registered or used for other purposes.

3 Message descriptions

3.1 Identification request

The identification 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/pnbeid/eidn.jsp”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
</FORM>

Form data group				
Field	**Data name**	**Length**	**Mandatory/ Optional**	**Note**
1. Message type	A01Y_ACTION_ID	3 - 4	M	Constant, “701”
2. Version	A01Y_VERS	4	M	Constant, “0002” Standard “0003” With additional information “0004” With personal legal ID and name for corporate clients
3. Service provider ID	A01Y_RCVID	10 -15	M	Customer ID

4. Service language	A01Y_LANGCODE	2	M	ET = Estonian
				LV = Latvian
				LT = Lithuanian
				EN = English

5. Request stamp	A01Y_STAMP	30	M	yyyymmddhhmmssxxxxxx
6. Identification type	A01Y_IDTYPE	2	M	Constant “02”
7. Return address	A01Y_RETLINK	199	M	Return address for successful identification
8. Cancel address	A01Y_CANLINK	199	M	Return address for cancellation
9. Reject address	A01Y_REJLINK	199	M	Return address for error situation
10. MAC key version	A01Y_KEYVERS	4	M	MAC key version
11. Algorithm	A01Y_ALG	2	M	01 = MD5, 02 = SHA-1
12. MAC	A01Y_MAC	32-40	M	Request MAC

Identification request field descriptions

1. Message type: constant "701"

2. Request message version number: constant "0002", "0003", "0004"
   For the case when personal legal ID and name is needed when customer logs in to corporate account, please use version 0004.

3. Service provider's customer ID. Nordea identifies the service provider on the basis of the customer ID and attaches the service provider's name from its customer register to the identification message.

4. The service language code indicates the language version of Nordea's service used by the service provider. The service opens in this language, if it is available for Nordea's E-Identification.

5. The stamp given to the identification request by the service provider that specifies the request. The stamp can be a reference number, customer number, or a combination of the date, time, running stamp and the reference number.

6. The identification type indicates which identification data the service provider wants on the customer. The type must correspond to the function agreed in the service agreement.
   01 = Encrypted basic code. A hexadecimal MAC calculated from the customer's identification data. May include the customer's complete Personal Identity Number (PIN) or Business Identity Code (BIC).
   02 = Plain text basic code. May include the customer's complete Personal Identity Number or Business Identity Code.
   03 = Plain text truncated code. May include the control sign of a Personal Identity Number without the century indicator, or a complete Business Identity Code.
   NB! In current implementation only constant "02" is available.

7. Service provider's Web site address, i.e. the checkpoint for successful identification. The return address must begin with https, i.e. be SSL protected.
   Example: VALUE=https://product.company.com/order/confirmation.html.

8. The checkpoint in the service provider's service, if the customer cancels the transfer of the identification.
   Example: VALUE=https://product.company.com/order/cancellation.html.

9. The checkpoint in the service provider's service, if a technical error has been detected in the identification. The return address can be the same as in the field 10. Example: VALUE=https://product.company.fi/order/error.html.

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

11. The type code of the algorithm used in the calculation of the MAC. Nordea's E-Identification uses 01 = MD5 and 02 = SHA-1 algorithms that produce a 32-

character MAC.

12. The MAC calculated from the encrypted data of the identification request and the service provider’s MAC key with the algorithm given in field 11. The receiver uses the MAC to confirm the sender and the integrity of the request.

3.2 Forming the MAC for the identification request

To add Nordea’s icon on the service provider’s Web page, the service provider forms an identification request which is protected with a MAC. The MAC is calculated from the FORM data group in the request with the MAC key given to the service provider by Nordea.

First, a character string is formed of the VALUES of all the fields in the FORM data group preceding the MAC (fields 1–11) and the service provider’s MAC key. This data is combined into a character string so that any blanks are left out. The data groups of the character string are separated by “&”. ”&” also goes in between the last data group (field 11) and the MAC key, and after the MAC key. The “&” characters are included in the calculation of the message MAC. The data is given in one line. "↵" character indicates line feed in this document.

A01Y_ACTION_ID&A01Y_VERS&A01Y_RCVID&A01Y_LANGCODE&A01Y_STAMP&↵
A01Y_IDTYPE&A01Y_RETLINK&A01Y_CANLINK&A01Y_REJLINK&A01Y_KEYVERS&↵A01Y_ALG&**MAC key**&

The result of the calculation is converted into hexadecimal presentation, in which values A–F are given in capital letters. The hexadecimal hash value is entered in the MAC field.

3.3 Return message and identification

Nordea adds the return message information into the successful identification return address in a query string form.

The MAC is calculated of the original message, after which Scandinavian characters and certain special characters (such as blanks, equal sign and quotation marks) are replaced by the corresponding hexadecimal sign (e.g. %20) for the message.

Nordea calculates the return message MAC with a service provider-specific key. With the MAC the service provider can verify that the identification was formed at the customer’s bank and that the return message data hasn’t changed.

Form data group				
Field	**Data name**	**Length**	**Mandatory/ Optional**	**Note**
1. Version	B02K_VERS	4	M	Constant, same as A01Y_VERS
2. Time stamp	B02K_TIMESTMP	19	M	NNNyyyymmddhhmmssxx
3. Number	B02K_IDNBR	10	M	Identification number given by Nordea
4. Request stamp	B02K_STAMP	30	M	Request field 7 (A01Y_STAMP)
5. Customer	B02K_CUSTNAME	40	M	Name of the customer
5A. Customer	B02K_CUSTNAME _PERSONAL	40	O	Personal name of customer in case if corporate login was used. For version 0004.
6. MAC key version	B02K_KEYVERS	4	M	MAC key version (A01Y_KEYVERS)
7. Algorithm	B02K_ALG	2	M	01 = MD5, 02 = SHA-1
8. Identification	B02K_CUSTID	40	M	Plain text Customer ID (Legal Id)
8A. Identification	B02K_CUSTID_PERSONAL	40	O	Personal Customer ID (Legal Id) in case if corporate login was used. For version 0004.
9. Identification type	B02K_CUSTTYPE	2	M	Constant “01”
10. MAC	B02K_MAC	32-40	M	Request MAC

3.4 Return message field descriptions

1. Return message version: constant “0002”,”0003”,”0004” from the identification request field 2 (A01Y_VERS).

2. Time stamp formed by Nordea, in which NNN is always 200 and which indicates that the message was sent by Nordea. Nordea returns 19 characters in the format NNNyyyymmddhhmmssxx, where the xx at the end indicate one hundredth of a second.

3. A number given to the identification by Nordea’s system, which specifies the identification in Nordea’s system.

4. A stamp specifying the identification request, from the identification request field 7 (A01Y_STAMP).

5. Customer name from Nordea’s customer register.

6. MAC key version, from the identification field 10 (A01Y_KEYVERS).

7. The type code of the algorithm used in the calculation of the MAC. Nordea’s E-Identification uses 01 = MD5 and 02 = SHA-1 algorithms that produce a 32-character MAC. From the identification field 11 (A01Y_ALG).

8. Customer identification. Legal ID is used.

9. Identification type. Indicates the form of the identification in field 8.
   The possible values are:
   00 = not known
   01 = plain text PIN
   02 = plain text control sign of PIN
   03 = plain text BIC
   04 = plain text electronic password. Not used in Nordea.
   05 = encrypted PIN
   06 = encrypted BIC
   NB! In current implementation only constant “01” is available.

3.5 Forming the MAC for the identification return message

When a return message has been received, the service provider checks its integrity by calculating a MAC and comparing it to the message MAC. The MAC is calculated from the fields 1–9 of the return message. In the calculation, the data and the MAC are separated by “&”, and it is also added to the end. The calculation is done with a service provider specific key. The data is given in one line. "↵" character indicates line feed in this document.

B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&B02K_CUST
NAME&↵
B02K_KEYVERS&B02K_ALG&B02K_CUSTID&B02K_CUSTTYPE&MAC
key&

For version 0004 two additional fields containing personal name and legal id are returned. In this case MAC is calculated with those fields included:

B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&B02K_CUST
NAME&B02K_CUSTNAME_PERSONAL↵
B02K_KEYVERS&B02K_ALG&B02K_CUSTID&
B02K_CUSTID_PERSONAL↵&B02K_CUSTTYPE&MAC key&

3.6 MAC verification and customer identification

The service provider calculates a MAC of the received message as described in section 3.6. If it matches the MAC in the bank’s return message, the return message in authentic.

4 Exceptions

The service provider must prepare for exceptions, such as:

1. The customer cancels the identification. The customer can cancel the identification transaction, either before the identification request is transferred to Nordea or after the identification is created, by clicking the “cancel” icon, the address of which is the Cancel address in the FORM data group 8 of the identification request.

2. The identification fails either due to incorrect information given by the customer or because the customer has requested for identification with a wrong bank.

3. Nordea detects an error in the identification request message.

4. The service provider detects an error in the return message. The error may be a content error, or the identification doesn’t correspond to the personal details given by the customer. The service provider must give the customer a note informing of the situation.

5. There is no return message. The break may be caused by an interruption in the communication or other technical failure, or the customer interrupts the session.

6. The same return message is received several times. The service provider should note that the customer may re-send the same return message several times, or he or she may send an old return message when moving back and forth the browser windows with the “next” and “previous” buttons.

5 Changing and storing the MAC

The MAC key used in the MAC calculation can be changed by Nordea’s or service provider’s request.

The key is delivered to the contact person named in the agreement. Together with the key the contact person receives the version number and the effective date of the new key. MACs are calculated with the new key from the effective date on.

To ensure an orderly key change, the service provider must allow the new key to be entered to the system in advance, i.e. simultaneous use of at least two keys. During the changeover, for about 15 minutes, it is possible that some of the identifications received by the service provider are calculated with the old key, and some with the new key.

After a successful use of the new key the old one can be erased or its use be prohibited in the service provider’s system.

The service provider must store the MAC key with care and in a safe place to prevent unauthorised use.

6 Function keys and icons

Only the following names can be used of Nordea in the service provider’s Internet service: Nordea, Nordea Bank.

In the service provider’s Internet service the E-Identification must be indicated by a visibly placed Nordea logo. Either the Nordea logo or the text “Nordea E-Identification” will serve as the icon.

The instructions and terms of the use of Nordea logos and other trademarks are given in the terms and conditions of the service agreement. The logo cannot be handed over to a third party or used for purposes other than that stated in the agreement. It is forbidden to make or form a Nordea logo.

7 Adopting E-Identification

7.1 Requirements

The service provider’s system must be capable of using Internet technology to form an identification request to a service user. After the service user has accepted the transfer of the identification to the service provider, the identification must be linked to the transaction order given by the service user, and it must be stored for as long as the transaction order. The identification cannot be registered or used for other purposes.

The E-Identification service doesn’t require certain Internet server software, but it must support 128-bit SSL encryption.

7.2 Agreements

The service provider makes a written agreement on the use of the E-Identification service with Nordea. The service provider’s information is registered at the bank, and a MAC key is sent to the contact person named in the agreement.

A separate service agreement must be made on each separate service. This also applies to each different function. However, one service can include several functions. Nordea makes agreements on the transfer of Personal Identity Numbers only with service providers who are authorised to register them.

The length of the MAC key and the service provider’s right to register Personal Identity Numbers are noted in the agreement.

The service provider must notify its Nordea branch of any changes in its services or information. The branch will amend the agreement with the changed information when necessary.

7.3 Testing

The adoption date of the service is agreed when the agreement is made.

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.

Address to the Internet test service: https://netbank.nordea.com/pnbeidtest/eidn.jsp

Service provider: MAC key: LEHTI

Netbank codes used by the customer in the identification test:
Customer number: 111111
Password: 9999

7.3.1 E-Identification request test message

Identification request – test message **Form data group**	
Field	**Value**
A01Y_ACTION_ID	701
A01Y_VERS	0002
A01Y_RCVID	87654321 (Latvia 87654321LV, Lithuania 87654321LT)
A01Y_LANGCODE	see description
A01Y_STAMP	see description
A01Y_IDTYPE	02
A01Y_RETLINK	see description
A01Y_CANLINK	see description
A01Y_REJLINK	See description
A01Y_KEYVERS	0001
A01Y_ALG	01 (01 – MD5, 02 – SHA-1)
A01Y_MAC	See description

7.3.2 E-Identification return test message

Identification return – test message **Form data group**	
Field	**Value**
B02K_VERS	0002
B02K_TIMESTMP	Sample test data
B02K_IDNBR	Sample test data
B02K_STAMP	Sample test data
B02K_CUSTNAME	Sample test data
B02K_KEYVERS	see description
B02K_ALG	see description
B02K_CUSTID	Sample test data
B02K_CUSTTYPE	see description
B02K_MAC	see description

8 Characters used in service

The service uses an 8 bit ISO 8859-1 (Latin1) character set. The table below lists the character codes.

æ	%00 %01 %02 %03 %04 %05 %06 %07	0 1 2 3 4 5 6 7	%30 %31 %32 %33 %34 %35 %36 %37	` a b c d e f g	%60 %61 %62 %63 %64 %65 %66 %67	‘ ’ “ ” • – —	%90 %91 %92 %93 %94 %95 %96 %97	À Á Â Ã Ä Å Æ Ç	%c0 %c1 %c2 %c3 %c4 %c5 %c6 %c7	ð ñ ò ó ô õ ö ÷	%f0 %f1 %f2 %f3 %f4 %f5 %f6 %f7
backspace tab linefeed c return	%08 %09 %0a %0b %0c %0d %0e %0f	8 9 : ; < = > ?	%38 %39 %3a %3b %3c %3d %3e %3f	h i j k l m n o	%68 %69 %6a %6b %6c %6d %6e %6f	˜ ™ š › œ Ÿ	%98 %99 %9a %9b %9c %9d %9e %9f	È É Ê Ë Ì Í Î Ï	%c8 %c9 %ca %cb %cc %cd %ce %cf	ø ù ú û ü ý þ ÿ	%f8 %f9 %fa %fb %fc %fd %fe %ff
	%10 %11 %12 %13 %14 %15 %16 %17	@ A B C D E F G	%40 %41 %42 %43 %44 %45 %46 %47	p q r s t u v w	%70 %71 %72 %73 %74 %75 %76 %77	¡ ¢ £ ¥ | §	%a0 %a1 %a2 %a3 %a4 %a5 %a6 %a7	Ð Ñ Ò Ó Ô Õ Ö	%d0 %d1 %d2 %d3 %d4 %d5 %d6 %d7		
	%18 %19 %1a %1b %1c %1d %1e %1f	H I J K L M N O	%48 %49 %4a %4b %4c %4d %4e %4f	x y z { | } ~	%78 %79 %7a %7b %7c %7d %7e %7f	¨ © ª « ¬ ¯ ® –	%a8 %a9 %aa %ab %ac %ad %ae %af	Ø Ù Ú Û Ü Ý Þ ß	%d8 %d9 %da %db %dc %dd %de %df		
Space ! " # $ % & '	%20 %21 %22 %23 %24 %25 %26 %27	P Q R S T U V W	%50 %51 %52 %53 %54 %55 %56 %57	€ ‚ ƒ „ … † ‡	%80 %81 %82 %83 %84 %85 %86 %87	° ± ² ³ ´ µ ¶ ·	%b0 %b1 %b2 %b3 %b4 %b5 %b6 %b7	à á â ã ä å æ ç	%e0 %e1 %e2 %e3 %e4 %e5 %e6 %e7		
( ) * + , - . /	%28 %29 %2a %2b %2c %2d %2e %2f	X Y Z [\ ] ^ _	%58 %59 %5a %5b %5c %5d %5e %5f	ˆ ‰ Š ‹ Œ Ž	%88 %89 %8a %8b %8c %8d %8e %8f	¸ ¹ º » ¼ ½ ¾ ¿	%b8 %b9 %ba %bb %bc %bd %be %bf	è é ê ë ì í î ï	%e8 %e9 %ea %eb %ec %ed %ee %ef		

9 Contact information

In problem situations call the e-banking help desk for corporate customers on banking days between 9:00 and 17:00

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