Certificate management

for Corporate Access File Transfer

6/8/2016

Version 1.0

This document describes the certificate management process and CSR (Certificate Signing Request) for automatic and manual download of Nordea eID for Nordea Corporate Access File Transfer.

Contents

1 Introduction

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

To enable end-to-end security of a file, Nordea have introduced a content signature model called Secure Envelope. With the Secure Envelope, security will be part of the content and related to the content owner. Specification of the signature process is described in the document called "Secure Envelope specification" (earlier "Content signature specification").

This document describes how to download and manage the Nordea eID on file certificate to be used as the key in the signing process of the Secure Envelope.

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). Usually the file format does not include security elements and therefore to provide security, something additional is needed. To harmonize and improve the content security for any channel or delivery method of files, an envelope containing a digital signature has been defined.

The digital signature requires a PKI key, also called as certificate, which is unique for each customer. The PKI certificate is made of a unique key pair which is generated at the customer side. The key pair contains one private key and corresponding public key. The private key must not leave the customer environment but in order for Nordea to accept this certificate to be used to sign files, it's public key must be presented to Nordea who signs it with Nordea's own key and return the signed key to customer.

This process is called a certificate download which is a standard process also called Certificate Signing request (CSR). The signing of customer's public key is done only if the information in CSR is correct and corresponds to information at Nordea and if the HMAC control string, calculated with specific activation code, is correct. The returned signed public key i.e. certificate contains customers unique ID.

Following chapters describes how to download a certificate for signing files.

3 Download of a certificate for signing

The certificate for signing can be downloaded by sending a CSR (Certificate Signing Request) with a Web Services call. The processes is explained below. Later there will be other protocols besides Web Services, such as sFTP and AS2 to be used to send CSR's to Nordea.

If more than one certificate is used by the customer, each download must use certificate specific data in the CSR and unique activation codes. The required information in download process is shown below. The correct values are found from the customer agreement and must be entered exactly as printed. The Activation code for HMAC calculation is received via a SMS message.

- Name of the certificate holder
  In Corporate Access this is a person who is named to receive a certificate. It may be also a company name in some other services.

- ID
  In Corporate Access this is a unique ID called Signer ID. In some other services it is called Logon ID.

- 10 digit activation code.
  This code is received via SMS message to the phone number which is registered at the Nordea fro the SignerID receiver. The SMS contains a text like following: "Message from Nordea. Activation code for Nordea eID on file: 1234567890. ID:…….035. Valid until 16.11.2015". The …035 in previous example is three last digits from the belonging Signer ID and can be used to identify which activation code belongs to which Signer ID if more than one certificate used. The Activation code must be consumed until the date mentioned. If needed, a new code can be requested from the bank to the same phone number. Activation code is not reusable.

- Country code
  This two letter code is depending on the country where the customer's main company is registered.

3.1 Automatic downloading of eID on File certificate

Nordea offers an automated way of downloading & renewing signing certificates to be used with Corporate Access File Transfer and Web Services channels. The ERP software-enabled download service is based on CSR sent to Nordea by the banking software using Web Services protocol. A specific XML structure called CertApplicationrequest is sent in SOAP request to Nordea. The schema for CertApplicationrequest is available at Nordea.com.

The PKCS#10 formatted CSR will be put in CertApplicationRequest/Content element in base64 coded format. In addition, in CertApplicationRequest there must be a HMAC check string which is calculated using the CSR and customer specific 10-digit activation code. The CSR and HMAC are explained in details below. Please see also a complete example in Appendix A.

If the needed information was correct in the request, the response to the request is CertApplicationResponse, which contains signed certificate in PKCS#7 format and can be paired with the private key waiting at the customer environment.

URL for the certificate download service is:
https://filetransfer.nordea.com/services/CertificateService

The WSDL for WS SOAP can be found here

The schemas to be used are found via these links:

CertApplicationrequestschema

CertApplicationresponseschema

> Please take into considerations different risk scenarios while working with certificates which are in form of data file. The customer is always responsible of storing the certificate secure, without unauthorized access to it.

3.1.1 Creation of the CSR

The CSR contains subject info fields of which three of them are important: “CN”, “serialNumber” and “C”. The data to put into these fields can be found from the customer agreement (see chapter 3 above).

1) CN = Name of the certificate holder
2) serialNumber = Signer ID (or Logon ID) from the agreement
3) C = country code.

The CSR is generated with the correct information in the above fields. There should not be empty fields. Other parameters to be used are: key length 1024bit, algorithm sha1 and DER –encoded.

A HMAC (sha1) check string is calculated from the CSR using the activation code as the key for it. Please note that hmac functions usually expects to have both CSR and activation code in byte format (ASCIIEncoding) for the calculation. The CSR and HMAC values both formatted into base64 coded presentation are put into a CertApplicationRequest as in picture below:

```
<CertApplicationRequest
xmlns="http://filetransfer.nordea.com/xmldata/">
  <CustomerId>1442672325</CustomerId>
  <Timestamp>2015-11-12T15:24:19Z</Timestamp>
  <Environment>PRODUCTION</Environment>
  <SoftwareId>PL Software</SoftwareId>
  <Command>GetCertificate</Command>
  <Service>service</Service>
  <Content>MIICnjCCAgc....3xImvzKyGm8=  </Content>
  <HMAC>/zxj/kPg9g13zLR/TPyW2CXHoxc=</HMAC>
</CertApplicationRequest>
```

Elements should be filled as follows:

- CustomerId: The Sender ID from the agreement/CAF schedule
- Timestamp: Creation time in UTC format: yyyy-mm-hhTmm:ss:nnZ
- Environment: Constant: “PRODUCTION”
- SoftwareId: Name of the software used
- Command: Constant: “GetCertificate”
- Service: Constant “service”
- Content: The CSR in base64 coded format
- HMAC: The computed hash as base64 coded HMAC string

The CertApplicationRequest is sent to Nordea. Currently Nordea supports only Web Services calls to send the CertApplicationRequest in SOAP message. Thee will be other protocols to be used later. The CertApplicationRequest is not signed because it is protected with the unique HMAC value, but the SOAP message can be signed. Please note that the response SOAP message is always signed and if the SOAP request must be therefore signed due to requirements of the programming language, the signing can be done using the Nordea Demo certificate. In this case the SOAP signature has no meaning.

The received certificate in response will be connected to the corresponding private key at the customer. It must be stored securely and protected with a strong password given by the user.

3.1.2 Automatic renewal of the certificate before its expiration

If the current valid Nordea eID certificate needs to be renewed before it will expire (after two years), the CertApplicationRequest with CSR can be signed with that certificate. The signature element follows the signature process of signed files and it will replace the HMAC element in the CertApplicationRequest. There is no need to request a new activation code via SMS if this renewal is done before certificate expiration. See an example in Appendix B.

3.2 If the response will not contain a certificate as expected

In some cases the response does not contain a certificate as expected but an error message instead. The reason for this is most likely a wrong content in CSR, wrong HMAC value or using wrong or expired activation code (valid for 7 days only, unique with each SignerID).

The CSR request must contain valid values for ID, country code and name fields and the given values will be also part of the created certificate. In case that the name is typed in differently than in Nordea records, the error code in response shows the correct typing for the name (assuming the ID and HMAC was correct). The request must be re-created using correctly typed name, the same activation code and sent to Nordea again. Wrong ID, country code or HMAC leads simply to rejection of the request.

3.3 Trying out of certificate download

It is possible to try out the automatic download process with demo activation code: 1234567890. In the Environment-element there should be a string “TEST” instead of “PRODUCTION”. Please note that the received “certificate” does not correspond to the request with the private key, but the process and the format of the messages can be verified with this process.

3.4 Manual downloading of certificate

It is no more possible to manually download a certificate from Nordea web site. If the automatic process described above in chapter 3.1 will not be utilized, then a certificate management client can be downloaded from Nordea.com. After installing the client it can be used to download the certificate using the above described process for automatic download.

Appendix A Example of a CertApplicationRequest in H2H


```
<CertApplicationRequest xmlns="http://filetransfer.nordea.com/xmldata/">
        <CustomerId>1442672325</CustomerId>
        <Timestamp>2015-12-03T11:11:04Z</Timestamp>
        <Environment>PRODUCTION</Environment>
        <SoftwareId>Petri</SoftwareId>
        <Command>GetCertificate</Command>
        <Service>service</Service>
        <Content>
MIICoDCCAgkCAQAwOjELMAkGA1UEBhMCRkkxEzARBgNVBAUTCjE0NDI2NzIzMjUx
FjAUBgNVBAMMDUEgQ29tcGFueSBMVEQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAM4aeLQKtLYi/Vg4cpVn1DWvaVdYw6zqwhuKur6p54rPUD6CG+umQ6xHk71Q
cb349rahmWdU8VBwC3VROhHPTYyNgMaatelBkxx+JH9Ia4yOZkc8tY5tznveJ5AM
oJYegb0sEHfFBylUE9HMHQM17HS6E1BpKTLRtRdAu57MZz4RAgMBAAGgggEkMBoG
CisGAQQBgjcNAgMxDBYKNi4xLjc2MDEuMjBJBgkrBgEEAYI3FRQxPDA6AgEFDBlG
SU5QV00xNTQ3MjE0NC5vbmVhZHIubmV0DA5PTkVBRFJcWjI3NTA2NwwKVGVzdGVy
LmV4ZTBTBgkqhkiG9w0BCQ4xRjBEMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAK
BggrBgEFBQcDAjAdBgNVHQ4EFgQUuYwlR2NFkh9+zL/aS+lm6D+Ie0MwZgYKKwYB
BAGCNw0CAjFYMFYCAQIeTgBNAGkAYwByAG8AcwBvAGYAdAAgAFMAdABvAG8AbgBn
ACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMB
ADANBgkqhkiG9w0BAQUFAAOBgQCQXem6FXqW4BwU/y1t6h7rAI/ySk9G4CeQhkCN
RnMiDBad0xKlKBNV9cjjTlL2lYi7sB2hrQibE7/89n097WXDfym/SkArLPTaKlEe
19u1E2j5dbL/rdZXKtMJKxkfG8ljns9ubRgxRinBVxleIfFgY3BlpbFpM/fKksPT
xhZx4w==
        </Content>
        <HMAC>kRtpBE+mrxAPuHRfKNP1beAsYo0=</HMAC>
</CertApplicationRequest>
```


The activation code used for HMAC above is 1234567890.

Appendix B Example of a CertApplicationRequest for renewal

```
<CertApplicationRequest xmlns="http://filetransfer.nordea.com/xmldata/">
  <CustomerId>1442672325</CustomerId>
  <Timestamp>2015-12-03T12:36:50Z</Timestamp>
  <Environment>PRODUCTION</Environment>
  <SoftwareId>Petri</SoftwareId>
  <Command>GetCertificate</Command>
  <Service>service</Service>
  <Content>
MIICpTCCAg4CAQAwODELMAkGA1UEBhMCRkkxEzARBgNVBAUTCjE0NDI2NzIzMjUx
FDASBgNVBAMMC0NvbXBhbnkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjC1QhafpcgVxZ/cg06bbzHi5B1MRxANd7xyMJf4czh5Z9gg8AnJCYxFNMfTf0
N/8ZdNc3UVMSWBFkzr2GGpwBct6kwk8Vkx82lOyc1Fm3NhBDxmyZdbjwkDx8sQ4r
f7LoMpjtbWrwZ2Q/BwJZX6i/nEWJzX+crkfhrgmuWfP/sQIDAQABoIIBKzAaBgor
BgEEAYI3DQIDMQwWCjYuMS43NjAxLjIwUAYJKwYBBAGCNxUUMUMwQQIBBQwZRklO
UFdNMTU0NzIxNDQub25lYWRyLm5ldAwOT05FQURSXFoyNzUwNjcMEVRlc3Rlci52
c2hvc3QuZXhlMFMGCSqGSIb3DQEJDjFGMEQwDgYDVR0PAQH/BAQDAgTwMBMGA1Ud
JQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBQxED9LPsc4Qb+uw2Jkj3n74B/XUzBm
BgorBgEEAYI3DQICMVgwVgIBAh5OAE0AaQBjAHIAbwBzAG8AZgB0ACAAUwB0AHIA
bwBuAGcAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABrAG8AdgBpAGQA
ZQByAwEAMA0GCSqGSIb3DQEBBQUAA4GBADexXHDh7wPW+jM1if+Tk7f1rUbEuM8b
xn/0UF9/0rBALa54ndvUSipQGjqZakeT0qrgKAPOQvmNV3xXQyT0PupyGtGt10kC
l0nIAObasSXcDwlMVZffVjaVCk6GZr9x7B25m6llB9StuyI5RsDnp5NoiLAaeJnL
UW3vfXIm3cZQ
  </Content>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="">
     <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     </Transforms>
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <DigestValue>kzrgUHdYRHdciETFz5dH4XMNqsI=</DigestValue>
    </Reference>
   </SignedInfo>
   <SignatureValue>DCb+lj8Zp6fZ4uqHOVu1G590gM… ZXB2KfzCyfZm5g=</SignatureValue>
   <KeyInfo>
    <X509Data>
     <X509IssuerSerial>
      <X509IssuerName>System.Security.Cryptography.X509Certificates.X500DistinguishedName</X509IssuerName>
      <X509SerialNumber>28864331</X509SerialNumber>
     </X509IssuerSerial>
     <X509Certificate>
      MIIDwTCCAqmgAwIBAgIEAbhvSzANBgkqhHQ….3UReUucpKEB+fOyZiWNjYbxGvbqShU=
     </X509Certificate>
    </X509Data>
   </KeyInfo>
  </Signature>
</CertApplicationRequest>
```

Note! Part of the content is truncated.