Nordea

# Corporate Access

# Web Services

**File Transfer Service Description**

# Contents

# 1 General

This document describes the Web Services data communication protocol (hereinafter 'the protocol') for Corporate Access File Transfer customers provided by Nordea (hereinafter 'Nordea' or 'the bank').

Web Services (WS) is Nordea's data communication protocol for file transfer between the bank and its corporate customers. The Web Services protocol is based on common global standards and complies with the definitions of the World Wide Web Consortium (W3C); see *www.W3.org*. In the WS connection, data is always SSL encrypted in the Internet TCP/IP network. Customers are identified by Public Key Infrastructure (PKI) certificates given by the bank. The bank is the issuer of the certificates (Certificate Authority, CA).

The Web Services standard enables Nordea to offer companies a data communication protocol, PKI identification and security specifications in line with the definitions of the Web Services Interoperability Organisation, see *www.ws-i.org*. This document describes the standard in the form applied by Nordea.

The Web Services connection can be used to transmit Cash Management service files listed in the Corporate Access File Transfer Service Description –document.

## 1.1 Web Services

The Web Services protocol is intended for the transmission of Cash Management files such as XML files based on the ISO20022 standard and Corporate Access files. A list of the file types transmitted with the WS connection can be found from Corporate Access File Transfer Service Description – document.

The WS connection is designed for the transmission of files from the customer or to the customer. In WS communication, the customer is the active party that opens the connection whether uploading files to the bank or downloading them from the bank (push-pull communication).

The company needs a bank connection software (Web Services connection client) that supports Nordea compatible Web Services protocol. Nordea does not offer a bank connection software but instead companies should contact software suppliers to obtain a suitable software.

## 1.2 Abbreviations and terms used in the service description

| | |
|---|---|
| WS | Web Services. A *de facto* standard of data communication complying with international specifications such as SOAP and XML. |
| PKI | Public Key Infrastructure. International specification for the identification of a party in communication (Owner of certificate). |
| XML | Extensible Markup Language. Format used, for instance, with the Corporate payments service and in SOAP messages. |
| CA | Certificate Authority. Issuer of the PKI certificate. |
| SSL | Secure Sockets Layer. Encryption scheme used with Internet connections. |
| HTTPS | Hypertext Transfer Protocol Secure. Encrypted version of the http protocol. |
| SOAP | Standardised message format in WS communications. |
| Administrator | An user named in a customer's (company) agreement whom the customer authorises to receive from the bank the user's personal /company-specific identification data based the PKI system. The administrator manages the user rights related to the identification data and attends to other administrative matters on behalf of the customer. |
| User | An user named in a company's agreement who is authorised to use the Cash Management services specified in the agreement. The user can be a different person than the file sender. |
| Deliverer | The party who signs the SOAP message. Authorised to communicate with the bank using the WS connection and to send ApplicationRequest messages signed by the user or to receive ApplicationResponse messages signed by the bank. The sender can be a third party who has an agreement with the company. (Nordea not being a party to this agreement.) |

# 2 Agreement on the use of the Web Services connection

The customer makes an Corporate Cash Management (CCM) agreement with Nordea on the use of the file types and certificate(s) needed for the Web Services connection

In the agreement the parties specify the company and the company's contact person (administrator) who represents the company's user, and if necessary, any other users. By virtue of the agreement the company can upload and download batch files using the Web Services data communication and PKI security protocol.

If the file sender (i.e. signer of SOAP messages) is a third party who has made an agreement with the company, the sender is not a party to the agreement between Nordea and the customer. The authorisation for a service or an account is always verified with the user company's digital signature (ApplicationRequest signature).

## 2.1 Certificates and keys

In Web Services connections, the customer is identified by certificate issued from Nordea.

The customer can download the certificate needed for the Web Services protocol with its bank connection program if it supports the certificate download. In that case, the customer's bank connection program sends the certification request based on the customer's information and the activation code obtained by a SMS. The certificate can also be downloaded by using the *Nordea Security Client (NSC)* which is provided by Nordea.

Nordea recommends that customers primarily download certificates through their bank connection program.

The customer's certificate is with 2-year validity. when it is going to expire, customer can either renew it or download a new certificate.

More specific instructions for download and renew certificates are described in *section 8.*When an user receives a PKI certificate, it must be protected by a PIN entered by the user. It must not be possible to use the certificate without this PIN except when the software otherwise controls the user's user rights reliably. The software can store private keys and allow their usage without a PIN given by the user to enable, for example, automatic connections. In such a case, the bank connection software must control the user role and save the transactions related to the usage of the key in the software's log information. Nordea's system always verifies a service request by the specific certificate and the owner of the certificate is responsible for the requests. When sending a service request, the user (the signer of the file) represents the company that has made the CCM agreement.

In Nordea's agreement database, a certificate is always assigned to a certain person or company. It is the company's responsibility to ensure that the certificates are duly stored and that they are only used in the authorised manner. Backup copies of the certificates, if any, must also be stored in a secure manner.

## 2.2 Prerequisites for using the Web Services connection

- The customer must have a valid CCM agreement with Nordea on the use of the Web Services connection.
- The user must have Signer ID (received from the bank upon concluding the agreement) with which the PKI certificate is downloaded from Nordea to the customer's system. The digital signature based on the certificate, the user identification and the user's authorisation to use the Cash Management service in question are verified by Nordea on the basis of the certificate.
- The company must have the software able to create the digital signature and the bank connection. Payment files to be uploaded or a download request is signed digitally with the private key belonging to the user's[1] or the company's PKI certificate before the bank connection is made. The signature can be created with separate software or with a function integrated in the bank connection program.

The digital signature is created and the bank connection is opened with software that supports a connection that complies with Nordea Web Services protocol description.

Before any messages are sent to the bank, their structural correctness must be ensured and they must be tested; see *section 5*.

A PKI certificate is valid for two years. A bank connection will not be possible with an expired certificate. The bank connection program must track the expiry of the certificates and inform the user

well in advance of a certificate's upcoming expiry. No discontinuities will occur in the service if a certificate is renewed in advance. See *section 3.3* Expiry of certificates.

# 3 Use of certificates and PKI keys

In Web Services connections, the customer is identified with PKI technology and certificates. PKI, Public Key Infrastructure, is an operating model for the use of keys and certificates. This operating model makes use of asymmetric cryptography based on key pairs. It allows the basic forms of secured electronic communication, such as digital signatures, to be employed with the private key of a signer.

'Certificate' refers specifically to certificates in X.509 format issued by Nordea (Certificate Authority). In this confidential relationship there are only two parties, Nordea and the corporate customer. A certificate is issued on the basis of the CCM agreement to person(s) working in the company who have been specified in the company's CCM agreement.

The certificate, or rather the private and public keys belonging to it, is used by the customer to digitally sign files and then by Nordea to identify the customer. The signature allows Nordea to verify that files were confirmed and signed by the person authorised to use the certificate and the corresponding Cash Management service. It also proves that the files were not altered after they were signed.

The PKI certificate is valid for two years, after which it must be renewed.

The application procedure and the guidelines for renewing PKI certificates can be found in *section 8*.

The digital signature is created in the manner described in the banks' common Web Services description, where a XML structure named 'ApplicationRequest' is the object of the signature. ApplicationRequest is a simple XML structure that includes information specifying the customer and the files.

The digital signature is enveloped. It means that the entire content of the message to be signed, including possible files, is covered by the signature. The digital signature both identifies the sender and ensures content integrity. Any modification to the content will break the signature. The modification would be recognised by Nordea's receiving system and the connection would be rejected.

Correspondingly, the bank's system signs an ApplicationResponse message when creating messages to the customer with the Web Services connection. The signature allows the user to ensure that the message has come from an agreement party and that the information has not been modified on the way.

It is possible to duplicate an enveloped signature. In this case, the latter signer signs all of the content and the previous signature.

## 3.1 Customer authentication and authorisation based on digital signature

The authorisation to use the Nordea Cash Management service is based on the digital signature of the SOAP message and ApplicationRequest message, i.e. the company/the user is identified and the authorisation checked from the bank's agreement system.

An ApplicationRequest message signed before the bank connection is delivered inside a SOAP message in its body element. The ApplicationRequest can be signed in advance before transmission.

The SOAP message is signed with the file sender's PKI a maximum of two hours before the bank connection is established. This signature is only an authorisation to use the Web Services connection, not an authorisation to use any Cash Management services. The signing of the SOAP message only ensures that the file sender is authorised to contact the bank's file transfer service through the Web Services connection, to send ApplicationRequest messages signed by the user and to receive ApplicationResponse messages signed by Nordea addressed to the user.

A customer is identified, and user authorisation verified, only on the basis of the company's/user's certificate.

*Image 1* below illustrates the connections between the files to be sent (Payload), the ApplicationRequest to be signed and the SOAP messages sent to Nordea. To avoid interdependencies of nested XML structures, the messages are base64 coded before they are placed as field content.

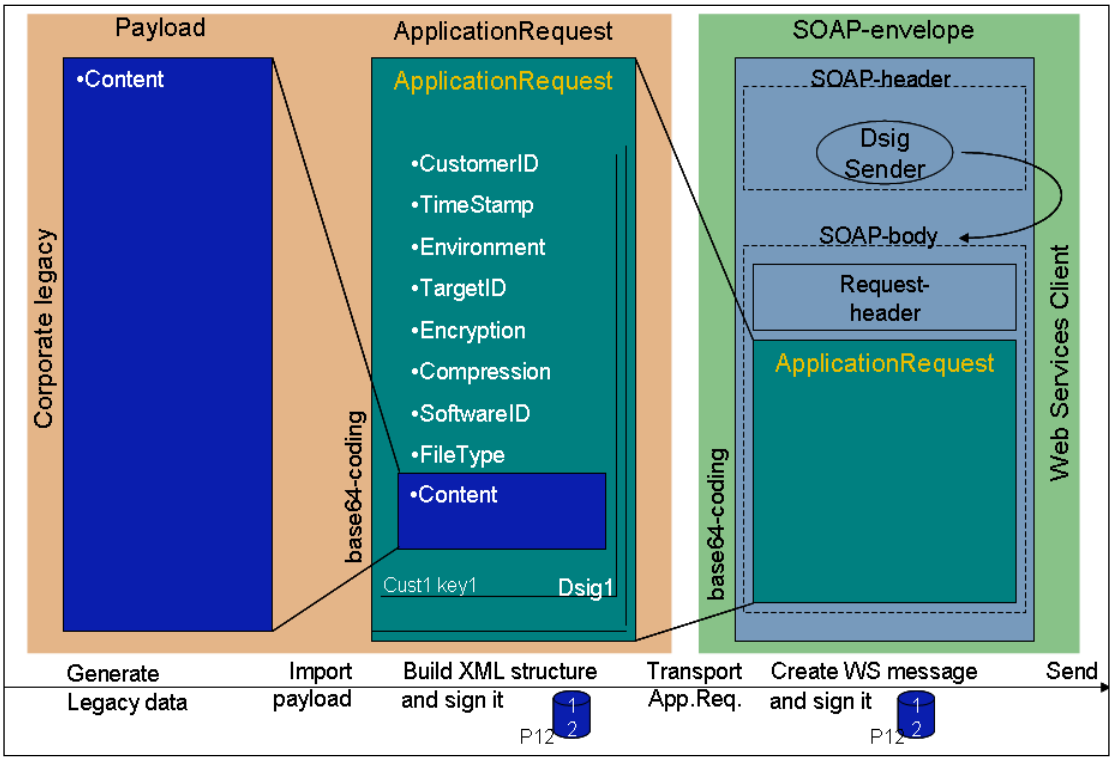


*Image 1*

When the user is also the file sender in the bank connection software, the SOAP message can be signed using the same PKI key with which the ApplicationRequest was signed.

When an user requests a file download from Nordea, the Content field in the ApplicationRequest is skipped. Also in this case the ApplicationRequest must be signed, just as when uploading files to the bank.

The field content of ApplicationRequest is described in more detail in the document *'Secure Envelope Specification'* , which is intended for software houses and vendors.

## 3.2 Invalidation of certificates

If a person authorised in the agreement as the administrator no longer works for the company or no longer does tasks involving bank connections, the person's certificate must be cancelled and the bank must be informed of the new administrator. To invalidate a certificate, and to order a new one, if necessary, the customer must contact Customer support or the Nordea branch. The customer must inform the bank of the Signer ID connected to the certificate. Outside the bank's service hours, **c**all Blocking service to invalidate the certificate. The contact information can be found at https://www.nordea.com/en/our-services/contact-cash-management >>Contacts >> Corporate Netbank contact details and blocking service

## 3.3 Expiry and renewal of certificates

A customer's certificate is valid for two years and must be renewed before its expiry. The bank connection program should monitor the situation and warn the user of the expiry in advance.

The renewal should be done well in advance with the bank connection program if it supports the renewing of certificates. The new certificate can be obtained by signing a certificate request digitally with a valid certificate. Nordea recommends that customers download certificates through their bank connection program.

Nordea Security Client (NSC) also supports the renewing of certificates.

If the certificate has already expired, the customer can request an activation code from Customer support for downloading a new certificate. However, this procedure requires that the customer's CCM agreement has the valid administrator's mobile phone number to which the activation code can be sent as a SMS message.

More information is available in section 8.2.

# 4 General description of the data communication protocol

The Web Services data communication involves the transfer of sessionless request-reply messages. With the Web Services connection the customer's identification data accompany the transmission in every single connection.

The data connection is based on a Web Services standard: The sending and receiving of a XML structure complying with the SOAP specification. SOAP is the standardised message format in the WS connection.

## 4.1 Message structure

A SOAP message contains 'header' and 'body' elements. The body element contains the ApplicationRequest or ApplicationReponose, and is signed with the file sender's key before transmission.

In summary, the Web Services message consists of the following components:

- Service Content, Payload (optional)
- ApplicationRequest, signed, or
- ApplicationResponse, signed
- SOAP envelope, signed (body)

These components are described below in detail.

### 4.1.1 Service Content (Payload)

Service Content is the actual data content aimed for service agreed with the bank. The format of the data is not visible to the Web Services channel because it is base64-coded. This means that any file format (Binary, ASCII, XML etc.) can be transported through the channel.

The content is irrelevant for used transport channel and is presented the same way for example in Corporate Netbank File Transfer. This enables also any backup channel to be used if appropriate identification and authority to use this channel is in place.

The signer of ApplicationRequest must have the authority to deliver this file type to the bank.

This component is optional in the message structure, because ApplicationRequest is used also for requesting data from the bank (DownloadFile, DownloadFileList and GetUserInfo). In this case there is no data to be sent to the bank and thus Content element is empty.

### 4.1.2 ApplicationRequest and ApplicationResponse

ApplicationRequest or ApplicationResponse is a wrapper for transported data (Payload) to enable a XML digital signature to any file type, whether it is a XML, ASCII or binary format. The Payload is inserted in one element, called Content. It is base64-coded to make it loose from ApplicationRequest and ApplicationResponse schema.

ApplicationRequest and ApplicationResponse has some supporting elements for information purposes, like CustomerId, TimeStamp, SoftwareId etc.

The ApplicationRequest is always signed with the private key of the user specified in the agreement. The signed ApplicationRequest is base64 coded and placed in the body element of the SOAP message; see *image 1* in *section 3.1*.

The commands allowed in ApplicationRequest are :

- UploadFile for uploading files to Nordea
- DownloadFile for downloading files from NordeaDownloadFileList downloads a list of files to be

downloaded.

- GetUserInfo downloads agreement specific information on the agreed Cash Management services.

Nordea recommends that the customer perform a GetUserInfo query when adopting the protocol and check that all the services needed are shown in the reply. The response message also includes each file's file type and customer-specific Service IDs related to the files (if applicable) .

| | |
|---|---|
| GetUserInfo | The service will provide the client with information of authorized user file types and service ID's |
| DownloadFileList | The service will provide the client with a list of files that are available for download from Nordea |
| DownloadFile | The service will provide the client with requested files. Downloadable files can be checked by DownloadFileList –service. The query may be:<br>• download single file<br>• download multiple files<br>• download all files of type<br>• download all files<br>File(s) are flagged as downloaded. They can be downloaded again, but will no longer show up as "new files". |
| UploadFile | The Service will provide the transport of the customers file to Nordea. The response from Nordea will be a transport acknowledgement with details regarding the status of the transport.<br>Backend system will process the files in batch mode. This means that the only verification of a file transfer, successful or not, will be a transfer acknowledgement. The client will not usually receive any other notification and the result must be retrieved with a new call later. |

Nordea replies to each Request message with a Response message. For an UploadFile command the ApplicationResponse includes a confirmation that the files have been received or rejected. The different Cash Management services generate status and feedback messages according to their specific timetables. Note that it is possible that the uploaded file is later rejected because of for instance, an insufficient balance on an account.

When the system has failed to verify an ApplicationRequest or a signature, it delivers an error message with a SOAP fault message. However, in most cases the reason for the error is in the data content of the ApplicationResponse message, in which case the system reports a numeric error code and an error text. More detailed information of error codes is available in document "Secure Envelope Specification"

Correspondingly, Nordea replies to a Download request by delivering the requested file(s), base64 coded, in the Content field of an ApplicationResponse. If the requested files are not available, the ApplicationResponse message will include an explanatory error message. Nordea's reply always includes an ApplicationResponse with fields corresponding to those of the ApplicationRequest message; for example, the Content including the file to be downloaded.The ApplicationResponse is always digitally signed by the bank, so that the customer or the customer's software can verify the identity of the sending party and the integrity of the message after it was signed.

The structure of ApplicationRequest, ApplicationResponse messages are described in more detail in the document *'Secure Envelope Specification'* .

### 4.1.3 SOAP Envelope

SOAP envelope is a standard message format used to send and receive requests/responses in Web Services communication, and follows WS-I recommendations. It is always digitally signed with certificate for authority to communicate to bank with Web Services.

It has two parts: SOAP:Header and SOAP:Body.

The SOAP:Header part contains all the information regarding security and signatures. SOAP:Header should include

- the digital signature which is produced by signing the whole SOAP:Body.
- Timestamp element of WS-Security (WSS)

The SOAP:Body part can be divided further in two: RequestHeader and ApplicationRequest.

The ApplicationRequest has been explained detailed above. The field contains the ApplicationRequest XML-structure in base64 coded format, including the payload in any format.

The RequestHeader contains information about the ender, like: SenderId, RequestId, Timestamp, Language, UserAgent and ReceiverId. Those fields are described below.

When SOAP message has been received by Nordea, first the validity of the Sender certificate is checked. If OK then the ApplicationRequest will be extracted and processed further. If the validity of the sender certificate is not OK, then a SOAP fault -message is sent and ApplicationRequest will not be processed.

The following describes each element in SOAP:Body/RequestHeader/ResponseHeader, and how it is used when uploaded/downloaded to/from the bank.

RequestHeader:
SenderId: The unique identification of the sender of this request message. The message sender can be a 3rd party service bureau. This identification is issued and managed by the bank. The SenderId identity is authenticated by the digital signature in the SOAP:Header.
RequestId: The unique identification for this request. This unique ID is copied to the ResponseHeader. This value must be unique for three months.
Timestamp: Time and date when the request was sent. ISODateTime, if no time zone specified, UTC time zone is assumed.
Language: Language attribute is used to request language version for certain information in human readable format. One of the following codes must be used: EN, SV or FI (not used currently).
UserAgent: The name and version of the software which was used to send this request.
ReceiverId: Identification of the receiver of this request message

ResponseHeader:
SenderId: The unique identification of the sender of the original request message for this response
RequestId: The unique identification copied from the original request for this response.
Timestamp: Time and date when the response was sent, ISODateTime
ResponseCode: The code is used to indicate the file delivery condition. The codes are indicated in this Web Services Security and Communication Description. ResponseText:The textual explanation of the condition.
ReceiverId: Identification of the receiver of the original request message for this response (the sender of this response)

## 4.2 Steps for creating and uploading files

The steps needed to create and upload messages are described below.

Usually a bank connection program does these steps without the user seeing them. If files are signed and uploaded with different software, the message is signed in accordance with steps 1–6 and uploaded in accordance with steps 7–9.

See also *image 1* on the interconnection of the messages in *section 4.1.3*.

### 4.2.1 Signing the file

1. Create the payment file in your system. If the file is very large, it must be compressed (see *section 4.1.3*). Convert the file or compressed file into base64 code for the uploading. The file is called ‘Payload’.
2. Create a XML structure called ApplicationRequest.
3. Place the Payload in the Content element of the ApplicationRequest.

4. Digitally sign the whole ApplicationRequest using the certificate and its private key.
5. Convert the signed message into base64 code.
6. Transfer the message to communication software.

### 4.2.2 Uploading the file

7. Place the signed and base64 coded ApplicationRequest in the ApplicationRequest field in the body element of a new SOAP message.
8. Digitally sign the SOAP message with the private key of the file sender's certificate. The key may be the same as the above-mentioned key which was used to sign the ApplicationRequest message.
9. Upload the SOAP message using the WS protocol and wait for a reply from Nordea. Confirm the signature in the reply message and show the content of the ApplicationResponse to the user.

. Nordea's reply includes a status code indicating that the transmission has succeeded (=0) or failed (>0).

### 4.2.3 File compression

If a XML format file sent to the bank, e.g. XML payments includes tens of thousands of transactions, the file must be compressed. Do this before signing and uploading the file. In this way the size of the file can be decreased significantly for the signature process and the transmission.

The supported compression algorithms are GZIP and PKZIP (only the deflate algorithm is supported). Nordea recommends using the GZIP compression algorithm.

The Compression element of the compressed file's ApplicationRequest message must include the value 'true' and the value of the CompressionMethod element must be the name of the compression algorithm, e.g. GZIP.

Feedback on the transmission of the compressed file (e.g. pain.001, pain.002) is not created during the same connection, and it must be downloaded separately.

## 4.3 Downloading files

File downloading is done as described above, but because there are no files to upload, the Content field is skipped. The content of the Command field is GetUserInfo, DownloadFileList or DownloadFile.

Nordea's reply complies with the ApplicationResponse message. If the reply includes the requested file, it is located in the Content field of the ApplicationResponse, base64 coded. The ApplicationResponse is always signed by the bank's system so the customer or the customer's software can verify that the message was sent by the agreed party.

### 4.3.1 Downloading compressed files

Files can be requested as compressed. It is important to do so especially if it is known that the file is very large, for example a XML account statement. The download of a compressed file uses the same principles as the sending of compressed files: the Compression-element must be set to 'true' and the CompressionMethod must contain the algorithm. Only the GZIP algorithm is supported.

## 4.4 Technical instructions for developing bank connection software

Nordea's Web Services data communication protocol is described in more detail in separate instructions. These instructions are mainly intended for companies producing bank connection software to ensure that all the properties and safety features of the Web Services can be complied with accurately.

The instructions are divided into the following classes (the date in the filename extension indicates the latest version and can vary):

1. Web Services Messages

   The security and message specification for a Web Services. The file name is in format Web Services Messages v x.xx yyyymmdd in which 'yyyymmdd' indicates version update.

2. Bank Corporate File Service WSDL (Web Services Description Language)

   aTechnical description of WS client software. This is a configuration file in a XML format created for the automatic processing of a client application. The file name is in the format BankCorporateFileService-yyyymmdd.wsdl, in which 'yyyymmdd' indicates version update.

3. ApplicationRequest-yyyymmdd.xsd and ApplicationResponse-yyyymmdd.xsd

   The banks have common schema files of these XML structures. ‘yyyymmdd’ indicates version update; for example 20080114.

4. Corporate Access Web Services Service Description (this document)

   The description defines Nordea’s requirements for the use of the WS protocol in more detail.

5. Secure Envelope Specification

   The description specifies in detail the message structure and its security features and the field contents in line with Nordea’s requirements.

6. Certificate Management

   The description specifies how to build certificate download and certificate renew functions

7. CertificateService_20100219.WSDL

   Technical description of WS client software for downloading WS certificates. The banks do not have a common procedure for certificate download.

Documents 1, 2 and 3 can be downloaded from the website of the Federation of Finnish Financial Services at *www.fkl.fi*.

Documents 2 and 3 are also available on www.nordea.com >> Corporate Access>> File Communication Service>> Format and implementation

Documents 4 is this document.

Document 5 is available on www.nordea.com >> Corporate Access>> File Communication Service

Document 6 is available on www.nordea.com >> Corporate Access>> File Communication Service

Document 7 is available on www.nordea.fi >> Business >> Services>>Digital Services >> Web Services >> Instructions and sample files >> Testing >> Web Services

# 5 Testing

Nordea offers vendors and developers a possibility to test the WS connection towards production environment to ensure smooth usage later for their customers.

Nordea recommends that, before testing, you read this *Web Services Service Description*,

Nordea is not liable for damage caused by the incorrect functioning of bank connection software and a bank connection software must be tested before implementation.

## 5.1 Testing ApplicationRequest with Corporate Access Test Tool

Customers can use the New Corporate Access Test Tool to validate the ApplicationRequest. In the tool, there is the function to check Secure Envelope which is of the same specification as of ApplicationRequest in Web Services.

In the test tool, both the XML structure and digital signature are verified.

## 5.2 Testing in production using customer's own production certificate

The purpose for testing with customer's production certificate, is to verify in new implementations, that customer material meets the requirements and is validated without errors. All accounts, references and other content of the file should be real production information. Also Cash Management service agreements must be in place.

When testing, customer should start with trying GetUserInfo command, then DownloadFileList and DownloadFile. Only when these commands work ok, customer can proceed with command UploadFile.

Customer support assists in matters related to file testing; see *section 9*.

# 6 Schedules and availability

Web Services is available 24 hours a day, seven days a week.

Note: Web Services is not available during service breaks.

# 7 Web Services production connection address

*Htpps://ws.ebridge.prod.nordea.com/ws/CorporateFileService*

Write the address exactly in the format given above (upper case, lower case). The connection in production environment is always SSL encrypted.

# 8 Technical information of PKI service

## 8.1 Distribution of certificates

Upon making the CCM agreement, the company's representative names the persons authorised to upload and download Cash Management files to and from Nordea with the WS connection.

A certificate request based on the agreement data and one-time activation code can be sent through the Web Services channel. The activation code is delivered as a SMS to a mobile phone number given in advance and stated in the agreement. If the request is correctly formed and accepted, the certificate is returned in a response message and can be saved directly in the bank connection program.

In addition to the download with the bank connection program in the Web Services channel, the certificate can be downloaded using the *Nordea Security Client (NSC)*. The activation code and other necessary information are the same as in the download with the bank connection program.

A certificate downloaded from these services can also be renewed. The renewal request must be submitted before the expiry of the current certificate in order to ensure the uninterrupted use of the services. Only one version of the certificate can be valid at a time, so when a certificate is renewed, the previous one is automatically revoked.

### 8.1.1 Download using own software

Activation code needed for downloading the certificate can be obtained by calling Customer support. The administrator's mobile phone number is saved in the bank's agreement database for the delivery of a 10-digit activation code, which is sent as a SMS message to this mobile phone number. The message is normally delivered during the same working day, and the code is valid for 7 days.

Nordea recommends that customers primarily download certificates through their bank connection program.

The administrator enters the CCM agreement data which is added to the data of the signed certificate:

- company name
- Signer ID
- country code (two letters, e.g. DK, FI, NO, SE )
- activation code from the SMS message

The bank connection program creates a key pair and sends the public key to Nordea for signing. If the request is accepted, the program receives the certificate which it will use in subsequent bank connections. The old certificate can no longer be used after this.

If the first request returns an error because of an invalid company name, rectify the data on the basis of the error response data, recreate the certificate and use the same activation code.

The address of the automatic certificate service in production environment is:
*https://filetransfer.nordea.com/services/CertificateService/sha2*

The process is described in more detail in the document "Certificate Management" intended for software houses, vendors.

### 8.1.2.Download using Nordea Security Client (NSC)

The certificate can be downloaded to the customer's system by using the *Nordea Security Client (NSC)* which is provided by Nordea. Only the Windows environment is supported.

Identification data for downloading, such as name and Signer ID, are found in the CCM agreement. The one-time activation code is received as a SMS message to the administrator's mobile phone number indicated in the agreement.

In order to use the certificate in the bank connection software, you must give the software access to the certificate file. More detailed instructions are available in each bank connection program's own instructions.

You can save the certificate to an USB memory stick, in which case no copy of the certificate will be saved on the hard drive. The USB stick can also serve as a backup copy if it is stored in a secure place. If the certificate is temporarily saved on the hard drive, it should be deleted after use for security reasons. Take a backup copy and delete the copies from the hard drive.

## 8.2 Renewal of a certificate

A PKI certificate used in the Web Services protocol is valid for two years. After the expiry of a certificate it cannot be used for bank connections. The certificate must be renewed before the expiry of the certificate currently in use. Nordea recommends that a new certificate is downloaded at least one month before the expiry of the current certificate. The bank connection program should warn the user of the expiry of the certificate well in advance.

Nordea's Web Services connection supervises the expiry of the certificate and add a remark concerning the matter to SOAP and ApplicationRequest messages if there is less than one month to the expiry of the certificate. When the response code is 0 and the text corresponding to it is 'OK', the remark is added after 'OK' message. The remark indicates the number of days left until expiry. All bank connection programs do not perhaps show this text, but they write it in the contact log.

A bank connection program can renew the certificate by signing the renewal request with a valid certificate.

Nordea Security Client (NSC) also supports the renewing of certificates.

When a certificate is renewed, the previous certificate is simultaneously revoked. A new certificate can be downloaded at any time, but only one certificate is valid at a time. If the certificate has already expired, you must order an activation code by calling the Customer support.

More detailed information can be found from the document "Certificate Management".

## 8.3 Security instructions

A password linked to the certificate's private key must always be used to protect the certificate when it is used for digital signing. Certificates and their private keys must only be kept in the hands of their proper owners so prevent the inappropriate use of the certificate.

Orders made with the customer's certificate are always considered having been made by the customer, so the certificate and the computer together with the software in which the certificate is saved must be properly and securely protected at all times. A customer is identified, and the user authorisation verified, only on the basis of the certificate.

# 9 Customer support

## Denmark

**Service Support for Corporate Access**

| Telephone number/E-Mail | Banking hours | |
|---|---|---|
| (+45) 70 33 65 00<br><br>cn.support@nordea.dk | Monday - Friday | 8.00 to 17.00 CET |
| Local network charge/mobile call charge or international call charge | | |

## Finland

**Service Support for Corporate Access**

| Telephone number/E-Mail | Banking hours | |
|---|---|---|
| (+358) 200 67210 (Finnish)<br>(+358) 200 67230 (English) | Monday – Friday<br>Monday – Friday | 7.00 to 16.00 CET<br>8.00 to 15.30 CET |
| Local network charge/mobile call charge or international call charge | | |

## Norway

**Service Support for Corporate Access**

| Telephone number/E-Mail | Banking hours | |
|---|---|---|
| (+47) 91 50 60 02 - choice 3 | Monday - Friday | 8.00 to 17.00 CET |
| Local network charge/mobile call charge or international call charge | | |

## Sweden

**Service Support for Corporate Access**

| Telephone number/E-Mail | Banking hours | |
|---|---|---|
| (+46) 771 77 69 91 | Monday - Friday | 8.00 to 17.00 CET |
| Local network charge/mobile call charge or international call charge | | |

# 10 Additional information

More detailed information on the service is available at *www.nordea.com/CorporateAccess*