Web Services, SHA1 – SHA256 changes

Technical Description

Table of Contents

Appendix

1. General

This document describes the SHA1 to SHA256 change in Web Services data communication protocol (hereinafter 'the protocol') produced by Nordea (hereinafter 'Nordea' or 'the bank').

1.1 Web Services

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

The Web Services connection can be used to transmit local Cash Management service files used in Finland, Estonia, Latvia and Lithuania. Web Services connection supports also file types which are used in Corporate eGateway service.

1.2 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 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 logon 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 request files in Appendix

d. When Nordea sends customers responses, the responses 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.

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, 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). Nordea recommends customer to use 2048. The new version of NSC client offered by Nordea will support both 1024 and 2048 key length

After Sep 27th 2022, even if customer defines the algorithm as SHA1 in the CSR, Nordea will overwrite it to SHA256 and issue SHA256 certificate.

2.1 Customer effort

2.1.1 Development in Web Services 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 provided new version of NSC client in Q4 2022, which support 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

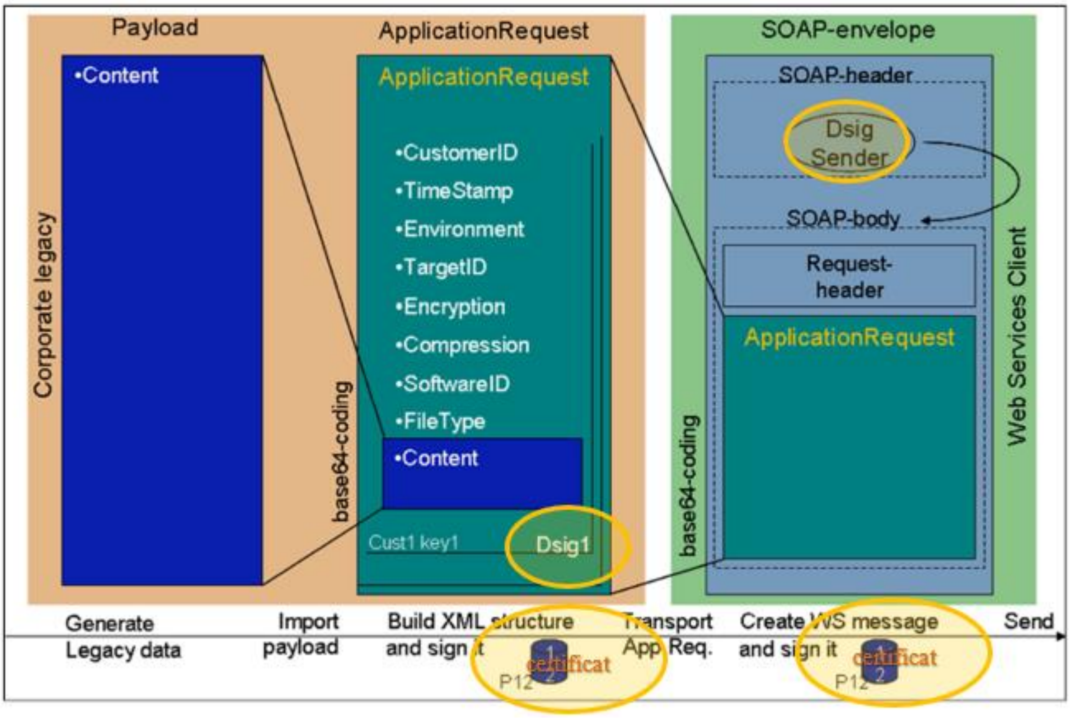
Nordea had implemented the change to issue SHA256 certificates to customers on Sep 27th 2022.

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

3. Change in Web Services Requests

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

Diagram below shows the process of creating ApplicationReques 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.



Previously, 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.

Now, in additional to old supported algorithms, Nordea will also support 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 Q1-Q2 of 2024, Nordea will stop supporting the SHA1 algorithm. Requests signed with SHA1 algorithm will be rejected.

3.1 Customer effort

3.1.1 Development in Web Services software client

Customers need to develop own software client so that the SHA256 algorithm will be used when creating the digital signature in the ApplicationRequest and SOAPRequest to Nordea.

3.1.2 Testing and Migration

Nordea will support both SHA1 and SHA256 algorithms for a period and discontinue support of SHA1 in Q1-Q2 of 2022. 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 Web Services responses from Nordea

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

Nordea's responses have been signed with SHA1 certificate and SHA1 algorithms. In Feb 2022, Nordea deployed parallel services

Existing service https://filetransfer.nordea.com/services/CorporateFileService

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

- No change as of today. Nordea's messages will be signed with SHA1 certificate and SHA1 algorithms
- For customers messages towards Nordea, service supports both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
- And in the end of Q1 of 2024, Nordea will close this service though

New service https://filetransfer.nordea.com/services/CorporateFileService/sha2

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

- Nordea's ApplicaResponses and SOAP-envelope messages will be signed with SHA256 certificate and SHA256 algorithms
- For customers messages towards Nordea, service support both SHA1 and SHA256 certificates, and SHA1 and SHA256 signing algorithm
    - However during Q1-Q2 of 2024, Nordea will stop supporting the SHA1 algorithm in this service, customer messages towards Nordea signed with SHA1 algorithm will be rejected.

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

Nordea's new SHA256 signing certificate and the Root CA certificate are published in Nordea.fi

4.1 Customer effort

4.1.1 Development in 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.

4.1.2 Testing and Migration

Customers can use the new service to develop and test, while still use the old service in the daily operation.

Customers have long period for development, testing and migration before Nordea stops support of SHA1 in Q1-Q2 of 2024. Nordea will send newsletters to customers in advance to inform the exact date.

5. Change of Disabling TLS 1.0 and 1.1

Transport Layer Security (TLS) 1.0 and 1.1 are security protocols for establishing encryption channels over computer networks. Nordea Web Services 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' Web Services client software, and Nordea will stop the support of TLS 1.0 and 1.1 in Q2 2024. Nordea will send newsletter to customers in advance to inform the exact date.

6. Summary on customer efforts

Change area	Customer development efforts needed	Customer testing and migration efforts needed	Timeline
The customer signing certificate (linked to each logon 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 by Nordea. Nordea will overwrite the algorithm setting customer defines in CSR (certificate signing request) and issue SHA256 certificate. Both the current vesion 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 Q1-Q2 2024, 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.
In the new service which runs parallelly to the existing service, when Nordea sends customers responses, the responses are signed with Nordea's new SHA256 certificate and with SHA256 signing algorithm.	Yes	Yes	Nordea uses SHA256 certificate and algorithm in the new services. Existing services remain unchanged and it is with SHA1. Nordea will stop SHA1 service in Q1 2024 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	Yes if customers uses own software client to download certificate. Otherwise, customers can use the new		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.

Nordea, so that the customer signing certificate will have key length 2048.	NSC client which Nordea provides		A new version of NSC client which supports 2048 key length has been available since Q4 2022
Nordea will stop support of TLS 1.0 and 1.1	Yes	Yes	By Q2 2024, will inform exact time later

Appendix

Examples of ApplicationRequest with SHA256 algorithm

Part of XML

```
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
   <CustomerId>11111111</CustomerId>
   <Command>DownloadFileList</Command>
   <Timestamp>2022-01-12T11:13:50.907+02:00</Timestamp>
   <Status>ALL</Status>
   <Environment>PRODUCTION</Environment>
   <SoftwareId>NordeaTest</SoftwareId>
   <FileType>VKEUR</FileType>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
         <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>k9HODYPZaWAoM3GCLTbodICPzZxsH+OLKb7kAEc4yv4=</DigestValue>
         </Reference>
      </SignedInfo>
<SignatureValue>MvLEc8SsHlZ45dsQ8cBWwJo2QqshlAAGidEPgJ26mNNv2GJLAY1i9URg2Kawf9/flk7a/
45T4uMwUtVcVw5useEo=</SignatureValue>
      <KeyInfo>
         <X509Data>
<X509Certificate>MIIC9DCCAdygAwIBAgICP3UwDQYJKoZIhvcNAQELBQAwaTELMAkGA1UEBhMCU0UxHjAcBgNV
BAoT FU5vcmRlYSBCYW5rIEFCIChwdWJsKTEkMCIGA1UEAxMbTm9yZGVhIFRlc3QgQ29ycG9yYXRlIENB
5mecJ0qsNc0GI2BtWoZ1FBlwR8huZ5u6yFwOV2UNWGk0msFS11DyLxRuLMpXcDhaaBZnB5RvpLlC
UcDAqpYXrK+nYtHmJJFSCsl6WA==</X509Certificate>
            <X509IssuerSerial>
               <X509IssuerName>2.5.4.5=#130b3531363430362d30313230,CN=Nordea Corporate CA 01,O=Nordea Bank AB
```

```
(publ),C=SE</X509IssuerName>
          <X509SerialNumber>76885</X509SerialNumber>
        </X509IssuerSerial>
      </X509Data>
    </KeyInfo>
  </Signature>
</ApplicationRequest>
```

Examples of SOAP Request with SHA256 algorithm

Part of XML

```
<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-16419789927838309487l9">
        <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+zCCAeOgAwIBAgIDASxVMA0GCSqGSIb3DQEBBQUAMGQxCzAJBgNVBAYTAlNFMR4wHAYDV
QQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxHzAdBgNVBAMTFk5vcmRlYSBDb3Jwb3JhdGUgZmljYXRlMRMwEQY
DVQQFEwo1NzgwODYwMjM4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCClmzyaVAEr2cTt5gGPxuiMxZ5
JZRIDHUwyUMIags/JYbKCq/MhumUEDDAKMAgGBiqFcEcBAzATBgNVHSMEDDAKgAhAC3XW288LpzAOBgNVHQ8
BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQADggEBADVuzhr4KJwDXHph5fm5BOqufAI0fnUP5rFYfpDz3gRbyicRcBFj2
hkIG+8wMUKiTfASheRYL1hydk4ElJ3gaeieD7Yn9OxMILy+svh3YXGWnw9z9msRRyvJdVNLwws2sUgxlv66iPJR0qVIT55f
Led9YXbfdb/tPE+g10Qw62kXyZkDNoxeI8lUuihFLX20H/SPaRRHCAootUoNxuzFIuEHl/5zL3FMBWSsxdkfGrqmzF8/C5a31
GXWGgn/JK7KI1BYKx/weVWRui0FI5nfIJQ=</wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-16419789926732541 48581">
        <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-16419789927838309487 19">
            <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&#13;
SexTD/5LN6q7OMdpJ2dhA3xtEtU5LOz4geQ6Gh1DycI6WuLxce3cNDpGL7gPUhw&#13;
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>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48QXBwbGljYXRpb25SZXF1ZXN0I
HhtbG5zPSJodHRwOi8vYnhkLmZpL3htbGRhdGEvIj4NCiAgICA8Q3VzdG9tZXJJZD4xMTExMTExMTwvQ3VzdG9tZXJJZ
D4NCiAgICA8Q29tbWFuZD5Eb3dubG9hZEZpbGVMaXN0PC9Db21tYW5kPg0KICAgIDxUaW1lc3RhbXA+
jZpUEpSMHFWSVQ1NWZMZWQ5WVhiZiYjMTM7DQpkYi90UEUrZzEwUXc2MmtYeVo5MzROS0xVWHZ4eGdBaWlw
WXlSd0FWTHNsYmcwdThQT0tCeFQ1MjdmNHRXRHc1cGVpS3A3bHRzRUNMJiMxMzsNCkJYYXZjMGtETm94ZUk4bF
V1aWhGTFgyMEgvU1BhUlJIQ0Fvb3RVb054dXpGSXVFSGwvNXpMM0ZNQldTc3hka2ZHcnFtekY4L0M1YTMmIzEzOw0
```

```
KMUdYV0dnbi9KSzdLSTFCWUt4L3dlVldSdWkwRkk1bmZJSlE9PC9YNTA5Q2VydGlmaWNhdGU+PFg1MDlJc3N1ZXJT
ZXJpYWw+PFg1MDlJc3N1ZXJOYW1lPjIuNS40LjU9IzEzMGIzNTMxMzYzNDMwMzYyZDMwMzEzMjMwLENOPU5vc
mRlYSBDb3Jwb3JhdGUgQ0EgMDEsTz1Ob3JkZWEgQmFuayBBQiAocHVibCksQz1TRTwvWDUwOUlzc3Vlck5hbWU+PF
g1MDlTZXJpYWxOdW1iZXI+NzY4ODU8L1g1MDlTZXJpYWxOdW1iZXI+PC9YNTA5SXNzdWVyU2VyaWFsPjwvWDU
wOURhdGE+PC9LZXlJbmZvPjwvU2lnbmF0dXJlPjwvQXBwbGljYXRpb25SZXF1ZXN0Pg==</ApplicationRequest>
    </ns2:downloadFileListin>
  </S:Body>
</S:Envelope>
```

Examples of ApplicationResponse with SHA256 algorithm

Part of XML

```
<c2b:ApplicationResponse xmlns:c2b="http://bxd.fi/xmldata/">
  <c2b:CustomerId>1753419215</c2b:CustomerId>
  <c2b:Timestamp>2022-01-03T11:18:18+01:00</c2b:Timestamp>
  <c2b:ResponseCode>00</c2b:ResponseCode>
  <c2b:ResponseText>OK.</c2b:ResponseText>
  <c2b:Encrypted>false</c2b:Encrypted>
  <c2b:Compressed>false</c2b:Compressed>
  <c2b:UserFileTypes>
    <c2b:UserFileType>
      <c2b:TargetId>0000602153</c2b:TargetId>
      <c2b:FileType>INFO</c2b:FileType>
      <c2b:FileTypeName>Info</c2b:FileTypeName>
      <c2b:Country>FI</c2b:Country>
      <c2b:Direction>Download</c2b:Direction>
      <c2b:FileTypeServices>
        <c2b:FileTypeService>
          <c2b:ServiceId/>
          <c2b:ServiceIdOwnerName/>
          <c2b:ServiceIdType>N</c2b:ServiceIdType>
          <c2b:ServiceIdText/>
        </c2b:FileTypeService>
      </c2b:FileTypeServices>
    </c2b:UserFileType>
    <c2b:UserFileType>
      <c2b:TargetId>0000602153</c2b:TargetId>
      <c2b:FileType>VKEUR</c2b:FileType>
      <c2b:FileTypeName>Rates of exchange</c2b:FileTypeName>
      <c2b:Country>FI</c2b:Country>
      <c2b:Direction>Download</c2b:Direction>
      <c2b:FileTypeServices>
```

```
        <c2b:FileTypeService>
          <c2b:ServiceId/>
          <c2b:ServiceIdOwnerName/>
          <c2b:ServiceIdType>N</c2b:ServiceIdType>
          <c2b:ServiceIdText/>
        </c2b:FileTypeService>
      </c2b:FileTypeServices>
    </c2b:UserFileType>
  </c2b:UserFileTypes>
  <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>Vs/PeGRIiXx/qSWirbhcHy3REYse6HyvjaF6kI=</DigestValue>
 </Reference>
</SignedInfo>
<SignatureValue>qG54/FBZeoOP0KK47O/b0Gz51m/SHgQOi0lWVKtnk3s57v3PV3EsxkRRjMdal1InZn4KHon9Ae6mgdHS5
wJbj/OV64jlNevao5+gMjLaG2qFzkIVWpGgZiEweGyMWQ7X4BiLw0BtUnWkK+zIsrj+3dJkp95OcRvXnUXX1dDYp83eup5
lF+zMx3rqghg7xUMh1honXRtIRm+R24wNUPCYDKsoeh4AUfZmpQO9LHgKLLOGZXK20G+LGWhOAo+gcNe/gfMmVk
GeMCQtimx/T6mejNv0vBqB0XlCsEcLVv/2zlFeFJHC9eiLDc3DxC5QtW2loGWKK8qHFLuuvlRQ==</SignatureValue>
    <KeyInfo>
      <X509Data>
<X509Certificate>MIIDizCCAnOgAwIBAgIDASP+MA0GCSqGSIb3DQEBCwUAMGsxCzAJBgNVBAYTAlNFMR4wHAY
DVQQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxJjBgNVBAMTHU5vcmRlYSBDb3Jwb3JhdGUgU2VydmVyIENBIDAx
MRQwEgYDVQQFEws1MTY0MDYtMDEyAeFw0yMDEyMjExMjMxMDVaFw0yMjExMjcxMjMzNTBaMG4xCzAJBgNV
BAYTAlNFMRgwFgYDVQQKDA9Ob3JkZWEgQmFuayBBYnAxGzAZBgNVBAsMEkNvcnBvcmF0ZSBDaGFubmVsczEo
MCYGA1UEAwwfRmlsZSBUcmFuc2ZlciBXZWIgU2VydmljZXMgVGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPAD
CCAQoCggEBAPJE8EzsdUL4vg/01xmhdWDnYhP0jsWrpWKXD8RPM2XMVhslnNHrIZNEXC15AUzep27fVF3Y7ujbu+vJC
U7ECAwEAAaM1MDMwCQYDVRTBAIwADARBgNVHQ4ECgQIQrtcU9YxVbUwEwYDVR0jBAwwCoAIRMeT2dl7VsE
wDQYJKoZIhvcNAQELBQADggEBAKD2tlB86c/lmkG2ntXkAqiAzZMipRVSN1/ZZkOtmBuf56ziUQQMLORipMjlyP9grDh
JIIOqqhsL1jo+GSDBSdceW0o8Uh5bhrnGT864Ozj4tS354sgE5UUKcUYZUiw70PGP9gJKlp6kLFTlKNhJ0oI8eaItbU5A6c7K
Xgou44SfaN12I4m/wBZY1147PQa8X5B1npHruVbhbhbQccVurnF3qjpLHFKslnBl39tJ4taYwBqRe81pR3S6p2Hm9lWFK5nU
3Ef/LIeeFsWVCpfR2x0BOB0gFbLOPFjC+FfQvLZ2A4I4+gjL321mVz7sp4zVZ86oKXolrTzexg+E=</X509Certificate>
        <X509IssuerSerial>
          <X509IssuerName>serialNumber=516406-0120, CN=Nordea Corporate Server CA 01, O=Nordea Bank AB (publ),
C=SE</X509IssuerName>
          <X509SerialNumber>74750</X509SerialNumber>
        </X509IssuerSerial>
      </X509Data>
```

```
        </KeyInfo>
    </Signature>
</c2b:ApplicationResponse>
```

Examples of SOAP Response with SHA256 algorithm

Part of XML

```
<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+MA0GCSqGSIb3DQEBCwUAMGsxCzAJBgNVBAYTAlNFMR4wHAYDV
QQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxJjAkBgNVBAMTHU5vcmRlYSBDb3Jwb3JhdGUgU2VydmVyIENBIDAx
MR1MTY0MDYtMDEyMDAeFw0yMDEyMjExMjMxMDVaFw0yMjExMjcxMjMzNTBaMG4xCzAJBgNVBAYTAlNFMRg
wFgYDVQQKDA9Ob3JkZWEgQmFuayBBYnAxGzAZBgNVBAsMEkNvcnBvcmF0ZSBDaGFubmVsczEoMCYGA1UEAw
wfRmlsZSBUcmFuc2ZlciBXZWIgU2VydmljZXMgVGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
+vJCU7ECAwEAAaM1MDMwCQYDVR0TBAIwADARBgNVHQ4ECgQIQrtcU9YxVbUwEwYDVR0jBAwwCoAIRMeT2dl
7VsEwDQYJKoZIhvcNAQELBQADggEBAKD2tlB86c/lmtXkAqiAzZMipRVSN1/ZZkOtmBuf56ziUQQMLORipMjlyP9grDh
JIIOqqhsL1jo+BSdceW0o8Uh5bhrNeC6roLnGT864Ozj4tS354sgE5UUKcUYZUiw70PGP9gJKlp6kLFTlKNhJ0oI8eaItbU5A6c
7KXgou44SfaN12I4m/wBZY1147PQa8X5B1npHruVbhbhbQccVurnF3qjpLHFKslnBl39tJ4taYwBqRe81pR3S6p2Hm9lWFK5
nU3Ef/LIeeFsWVCpfR2x0BOB0gFbLOPFjC+FfQvLZ2A4I4+gjL321mVz7sp4zVZ86oKXolrTzexg+E=</wsse:BinarySecurity
Token>

      <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+t2L0
7X9jhoprpYH1O3ZoVDQ5DHrnnBlnJJXy2X9N3m/q2zUVp2mEKp8VT1pTDbGtfMPqPVz5eq15SPVHsX3wLYpB4Qu+BYqj
H4ZBQ8M6ybF3HObqH80vz8n3tWK53vY6OobBu9itFbywvSGL163ZUxH4BtjvOk0SZgB0bSecudSKLpRxcOYSxTjcZJbno4
bsohwRnaHKZvr4TJhKH1eMQx/TdEprSSrxWdvoUIlIwV71LJ0MOw==</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>PGMyYjpBcHBsaWNhdGlvblJlc3BvbnNlIHhtbG5zOmMyYj0iaHR0cDovL2J4ZC5maS94bWxkY
XRhLyI+PGMyYjpDdXN0b21lcklkPjE3NTc1MTkyMTU8L2MyYjpDdXN0b21lcklkPjxjMmI6VGltZXN0YW1wPjIwMjItMD
EtMDNUMTE6MTg6MTgrMDE6MDA8L2MyYjpUaW1lc3RhbXA+PGMyYjpSZXNwb25zZUNvZGU+
+PGMyYjpTZXJ2aWNlSWRPd25lck5hbWU+VElMSVRBTE8gT1lKPC9jMmI6U2VydmljZUlkT3duZXJOYW1lPjxjMmI6U2
VydmljZUlkVHlwZT5BPC9jMmI6U2VydmljZUlkVHlwZT48YzJiOlNlcnZpY2VJZFRleHQ+RkkwOSAxNTcyIDMwMDAgM
zI4NSA2NzwvYzJiOlNlcnZpY2VJZFRleHQ+PC9jMmI6RmlsZVR5cGVTZXJ2aWNlPjwvYzJiOkZpbGVUeXBlU2VydmljZX
M+PC9jMmI6VXNlckZpbGVUeXBlPjxjMmI6VXNlckZpbGVUeXBlPjxjMmI6VGFyZ2V0SWQ+MDAwMDYwMjE1Mzwv
YzJiOlRhcmdldElkPjxjMmI6RmlsZVR5cGU+ +PGMyYjpGaWxlVHlwZVNlcnZpY2U+
+MDAwMDYwMjE1MzwvYzJiOlRhcmdldElkPjxjMmI6RmlsZVR5cGU+VElUTzwvYzJiOkZpbGVUeXBlPjxjMmI6RmlsZV
R5cGVOYW1lPkFjY291bnQgU3RhdGVtZW50IEZJPC9jMmI6RmlsZVR5cGVOYW1lPjxjMmI6Q291bnRyeT5GSTwvYzJiO
PGMyYjpEaXJlY3Rpb24+RG93bmxvYWQ8L2MyYjpEaXJlY3Rpb24+PGMyYjpGaWxlVHlwZVNlcnZpY2VzPjxjMmI6Rml
sZVR5cGVTZXJ2aWNlPjxjMmI6U2VydmljZUlkLz48YzJiOlNlcnZpY2VJZE93bmVyTmFtZS8+PGMyYjpTZXJ2aWNlSWR
UeXBlPk48L2MyYjpTZXJ2aWNlSWRUeXBlPjxjMmI6U2VydmljZUlkVGV4dC8+PC9jMmI6RmlsZVR5cGVTZXJ2aWNlPj
wvYzJiOkZpbGVUeXBlU2VydmljZXM+PC9jMmI6VXNlckZpbGVUeXBlPjwvYzJiOlVzZXJGaWxlVHlwZXM+PFNpZ25hd
HVyZSB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+CjxTaWduZWRJbmZvPgogIDxDYW5v
bmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvVFIvMjAwMS9SRUMteG1sLWMxNG
4tMjAwMTAzMTUiLz4KICA8U2lnbmF0dXJlTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8wN
C94bWxkc2lnLW1vcmUjcnNhLXNoYTI1NiIvPgogIDxSZWZlcmVuY2UgVVJJPSIiPgogICAgPFRyYW5zZm9ybXM+
+PFg1MDlTZXJpYWxOdW1iZXI+NzQ3NTA8L1g1MDlTZXJpYWxOdW1iZXI+PC9YNTA5SXNzdWVyU2VyaWFsPjwvW
DUwOURhdGE+PC9LZXlJbmZvPjwvU2lnbmF0dXJlPjwvYzJiOkFwcGxpY2F0aW9uUmVzcG9uc2U+</mod:ApplicationRes
ponse>

    </cor:getUserInfoout>

  </soapenv:Body>

</soapenv:Envelope>
```