Corporate Access File Transfer

Service Description

Version 1.2

09/11/2017

This document describes the characteristics and usage of the Corporate Access File Transfer service, which is for transferring cash management files (e.g. a payment file) between Nordea and a corporate customer via a public network. Technical details, such as Secure Envelope specification and communication protocol dependent instructions are explained in a separate, related document.

Contents

1 Introduction

File transfer is used for exchanging files and messages via a network in Sweden, Denmark and Norway. Nordea's file transfer service in Corporate Access is called Corporate Access File Transfer (CAF). CAF is the entry point for Nordea customers, and supports various file transfer protocols and different cash management file formats. The service is used by customers' banking software products for automatic host-to-host file transfer and for manual up- and download of files through the Corporate Netbank (CN) user interface.

Besides the secure exchange of files, CAF also includes a user interface for a set of additional services to view the status of file transfers. With the user interface the customer can view the status, a history of transferred files. Manual File Transfer can also be used in cases when a backup channel for host-to-host channel is needed. The user interface is provided via Corporate Netbank service.

This document describes the usage of the Corporate Access File Transfer service.

Technical details regarding connectivity and end-to-end security in file transfer are described in a separate document called "Secure Envelope specification". The latest version of the Corporate Access File Transfer documentation can be found at www.nordea.com/corporateaccess.

2 Prerequisites for using Corporate Access File Transfer

2.1 Agreement

Before the file transfer service can be used, an agreement (Corporate Cash Management Agreement with a CAF eService) must be signed by the customer.

In CAF, the customer is assigned a unique SenderID, used to determine from and to which party files should be transferred.

For authorising access to the Corproate Access services, SignerIDs are created in CAF.

The customer can choose to use host-to-host communication only, or in combination with the user interface via Corporate Netbank (CN). CN offers additional tools for users to view the file transfer status and maintain files. In CN the customer's administrator can appoint users to have access to manual file transfer services.

2.2 Certificates

In CAF it is possible to create one or more SignerIDs. Each SignerID is associated with a unique certificate. This certificate is used to digitally sign the Secure Envelope (if used) before sending files to Nordea.

The persons who receives the certificate activation code for each SignerID are named by the corporate administrator in CCM agreement.

When Nordea receives files, authorisation for customers to use a cash management

service is always verified by the bank from the digital signature of the Secure Envelope. If authorisation fails, the files are rejected and a response is sent to the customer.

Further information about the certificate download process can be found in the document "Certificate Management" available at nordea.com/corporateaccess.

2.3 Bank connectivity software

Files are sent to Nordea using bank connectivity software which supports one of the available communication protocols. Software to enable automatic transfer of files to Nordea Corporate Access can be obtained from software vendors.

Alternatively, files can be sent and retrieved from the bank manually by using Nordea Corporate Netbank File transfer.

Before the connection is established, the file to be uploaded to the bank must be signed digitally using the private key linked to the user/company's certificate. The digital signature can be created:

a) in the ERP system where the actual file is created (recommended)

b) using separate software from a third party vendor, or

c) using a function integrated in the bank connectivity program.

Alternative a) is the most secure, enabling end-to-end security, including the corporate customer's own internal network, because the file content is protected from the moment it was created.

As part of the onboarding to CAF, the files created by the ERP and bank connectivity software needs to be verified using the validation tools provided by Nordea at nordea.com/corporateaccess. See section 4.1 Testing.

2.4 Character set and encoding

The files sent to Nordea must be in UTF-8 format and Nordea will use UTF-8 format for all Messages sent to customers.

3 Schedules and availability

Files can be uploaded and downloaded 24 hours a day, seven days a week. The execution of uploaded files will not happen in real-time, so the processing and response schedules vary depending on the service. Further information about schedules can be found in the respective service descriptions in Nordea.com.

Nordea will have scheduled service breaks in Corporate Access. The file transfer service is not available during these periods. The breaks are scheduled to take place at night and over the weekend, when traffic is very limited. Such service breaks will be announced according to Nordea's policy.

4 Corporate Access File Transfer connectivity

CAF can be reached via different communication methods:

- sFTP
- AS2
- FTP(VPN)
- Corporate Access Web Services
- Corporate Netbank File Transfer
- SWIFTNET FileAct

For more information, see fact sheets for the each method on www.nordea.com/corporateaccess.

4.1 Testing

It is possible to test the Secure Envelope with online connection by uploading the signed file with a browser to the CAF Test Tool. The link can be found at www.nordea.com/corporateaccess.

Bank connection software must be tested with Nordea's test system before it can be used in production. The connection with the test environment uses test certificates and other Nordea test IDs.

4.2 Security instruction

Certificates and their private keys are solely for their proper owners, who must safe-guard against inappropriate use of the certificate.

Orders made using the customer's certificate are always assumed to have been issued by the customer, therefore the certificate and the computer, along with the software in which the certificate is saved, must be properly and securely protected.

5 Customer support

Nordea provides support for CAF. You can find more information on how to get help, Q&A, and Support contact information at nordea.com/corporateaccess.

Appendix A Abbreviations and terms used in the service description

The following table provides a list of commonly used abbreviations and terms in this document.

CAF	Corporate Access File Transfer. A global data communication hub at Nordea complying with international specifications such as PKI 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 payments service and in Secure Envelope messages.
UI	User Interface. Usually an online manual service used with a browser.
CA	Certificate Authority. Issuer of a PKI certificate.
SSL	Secure Sockets Layer. Encryption scheme used with Internet connections.
HTTPS	Hypertext Transfer Protocol Secure. Encrypted version of the http protocol.
CAF Administrator	A special user named in the CCM Agreement, who has access to the self-administration user interface for CAF.
User	A user using the service on behalf of the company. In host-to-host channels there are no users from an agreement perspective, but users may be assigned by the company administrator to connect to services via online UI
SignerID	The party (company) that owns the digitally signed content to be sent. One agreement can have several signers, represented by SignerID's, each with their own signing certificate. Signature is an XML digital signature made with PKI keys, given to the party by the bank.
SenderID	The party (company) that actually sends the message. Authorised to communicate with the bank using the connection and to send files signed by the SignerID.
Certificate	A key pair with private and public keys. The private key is used by the signer to digitally sign the content (payload). The public key is included in the signature element. The Certificate is connected to the SignerID in the CAF eService of the CCM agreement.
CN	An abbreviation of Corporate Netbank. Also CN FT: a manual File Transfer in Corporate Netbank
SWIFTNet FileAct ID	In SWIFTNet FileAct a Security Envelope is not mandatory and if not used, then the user can use only one SignerID which is used as default. The used SignerID is agreed in agreement schedule as FileAct ID.

Appendix B Available File types

File to Nordea	File type	Supported Countries	Comments
Corporate Access Payments	NDCAPXMLI	DK, NO, SE	pain.001.001.03
Corporate Access Cancellation	NDCAPCANXMLI	DK, NO, SE	camt.055.001.01

File from Nordea	File type	Supported Countries	Comments
Corporate Access Payments Feedback	NDCAPXMLO	DK, NO, SE	pain.002.001.03
Corporate Access Debit Advices	NDCAPXMLD54O	DK, NO, SE	camt.054.001.02 (Debit)
Corporate Access Response of Investigation	NDCAPCANXMLO	DK, NO, SE	camt.029.001.01
SWIFT MT940	NDSWMT940O	All countries	MT940
SWIFT MT941	NDSWMT941O	All countries	MT941
SWIFT MT942	NDSWMT942	All countries	MT942

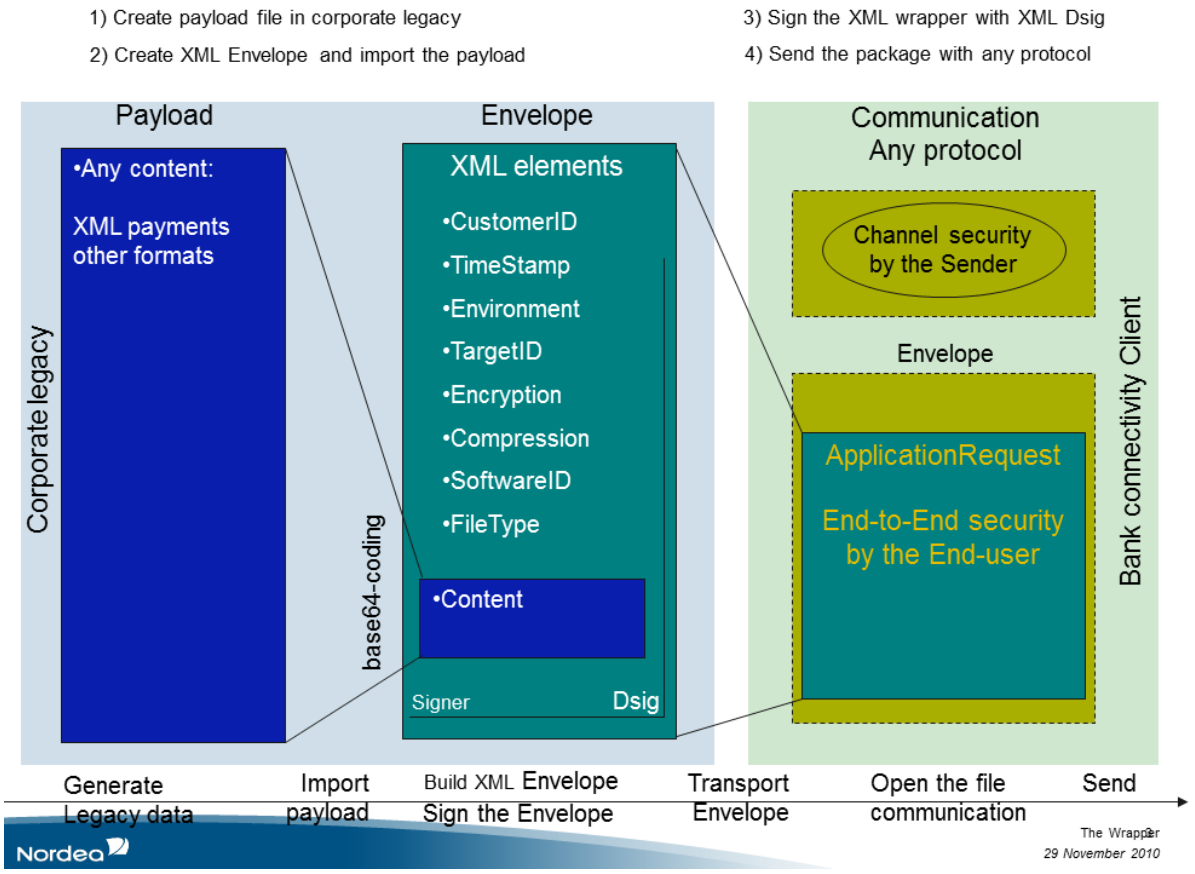
Appendix C Data communication in Corporate Access File Transfer

The following describes the data communication process steps.

Identification of the user and authorisation to use the service

Authorisation to use the Nordea Cash Management file-based services in Corporate Access is based on the digital signature of the content and the Secure Envelope. The Secure Envelope is signed in advance before transmission. It can be used in all file transfer channels connected to Corporate Access. It is mandatory in other channels but optional when using CN manual file transfer. For SWIFTNet FileAct connections special rules applies.

picture below describes connections between the file to be sent (the payload) and the Secure Envelope based on ApplicationRequest schema, to be signed and sent to Nordea. To avoid interdependencies of nested XML structures the payload message is base64 coded before it is placed as text in the content element.



Use of certificates and PKI keys in bank connections

In CAF, the customer is identified by using Public Key Infrastructure (PKI) certificates. The certificates referred to here are in X.509 format and issued by Nordea. Those certificates are created in the CAF eService.

The certificate is used by the customer to digitally sign the file and by Nordea to identify the customer. Nordea can use the signature to verify that files signed by the company authorised

to use the certificate and the requested cash management service. It also proves that the files were not altered after they were signed.

The file-based certificate is valid for two years, after which it must be renewed. For more information on the management of certificates, please see the document "Certificate Management" on nordea.com/corporateaccess.

The digital signature both identifies the signer and ensures content integrity. Any modification to the content invalidates the signature, which would be recognised by Nordea's receiving system. In such cases file would be rejected.

Correspondingly, the bank's system signs the Secure Envelope using Nordea's certificate, when sending files to the customer. The signature provides assurance to the user that the message has come from an agreed party and that the information has not been altered during transmission.

While the Secure Envelope ensures the identification of parties and integrity control of the message, confidentiality is achieved via encrypted communication lines.

General description of data communication protocols

Corporate Access File Transfer data communication consists of various protocols in push-push or push-pull mode.

Push-Push protocol means that a party that wants to send data over the internet establishes a connection. The bank can then set up a connection and transport data, such as an account statement, to the customer. The bank must have customer-specific IP addresses and keys registered to be able to set up the connection. The customer must allow the bank to connect via their firewall. Typical push-push protocols include ftp, sFTP, AS2 and SWIFTNet FileAct.

Push-Pull protocol means the bank server does not connect to the customer, but the customer server connects to the bank when requesting data, such as account statements from the bank. In push-pull connections, the bank does not need to maintain customer-specific information about IP addresses and customer server keys, and no firewall opening is needed. Typical push-pull connections include Web Services, and manual File Transfer in Corporate Netbank.

A Secure Envelope is used in all the protocols mentioned above, including in manual file transfer in Corporate Netbank. The Secure Envelope is optional in manual file transfer. If not used, the payment transactions must be confirmed manually via netbank UI after transmission The exception is SWIFTNet FileAct where the Secure Envelope cannot be used, but files may still be pre-confirmed.

Nordea replies to each request message with a response message. When managing very large files, the creation of a response message may take some time.

Technical instructions for bank connection software

In addition to this service description, CAF and data communication protocols are described in more detail in separate documents. These guidelines are mainly intended for companies producing bank connection software and are available at nordea.com/corporateaccess. The documentation is divided up as follows:

1. *Secure Envelope Specification*
   This specification is used to develop software for creating a Security Envelope and digital signature for files to be sent to Nordea Corporate Access.
2. *Protocol specification documents for sFTP, SWIFTNet FileAct, Web Services and AS2.*
   These specification documents can be used to develop or configure banking software communicating with Nordea Corporate Access. The documents are available at nordea.com/filetransfer
3. *Technical documentation for testing*

   This document specifies how testing can be performed at Nordea using one or multiple alternatives.