

Web Services, SHA1 – SHA256 changes

Technical Description

Table of Contents

Technical Description	1
1. General	3
1.1 Web Services.....	3
1.2 SHA1 – SHA256 Change	3
2. Change in customer signing certificate.....	3
2.1 Customer effort	4
2.1.1 Development in Web Services software client.....	4
2.1.2 Testing and Migration	4
3. Change in Web Services Requests	4
3.1 Customer effort	5
3.1.1 Development in Web Services software client.....	5
3.1.2 Testing and Migration	5
4. Change in Web Services responses from Nordea	6
4.1 Customer effort	6
4.1.1 Development in Web Services software client.....	6
4.1.2 Testing and Migration	6
5. Change of Disabling TLS 1.0 and 1.1	7
6. Summary on customer efforts	7
Appendix	
Examples of ApplicationRequest with SHA256 algorithm	8
Examples of SOAP Request with SHA256 algorithm.....	9
Examples of ApplicationResponse with SHA256 algorithm.....	11
Examples of SOAP Response with SHA256 algorithm	13

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

As of now, the customer signing certificate issued from Nordea is

- 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 planned in Q3 2022, the certificate will be

- 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 the change, 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 will also provide new version of NSC client by Q3 2022, which will 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 will inform customers via newsletters about the date and time when Nordea will start to issue SHA256 certificates to customers.

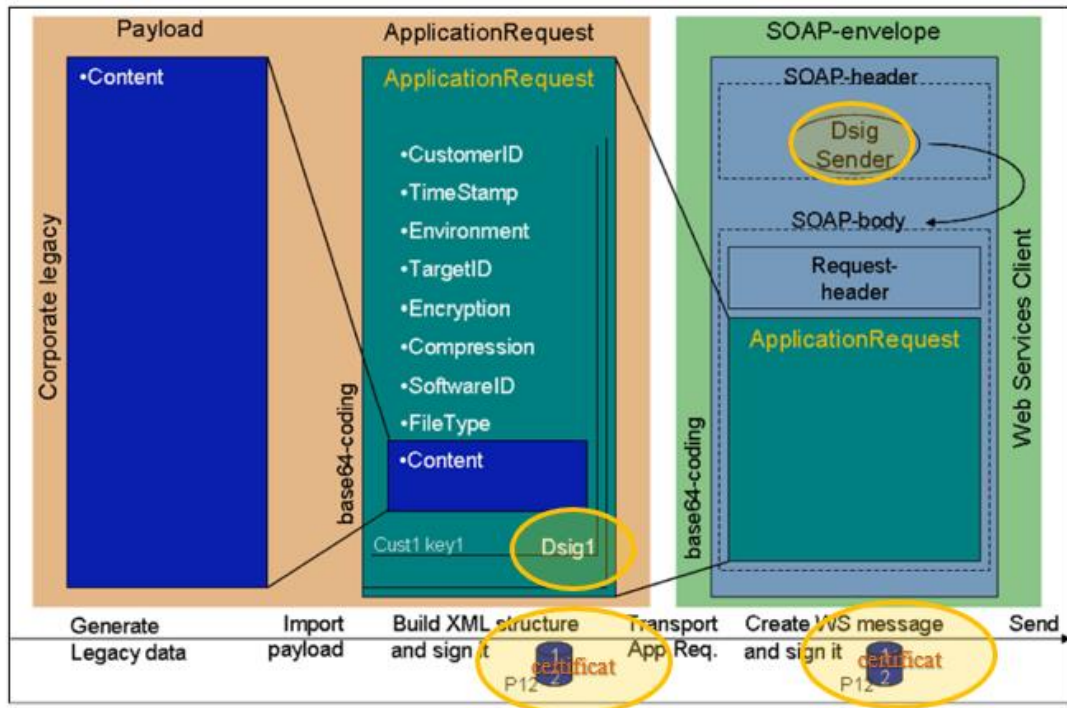
Before the change time/date, customer can take example test certificates which Nordea publishes on Nordea.fi to test whether own Web Services software client works ok with SHA256 certificates.

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 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.



Currently, 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>.

After change, in addition to existing 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 Q2 of 2023, Nordea will stop supporting the SHA1 algorithm.

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 Q2 of 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 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 during Q2 of 2023, Nordea will stop supporting the SHA1 algorithm.

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
- And during Q2 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 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 Q2 of 2023. 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 2023. 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	will be changed in Q3 2022 by Nordea, Nordea will inform the exact time later. Nordea will overwrite 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 Q2 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.
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 Q2 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. A new version of NSC client which supports 2048 key length will be available by Q3 2022
Nordea will stop support of TLS 1.0 and 1.1	Yes	Yes	By Q2 2023, 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>MvLEc8SsHIZ45dsQ8cBWwJo2QqshlAAGidEPgJ26mNNv2GJLAY1i9URg2Kawf9/flk7a/
45T4uMwUtVcVw5useEo=</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIC9DCCAdygAwIBAgICP3UwDQYJKoZIhvcNAQELBQAwaTELMakGA1UEBhMCU0UxHjAcBgNV
BAoT FU5vcmlRISBCYXZ5W5rIEFCIChwdWJsKTEkMCIGA1UEAxMmTm9yZGVhIFRlc3QgQ29ycG9yYXRlIENB
5mecJ0qsNc0GI2BtWoz1FB1wR8huZ5u6yFwOV2UNWGk0msFS11DyLxRuLMpXcDhaaBZnB5RvpLIC
UcDAqpYXrK+nYtHmJFSCsl6WA==</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-1641978992783830948719">
        <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+zCCAeOgAwIBAgIDASxVMA0GCSqGSIb3DQEBBQUAMGQxCzAJBgNVBAYTAINFMR4wHAYDV
QQKEExVOb3JkZWVgQmFuayBBQiAocHVibCkxHzAdBgNVBAMTFk5vcmlYSDb3Jwb3JhdGUgZmljYXRIRMRMwEQY
DVQQFEwo1NzgwODYwMjM4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCCLmzyaVAEr2cTt5gGPxuiMxZ5
JZRIDHUwyUMlags/JYbKCq/MhumUEDDAKMAgGBiqFcEcBAzATBgNVHSMEDDAKgAhAC3XW288LpzAOBgNVHQ8
BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQADggEBADVuzhr4KJwDXHph5fm5BOqfAI0fnUP5rFYfpDz3gRbyicRcBFj2
hkIG+8wMUKiTfASheRYL1hydK4EIJ3gaeieD7Yn9OxMILy+svh3YXGWnw9z9msRRyvJdVNLwws2sUgxlV66iPJR0qVIT55f
Led9YXbdfdbtPE+g10Qw62kXyZkDNoxeI8IUuihFLX20H/SPARRHCAootUoNuzFluEHI/5zL3FMBWSSxdkfGrqzmzF8/C5a31
GXWGgn/JK7KI1BYKx/weVWRui0F15nfIJQ=</wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1641978992673254148581">
        <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/xmldsig#sha256"/>
            <ds:Digest Value>2hDXWPwOTrMIXCksTkj4ISZwrligDYTQbafaUr4=</ds:Digest Value>
          </ds:Reference>
          <ds:Reference URI="#XWSSGID-1641978992783830948719">
            <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:Reference>
        </ds:SignedInfo>
      </ds:Signature>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
  </SOAP-ENV:Body>
</S:Envelope>
```

```

        </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>PD94bWwgdMvyc2lvbj0iMS4wIiBlbmNvZGluz0iVVRGLTgiPz48QXBwbGJyYXRpb25SZXF1ZXXN0I
HhtbG5zPSJodHRwOi8vYnhkLmZpL3htbGRhdGEvIj4NCiAgICA8Q3VzdG9tZXJJZD4xMTEwMTEwMTwvQ3VzdG9tZXJJZ
D4NCiAgICA8Q29tbWFuZD5Eb3dubG9hZEZpbGVMaXN0PC9Db21tYW5kPg0KICAgIDxUaW1lc3RhbXA+
jZpUEpSMHFWSVQ1NWZMZWQ5WVhiZiYjMTM7DQpkYi90UEUrzEwUXc2MmtYeVo5MzROS0xVWHZ4eGdBaWlw
WXISd0FWTHNsYmewdThQT0tCeFQ1MjdmNHRXRHc1cGVpS3A3bHRzRUNMjMxMzNCKjYyXZjMGtETm94ZUk4bF
V1aWhGTFgyMEgvU1BhUlJlQ0Fvb3RvVb054dXpGSXVFSGwvNXpMM0ZNQldTc3hka2ZHcnFtekY4L0M1YTMmIzEzOw0
KMudYV0dnbi9KSzdLSTFCWUt4L3dlVldSdWkwRkk1bmZJSiE9PC9YNTA5Q2VydGlmaWNhdGU+PFg1MDIjc3N1ZXJT
ZXJpYWw+PFg1MDIjc3N1ZXJOYWw1IPjUuNS40LjU9IzEzMGZlNTMxMzYzNDMwMzYyZDMwMzEzZmJmWLENOPU5vc
mRlYSBDb3Jwb3JhdGUgQ0EgMDEsTz1Ob3JkZWVgQmFuayBBQiAocHVibCksQz1TRTwwWUwOUlzc3Vlck5hbWU+PF
g1MDITZXJpYWwOdW1iZXI+NzY4ODU8L1g1MDITZXJpYWwOdW1iZXI+PC9YNTA5SXNzdWV5U2VyaWFsPjwvWU
wOURhdGE+PC9LZXIjbmZvPjwvU2lnbmF0dXJlPjwvQXBwbGJyYXRpb25SZXF1ZXXN0Pg==</ApplicationRequest>
    </ns2:downloadFileListin>
</S:Body>
</S:Envelope>

```

Examples of ApplicationResponse with SHA256 algorithm

Part of XML

```
<c2b:ApplicationResponse xmlns:c2b="http://bx.d.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>
</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+MA0GCSqGSIb3DQEBCwUAMGsxGzAJBgNVBAYTAINFMR4wHA YDV
QQKExVOb3JkZWVgQmFuayBBQiAocHVibCkxJjAkBgNVBAMTHU5vcmlRYSBDb3Jwb3JhdGUgU2VydmljZmVudmVzIENBIDAx
MR1MTY0MDYtMDEyMDAeFw0yMDEyMjExMjMxMDVaFw0yMjExMjcxMjMzNTBaMG4xCzAJBgNVBAYTAINFMRg
wFgYDVQQKDA9Ob3JkZWVgQmFuayBBYnAxGzAZBgNVBAsMEkNvcnBvcmlRYSBDb3Jwb3JhdGUgU2VydmljZmVudmVzIENBIDAx
wFRmlsZSBUcmFuc2ZleiBXXWlU2VydmljZmVudmVzIENBIDAxGzAZBgNVBAsMEkNvcnBvcmlRYSBDb3Jwb3JhdGUgU2VydmljZmVudmVz
+vJCU7ECAwEAAM1MDMwCQYDVROTBAlwADARBgNVHQ4ECgQIQrtcU9YxVbUwEwYDVR0jBAwwCoAIRMeT2dl
7VsEwDQYJKoZIhvcNAQELBQADggEBAKD2tlB86c/lmtXkAqiAzZMipRVSN1/ZZkOtmBuf56ziUQQMLORipMjlyP9grDh
JIIQqhsL1jo+BSdceW0o8Uh5bhrNeC6roLnGT864Ozj4tS354sgE5UUKcUYZUiw70PGP9gJKlp6kLFTIKNhJ0oI8eaItbU5A6c
7KXgou44SfaN12I4m/wBZY1147PQa8X5B1npHruVbhbbhQccVurnF3qjpLHFKslnB139tJ4taYwBqRe81pR3S6p2Hm9lWFK5
nU3Ef/LleeFsWVCpfR2x0BOB0gFbLOPFjC+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>U9cNMydSuDpQ1SU9WU++I0UTWrfjmTELDTCsfkitzU=</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>OiF1RYFdqc4rnsfmz00khrFF800Ye7A6Pv2HMBFxs=</DigestValue>
    </Reference>
  </wsse:Security>
</soapenv:Header>
</soapenv:Envelope>
```

