Nordea

Corporate Access Secure Envelope, Corporate Access Web Services, SHA1 – SHA256 changes

Technical Description

Open

Nordea

Table of Contents

1. General

This document describes the SHA1 to SHA256 change in Corporate Access Secure Envelope which is the Nordea (hereinafter 'Nordea' or 'the bank') specification around file protection using digital signature, and the SHA1 to SHA256 change in Corporate Access Web Services which is one of the data communication protocol supported in Corporate Access File Transfer.

1.1 Corporate Access Secure Envelope

Corporate Access File Transfer is the service for Nordic and Baltic Corporate Access customers to utilize host to host file transfer protocols to connect, and send/receive different file formats to and from Nordea.

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

1.2 Corporate Access Web Services

Corporate Access Web Services (CA WS) is one of the data communication protocols supported in Corporate Access File Transfer. The protocol is based on common global standards and complies with the definitions of the World Wide Web Consortium (W3C); see www.W3.org.

In CA 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), which follows the same process used in Corporate Access Secure Envelope Signer certificate. The specification of ApplicationRequest in Corporate Access Web Services is the same as of Corporate Access Secure Envelope.

1.3 SHA1 – SHA256 Change

In support to provide secure services and solutions to our customers, Nordea will discontinue the support of the SHA1 certificate and signing signature in Corporate Access Secure Envelope because of weaknesses in the SHA1 algorithm, and replace it with SHA256.

The areas of change are:

a. The customer signing certificate (linked to each signer ID) used to create digital signatures will be changed to use SHA256 signature hash algorithm. Chapter 2 describes this in more details.

b. Nordea recommends customer to use key length 2048 in the certificate signing request (CSR) when downloading certificate from Nordea, so that the customer signing certificate will have key length 2048. Chapter 2 describes this in more details

c. Customers need to use SHA256 signing algorithm when creating the digital signature. Chapter 3 describes this in more details, and there example Secure Envelope files in Appendix

d. When Nordea sends customers messages in Secure Envelope, the Secure Envelope are signed with Nordea's new SHA256 certificate and with SHA256 signing algorithm. Chapter 4 describes this in more details, and there are example responses files in Appendix

e. Nordea will stop support of TLS 1.0 and 1.1. Chapter 5 describes this in more details.

f. For customers who download signer certificate using own software, the ApplicationRequests and SOAP-Requests should be signed with SHA256 signing algorithm, and Nordea's responses are created with SHA256 certificate and signing algorithm too. Chapter 6 describes this in more details.

2. Change in customer signing certificate

Before Sep 27th 2022, the customer signing certificate issued from Nordea was

- With SHA1 signature hash algorithm.
- Key length could be either 1024 or 2048 depending on how it is defined in the certificate signing request (CSR) which customer sends in when downloading the certificate. Currently NSC client offered by Nordea only supports 1024 key length.

With the change implemented on Sep 27th 2022 at 10:00 CET, the certificate is

- With SHA256 signature hash algorithm
- Key length could be either 1024 or 2048 depending on how it is defined in the certificate signing request (CSR) sent in by customers. Nordea recommends customers to use 2048. The new version of NSC client offered by Nordea will support both 1024 and 2048 key length

After the change, even if customer defines the algorithm as SHA1 in the CSR, Nordea overwrites it to SHA256 and issue SHA256 certificate.

2.1 Customer effort

2.1.1 Development in Corporate Access software client

If customer uses own software client to download certificate from Nordea, and the software only supports 1024 key length in CSR, Nordea strongly recommends customer to make development to download certificate with 2048 key length.

Nordea also offers the new version of NSC client since Dec of 2022, which supports key length of 2048. So customers can use it download certificate of key length of 2048.

For the change of SHA256 signature hash algorithm in certificate, based on our analysis, customers don't need make development in order to download SHA256 certificate. Even if customer defines the algorithm as SHA1 in the CSR, Nordea will overwrite it to SHA256 and issue SHA256 certificate. However customers should analyze the need of development themselves still. Both the current version and new version of NSC client support downloading SHA256 certificates.

2.1.2 Testing and Migration

The change has been implemented by Nordea on Sep 27th 2022 at 10:00 CET.

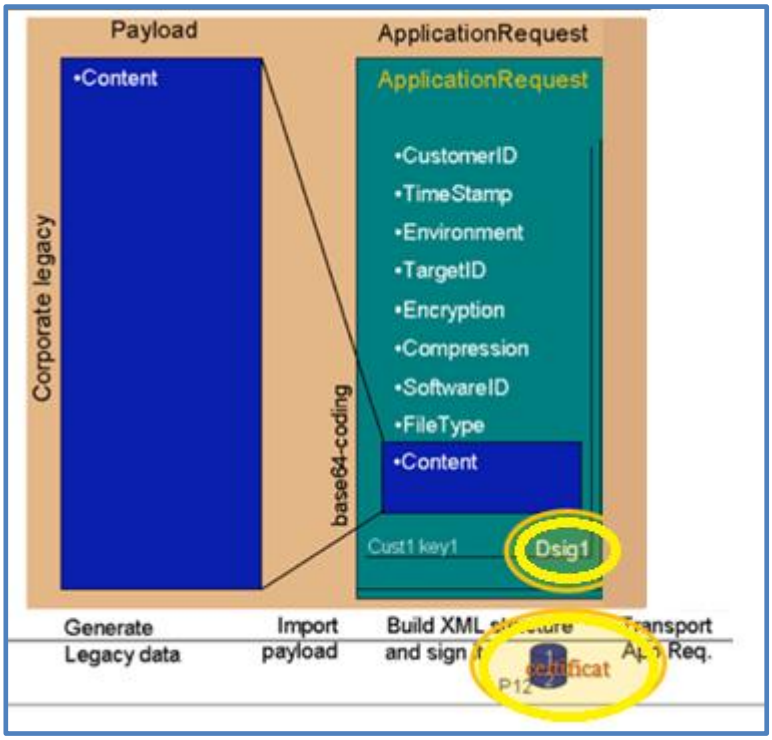
After the change time/date, when customer make a certificate download request to download or renew customer signing certificate, customer will get SHA256 certificates from Nordea.

3. Change in specification for incoming flow of customers to Nordea

3.1 For Host-to-Host protocols other than Web Services

In Corporate Access Secure Envelope specification, the ApplicationRequest following XML schema should be digitally signed.

Diagram below shows the process of creating ApplicationRequest from the payload data, and the steps of creating digital signature with certificate are the areas of the change, and they are also highlighted with circles in the diagram.



Originally, in digital signature, Nordea supports SHA1 algorithm

- SignatureMethod Algorithm = http://www.w3.org/2000/09/xmldsig#rsa-sha1
- DigestMethod Algorithm =http://www.w3.org/2000/09/xmldsig#sha1.

Since Q2 2022, in additional to SHA1 algorithms, Nordea also supports SHA256

- SignatureMethod Algorithm = http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- DigestMethod Algorithm = http://www.w3.org/2001/04/xmlenc#sha256

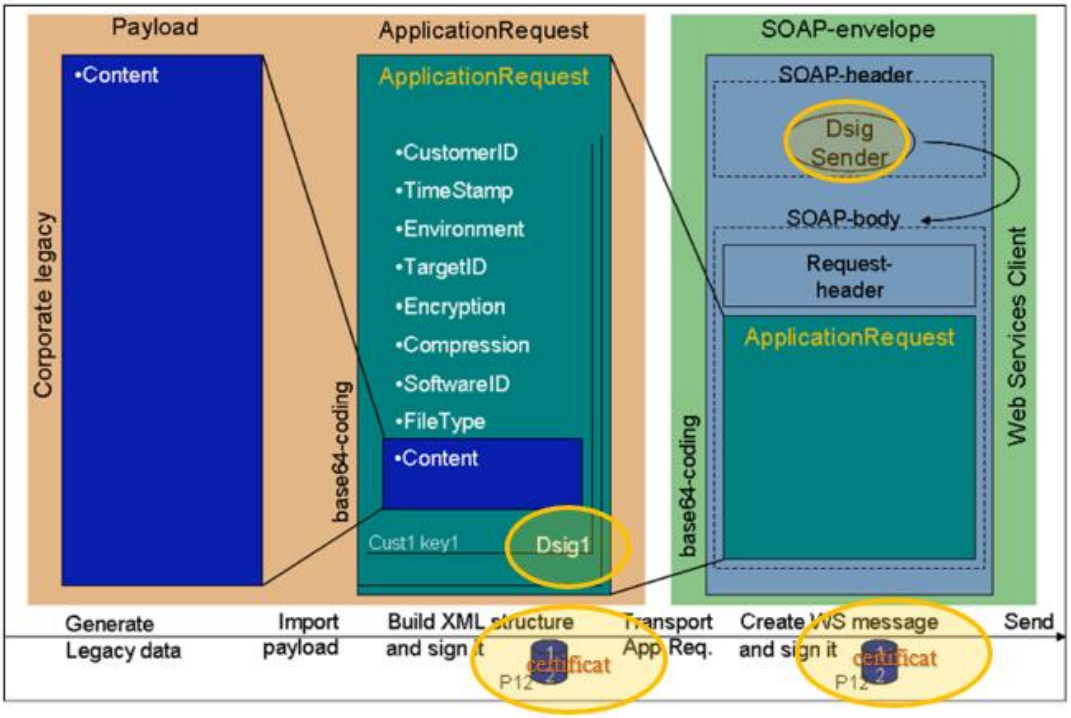
Example files are available in the appendix.

And during Q3 of 2023, Nordea will stop supporting the SHA1 certificate and algorithm.

3.2 For Corporate Access Web Services

In Corporate Access Web Services, both ApplicationRequest and SOAP-envelope should be signed.

Diagram below shows the process of creating ApplicationRequest and SOAP-envelope, and the steps of creating digital signature with certificate are the areas of the change, and they are also highlighted with circles in the diagram.



Originally, in digital signature, Nordea supports SHA1 algorithm

- SignatureMethod Algorithm = http://www.w3.org/2000/09/xmldsig#rsa-sha1
- DigestMethod Algorithm =http://www.w3.org/2000/09/xmldsig#sha1.

Since Q2 2022, in additional to SHA1 algorithms, Nordea also supports SHA256

- SignatureMethod Algorithm = http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- DigestMethod Algorithm = http://www.w3.org/2001/04/xmlenc#sha256

Example files are available in the appendix.

And during Q3 of 2023, Nordea will stop supporting the SHA1 algorithm.

3.3 Customer effort

3.3.1 Development in Corporate Access software client

Customers need to develop own software client so that the SHA256 algorithm will be used when creating the digital signature in the Secure Envelope ApplicationRequest and SOAPRequest (for Web Services) to Nordea.

3.3.2 Testing and Migration

Nordea now supports both SHA1 and SHA256 algorithms, and this setup will be kept for a period, and Nordea will discontinue support of SHA1 in the end of Q3 2023. So customers will have a long period of time for development, testing and migration before Nordea stops supporting SHA1.

Nordea will send newsletters to customers in advance to inform the exact date when Nordea will stop support of SHA1.

4. Change in specification for outbound flow of Nordea to customers

4.1 For Host-to-Host protocols other than Web Services

According to Corporate Access Secure Envelope specification, when Nordea sends customers ApplicationResponses, those are signed with Nordea's signing certificate.

Nordea's responses have been signed with SHA1 certificate and SHA1 algorithms. In Q3 2023, Nordea will change to use SHA256 algorithm:

- Nordea's ApplicationResponses will be signed with SHA256 certificate and SHA256 algorithms
- As explained already in chapter 3:
  - For customers messages towards Nordea, service support both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm before Q3 2023
  - And during Q3 of 2023, Nordea will stop supporting the SHA1 algorithm.

Example files for Nordea's responses are available in the Appendix.

Nordea's new SHA256 signing certificate and the Root CA certificate will be published in Nordea.com

4.2 For Corporate Access Web Services

According to Web Services standard, when Nordea sends customers ApplicationResponses and SOAP-envelope messages, those are signed with Nordea's signing certificate.

Nordea's ApplicationResponses and SOAPResponses have been signed with SHA1 certificate and SHA1 algorithms. In Q3 2023, Nordea will change to use SHA256 algorithm:

- Nordea's ApplicationResponses and SOAP-envelope messages will be signed with SHA256 certificate and SHA256 algorithms
- As explained already in chapter 3:
  - For customers messages towards Nordea, service support both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm before Q3 2023

- And during Q3 of 2023, Nordea will stop supporting the SHA1 algorithm.

Example files for Nordea's ApplicationResponses and SOAPResponses are available in the Appendix.

Nordea's new SHA256 signing certificate and the Root CA certificate will be published in Nordea.com

4.3 Customer effort

4.3.1 Development in Corporate Access Web Services software client

Customers need to develop own software client so that the client can process Nordea's responses which are signed with SHA256 certificate and SHA256 algorithm.

4.3.2 Testing and Migration

Nordea will provide more information about the testing possibilities.

5. Change of Disabling TLS 1.0 and 1.1, and unsafe algorithms in AS2 and SFTP

Transport Layer Security (TLS) 1.0 and 1.1 are security protocols of HTTPS service for establishing encryption channels over computer networks. Corporate Access File Transfer has supported these protocols in the past. However, due to evolving regulatory requirements as well as new security vulnerabilities in TLS 1.0, Nordea requires customers to remove TLS 1.0/1.1 dependencies in customers' software, and Nordea will stop the support of TLS 1.0 and 1.1 by the end of Q3 2023. Nordea will send newsletter to customers in advance to inform the exact date.

There is also another initiatives ongoing to remove insecure settings in AS2 and SFTP protocols. In general, SHA1, 3DES and MD5 algorithm support in AS2 and SFTP will be removed by Q3 2023 . Nordea will send newsletter containing detailed information and exact change date.

6. Change of certificate download

This change is only relevant for customers who download certificates using own software. If you use NSC to download certificate, this is not relevant for you.

Nordea has deployed a new service for certificate download. In the new service, SHA256 certificate and signing algorithm are used. Customers should make change in own solution to be able to send SHA256 requests to Nordea and accept SHA256 responses from Nordea, because during Q3 2023, Nordea will stop supporting SHA1.

Existing service operates as of today without changes before Q3 2023, and in parallel, the new service with SHA256 certificate and signing algorithm are open for customer to test and use.

Existing service

https://filetransfer.nordea.com/services/CertificateService

- No change as of today. Nordea's messages are signed with SHA1 certificate and SHA1 algorithms.
- Delivered SHA1 signer certificate before Sep 27th 2022 and SHA256 signer certificate after.
- For customers messages towards Nordea, service supports both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
- And during Q3 of 2023, Nordea will stop supporting the SHA1 algorithm.

New service

https://filetransfer.nordea.com/services/CertificateService/sha2

- Nordea's ApplicationResponses and SOAP-envelope messages are signed with SHA256 certificate and SHA256 algorithms
- Delivered SHA1 signer certificate before Sep 27th 2022 and SHA256 signer certificate after
- For customers messages towards Nordea, service support both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
- And during Q3 of 2023, Nordea will stop supporting the SHA1 algorithm.

Example files for Nordea's responses are available in the Appendix.

Nordea's new SHA256 signing certificate and the Root CA certificate for certificate download service are published in Nordea.com

7. Summary on customer efforts

Change area	Customer development efforts needed	Customer testing and migration efforts needed	Timeline
The customer signing certificate (linked to each Signer ID) used to create digital signatures will be changed to use SHA256 signature hash algorithm.	Customer needs to analyze the need. Based on our analysis, no development is needed in most cases	Yes	Changed on Sep 27th 2022, at 10:00 CET Nordea overwrites the algorithm setting customer defines in CSR (certificate signing request) and issue SHA256 certificate. Both the current version and new version of NSC client supports downloading SHA256 certificates.
Customers need to use SHA256 signing algorithm when creating the digital signature.	Yes	Yes	Nordea already supports SHA256 algorithm in requests sent by customers. In Q3 2023, Nordea will stop the support of SHA1, and we will inform the exact time later. Customer needs to be ready with the change by that time.

For responses messages Nordea sending to customers, the responses will be signed with Nordea's new SHA256 certificate and with SHA256 signing algorithm.	Yes	Yes	Nordea will uses SHA256 certificate and algorithm in Q3 2023 and we will inform the exact time later. Customer needs to be ready with the change by that time.
Nordea recommends customer to use key length 2048 in the certificate signing request (CSR) when downloading certificate from Nordea, so that the customer signing certificate will have key length 2048.	Yes if customers uses own software client to download certificate. Otherwise, customers can use the new NSC client which Nordea provides		Nordea supports issuing certificate of 2048 key length already. Nordea issues 1024 or 2048 key length certificate based on the setting customers define in CSR. The new version of NSC client which supports 2048 key length is available since Dec 15th 2022.
Nordea will stop support of TLS 1.0 and 1.1 and insecure setting in AS2 and SFTP	Yes	Yes	By Q3 2023, will inform exact time later

Appendix

Examples of Secure Envelope ApplicationRequest with SHA256 algorithm

Part of XML, some parts are scrambled


```
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
  <CustomerId>7777711111</CustomerId>
  <Command>UploadFile</Command>
  <Timestamp>2022-06-15T13:00:38.6061065+02:00</Timestamp>
  <Environment>PRODUCTION</Environment>
  <TargetId>1111177777</TargetId>
  <ExecutionSerial>1111177777</ExecutionSerial>
  <SoftwareId>DEMOCORPAccess</SoftwareId>
  <FileType>NDCAPXMLI</FileType>
<Content>PERvY3VtZW50IHhtbG5zPSJ1cm46aXNvOnN0ZDppc286MjAwMjI6dGVjaDp4c2Q6cGFpbi4wMDEuMDAxLjAzIiB4b
Wxuczp4c2k9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hLWluc3RhbmNlIj4NCgk8Q3N0bXJDZHRUcmZJbml0
bj4NCgkJPEdycEhkcj4NCgkJCTxNc2dJZD5XVFNTLUNBLVNGVC1OT05PLURPTUUtNTg0NjU8L01zZ0lkPg0KCQkJPENyZU
R0VG0+MjAyMi0wNi0xNVQxMzowNjoyMjwvQ3JlRHRUbT4NCgkJCTxOYk9mVHhzPjE8L05iT2ZUeHM+DQoJCQk8SW5pdGd
QdHk+DQoJCQkJPElkPg0KCQkJCQk8T3JnSWQ+DQoJCQkJCQk8T3Rocj4NCgkJCQkJCQk8SWQ+NzE0MTYyNzA3MzwvSWQ
+DQoJCQkJCQkJPFNjaG1lTm0+DQoJCQkJCQkJCTxDZD5DVVNUPC9DZD4NCgkJCQkJCQk8L1NjaG1lTm0+DQoJCQkJCQk8
L090aHI+DQoJCQkJCTwvT3JnSWQ+DQoJCQkJPC9JZD4NCgkJCTwvSW5pdGdQdHk+DQoJCTwvR3JwSGRyPg0KCQk8UG10
SW5mPg0KCQkJPFBtdEluZklkPldUU1MtQ0EtU0ZULU5PTk8tRE9NRS01ODQ2NTwvUG10SW5mSWQ+DQoJCQk8UG10TXRk
PlRSRjwvUG10TXRkPg0KCQkJPFJlcWRFeGN0bkR0PjIwMjItMDYtMTU8L1JlcWRFeGN0bkR0Pg0KCQkJPERidHI+DQoJCJ
PE5tPldUU1MgQlY8L05tPg0KCQkJCTxQc3RsQWRyPg0KCQkJCQk8Q3RyeT5OTzwvQ3RyeT4NCgkJCQk8L1BzdGxBZHI+
+DQoJPC9Dc3RtckNkdFRyZkluaXRuPg0KPC9Eb2N1bWVudD4NCg==</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/2001/04/xmldsig-more#rsa-sha256"/>
                <Reference URI="">
                        <Transforms>
                                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                        </Transforms>
                        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <DigestValue>ykr+mdCMpTTThts4BzAXypuygDqwxK8J4VZpt55f4R0=</DigestValue>
                </Reference>
        </SignedInfo>
        <SignatureValue>
XCO1oTKTmopZfzjxbOBFzuUE2K35+Z/8dQw17o7HA9utc2wUpve2SkAKSgiR4jC7
C+oJacqgxJhHWZOxiBVOgjcaWSAMBRAeDND1imyIH97QoTh6DHnsmNxZnpiyeMsR
sRbN8JLkI5WOZ/bD0LM8YfDtYUtspz3KJsXv9M1FKIA=
        </SignatureValue>
        <KeyInfo>
                <X509Data>
                        <X509IssuerSerial>
                                <X509IssuerName>2.5.4.5=#130B3531363430362D30313230, CN=Nordea
Corporate CA 01, O=Nordea Bank AB (publ), C=SE</X509IssuerName>
                                <X509SerialNumber>80449</X509SerialNumber>
                        </X509IssuerSerial>
                        <X509Certificate>
MIIC8TCCAdmgAwIBAgIDATpBMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNVBAYTAlNF
MR4wHAYDVQQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxHzAdBgNVBAMTFk5vcmRl
NdbHaK9A9x545N4x+RRt6jwKQ8iM4me6IHfGDEZG7cthuVZCykr6iMJfLTL1h2QU
LSZP7jv3j/cVWTCIw61tdc0XKfa3+F+DE7legXR6kiCh0fOImHRoBez90OFJVWc1
yvf1LdtebDSZBaRwt6Ib18VLCj6wBrURr6gYH02xvupt3OM7sjqERcVzzEh1ycbu
```

3nu7AGgU34/yZ66R5igOy4TNDfoX8/6KrMi1UmH/lQgQl2WiHZsafRHcsa/0/5w+
hTT95z3tHhKM9NbZdZq2OwvGdbo6z8EYkJtOtwx9lKaQwqi3Wg==</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</ApplicationRequest>

Examples of Secure Envelope ApplicationResponse with SHA256 algorithm

Part of XML, some parts are scrambled

<?xml version="1.0" encoding="UTF-8"?>

<ApplicationResponse xmlns="http://bxd.fi/xmldata/">

<CustomerId>7777711111</CustomerId>

<Timestamp>2022-06-17T08:30:36.000Z</Timestamp>

<ResponseCode>00</ResponseCode>

<ResponseText>OK.</ResponseText>

<ExecutionSerial>1111177777</ExecutionSerial>

<Encrypted>false</Encrypted>

<Compressed>false</Compressed>

<FileDescriptors><FileDescriptor>

<FileReference>NOTPROVIDED</FileReference>

<TargetId>NOTPROVIDED</TargetId>

<ParentFileReference>1111177777</ParentFileReference>

<FileType>NDCAPXMLO</FileType>

<FileTimestamp>2022-06-17T08:30:36.000Z</FileTimestamp>

<Status>DLD</Status>

</FileDescriptor>

</FileDescriptors>

<FileType>NDCAPXMLO</FileType>

<Content>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48RG9jdW1lbnQgeG1sbnM9InVy

bjppc286c3RkOmlzbzoyMDAyMjp0ZWNoOnhzZDpwYWluLjAwMi4wMDEuMDMiPjxDc3RtclBtdFN0

c1JwdD48R3JwSGRyPjxNc2dJZD5YTUw5OTA5MjAyMjA2MTcxMDMwMzYxNDU8L01tzZ0lkPjxDcmVE

dFRtPjIwMjItMDYtMTdUMDg6MzA6MzZaPC9DcmVEdFRtPjxJbml0Z1B0eT48SWQ+PE9yZ0lkPjxC

SUNPckJFST5OREVBU0VTUzwvQklDT3JCRUk+PElkPjxNDE2MjcwNzM8L0lkPjxTY2ht

bT48T3JnbmxOYk9mVHhzPjE8L09yZ25sTmJPZlR4cz48R3JwU3RzPkFDVEM8L0dycFN0cz48L09y

Z25sR3JwSW5mQW5kU3RzPjwvQ3N0bXJQbXRTdHNScHQ+PC9Eb2N1bWVudD4=</Content>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"></ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:SignatureMethod>

<ds:Reference URI="">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform>

<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod>

<ds:DigestValue>nUhjo5MiXXNsTeWPQalIoYH7DGs7g=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>W063Rc2MsXurkJ+8/1utoXeLhrX2aaIHENZuiJxtypPRgq4GXzaLzeIvh6keapRnuzz5uy8OINhlexfDLTol
ZwyVDywvTvAm2KG2kPas9xJA2a7+VCAb7jSEUx4UYeN4GQxxiIsBjAyueGKPmiMwdG0b7nzQ6ijvt62hCdCdIhLAWIGqP
SxgEg2IpG3MaxTPw4yRVT0o3Fmxm2Vh/NLl1kfjQ5NasX+SinXrzMZnmzzfuJ0IA==</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>MIIDrDCCApSgAwIBAgIDAT1tMA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNVBAYTAlNFMRgwFg
YDVQQKEw9Ob3JkZWEgQmFuayBBYnAxJjAkBgNVBAMTHU5vcmRlYSBDb3Jwb3JhdGUgU2VydmVyIENBIDAzMRQ
wEgYDVQQFEws1MTY0MTEtMTY4MzAeFw0yMjA0MDUwNjQzNTVaFw0yNDA0MDUwNjQzNTVaMHAxCzAJBgNVB
AYTAlNFMRgwFgYDVQQKDA9Ob3JkZWEgQmFuayBBYnAxHjAcBgNVBAsMFUNNIFByb2Nlc3MgTWFuYWdlbWVud
DEnMCUGA1UEAwweQ29ycG9yYXRlIEFjY2VzcyBGaWxlIFRyYW5zZmVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
+lA1Bx8cVuVp7GFlefHqzaG1xUiJ49mEvn9qa6tY1oUrTaNh/ukunk9U67DmcPRU/hgG0RkTVRF64JxYFOoESHBlY+UEV4
G0qsBQU1ZAfqWHL1ueoAAaK4Il/xI5s5FYIpdUP+6us8HyOQ99X2ypiwJJ1MRWFQ7iCDV/+EJV+PuSeiBWAVBqtSMYdS
ZBhpHqKPt9+pfcHwlHvHjMYpQp20O8vztrAjjkF/tu8gvTwnFmMpxutEP8ch4hKUj3Qpkl0eV44sQeU4Lobn9r2XyCdIRIE5e8
0DKY8tDCYNSGp4PKxEguTVVz/bwNZ+Qq5OpXCzQULtl14afdZ6kvk4qE=</ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</ds:Signature>

</ApplicationResponse>

Examples of SOAP Request with SHA256 algorithm (for Web Services)

Part of XML, some parts are scrambled

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">

<SOAP-ENV:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
S:mustUnderstand="1">

<wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="XWSSGID-164197899278383094871 9">

<wsu:Created>2022-01-12T09:16:32.733Z</wsu:Created>

<wsu:Expires>2022-01-12T09:21:32.733Z</wsu:Expires>

</wsu:Timestamp>

<wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="XWSSGID-1641978992675-1475305108">MIIC+zCCAeOgAwIBAgIDASxVMA0GCSqGSIb3DQEBBQUAMGQxCzAJBgNVBAYTAlNFMR4wHAYDVQQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxHzAdBgNVBAMTFk5vcmRlYSBDb3Jwb3JhdGUgZmljYXRlMRMwEQYDVQQFEwo1NzgwODYwMjM4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCClmzyaVAEr2cTt5gGPxuiMxZ5JZRIDHUwyUMIags/JYbKCq/MhumUEDDAKMAgGBiqFcEcBAzATBgNVHSMEDDAKgAhAC3XW288LpzAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQADggEBADVuzhr4KJwDXHph5fm5BOqufAI0fnUP5rFYfpDz3gRbyicRcBFj2hkIG+8wMUKiTfASheRYL1hydk4ElJ3gaeieD7Yn9OxMILy+svh3YXGWnw9z9msRRyvJdVNLwws2sUgxlv66iPJR0qVIT55fLed9YXbfdb/tPE+g10Qw62kXyZkDNoxeI8lUuihFLX20H/SPaRRHCAootUoNxuzFIuEHl/5zL3FMBWSsxdkfGrqmzF8/C5a31GXWGgn/JK7KI1BYKx/weVWRui0FI5nfIJQ=</wsse:BinarySecurityToken>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-164197899267325414858 1">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse S SOAP-ENV"/>

</ds:CanonicalizationMethod>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<ds:Reference URI="#XWSSGID-1641978992781-412569123">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="S SOAP-ENV ns2"/>

</ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>2hDXWPwOTrMIXCksTkj4ISZwrligdYTQbafaUr4=</ds:DigestValue>

</ds:Reference>

<ds:Reference URI="#XWSSGID-164197899278383094871 9">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

<InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsu wsse S SOAP-ENV"/>

</ds:Transform>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>pqwOmR08W2V5KEgsh3+fFmu94EHukEk=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue> MrQNHTalxYFm5FukMIrhb+XaOL+xkl6I5+PsUHju9Nco/YQ

SexTD/5LN6q7OMdpJ2dhA3xtEtU5LOz4geQ6Gh1DycI6WuLxce3cNDpGL7gPUhw

TBBnyl+OhA/yIJeLfmA=</ds:SignatureValue>

<ds:KeyInfo>

<wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1641978992756-860740920">

<wsse:Reference URI="#XWSSGID-1641978992675-1475305108" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>

</wsse:SecurityTokenReference>

</ds:KeyInfo>

</ds:Signature>

</wsse:Security>

</SOAP-ENV:Header>

<S:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1641978992781-412569123">

<ns2:downloadFileListin xmlns="http://model.bxd.fi" xmlns:ns2="http://bxd.fi/CorporateFileService">

<RequestHeader>

<SenderId>1205585055</SenderId>

<RequestId>1</RequestId>

<Timestamp>2022-01-12T11:13:50.907+02:00</Timestamp>

<Language>FI</Language>

<UserAgent>NEA</UserAgent>

<ReceiverId>123</ReceiverId>

<ApplicationRequest>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48QXBwbGljYXRpb25SZXF1ZXN0IHhtbG5zPSJodHRwOi8vYnhkLmZpL3htbGRhdGEvIj4NCiAgICA8Q3VzdG9tZXJJZD4xMTExMTExMTwvQ3VzdG9tZXJJZD4NCiAgICA8Q29tbWFuZD5Eb3dubG9hZEZpbGVMaXN0PC9Db21tYW5kPg0KICAgIDxUaW1lc3RhbXA+MjAyMi0wMS0xMlQxMTo1MzoxMy45MDcrMDI6MDA8L1RpbWVzdGFtcD4NCiAgICA8TGFuZ3VhZ2U+RkkvTGFuZ3VhZ2U+DQogICAgPFVzZXJBZ2VudD5ORUE8L1VzZXJBZ2VudD4NCiAgICA8UmVjZWl2ZXJJZD4xMjM8L1JlY2VpdmVySWQ+DQo8L0FwcGxpY2F0aW9uUmVxdWVzdD4=</ApplicationRequest>

</ns2:downloadFileListin>

</S:Body>

</S:Envelope>

Examples of SOAP Response with SHA256 algorithm (for Web Services)

Part of XML, some parts are scrambled

<soapenv:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cor="http://bxd.fi/CorporateFileService" xmlns:mod="http://model.bxd.fi" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

<soapenv:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">

<wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-a0f4d549-cca6-4a1c-bbf9-1672976fda29">

<wsu:Created>2022-01-03T10:18:19Z</wsu:Created>

<wsu:Expires>2022-01-03T10:23:19Z</wsu:Expires>

</wsu:Timestamp>

<wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="SecurityToken-7c9e3edc-6cad-41c1-8585-1672976fbafd">MIIDizCCAnOgAwIBAgIDASP+MA0GCSqGSIb3DQEBCwUAMGsxCzAJBgNVBAYTAlNFMR4wHAYDVQQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxJjAkBgNVBAMTHU5vcmRlYSBDb3Jwb3JhdGUgU2VydmVyIENBIDAxMR1MTY0MDYtMDEyMDAeFw0yMDEyMjExMjMxMDVaFw0yMjExMjcxMjMzNTBaMG4xCzAJBgNVBAYTAlNFMRgwFgYDVQQKDA9Ob3JkZWEgQmFuayBBYnAxGzAZBgNVBAsMEkNvcnBvcmF0ZSBDaGFubmVsczEoMCYGA1UEAwwfRmlsZSBUcmFuc2ZlciBXZWIgU2VydmljZXMgVGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA+vJCU7ECAwEAAaM1MDMwCQYDVR0TBAIwADARBgNVHQ4ECgQIQrtcU9YxVbUwEwYDVR0jBAwwCoAIRMeT2dl7VsEwDQYJKoZIhvcNAQELBQADggEBAKD2tlB86c/lmtXkAqiAzZMipRVSN1/ZZkOtmBuf56ziUQQMLORipMjlyP9grDhJIIOqqhsL1jo+BSdceW0o8Uh5bhrNeC6roLnGT864Ozj4tS354sgE5UUKcUYZUiw70PGP9gJKlp6kLFTlKNhJ0oI8eaItbU5A6c7KXgou44SfaN12I4m/wBZY1147PQa8X5B1npHruVbhbhbQccVurnF3qjpLHFKslnBl39tJ4taYwBqRe81pR3S6p2Hm9lWFK5nU3Ef/LIeeFsWVCpfR2x0BOB0gFbLOPFjC+FfQvLZ2A4I4+gjL321mVz7sp4zVZ86oKXolrTzexg+E=</wsse:BinarySecurityToken>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<Reference URI="#Timestamp-a0f4d549-cca6-4a1c-bbf9-1672976fda29">

<Transforms>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>U9cNMytdSuDpQ1SU9WU++I0UTWrjfmTELDTcsfkitzU=</DigestValue>

</Reference>

<Reference URI="#Body-e4b05d21-45c7-4dfb-ba48-1672976ff6ca">

<Transforms>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>OiF1RYFdqc4rnsmfz00khrFF800Ye7A6Pv2HMBFxs=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>pmQ1E5zIpwRB5JLliUoa7mHyolZuoG5o5Vf9dqHmfemBu1qCobe0saMC4SWZLaShvVF9rIg+i4mM+t2L07X9jhoprpYH1O3ZoVDQ5DHrnnBlnJJXy2X9N3m/q2zUVp2mEKp8VT1pTDbGtfMPqPVz5eq15SPVHsX3wLYpB4Qu+BYqjH4ZBQ8M6ybF3HObqH80vz8n3tWK53vY6OobBu9itFbywvSGL163ZUxH4BtjvOk0SZgB0bSecudSKLpRxcOYSxTjcZJbno4bsohwRnaHKZvr4TJhKH1eMQx/TdEprSSrxWdvoUllIwV71LJ0MOw==</SignatureValue>

<KeyInfo>

<wsse:SecurityTokenReference xmlns="">

```
<wsse:Reference URI="#SecurityToken-7c9e3edc-6cad-41c1-8585-1672976fbafd" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>

</wsse:SecurityTokenReference>

</KeyInfo>

</Signature>

</wsse:Security>

</soapenv:Header>

<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Body-e4b05d21-45c7-4dfb-ba48-1672976ff6ca">

<cor:getUserInfoout>

<mod:ResponseHeader>

<mod:SenderId>1205585055</mod:SenderId>

<mod:RequestId>1</mod:RequestId>

<mod:Timestamp>2022-01-03T11:18:18+01:00</mod:Timestamp>

<mod:ResponseCode>00</mod:ResponseCode>

<mod:ResponseText>OK.</mod:ResponseText>

<mod:ReceiverId>123</mod:ReceiverId>

</mod:ResponseHeader>

<mod:ApplicationResponse>PGMyYjpBcHBsaWNhdGlvblJlc3BvbnNlIHhtbG5zOmMyYj0iaHR0cDovL2J4ZC5maS94bWxkYXRhLyI+PGMyYjpDdXN0b21lcklkPjE3NTc1MTkyMTU8L2MyYjpDdXN0b21lcklkPjxjMmI6VGltZXN0YW1wPjIwMjItMDEtMDNUMTE6MTg6MTgrMDE6MDA8L2MyYjpUaW1lc3RhbXA+PGMyYjpSZXNwb25zZUNvZGU+
+PGMyYjpTZXJ2aWNlSWRPd25lck5hbWU+VElMSVRBTE8gT1lKPC9jMmI6U2VydmljZUlkT3duZXJOYW1lPjxjMmI6U2VydmljZUlkVHlwZT5BPC9jMmI6U2VydmljZUlkVHlwZT48YzJiOlNlcnZpY2VJZFRleHQ+RkkwOSAxNTcyIDMwMDAgMzI4NSA2NzwvYzJiOlNlcnZpY2VJZFRleHQ+PC9jMmI6RmlsZVR5cGVTZXJ2aWNlPjwvYzJiOkZpbGVUeXBlU2VydmljZXM+PC9jMmI6VXNlckZpbGVUeXBlPjxjMmI6VXNlckZpbGVUeXBlPjxjMmI6VGFyZ2V0SWQ+MDAwMDYwMjE1MzwvYzJiOlRhcmdldElkPjxjMmI6RmlsZVR5cGU+ +PGMyYjpGaWxlVHlwZVNlcnZpY2U+
+MDAwMDYwMjE1MzwvYzJiOlRhcmdldElkPjxjMmI6RmlsZVR5cGU+VElUTzwvYzJiOkZpbGVUeXBlPjxjMmI6RmlsZVR5cGVOYW1lPkFjY291bnQgU3RhdGVtZW50IEZJPC9jMmI6RmlsZVR5cGVOYW1lPjxjMmI6Q291bnRyeT5GSTwvYzJiOPGMyYjpEaXJlY3Rpb24+RG93bmxvYWQ8L2MyYjpEaXJlY3Rpb24+PGMyYjpGaWxlVHlwZVNlcnZpY2VzPjxjMmI6RmlsZVR5cGVTZXJ2aWNlPjxjMmI6U2VydmljZUlkLz48YzJiOlNlcnZpY2VJZE93bmVyTmFtZS8+PGMyYjpTZXJ2aWNlSWRUeXBlPk48L2MyYjpTZXJ2aWNlSWRUeXBlPjxjMmI6U2VydmljZUlkVGV4dC8+PC9jMmI6RmlsZVR5cGVTZXJ2aWNlPjwvYzJiOkZpbGVUeXBlU2VydmljZXM+PC9jMmI6VXNlckZpbGVUeXBlPjwvYzJiOlVzZXJGaWxlVHlwZXM+PFNpZ25hdHVyZSB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+CjxTaWduZWRJbmZvPgogIDxDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvVFIvMjAwMS9SRUMteG1sLWMxNG4tMjAwMTAzMTUiLz4KICA8U2lnbmF0dXJlTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8wNC94bWxkc2lnLW1vcmUjcnNhLXNoYTI1NiIvPgogIDxSZWZlcmVuY2UgVVJJPSIiPgogICAgPFRyYW5zZm9ybXM+
+PFg1MDlTZXJpYWxOdW1iZXI+NzQ3NTA8L1g1MDlTZXJpYWxOdW1iZXI+PC9YNTA5SXNzdWVyU2VyaWFsPjwvWDUwOURhdGE+PC9LZXlJbmZvPjwvU2lnbmF0dXJlPjwvYzJiOkFwcGxpY2F0aW9uUmVzcG9uc2U+</mod:ApplicationResponse>

</cor:getUserInfoout>

</soapenv:Body>

</soapenv:Envelope>
```

Nordea

Examples of Certificate download ApplicationResponse with SHA256 algorithm

Part of XML, some parts are scrambled

<bxd:CertApplicationResponse xmlns:bxd="http://filetransfer.nordea.com/xmldata/">

<bxd:CustomerId>123</bxd:CustomerId>

<bxd:Timestamp>2022-07-26T09:07:39+02:00</bxd:Timestamp>

<bxd:ResponseCode>00</bxd:ResponseCode>

<bxd:ResponseText>OK</bxd:ResponseText>

<bxd:Certificates>

<bxd:Certificate>

<bxd:Name/>

<bxd:Certificate>MIIDhzCCAm+
/V4fF7nTuojoH5fyMPfVG1w51z6bQd3nH/Dv43cE63XN+PB01YYbitumaIemlOLtecaoTnXOC5IkUvil/BuC0Pl5
G2W6QtF+bVT+OcnqW90KXFM8hPRZ3Pv2xmasYWzO9G01B19jcOifNWOldaPHvYXaYnN8fkYh3U958L2w
248ltUWAEGNFJ5RLIFvlbDT4q6p7RsWKhj/P3sChsr7K2KLkqmw9+cktwC2cx/JhOIm5Cxa8cnHuKfeVAgMBA
AGjWjBYMAkGA1UdEwQCMAAwEQYDVR0OBAoECEkxiik2O6AGMBMGA1UdIAQMMAowCAYGKoVw
RwEDMBMGA1UdIwQMMAqACEhef7PQ7k5qMA4GA1UdDwEB/wQEAwIFoDANBgkqhkiG9w0BAQUFAA
OCAQEAbphK4XcwvUplchs1wRUdEI08sQF4EXagoS604HJzwiqXHJWegu8LuyboijM5TqBa3vG5DJN6bqDZPg
cCTsuM4EZb9rhcsskjNrzRAOHbGg1RL1DRLBfAl1NudO2GDgXVT3V0G1sc3QeWVa09zrDfIEnJeb4opju6L9G
BjSfe5+Q6dWAQM0lDX73PepYoClVdku8YMoDSYQAYtSSpVif+WNfpEejmiqsExoMxJLFDQy28EmvqVIaKw
wVXsutP/rAOcR4PHUj6c0TjasuM1EzuwjdtLE+Qm7o0fMIK19zEt80msJuP9PtpPhVgfcRCW86jhqYEazhY1pRlB
fdACgQ==</bxd:Certificate>

<bxd:CertificateFormat>X509v3</bxd:CertificateFormat>

</bxd:Certificate>

</bxd:Certificates>

<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/2001/04/xmldsig-more#rsa-sha256"/>

<Reference URI="">

<Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>YVZZReQcxerescx322QDY80vaCn8VM=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>orIw0FOtBCY3iakHpyZ7+2KZ0Uw9Gx1vg0F5M2nzuebJpvM0+4YQfMPV5G+jCz9iG87M+5nyJHt4jhoPE/wRKL1mgZLd8mFQmPaHMlSS5WTv/ ==</SignatureValue>

<KeyInfo>

<X509Data>

<X509Certificate>MIIDqjCCApKgAwIBAgIDAS/ +kg7x+iVaRgjQ1rGSIgx6/zklacH/TQH+ +HnJwn2L+/ksgLg3RLgeYvxcErP8B9MIjae/UvVHBGQJs19jqcrRuYBohytsjvVN4vS2300wCdMBKfDmQ74h8rvDe6YcnHUNtH8HYATxkC4MpVRxQArM4z3oe0qV7tFh5rizle+lT6UTOt2vtmJ+HQ3R+ve322zd2ykslroN7sxK3Q0VbM3pqU9MiGljR5nMQaFJasZJotvGrN9rdmh</X509Certificate>

<X509IssuerSerial>

<X509IssuerName>serialNumber=516411-1683, CN=Nordea Corporate Server CA 03, O=Nordea Bank Abp, C=SE</X509IssuerName>

<X509SerialNumber>77769</X509SerialNumber>

</X509IssuerSerial>

</X509Data>

</KeyInfo>

</Signature>

</bxd:CertApplicationResponse>

Examples of Certificate download SOAP Response with SHA256 algorithm

Part of XML, some parts are scrambled

<soapenv:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cer="http://bxd.fi/CertificateService" xmlns:mod="http://model.bxd.fi" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

<soapenv:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">

<wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-adacf386-21bc-4de3-ae87-0d61fa04576f">

<wsu:Created>2022-07-26T07:07:39Z</wsu:Created>

<wsu:Expires>2022-07-26T07:12:39Z</wsu:Expires>

</wsu:Timestamp>

<wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="SecurityToken-eda9b57c-ef09-4ec9-978f-0d61fa046871">MIIDqjCCApKgAwIBAgIDAS/ +OOeswDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBQUAA4IBAQBFqzjSxuW1S8yB27HQ//9eOcaWGtsp/5Ev388mpm9dKbcE+qFf45r9C/XUTudl3KTsQd+PeUwUYLxXDjnkSiO8ppnurfcM80XhZoE6SCVGsEiK5aDt9A9Zt28a5+LBvcJaA+HnJwn2L+/ksgLg3RLgeYvxcErP8B9MIjae/UvVHBGQJs19jqcrRuYBohytsjvVN4vS2300wCdMBKfDmQ74h8rvDe6YcnHUNtH8HYATxkC4MpVRxQArM4z3oe0qV7tFh5rizle+lT6UTOt2vtmJ+HQ3R+ve322zd2ykslroN7sxK3Q0VbM3pqU9MiGljR5nMQaFJasZJotvGrN9rdmh</wsse:BinarySecurityToken>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

<SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

<Reference URI="#Timestamp-adacf386-21bc-4de3-ae87-0d61fa04576f">

<Transforms>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>YAfrgJN3ujWRERETZ31qT3c546PDg=</DigestValue>

</Reference>

<Reference URI="#Body-a791e2b5-6006-4591-8757-0d61fa048ad6">

<Transforms>

<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</Transforms>

<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>FioIa89pAWEREGXIrxzP6ipLSaMk=</DigestValue>

</Reference>

</SignedInfo>

<SignatureValue>wA6JQzRRTSTWii3RKoX+XFByO81ejs7gdkNEIxSePDbtykcv1spklADgZkiKPcK4IxyuDIrEjJf57kZqR2OhXvROKX8wDSlKAmrdnDhu/Ze45fQD6RgceoyQYWj0ElSmGTxP4YqqbuIG7phxMRn4jUQ==</SignatureValue>

<KeyInfo>

<wsse:SecurityTokenReference xmlns="">

<wsse:Reference URI="#SecurityToken-eda9b57c-ef09-4ec9-978f-0d61fa046871" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>

</wsse:SecurityTokenReference>

</KeyInfo>

</Signature>

</wsse:Security>

</soapenv:Header>

<soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Body-a791e2b5-6006-4591-8757-0d61fa048ad6">

<cer:getCertificateout>

<cer:ResponseHeader>

<cer:SenderId>123</cer:SenderId>

<cer:RequestId>123</cer:RequestId>

<cer:Timestamp>2022-07-26T09:07:39+02:00</cer:Timestamp>

<cer:ResponseCode>00</cer:ResponseCode>

<cer:ResponseText>OK</cer:ResponseText>

</cer:ResponseHeader>

<cer:ApplicationResponse>PGJ4ZDpDZXJ0QXBwbGljYXRpb25SZXNwb25zZSB4bWxuczpieGQ9Imh0dHA6Ly
9maWxldHJhbnNmZXIubm9yZGVhLmNvbS94bWxkYXRhLyI+PGJ4ZDpDdXN0b21lcklkPjEyMzwvYnhkOkN1
c3RvbWVySWQ+PGJ4ZDpUaW1lc3RhbXA+MjAyMi0wNy0yNlQwOTowNzozOSswMjowMDwvYnhkOlRpbW
VzdGFtcD48YnhkOlJlc3BvbnNlQ29kZT4wMDwvYnhkOlJlc3BvbnNlQ29kZT48YnhkOlJlc3BvbnNlVGV4dD5P
SzwvYnhkOlJlc3BvbnNlVGV4dD48YnhkOkNlcnRpZmljYXRlcz48YnhkOkNlcnRpZmljYXRlPjxieGQ6TmFtZS8
+PGJ4ZDpDZXJ0aWZpY2F0ZT5NSUlEaHpDQ0FtK2dBd0lCQWdJQ1VUc3dEUVlKS29aSWh2Y05BUUVGQlF
Bd2FURUxNQWtHQTFVRUJoTUNVMFV4SGpBY0JnTlZCQW9URlU1dmNtUmxZU0JDWVc1cklFRkNJQ2h3
ZNzc2tqTnJ6UkFPSGJHZzFSTDFEUkxCZkFsMU51ZE8yR0RnWFZUM1YwRzFzYzNRZVdWYTA5enJEZklFb
kplYjRvcGp1Nkw5R01tQUJqU2ZlNStRNmRXQVFNMGxEWDczUGVwWW9DbFZka3U4WU1vRFNZUUFZd
FNTcFZpZitXTmZwRWVqbWlxc0V4b014SkxGRFF5MjhFbXZxVklhS3d3VlhzdXRQL3JBT2NSNFBIVWo2Yz
BUamFzdU0xRXp1d2pkdExFK1FtN28wZk1JSzE5ekV0ODBtc0p1UDlQdHBQaFZnZmNSQ1c4NmpocVlFYXpo
WTFwUmxCZmRBQ2dRPT08L2J4ZDpDZXJ0aWZpY2F0ZT48YnhkOkNlcnRpZmljYXRlRm9ybWF0Plg1MDl2
MzwvYnhkOkNlcnRpZmljYXRlRm9ybWF0PjwvYnhkOkNlcnRpZmljYXRlPjwvYnhkOkNlcnRpZmljYXRlcz48
U2lnbmF0dXJlIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4KPFNpZ25lZEluZm
8+CiAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy9UUi8y
MDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIvPgogIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJo
dHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjcnNhLXNoYTEiLz4KICA8UmVmZXJlbmNlIFVSS
T0iIj4KICAgIDxUcmFuc2Zvcm1zPgogICAgICA8VHJhbnNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5v
cmcvMjAwMC8wOS94bWxkc2lnI2VudmVsb3BlZC1zaWduYXR1cmUiLz4KICAgICAgPFRyYW5zZm9ybSBBbG
Gdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvUkVDLXhtbC1jMTRuLTIwMDEwMzE1Ii8+CiA
gICA8L1RyYW5zZm9ybXM+CiAgICA8RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vc
mcvMjAwMC8wOS94bWxkc2lnI3NoYTEiLz4KICAgIDxEaWdlc3RWYWx1ZT5ZVlpaUmVRY3g2eFU3ZzJRR
Fk4MHZhQ244Vk09PC9EaWdlc3RWYWx1ZT4KICA8L1JlZmVyZW5jZT4KPC9TaWduZWRJbmZvPgogICAg
PFNpZ25hdHVyZVZhbHVlPm9ySXcwRk90QkNZM2lha0hweVo3KzJLWjBVdzlHeDF2ZzBGNU0ybnp1ZWJKc
HZNMCs0WVFmTVBWNUcrakN6OWlHODdNKzVueUpIdDRqaG9QRS93UktMMW1nWkxkOG1GUW1QYUh
NbFNTNVdUdi9JSWtteFNkb3FUaWxGblU1WHYydDhTREx6ODNONmVOVE9GY3F3NzZrM1ltNEY1WC9Oc
WdtTmpSSS9XYmZ4Vk1EaDlJZnVnQWl4WFBFMmMvRDVJT3VvNlBPdkNjZjdDK1NnYUNZdXFDdWkzW
XVoUzhkNDBzRkFUT0g2NnB0aUh2Y2YvcXpGbllQWitkK09uclRFTVBnUzJtL2VyYmxMN2dvcnFsNU1MWn
hFM01UZjhaOFVJMXZMYWtqZHpoaHZ5eTFscUljVlA0a1lzVGpFR0lUaDNTRTQ2cEpUOXpDcUZBUVVDa
U03T285UT09PC9TaWduYXR1cmVWYWx1ZT48S2V5SW5mbz48WDUwOURhdGE+PFg1MDlDZXJ0aWZpY
2F0ZT5NSUlEcWpDQ0FwS2dBd0lCQWdJREFTL0pNQTBHQ1NxR1NJYjNEUUVCQlFVQU1HVXhDekFKQm
dOVkJBWVRBbE5GTVJnd0ZnWURWUVFLRXc5T2IzSmtaV0VnUW1GdWF5QkJZbkF4SmpBa0JnTlZCQU1U
SFU1dmNtUmxZU0JEYjNKd2IzSmhkR1VnVTJWeWRtVnlJRU5CSURBek1SUXdFZ1lEVlFRRkV3czFNVFkw
TVRF1FkK1BlVXdVWUx4WERqbmtTaU84cHBudXJmY004MFhoWm9FNlNDVkdzRWlLNWFEdDlBOVp0Mj
hhNStMQnZjSmFBK0huSnduMkwrL2tzZ0xnM1JMZ2VZdnhjRXJQOEI5TUlqYWUvVXZWSEJHUUpzMTlqcW
NyUnVZQm9oeXRzanZWTjR2UzIzMDB3Q2RNQktmRG1RNzRoOHJ2RGU2WWNuSFVOdEg4SFlBVHhrQzR
NcFZSeFFBck00ejNvZTBxVjd0Rmg1cml6bGUrbFQ2VVRPdDJ2dG1KK0hRM1IrdmUzMjJ6ZDJ5a3Nscm9ON3
N4SzNRMFZiTTNwcVU5TWlHbGpSNW5NUWFGSmFzWkpvdHZHck45cmRtaDwvWDUwOUNlcnRpZmljYX
RlPjxYNTA5SXNzdWVyU2VyaWFsPjxYNTA5SXNzdWVyTmFtZT5zZXJpYWxOdW1iZXI9NTE2NDExLTE2
ODMsIENOPU5vcmRlYSBDb3Jwb3JhdGUgU2VydmVyIENBIDAzLCBPPU5vcmRlYSBCYW5rIEFicCwgQz1T
RTwvWDUwOUlzc3Vlck5hbWU+PFg1MDlTZXJpYWxOdW1iZXI+Nzc3Njk8L1g1MDlTZXJpYWxOdW1iZXI
+PC9YNTA5SXNzdWVyU2VyaWFsPjwvWDUwOURhdGE+PC9LZXlJbmZvPjwvU2lnbmF0dXJlPjwvYnhkOk
NlcnRBcHBsaWNhdGlvblJlc3BvbnNlPg==</cer:ApplicationResponse>

</cer:getCertificateout>

</soapenv:Body>

</soapenv:Envelope>