

Secure Envelope specification

for Corporate Access File Transfer

Version 1.1

This document defines how a file (e.g. a payment file) which will be sent to the bank is digitally signed by the content owner. It also describes how a file received from the bank is digitally signed by Nordea. Digital signature is used for authentication and integrity control of the file. This model is used in Nordea's Global File Transfer solution.

Contents

1	Introduction.....	2
2	Background.....	2
3	Requirements	2
4	The Secure Envelope structure and elements used.....	3
4.1	ApplicationRequest	3
4.2	Application request description.....	5
4.3	ApplicationResponse.....	8
4.4	ApplicationResponse description.....	10
5	Security	12
5.1	XML Digital signature	12
5.2	Type of digital signature	12
5.3	Download of Signer ID certificate	13
5.4	Encryption	13
6	The file transfer process.....	13
6.1	Sending a file to bank.....	13
6.2	Receiving a file from bank.....	15
7	Service providers	16
7.1	A 3 rd party acting on behalf of the End-Customer	16
7.2	A VANS operator acting as a mailman / transporter	16
8	Testing	17
9	Vocabulary and abbreviations used.....	17
10	Contact information	18
	Appendix A Error codes	19
	Appendix B File types for Corporate Access	20
	Appendix C Application Request Syntax description	21
	Appendix D Application response Syntax description.....	27
	Appendix E The difference between Corporate Access Secure envelope and the Finnish national Web Services / ApplicationRequest.	31

1 Introduction

File transfer is used for exchanging files and messages via a network. Nordea's new file transfer service for its corporate customers' cash management files is called Corporate Access File Transfer. Corporate Access File Transfer will be the entry point for Nordic and Baltic customers, and will support various file transfer protocols and different file formats, including XML SEPA payments in the ISO20022 standard.

This specification describes how to protect file content using a digitally signed Secure Envelope, which is transported over different available communication protocols. All files exchanged through Nordea Corporate Access are digitally signed according to the specification in this document independent of the channel/protocol used.

This specification of securing the file content will not change or alter the security in any of the communication channels.

All example files, schema files, demo certificate etc. can be found from Nordea web site (www.nordea.com): Home /Our services /Cash Management /Our solutions /Corporate Access

<http://www.nordea.com/en/our-services/cashmanagement/oursolutions/corporateaccess/>

2 Background

Files which are to be exchanged with a bank are in a specified file format and layout according to the requested service (e.g. payments). Normally the file format specification does not include security elements. To enable end-to-end security of a file, Nordea introduces a content signature model called Secure Envelope which is described in this document. With the Secure Envelope, security will be part of the content, i.e. related to the content owner instead of the communication channel owner.

The new security model is based on PKI and XML digital signature technologies, which both are global standards. The XML structure, called Secure Envelope, is described in following chapters. Any file, whether it is XML, ASCII or binary, can be transported by using the Secure Envelope. Once the customer have added his/her digital signature to the Secure Envelope and thereby to the file, the file can be securely transported via any channel/protocol to Nordea.

3 Requirements

The sending of digitally signed files requires:

- Software which creates the Secure Envelope according to this specification
- Software to create a digital signature for the Secure Envelope

- File content (i.e. the payment file)
- PKI keys, i.e. the certificate. The certificate can be downloaded from Nordea (PKI X509 Certificate issued by Nordea)
 - Alt 1: Software to download the certificate via Web Services call
 - Alt 2: Manual download of the certificate through a browser

4 The Secure Envelope structure and elements used

The Secure Envelope described here is a XML structure following a public schema. The Secure envelope contains the file to be sent, and is digitally signed. The schema is based on an open specification and used in other contexts as well. The Secure Envelope is part of an open specification for Web Services, publicly available via Bankers' Association in Finland. The schema can be requested from Nordea, or downloaded via Nordea's open webpages. See chapter "Contact information".

The schema contains several elements, some mandatory and some optional (marked in the following picture with dotted lines). Nordea requires information for some optional elements, like Command and Signature. Below you will find a definition of each element used when sending and receiving files with Nordea Corporate Access. The rule is that one Secure Envelope is present for each physical file (the payload) . In case files are compressed, these files still forms one physical file of the same file type. The customer signature authorisation is then connected to that file, type of file and service.

4.1 ApplicationRequest

When sending a file to the bank, the Secure Envelope uses a schema called ApplicationRequest. It will use namespaces from <http://www.w3.org/2001/XMLSchema> and <http://www.w3.org/2000/09/xmldsig#>.

Below is a picture (Figure 1) showing the ApplicationRequest schema.

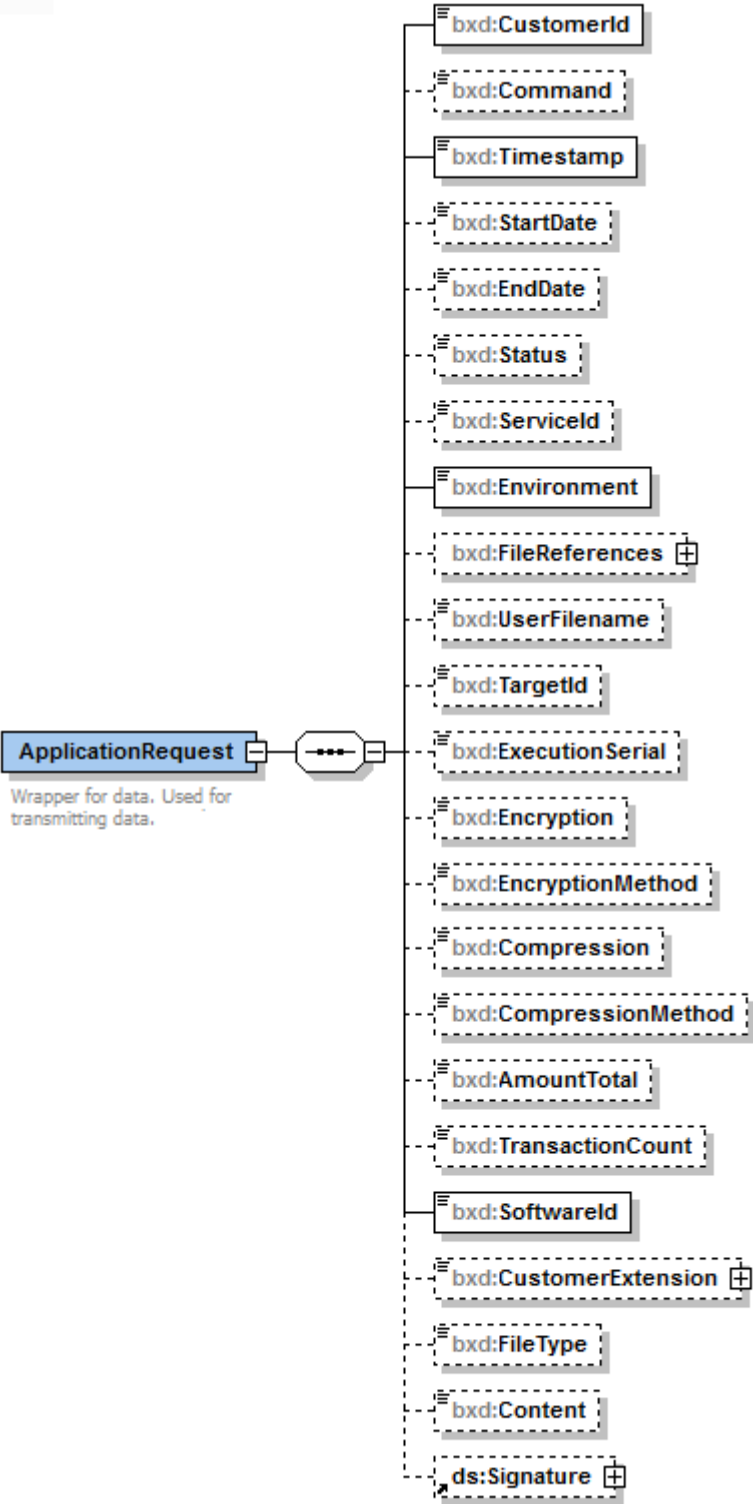


Figure 1

Some of elements in the schema are not used by Nordea Corporate Access, but may be used by other banks or in other contexts. The elements used when uploading a file to a bank are explained in the table below. The elements are marked with (M) if they are mandatory for Nordea, even if they are not a mandatory in the schema. Elements used should not be left empty.

The Secure Envelope will be used also for queries in push-pull protocols like Web Services/ApplicationRequest.

4.2 Application request description

Element name	M/O	Description
CustomerID (Numeric data)	M	<p>The content for this element is found in the file communication customer agreement as “Sender ID”. Each agreement contains only one Sender ID.</p> <p>In some special cases, when the signer of the content uses another party for transporting the signed file, this field contains the Sender ID of the other party.</p>
Command (Reserved words, not case sensitive)	M	<p>The command is dependent on the case used. When sending a file to the bank, the command is “UploadFile”.</p> <p>Simillarry if using a pull channel like Web Services, the command is DownloadFile”.</p>
Timestamp (Data Type: ISODateTime)	M	<p>Creation time of the ApplicationRequest Secure Envelope. UTC or local time. Example: 2014-06-03T14:45:35.424+03:00</p> <p>Valid values Current date -7 days, +1 day</p>
StartDate (Data Type: ISODateTime)	O	<p>When requesting data from the bank with the DownloadFileList operation, this element can be used to specify filtering criteria.</p>
EndDate (Data Type: ISODateTime)	O	<p>When requesting data from the bank with the DownloadFileList operation, this element can be used to specify filtering criteria.</p>
Status (Reserved words, case sensitive)	M	<p>When requesting data from the bank with the DownloadFileList operation, this element must be used as filtering criteria. One of the following codes are possible to use: NEW, DLD, ALL.</p> <p>Note! For compatibility reasons the word DOWNLOADED will be accepted instead of DLD.</p>

ServiceId	O	Currently not in use. Reserved for future use.
Environment (Reserved words, case sensitive)	M	This field specifies how the request will be handled. Currently the content of this field must be "PRODUCTION". "TEST" is <u>not</u> implemented, and will not be allowed in production.
UserFileName (String, not case sensitive)	O	A name given to the payload file by the customer. The value is stored in the bank and shown in the Online interface.
TargetId (Numeric data)	M	The content for this element is found in the File Communication Customer Agreement as "Signer ID". Each agreement may contain several Signer ID's. Each Signer ID is connected to a certain content signing certificate. The Signer ID authenticates the identity and the authorisation to the content or file type according to the agreement. This element is mandatory in all operations. There can be only one Signer ID in a SecureEnvelope.
ExecutionSerial (String, not case sensitive)	O	An identifier given by the customer to identify that particular request. The value is used only by the customer, and it is usually returned in the response file. Please note that the last character in the value cannot be the character '\'
Encryption (String, case sensitive)	O	If this element is present and the content is "false" (case-sensitive) it means that the uploaded content is not encrypted (or the requested data should not be encrypted by the bank). The value "true" is not implemented yet. If the value is "true", it means that the file is encrypted before base64 coding, but after possible compression. The value 'true' will be rejected for now.
EncryptionMethod (String, not case sensitive)	O	Will be defined later. Example: DES, 3DES, RSA, PGP
Compression	O	Compression indicator for the content. If this element is present and the content is

(String, case sensitive)		<p>"false" (case-sensitive) it means that the uploaded / downloaded content is not compressed.</p> <p>The value "true" indicates that the uploaded or downloaded content is compressed. In this case the compression method element must also have a value. Files are to be compressed before possible encryption and before base64 coding.</p> <p>It is recommended to always compress files. If this element is not present, files bigger than 1MB will be compressed.</p>
CompressionMethod (String, not case sensitive)	O	If compression is set to "true" there must be a value in CompressionMethod. At this stage only the value 'GZIP' is supported. It means that the Compression algorithm is RFC1952 GZIP.
SoftwareId (String, not case sensitive)	M	This element contains the name and version of the client side software which generated the ApplicationRequest Secure Envelope. It is used for statistics and customer support purposes. Example: "ABC Soft, version 1.0"
FileType (Reserved words, case sensitive)	M	<p>Specifies uniquely the type of file in the request. Available file types are specified in Appendix B</p> <p>Example: "NDCAPXMLI" for XML pain.001 to Corporate Access Payable.</p>
Content (Base64 coded)	M	<p>The actual payload file in the UploadFile operation. The content is in base64 encoded format. Only one logical file can be included in the content element.</p> <p>In the future it will be possible to encrypt the payload. Then the payload must be encrypted before inserting the compressed or encrypted file into the Content element. If a file is to be both compressed and encrypted, please make the compression first. .</p>
Signature http://www.w3.org/2000/09/xmldsig#	M	This element is created by the signature operation of the client software. It is recommended that the signature is calculated in the ERP system, or immediately after

		<p>creating the file to be protected.</p> <p>The signature is specified by the XML Digital Signature standard by W3C.</p> <p>This element is mandatory when sending requests to the bank, since it is used for integrity verification of the file content and authentication of the content owner. This element is defined as optional in the schema because the recipient can remove the signature element after verification of the signature, before schema validation.</p> <p><u>The public key of the used signing certificate must always be provided in the signature element.</u></p>
--	--	---

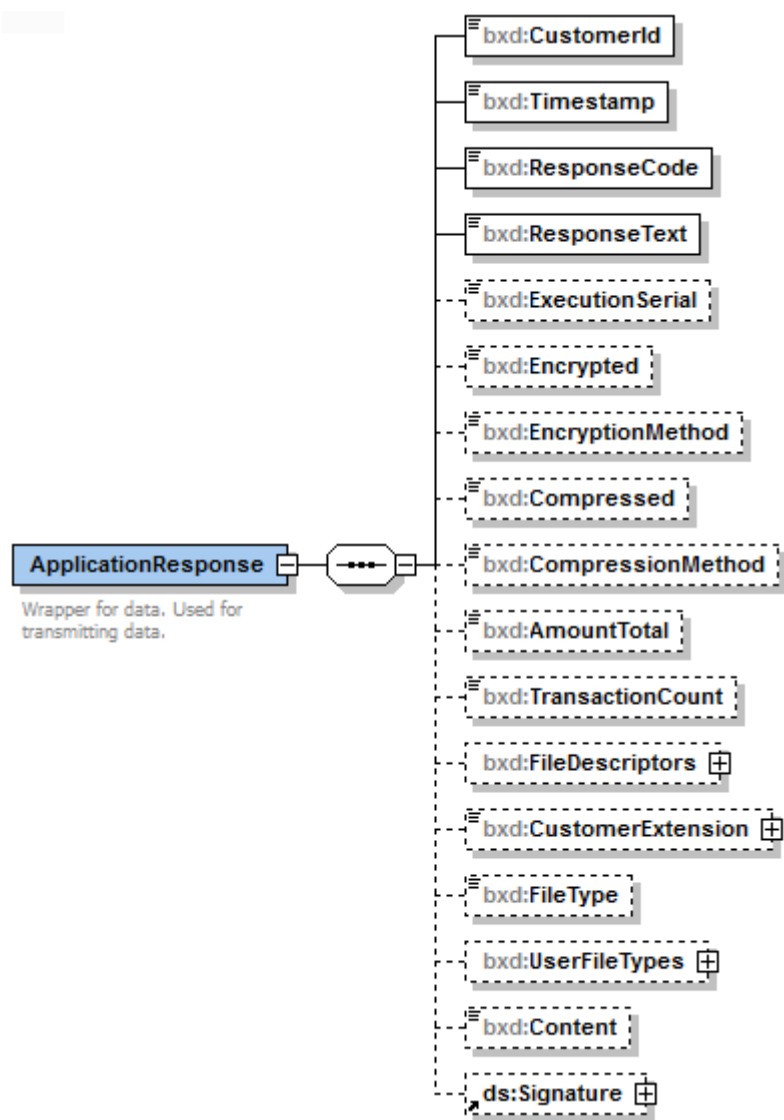
An example of signed ApplicationRequest is available at www.nordea.com:

4.3 ApplicationResponse

When receiving a file from the bank the Secure Envelope uses a schema called ApplicationResponse.

Below is a picture (Figure 2) showing ApplicationResponse schema.

Figure 2



Secure Envelope (using ApplicationResponse schema) is always used when files are transported from Bank to Customer. It enables XML digital signature to any file type, whether it is in XML, ASCII or binary format. The payload file is inserted into the element called Content. The payload file is base64 coded to make it independent of the ApplicationResponse schema. ApplicationResponse has some supporting elements for information purposes, like returned CustomerID, Timestamp, ResponseCode, Compression etc. Application response is used to enable file integrity and to validate that the message is received from the correct party.

4.4 ApplicationResponse description

Element name	Description
CustomerID (Numeric data)	This element contains the receiving customer's "Sender ID" as in ApplicationRequest.
Timestamp (ISODatetime)	The time when the ApplicationResponse was created. Data Type: ISODatetime, UTC. Example: 2014-06-03Z14:45:35.424
ResponseCode (Numeric data)	The content of this field is 0 if no error has been detected. Any error will generate an error code defined in Appendix A.
ResponseText (String)	The content of this field is 'OK' if the ResponseCode was 0. If there is an error a short text will appear describing the error as defined in Appendix A.
ExecutionSerial (String)	An identifier given by the customer is returned in response. Otherwise 0 (zero).
Encrypted (String, case sensitive)	Default: 'false'. The value "true" is not implemented yet. If this element is present and the content is "true" (case-sensitive) it means that the received Content is encrypted with the algorithm specified in EncryptionMethod element. The content should be decrypted after base64 decoding. The decrypted content may be compressed.
EncryptionMethod	To be defined later. Example: DES, 3DES, RSA,

(String)	PGP
Compressed (String, case sensitive)	Default: 'true'. Compression indicator for the content. If this element is present and the content is "true" (case-sensitive) it means that the received content is compressed using the algorithm shown in CompressionMethod element. Decompressing is the last action to be performed to the payload, after base64 decoding and possible decryption.
CompressionMethod (String)	Only the value 'GZIP' is supported. It means that the compression algorithm is RFC1952 GZIP.
Filetype (String, case sensitive)	Specifies uniquely the type of file to be received (e.g. pain.002 status message). File types are specified in appendix B. Example: "NDCAPXMLO" as pain.002 from Corporate Access Payable.
Content (Base64 encoded)	The actual file received from the bank. The content is base64 encoded. Nordea may compress the files sent to the customer, especially if the file is large. In that case the "compressed" flag is set to 'true' and the value 'GZIP' is entered in the CompressionMethod element. The receiver should verify the "compressed" flag and if 'true', decompress the payload after base64 decoding. In the future it will be possible to encrypt the payload. Then the "encrypted" flag will show if the file is to be processed accordingly and decrypted with the algorithm stated in EncryptionMethod.
Signature http://www.w3.org/2000/09/xmldsig#	This element is created by the signature operation in the bank. The signing process uses Nordea-specific CA and Nordea's content signing certificate. The CA certificate for the signing certificate is available at Nordea Open pages, or by request from Nordea. The signature is specified by the XML Digital Signature standard by W3C. This element will always contain Nordea's public key of the signing certificate will.

An example of signed ApplicationResponse is available at www.nordea.com.

5 Security

5.1 XML Digital signature

XML Digital Signature must be added to the Secure Envelope for all files sent to or received from Nordea Corporate Access File Transfer. However, there may be a transition period during which digital signature may not be necessary for some legacy file types.

In the new Corporate Access Payables payment process the Secure Envelope must always be signed, enabling STP (Straight Thru Processing). Any payment files for Corporate Access Payables will be considered as pre-confirmed by this digital signature, and therefore processed as soon as they have been received by the bank.

Later on Corporate Access Payables will add some functionality enabling manual confirmation via a user interface, if so requested. Then the file processing will be halted until a user makes the final confirmation.

Please note that all files sent via manual File Transfer, like Corporate Netbank File Transfer, to Corporate Access Payables, must be digitally signed until manual confirmation via the user interface is available.

5.2 Type of digital signature

XMLDsig is of type Enveloped, i.e. it signs the whole XML structure (Application-Request or ApplicationResponse). It is specified by W3C (<http://www.w3.org/TR/xmlldsig-core/>) and consists of a signature element in the <http://www.w3.org/2000/09/xmlldsig#> namespace.

The signature must contain the following elements with associated child elements: SignedInfo, SignatureValue and KeyInfo. KeyInfo should contain X509Data as well as the child element X509Certificate, including the customer's public key of the signing certificate.

Software for creating a Secure Envelope with digital signature can be purchased on the market. Please contact Nordea to get a list of possible vendors. If software development is part of the company's own area of activity and competence, it is relatively easy to build it as well.

Please see www.nordea.com for an example file with a valid signature.

See more information from:

<http://www.w3.org/TR/xmlldsig-core/>

http://en.wikipedia.org/wiki/XML_Signature

5.3 Download of Signer ID certificate

The Signer ID certificate must be downloaded either by

- Web Services request

The WSDL for download Certificate can be found here:

http://www.nordea.fi/Images/60-88699/CertificateService_20100219.zip

CertApplicationrequestschema:

<http://www.nordea.fi/Images/60-88711/CertApplicationRequest.zip>

CertApplicationresponseschema:

<http://www.nordea.fi/Images/60-88716/CertApplicationResponse.zip>

- With a separate software offered by Nordea

The certificate download process is described in details in the document Certificate management for Corporate Access File Transfer

5.4 Encryption

Encryption is currently not implemented and will be described later.

6 The file transfer process

6.1 Sending a file to bank

The file transfer process can be divided in different parts. The three main ones are:

1. Creating the file content to be sent e.g. pain.001 XML payment
2. Locking the file, i.e. signing the file content with XML digital signature, using the content signing security key
3. Moving the signed file to the communication software, which connects to a bank server and transports the signed file into Nordea using a file communication protocol security solution and key(s).

Depending on the infrastructure and legacy solutions in the company, the steps above can be carried out in different systems, or using just one solution.

The first step: The file content is usually created in a corporate legacy and the file type must follow the specifications of the requested service (i.e. a message implementation guideline).

Step nr 2 is described below:

After creation of the payload file, a Secure Envelope following the ApplicationRequest schema is created, according to the instructions in chapter 4.

The payload will be entered into the element called 'Content' of type base64Binary. The base64 coding hides the actual content format from the Secure Envelope. Thereby the content can be in binary, or XML or any other format.

The Secure Envelope model allows the encrypting and/or compressing of the payload. Encryption is not supported yet.

All needed elements must have specified values according to chapter 4. After that the Secure Envelope with payload can be locked, i.e. digitally signed by using customer content signing PKI key. Once it is locked the payload is protected against any changes from the moment of signing, until it is received by Nordea Corporate Access File Transfer. This is called integrity control.

The signature also uniquely defines the signing party of the payload, i.e. the content owner. Authentication of the customer is based on the content signature.

The signed Secure Envelope can be now sent to Nordea by any supported file transfer protocol.

Banking software is used to initiate a secure communication, using customer specific communication security key(s) received from Nordea. The key or keys are dependent on which communication protocol is used. Some communication protocols use PKI keys and others for example UserID & Password. However, the content signing key is always a PKI key and normally not used as the communication security key.

The different communication protocols (sFTP, AS2, Web Services or SwiftNet File-Act) are not described here. See specific communication description documents at www.nordea.com.

See Figure 2 below, which describes the steps in creating a payload file and a Secure Envelope, signing the Secure Envelope and sending it by any communication protocol to Nordea.

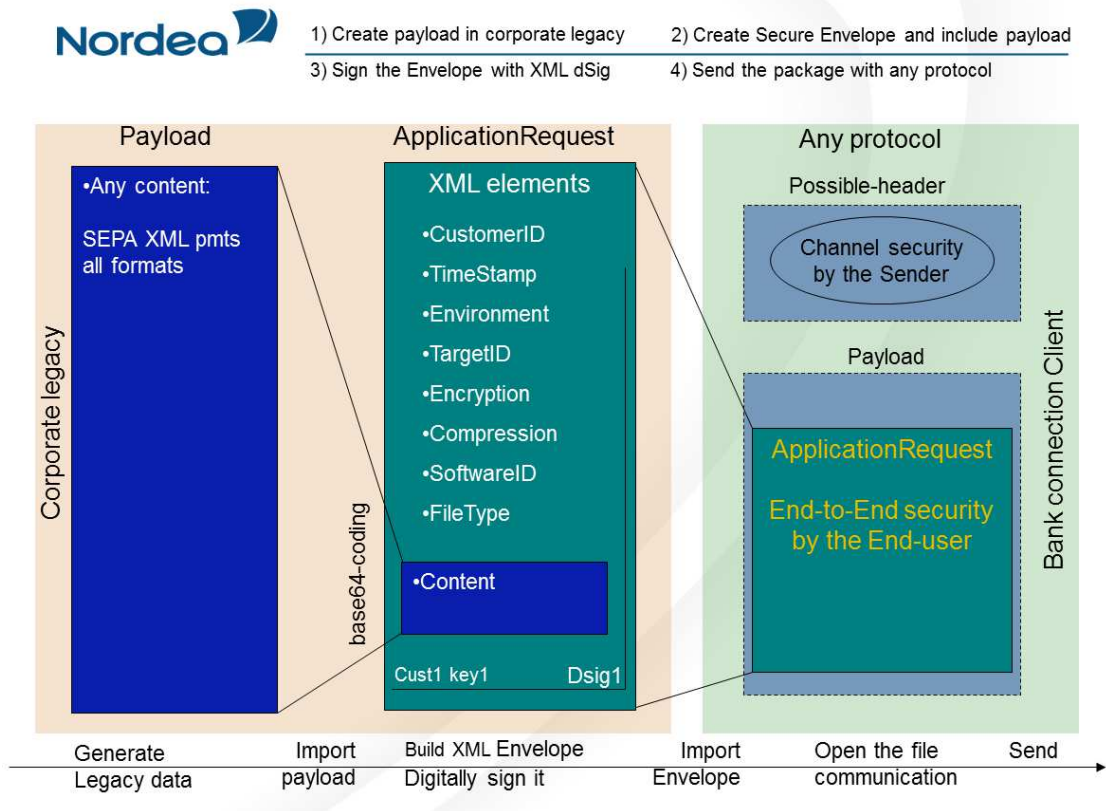


Figure 2

Normally a legacy system at the bank which received the file from the customer will send the customer a status message. A status message file may indicate that a sent file has been received by the bank, state the result after validation of the payload, etc. There may be multiple status messages created during the legacy process. See chapter 6.2.

6.2 Receiving a file from bank

Depending on which protocol is used, files from the bank are either sent to customer (push-push protocol), or made available for customer to retrieve them (push-pull protocol like Web Services).

The receiving of a file from Nordea is also based on a Secure Envelope, following ApplicationResponse schema. The signer in this case is Nordea and the receiver has a possibility to authenticate the real content signer by verifying the signature validity. Nordea provides the CA keys needed for this verification.

The signature ensures that the payload content created by Nordea is not changed by anyone. Any, even the smallest change of the content, would invalidate the signature. If so happens there is an additional channel/protocol independent integrity and authentication control mechanism for the customer. The process of creating Secure Envelope in the bank follows the same steps as in chapter “Sending files to the bank”. However,

the ApplicationResponse schema is different from the ApplicationRequest schema (see chapter 4).

The receiver of the Secure Envelope should first verify the signature, and then look into the elements in the Secure Envelope. If the response contains a (requested) payload, it may be encrypted and/or compressed following the values in the respective elements.

The response file may also contain an error message, in which case the ResponseCode-element in the Secure Envelope contains a value other than zero. The different error messages based on values are described in Appendix A.

The actual payload file can be extracted from the Secure Envelope by carrying out base64 decoding to the file in the Contentelement.

7 Service providers

7.1 A 3rd party acting on behalf of the End-Customer

A company or an entrepreneur may outsource the handling of cash management payables and receivables to a so-called third party. The 3rd party is thus acting on behalf of the end-customer. An example of this is a book-keeping agency which manages several customers' payables/receivables.

Another example could be a company with a "payment factory", where one legal unit manages payables and receivables on behalf of other units in the same company.

If a 3rd party is to create payment files using the end-customer's debit account on behalf of the end-customer, the end-customer must give the 3rd party power of attorney (PoA). Then the end-customer adds the Signer ID of the 3rd party to the service agreement. The PoA must be registered and be available at Nordea.

When the 3rd party sends a payment file, the signature in the Secure Envelope belongs to 3rd party, but the debit account in payment file may belong to end-customer. The authorization to use the debit account is verified before execution of the payment transactions, and a valid PoA must exist. If the PoA will be cancelled, it must be registered in Nordea, respectively.

When a 3rd party is sending files to Nordea, they must have an agreement with Nordea for file transfer. By that they will receive their own Sender ID and one or several Sign ID's/Certificates. If they will use any of the services, like payment services for their own purposes, they will need an agreement for that service as well.

7.2 A VANS operator acting as a mailman / transporter

In some cases the customer who owns the content, i.e. signs the Secure Envelope with their own certificate (connected to respective Sign ID), may not send the actual file themselves or via 3rd part communication. The technical file transfer via a dedicated protocol and channel security is done by an outsourced party, the 4th party, instead.

This requires that the 4th party has an agreement for file communication with Nordea, and that the Secure Envelope includes the Sender ID of that 4th party.

In this case either the end-customer or the third party (with PoA) is the content owner, and signs the Secure Envelope with their certificate. Before locking the Secure Envelope with their signature, the content owner enters the Sender ID of the 4th party, in the Customer ID element of the Secure Envelope. Nordea will not need a PoA to verify if a technical transport provider sends signed Secure Envelopes on behalf of the content owner, but the Customer ID shows that there is an agreement between content owner and file transfer provider. This scenario is applicable only for sending files to a bank, not vice versa.

8 Testing

A demo/test certificate in p12 format can be downloaded from www.nordea.com. Demo certificate can be used to validate the signature processes and correctness of the signature by sending the message to our test tool. The pin code for Demo certificate is WSNDEA1234.

The secure envelope can be validated towards our online test tool. The link to test tool is available on www.nordea.com.

9 Vocabulary and abbreviations used

CustomerID	Identifier provided by Nordea ("Sender ID") to identify a sender/customer in a file communication agreement.
Signature	A digital signature signing the content using a PKI key. An authorised signer may use the signature to pre-confirm payments. Also signig the SOAP envelope in Web Services.
Signer	A bank customer who has an agreement and authorisation to create a digital signature for the payload (e.g. a payment file), by using a customer-specific certificate/PKI key. In the response file Nordea is the signer.
File (Content, Payload, Message)	The message which is to be exchanged, e.g. a Credit Transfer initiation message. It should follow the Message Implementation Guideline (MIG) published by Nordea. The file content is sometimes referred to as the payload, i.e. the meaningful data to be transported.
File type	A pre-defined string entered in the Secure Envelope, introducing the type of file in the Content element, to be sent or retrieved to/from the specific service in the bank.

3 rd party	A bank customer who has a power of attorney from another bank customer, to act on the latter's behalf. An example is a book-keeping agency making payments on behalf of another customer.
ApplicationRequest	A name of a schema used for the Secure Envelope containing the file and signature to be sent to the bank.
ApplicationResponse	A name of a schema used for the Secure Envelope containing the file and signature to be received from the bank.
PKI	Public Key Infrastructure. A standard process for managing asymmetric key handling in digital signatures.

10 Contact information

All documentation for implementing and using Corporate Access File Transfer can be found on www.nordea.com where also contact information of the Support can be found.

Questions regarding content of this specification can be sent to:

ERPsupport@nordea.com

Appendix A

Error codes

Error	Name	Remarks
00	OK	
02	SOAP signature error	signature verification failed
03	SOAP signature error	
04	SOAP signature error	
05	Operation unknown	
07	SenderID not found	
08	SenderID locked	
12	Schema validation failed.	XML Envelope is not valid
14	CustomerID locked.	Sender ID
15	CustomerID outdated.	Sender ID
18	Content digital signature not	Signer ID
19	Content certificate not valid.	Signer ID
20	Content type not valid.	The content type does not match the file type
21	Deflate error.	Decompression of content not possible
22	Decrypt error.	Decryption of content not possible
23	Content processing error.	Error during content compliance check
24	Content not found.	Content element is missing
26	Technical error.	
29	Invalid parameters.	Invalid value found in Envelope
30	Authentication failed.	Sender ID or Signer ID unknown
31	Duplicate message rejected	
33	Error in customer information	
35	Authorisation failed	Signer ID not allowed for this file type
36	Technical error, contact bank helpdesk	Reserved for later use
37	Technical error with processing application request	please check application request

Errors 02-08 are especially related to SOAP level in Web Services

Appendix B

File types for Corporate Access


All Corporate Access file types should be supported by the receiving software and communication system.

Files to Nordea	File type	Comments/Filename
Corporate Access Payment file. Pain.001	NDCAPXMLI	Any Filename
Payment file cancellation file Camt.055	NDCAPCANXMLI	Available autumn 2016

Files from Nordea	File type	Comments/ Filename example
Corporate Access feedback file. Pain.002	NDCAPXMLO	NDCAPXMLO_0000123456-R_20150215-123456
Corporate Access Debit advice. Camt54	NDCAPXMLD54O	NDCAPXMLD54O_0000123456-R_20150215-123456
Payment cancellation feedback Camt.029	NDCAPCANXMLO	Available Autumn 2016

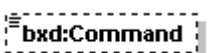
Standard file name in some channels for reply files within Corporate Access will be following the filename convention: Filetype_TrackID_DATE_timestamp.xml.
“TrackID” is a Nordea specific identifier for a file that can be used in support cases between Nordea and customers.

Appendix C


Diagram	
Nordea rule: Mandatory	SenderID Example: 1205585055
Type	restriction of xs:string
properties	isRef 0 content simple nillable false
Facets	minLength 1 maxLength 16

Application Request Syntax description element **ApplicationRequest/CustomerId**


element **ApplicationRequest/Command**

diagram	
Nordea rule: Mandatory	Example: UploadFile
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple nillable false
facets	minLength 1 maxLength 32

element **ApplicationRequest/Timestamp**

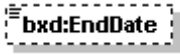
diagram	
Nordea rule: Mandatory	UTC or local time. Example: 2014-06-03T14:45:35.424+03:00 Valid values Current date -7 days, +1 day
type	xs:dateTime
properties	isRef 0 content simple

element **ApplicationRequest/StartDate**


diagram	
Nordea rule: Optional	Data Type: ISODate Example: 2008-06-03 (yyyy-mm-dd)
type	xs:date

properties	isRef	0
	minOcc	0
	maxOcc	1
	content	simple
	nillable	false

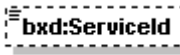
element ApplicationRequest/EndDate

diagram	
Nordea rule: Optional	Data Type: ISODate Example: 2008-06-03
type	xs:date
properties	isRef 0 minOcc 0 maxOcc 1 content simple


element ApplicationRequest/Status

diagram	
Nordea rule: Optional Mandatory in Download-FileList	When requesting data from the bank with the DownloadFileList operation, this element must be used as filtering criteria. One of the following codes are possible to use: NEW, DLD, ALL. Example: ALL
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 10


element ApplicationRequest/ServiceId

diagram	
Nordea rule: Optional	Not used yet
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 256


element ApplicationRequest/Environment

diagram	
Nordea rule: Mandatory	Example: PRODUCTION
type	bxd:EnvironmentCode
properties	isRef 0 content simple
facets	pattern PRODUCTION


element ApplicationRequest/FileReferences

diagram	
Nordea rule: Mandatory Download-File. Ignored in other operations	<p>Unique identification of the file which is the target of the operation This element is used and is mandatory in operation DownloadFile to specify one specific file as the target of the operation The customer must have obtained the FileReference values beforehand using the DownloadFileList operation.</p> <pre><FileReferences> <FileReference> 123456789</FileReference> <FileReference> ABCDEFGHI</FileReference> </FileReferences></pre>
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 16

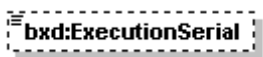
element ApplicationRequest/UserFilename

diagram	
Nordea rule: Optional in UploadFile. Ignored in all other operations	Example: SEPA_CAP1234.XML
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 80

element ApplicationRequest/TargetId


diagram	
Nordea rule: Mandatory	Signer ID. Example: 0012345678:
type	restriction of xs:string
properties	isRef 0 content simple
facets	minLength 1 maxLength 80

element ApplicationRequest/ExecutionSerial


diagram	
---------	---

Nordea rule: Optional	Example: Payments_20140603-144535-424
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 32

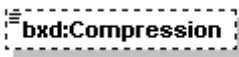
element ApplicationRequest/Encryption

diagram	
Nordea rule: Optional but must contain "false" if present	Example: false (case-sensitive) Not implemented yet
type	xs:boolean
properties	isRef 0 minOcc 0 maxOcc 1 content false

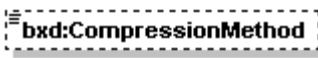
element ApplicationRequest/EncryptionMethod

diagram	
Nordea rule: Optional	Not implemented yet

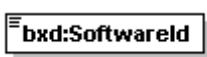
element ApplicationRequest/Compression

diagram	
Nordea rule: Optional	"false" "true" if present. Example: false
type	xs:boolean
properties	isRef 0 minOcc 0 maxOcc 1 content simple

element ApplicationRequest/CompressionMethod


diagram	
Nordea rule: Optional	<i>Only the value 'GZIP' is supported. It means that Compression algorithm is RFC1952 GZIP.</i>

element ApplicationRequest/SoftwareId


diagram	
Nordea rule: Mandatory	Example: ABC Soft version 1.0

type	restriction of xs:string	
properties	isRef	0
	content	simple
facets	minLength	1
	maxLength	80

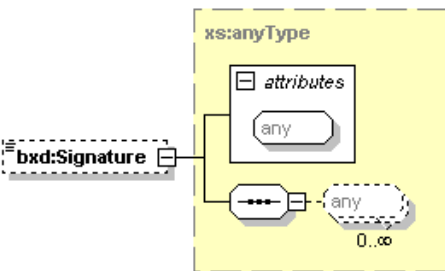
element ApplicationRequest/FileType

diagram		
Nordea rule: Mandatory in operation, UploadFile	Example Corporate Access Payments: NDCAPXMLI	
type	restriction of xs:string	
properties	isRef	0
	minOcc	0
	maxOcc	1
	content	simple
facets	minLength	1
	maxLength	40

element ApplicationRequest/Content

diagram		
Nordea rule: Mandatory in operation UploadFile. Ignored in other operations	<p>The actual file in the UploadFile operation. The content is in Base64 format.</p> <p>Example: TE0wMjAwMTY2MDMwMDEwMDY4MjcglCAglCAglCAw</p>	
type	xs: base64Binary	
properties	isRef	0
	minOcc	0
	maxOcc	1
	nillable	true

element ApplicationRequest/Signature

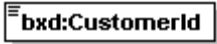
diagram		
Nordea rule Mandatory	<p>This element is created by the signature operation by the customer. It's content is specified by the XML Digital Signature standard.</p> <p>This element is mandatory when sending any request to the bank as it is used for integrity verification and authentication. This element is defined as optional in the schema because the recipient can remove the signature element after verification of the signature, before schema validation</p> <p>Example:</p> <pre><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"> <SignedInfo> <CanonicalizationMethod algorithm="http://www.w3.org <SignatureMethod Algorithm="http://www.w3.org <Reference URI=""> <Transforms> <Transform Algorithm="http://www.w3.org </Transforms> <DigestMethod Algorithm="http://www.w3.org</pre>	

	<DigestValue>PkNgWI1Tqr1D2YddYKA4a95XcNs </Reference> </SignedInfo> <SignatureValue>OoAzRt70BLo2baxrQOoBXmuObrUMa					
type	xs:anyType					
properties	isRef	0				
	minOcc	0				
	maxOcc	1				
	content	complex				
	mixed	true				
attributes	Name	Type	Use	Default	Fixed	annotation


Appendix D

Application response Syntax description


element ApplicationResponse/CustomerId

diagram	
Nordea rule: Mandatory	SenderID Example: 1205585055
type	restriction of xs:string
properties	isRef 0 content simple nillable false
facets	minLength 1 maxLength 16


element ApplicationResponse/Timestamp

diagram	
Nordea rule: Mandatory	Data Type: ISODateTime, UTC. Example: 2014-06-03Z14:45:35.424
type	xs:dateTime
properties	isRef 0 content simple

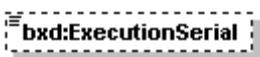
element ApplicationResponse/ResponseCode

diagram	
Nordea rule: Mandatory	Example: 00 Example: 20
type	restriction of xs:string
properties	isRef 0 content simple nillable false
facets	minLength 1 maxLength 16

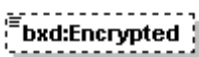
element ApplicationResponse/ResponseText

diagram	
Nordea rule: Mandatory	Example: OK Example: Content type not valid
type	restriction of xs:string
properties	isRef 0 content simple nillable false
facets	minLength 1 maxLength 80

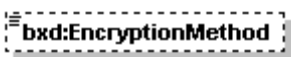
element ApplicationResponse/ExecutionSerial

diagram	
Nordea rule: Optional	Example: Payments_20140603-144535-424
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 32

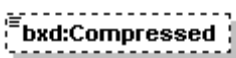
element ApplicationResponse/Encrypted

diagram	
Nordea rule: Optional	Not implemented yet Example: false(case-sensitive)
Type	xs:boolean
Properties	isRef 0 minOcc 0 maxOcc 1 content simple

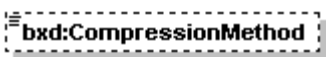
element ApplicationResponse/EncryptionMethod

Diagram	
Nordea rule: Optional	Not implemented yet
Type	restriction of xs:string
Properties	isRef 0 minOcc 0 maxOcc 1 content simple
Facets	minLength 1 maxLength 35


element ApplicationResponse/Compressed

Diagram	
Nordea rule: Mandatory	Default: 'true' (case-sensitive)
type	restriction of xs:string
properties	isRef 0 minOcc 0 maxOcc 1 content simple
facets	minLength 1 maxLength 35


element ApplicationResponse/CompressionMethod

diagram									
Nordea rule: Mandatory	Current the value 'GZIP' is supported. It means that Compression algorithm is RFC1952 GZIP.								
type	restriction of xs:string								
properties	<table> <tr><td>isRef</td><td>0</td></tr> <tr><td>minOcc</td><td>0</td></tr> <tr><td>maxOcc</td><td>1</td></tr> <tr><td>content</td><td>simple</td></tr> </table>	isRef	0	minOcc	0	maxOcc	1	content	simple
isRef	0								
minOcc	0								
maxOcc	1								
content	simple								
facets	<table> <tr><td>minLength</td><td>1</td></tr> <tr><td>maxLength</td><td>35</td></tr> </table>	minLength	1	maxLength	35				
minLength	1								
maxLength	35								

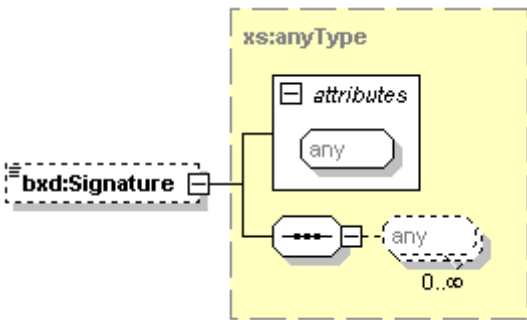
element ApplicationResponse/FileType

diagram							
Nordea rule: Mandatory	File types are specified in appendix B Example: "NDCAPXMLO" as pain002						
type	restriction of xs:string						
properties	<table> <tr><td>isRef</td><td>0</td></tr> <tr><td>minOcc</td><td>0</td></tr> <tr><td>maxOcc</td><td>1</td></tr> </table>	isRef	0	minOcc	0	maxOcc	1
isRef	0						
minOcc	0						
maxOcc	1						

element ApplicationResponse/Content

diagram											
Nordea rule: Mandatory	Example: TE0wMjAwMTY2MDMwMDEwMDY4MjcglCAglCAglCAw										
type	xs:base64Binary										
properties	<table> <tr><td>isRef</td><td>0</td></tr> <tr><td>minOcc</td><td>0</td></tr> <tr><td>max'occ</td><td>1</td></tr> <tr><td>content</td><td>simple</td></tr> <tr><td>nillable</td><td>false</td></tr> </table>	isRef	0	minOcc	0	max'occ	1	content	simple	nillable	false
isRef	0										
minOcc	0										
max'occ	1										
content	simple										
nillable	false										

element ApplicationResponse/Signature

Diagram	
Nordea rule: Mandatory	This element is created by the signature operation in the bank. The signing process is using Nordea specific CA and Nordea content signing certificate. The CA certificate for the Signing certificate is available at Nordea Open pages, or by re-

	quest from Nordea.	
	The Signature is specified by the XML Digital Signature standard by W3C.	
Type	xs:anyType	
Properties	isRef	0
	minOcc	0
	max'occ	1
	content	complex
	mixed	true

Appendix E

The difference between Corporate Access Secure envelope and the Finnish national Web Services / ApplicationRequest.

Nordea and other banks in Finland have used Web Services protocol during many years. That service has been defined by Nordea and other banks in Finland and common specifications are openly available at Federation of Finnish Financial Services FFI. That specification includes ApplicationRequest and ApplicationResponse schemas which are used to enable content offline security. Nordea Corporate Access File Transfer uses the same schemas for the same purposes, i.e. offline security, for all protocols, including Web Services.

In using this off line security model, there are no technical differences between the FI Web Services and Corporate Access File Transfer. The content to be uploaded/downloaded are secured immediately after the creation of the file and can be sent over to Corporate Access using any file transfer protocol at wanted time. See the figure 2 at chapter 6.1.

Because these services have some different characteristics, the content in some elements are different. Below are listed all those elements which may have differences in the contents. Other non-listed elements are not changed. However, some elements have not been implemented in Corporate Access. See chapter 4.2. for elements used.

ApplicationRequest

Element name	Corporate Access (all protocols)	Web Services Finland
CustomerID	Value of Sender ID from customer agreement, or if a 3 rd party sending customer's signed ApplicationRequests, 3 rd party's SenderID	Logon Id from the Web Services Agreement
Status	NEW, DLD, ALL. Note! For compatibility reasons the word DOWNLOADED is also accepted	NEW, DOWNLOAD-ED, ALL
ServiceId	Not yet implemented	Additional identification information of the Customer, for example an Account number or similar

Environment	PRODUCTION	PRODUCTION, TEST
TargetId	Value of the Signer ID from customer agreement. Each agreement may contain several Signer ID's, each of them connected to content signing certificates	The logical folder name where files are stored in the bank. A user can have access to several folders. TargetId's are included in the customer service agreement
FileType	Values specified in this document in Appendix B	Values specified in Web Services (FI) service description

The SOAP envelope

Like Web Services used by all banks in Finland, also Web Services in Corporate Access is following pure global specifications like Web Services Basic profile version 1.0, Web Services Security X.509 Certificate Token Profile used for digitally signing digests, SOAP 1.1 and HTTPS 1.1.

Any Web Services client made using these specs can be used both towards Finnish Web Services and Corporate Access Web Services. The WSDL for both of these services are the same.

URL

The URL for Corporate Access Web Services is ws.ebridge.prod.nordea.com/ws/CorporateFileService.