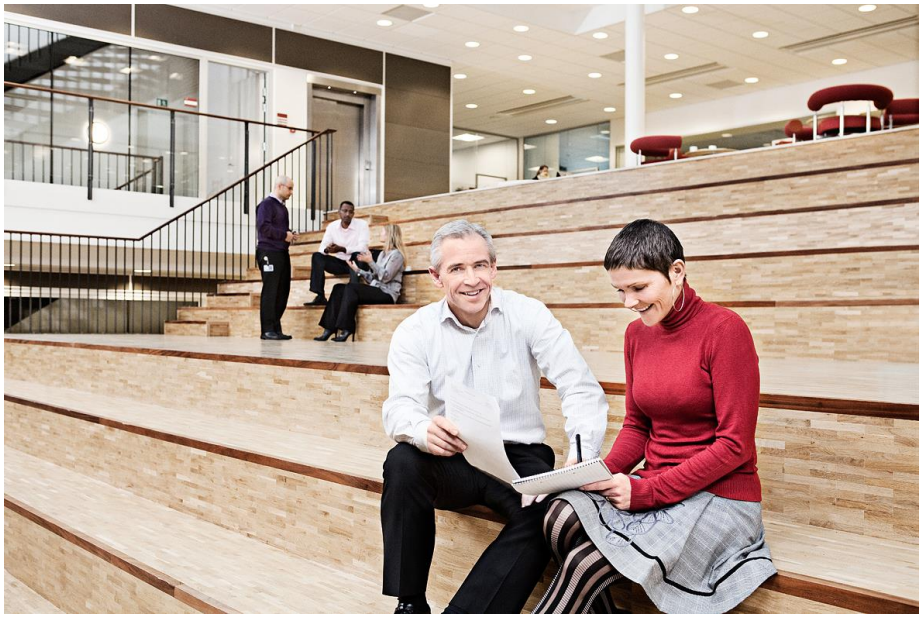


Digitaliseringsstyrelsen

Nemlog-in

Nemlog-in STS

Version: 1.3

ID: 32309

2015-03-20

NNIT

Conscience driven. Value adding

Table of Contents

1 Introduction

The purpose of this document is to describe how service providers and web service consumers can test the integration to the Security Token Service from here on named STS in the Nemlog-in integration test environment.

The audience is it-technicians who is going to perform the technical integration and testing and it is assumed that the reader already have knowledge about OIO Identity-based Web Services.

OIO Identity-based Web Services description and detailed information about the different usage scenarios are documented on digitaliser.dk [OIOIDWS].

Comments are used throughout the document and intended as a guide for the reader.

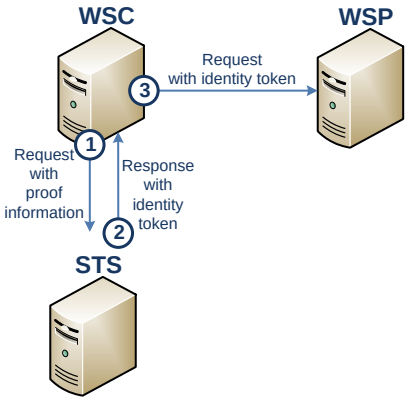
The document consists of the following sections:

- Section 2 describes the service and service methods
- Section 3 contains the configuration needed to call the STS service in the integration test environment
- Section 4 describes the test data available for the STS service

2 Service description

The Nemlog-in2 STS Service exposes a method for exchanging security tokens that can be used access specific web services.

The figure below illustrates the basic processing model:



Processing model and usage scenarios are described in detail in [STS-RULES] sections 2.1 and 2.2.

2.1 IssueToken

The IssueToken method is used to exchange a security token to an identity token usable with a specific web service provider. As of March 2015 the term "identity token" includes the variants for "System User" and "Local IDP" [STS-RULES].

Syntax:

IssueToken(stsRequest1 request)

- stsRequest1 message is described in detail in [STS-RULES] section 2.3

Returns:

stsResponse

- a security token containing the identity token for usage with the specified web service provider. The format is described in detail in [STS-RULES] section 2.5

Fault:

The STS returns WSTrust faultcodes.

Fault code	Fault string	Description
wst:InvalidRequest	The request was invalid or malformed	Validation of message failed with missing/illegal elements, attributes or values.
Wst:FailedAuthentication	Authentication failed	Sessionid, signature, cvr or certificatetype errors
wst:RequestFailed	The specified request failed	STS service failures frontend/backend
wst:InvalidSecurityToken	Security token has been revoked	Not used
wst:BadRequest	The specified RequestSecurityToken is not understood.	Message does not conform to general wstrust schema
wst:ExpiredData	The request data is out-of-date	If Envelope/Header/Security/Timestamp/Expires value is understood but not accepted this error will be returned Or If the NotOnOrAfter-attribute is understood but exceeded on either Envelope/RequestSecurityToken/ActAs/Assertion/Subject/SubjectConfirmationData or Envelope/RequestSecurityToken/ActAs/Assertion/Conditions
wst:InvalidTimeRange	The requested time range is invalid or unsupported	If unsupported or invalid values in Envelope/Body/RequestSecurityToken/LifeTime will return this error. (Requested lifetime will be overridden with default sts lifetime policy)

3 Configuration

3.1 Creating a WSC service for Integration test environment

To execute a STS call the proper registration of your service according to the test scenario must be configured and migrated to integration test in the CSS – "Tilslutning and administration" system.

Please refer to the user manual [CSS – USERMANUAL] for a more detailed description on how to accomplish this.

For the three scenarios there are different requirements for the WSC service configuration:

- Bootstrap token scenario
  In this scenario your service must be configured to have the `urn:liberty:disco:2006-08:DiscoveryEPR` attribute asserted, which will contain the bootstrap token from Nemlogin used for subsequent STS calls.

- Local token scenario
  In this scenario the user identity is proofed by a bootstrap token that is obtained from WSC's local STS hosted by the WSC organization itself. The local STS must be trusted by Nemlog-in STS. The local STS must be registered as WSC in Nemlog-in CSS and enter terms and conditions with Digitaliseringsstyrelsen.

  As of march 2015 there is a local IDP variant to the Local token scenario: it is determined by the registration in CSS which variant (local STS or local IDP) is in use for the WSC.

- Signature scenario
  In this scenario the user identity is proofed by the user signing the request to Nemlog-in STS. The scenario contains no bootstrap tokens. The WSC constitutes in this scenario any application hosted by any organization and no trust is established directly between WSC and Nemlog-in STS.
  As of March 2015 there is a new variant "System User" to the Signature scenario allowing a "system" to sign the request (rather than a user). The System User variant and it's different versions is configured for the WSP in CSS.

3.2 Binding

Connection to the web services is only allowed via SSL.

URL to the STS web service in integration test environment:

https://SecureTokenService.test-nemlog-in.dk/SecurityTokenService.svc

URL to STS web service in Production:
https://SecureTokenService.nemlog-in.dk/SecurityTokenService.svc

The STS used SOAP version 1.1 [SOAP11]. Hence the STS expects the following http headers and values when requesting a token:

SOAPAction: http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
Content-Type: text/xml;charset=utf-8

3.3 Nemlogin STS signing certificates

STS signs the response messages. The certificates used to validate the signature can be found on the testportal site.

Integration test certificate

[IntegrationTestSigning.cer]

Production certificate

[ProductionSigning.cer]

4 Test data

This section describes the available test data and documents a test call with response for each of the three usage scenarios. It is not possible to run the test calls directly against the sts test service as they will have expired time instant values.

4.1 WSP test certificate

In integration test a test web service provider WSP has been configured with the entityid https://saml.nnit001.dmz.inttest. This entity can be used as the test WSP if you do not create one for your system using the Nemlogin administration site.

The response assertion for the WSP entity https://saml.nnit001.dmz.inttest is encrypted with the public key of the DanID Voces testcertificate. Included in this document is a link to the certificate including the private key which can be used for decrypting the response for that WSP.

[DanIDVocesGyldig.p12]

4.2 WSP test endpoint

Integration test also has an ”ECHO” identity based web service, which can be called with the token issued by STS. The web service simply echoes the request.

Connection to the echo web service is only allowed via SSL.

URL to the STS “ECHO” web service in integration test environment:

https://securetokenwsp.test-nemlog-in.dk/SecurityTokenServiceMessageEcho.svc

4.3 Bootstrap token scenario

In this scenario your service is configured to receive urn:liberty:disco:2006-08:DiscoveryEPR attributes from NemLogin when a user login. The value of this attribute is used to request an identity token for the test WSP https://saml.nnit001.dmz.inttest in the below example request against sts.

Request and response messages are described in detail in [STS-RULES].

4.3.1 Request example

Note that the content of the `wst14:ActAs` can be sent Base64 encoded as it is received from the NemLogin assertion, but for purpose of this example is decoded. STS accepts both formats for the content of the ActAs element

```
POST https://securetokenservice.nemlog-in.dk/SecurityTokenService.svc HTTP/1.1
SOAPAction: http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
Content-Type: text/xml;charset=utf-8
Host: securetokenservice.nemlog-in.dk
Content-Length: [length]
```

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-
trust/200802" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="msgid">uuid:40ffa8d6-c575-4f38-8204-
8a5d541d5e59</wsa:MessageID>
    <wsa:To wsu:Id="to">https://bootstrap.sts.nemlog-in.dk/</wsa:To>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec-ts">
        <wsu:Created>2015-03-19T09:06:04Z</wsu:Created>
        <wsu:Expires>2015-03-29T09:06:04Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken wsu:Id="sec-binsectoken" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIGIDCCBQigAwIBAgIETAV1TzANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEyMD
ExMjE0MTQwNloXDTE2MDExMjE0MTM1MlowdjELMAkGA1UEBhMCREsxKjAoBgNVBAoMIcOYa29ub21pc3R5cmVs
c2VuIC8vIENWUjoxMDIxMzIzMTE7MBcGA1UEAwwQTW9ydGVuIE1vcnRlbnNlbjAgBgNVBAUTGUNWUjoxMDIxMz
IzMS1SSUQ6OTM5NDc1NTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXxgVHipGqErG8xLbYqxmP
vyZzh1aBK4th2YaiIbRyZfSO3gOxhWs+XR3JLOrVMgKxERYGD4fTnNfWU7TpYaTO8pnXEx2+bV2ohIzcyavQYW
21KMgcp1psWr6wv5IuF0Ykhydv9OOqJRouBh4oHJwvBjVJQLDw0L+d6bJ/DjW+tHWtuWMyPUKZRjQf6dWIA45p
kLH8mcFNztxGIOZHvlqH7IiPHc73KKqxmig/vvdUCVI15MADeCsQQ8ds0Aw7uFJiytROF/5wD0jJOZHJToBLvt
Qd8UShEtL6TSiEchi2ZVPf/tJmiRriQQNHQy/sWEPlnkt2HZxRkuPNzt1GeMVBAgMBAAGjggLiMIIC3jAOBgNV
HQ8BAf8EBAMCA/gwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcC5zeXN0ZW10ZX
```

Commented [A1]: Bootstrap scenario

N0OC50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL20uYWlhLnN5c3RlbXRlc3Q4
LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARMwggEPBg0rBgEEAYH0UQ
IEBgIFMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb3NpdG9yeTCByQYIKwYB
BQUHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZyYSBkZW5uZSBDQSB1ZH
N0ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41LiBEYW5JRCB0ZXN0IGNlcnRpZmlj
YXRlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi
41LjAYBgNVHREEETAPgQ1qZWxmQG5uaXQuY29tMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lz
dGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMB
AGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQD
DAdDUkwxMTI0MB8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTv7aQGa8L1qrrstR
8ItB9Lz0RT/zAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQA0Pd04cFScEKoZgug3x+GBFoYzDgYBZR/d
SJexU3N9+e5wTgwterC9Ykk3BTV4VlBl6NFUjP9TPqOZaCkqTdWlXruy0wNKvMNGacVZJhS91baTW3ZnNIhAE5
x5gDxvsjuRVc0xZvyAhT7jkp4J62haMoDt+pRsZoDcVCN0KuLWL+Lh5efaB9vSCMsyKUjXf9A/F21nhBiNsECs
WjNXyt2/igbTuYCST12dTCpHs+sDEAnaZlTJa2B/CMUPo15niVLFuOWCPPyxurUZfB3bK/9qdHT60JvaVezwAA
mCWYEW7CW4AAGKDPMDG1qsRxFgaObB3bd5zCbnJkW/SNhg8/lc</wsse:BinarySecurityToken>

Commented [A2]: Certificate used to sign the request

```
      <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="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>NrdtWxaigbkMffHPgKCAMndq0hRMvsKQSkNelmS5cAE=</DigestValue>
          </Reference>
          <Reference URI="#msgid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>94gI1eCKv6T4JKBsEG3FXvvS1Nz4cqbsepvHzgKUJ30=</DigestValue>
          </Reference>
          <Reference URI="#to">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>PN0/5l60jJ4gfW7vMa/rg6cSznZbiHBuVetvfGLuxZ4=</DigestValue>
          </Reference>
          <Reference URI="#sec-ts">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>4w+7pyUBnARsO7P6K3gqLZyZQcS4fVX5hXOjpzJUpv4=</DigestValue>
          </Reference>
          <Reference URI="#sec-binsectoken">
```

```
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>gC0rvFzqTwR4HgCX5liQ6AnQuriSEQw9PUZlHDD9nn0=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>uGMGz3+ryLv0UqCRYI2vxbHZLtwjwMpAFvf2g691is8=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>UpsGHBJSLlBiaBwvGS7cz4G0vuJCrXCQrXg54Wm1rDJ/XjFQ1bRgvoyLdFFa9pnWmLtlOy
bxGMw+v98xOL0hyBDzrQIQp/TjWjwapWxvz4yoexN0u/C3htCD0INofwTWyRhgfpJcRS7jc4XJdtlvQr2npjq4
Hy8mdLljAIt87DAUkpiu4Gv62Xj+1v0C/FvnXaGfpnMMD5NWdbsghnFOu3ZNwKKKT2fPDlmIsbgFLvYH7iP2Dd
0TKJ30pH+8rgkGcXbaTwJSWjNycJFjpK5lGbJiA/DOVykiAyGcZJUMaO26kYZn1vSWUNOAAaCtJTDC+6SQ6wA1
YwPUMuUnkJ3oig==</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#sec-binsectoken" />
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <wst:RequestSecurityToken Context="urn:uuid:9cefa774-2922-4a49-afbe-d7d81fb11d79">
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wst14:ActAs>
        <saml2:Assertion ID="984be972-3e03-4002-afb5-906d56fea0ca" IssueInstant="2015-
03-19T09:06:04.2Z" Version="2.0">
          <saml2:Issuer>https://saml.nemlog-in.dk</saml2:Issuer>
          <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="#984be972-3e03-4002-afb5-906d56fea0ca">
                <Transforms>
                  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
```

```
<DigestValue>Z9fLQXTfu35PaenI+Unz9bqmZWMH2OumocZozz8cSkE=</DigestValue>
              </Reference>
            </SignedInfo>
<SignatureValue>Eb9vWhlflGBxKYEatsurCIUEysqJMHwGvwWTIICcS3xxjADO0l3L3gzqCpWdqVM/YqXZBG
5o1MJGe8s9Q9H+1y60eNTdKiA5B6oK1l2Soi/ovgWzTcTYmHYANvZyuSMcaZWYYg/ShrXGNi6VOtJ4dbg2X1gS
oxwNFqGYV2+9VSurTFVYEEMb5mFUEPkyfVZsWilGlMULewVEBB9lpBQTSV+ZVt9Mr5W2wHtUuYQNMMjZnyfHch
zAfhMZX6HfWp8XtQzlrXbqMquIrK+64cDQOj//M8hdhxjN5+7oZJZGUZGeqv8wwyu1Z16i6P/YqVNaeA1APS5p
Tt+Y57aXLlHcuA==</SignatureValue>
          </Signature>
          <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-
of-key">
              <saml2:SubjectConfirmationData
xsi:type="saml2:KeyInfoConfirmationDataType">
                <ds:KeyInfo>
                  <ds:X509Data>
<ds:X509Certificate>MIIGIDCCBQigAwIBAgIETAV1TzANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESz
ESMBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEy
MDExMjE0MTQwNloXDTE2MDExMjE0MTM1MlowdjELMAkGA1UEBhMCREsxKjAoBgNVBAoMIcOYa29ub21pc3R5cm
Vsc2VuIC8vIENWUjoxMDIxMzIzMTE7MBcGA1UEAwwQTW9ydGVuIE1vcnRlbnNlbjAgBgNVBAUTGUNWUjoxMDIx
MzIzMS1SSUQ6OTM5NDc1NTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXxgVHipGqErG8xLbYqx
mPvyZzh1aBK4th2YaiIbRyZfSO3gOxhWs+XR3JLOrVMgKxERYGD4fTnNfWU7TpYaTO8pnXEx2+bV2ohIzcyavQ
YW21KMgcp1psWr6wv5IuF0Ykhydv9OOqJRouBh4oHJwvBjVJQLDw0L+d6bJ/DjW+tHWtuWMyPUKZRjQf6dWIA4
5pkLH8mcFNztxGIOZHvlqH7IiPHc73KKqxmig/vvdUCVI15MADeCsQQ8ds0Aw7uFJiytROF/5wD0jJOZHJToBL
vtQd8UShEtL6TSiEchi2ZVPf/tJmiRriQQNHQy/sWEPlnkt2HZxRkuPNzt1GeMVBAgMBAAGjggLiMIIC3jAOBg
NVHQ8BAf8EBAMCA/gwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcC5zeXN0ZW10
ZXN0OC50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL20uYWlhLnN5c3RlbXRlc3
Q4LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARMwggEPBg0rBgEEAYH0
UQIEBgIFMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb3NpdG9yeTCByQYIKw
YBBQUHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZyYSBkZW5uZSBDQSB1
ZHN0ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41LiBEYW5JRCB0ZXN0IGNlcnRpZm
ljYXRlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYu
Mi41LjAYBgNVHREEETAPgQ1qZWxmQG5uaXQuY29tMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3
lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQ
QDDAdDUkwxMTI0MB8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTv7aQGa8L1qrrs
tR8ItB9Lz0RT/zAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQA0Pd04cFScEKoZgug3x+GBFoYzDgYBZR
/dSJexU3N9+e5wTgwterC9Ykk3BTV4VlBl6NFUjP9TPqOZaCkqTdWlXruy0wNKvMNGacVZJhS91baTW3ZnNIhA
E5x5gDxvsjuRVc0xZvyAhT7jkp4J62haMoDt+pRsZoDcVCN0KuLWL+Lh5efaB9vSCMsyKUjXf9A/F21nhBiNsE
CsWjNXyt2/igbTuYCST12dTCpHs+sDEAnaZlTJa2B/CMUPo15niVLFuOWCPPyxurUZfB3bK/9qdHT60JvaVezw
AAmCWYEW7CW4AAGKDPMDG1qsRxFgaObB3bd5zCbnJkW/SNhg8/lc</ds:X509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
              </saml2:SubjectConfirmationData>
            </saml2:SubjectConfirmation>
          </saml2:Subject>
```


Commented [A3]: Subject that logged into Nemlogin

```
          <saml2:Conditions NotBefore="2015-03-19T09:06:04.2Z" NotOnOrAfter="2015-03-
19T17:06:04.2Z">
            <saml2:AudienceRestriction>
              <saml2:Audience>https://bootstrap.sts.nemlog-in.dk/</saml2:Audience>
            </saml2:AudienceRestriction>
          </saml2:Conditions>
          <saml2:AttributeStatement>
            <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" Name="dk:nemlogin:saml:attribute:IdPSessionIndex">
              <saml2:AttributeValue xsi:type="xs:string">58-31-13-5C-12-02-45-D0-57-
35-33-3E-B9-D9-D7-8D-FE-70-D4-27</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" Name="dk:nemlogin:saml:attribute:SpEntityId">
              <saml2:AttributeValue xsi:type="xs:string">https://sp1.dev-nemlog-
in.dk</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:SpecVer">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:AssuranceLevel">
              <saml2:AttributeValue xsi:type="xs:string">True</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Surname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="urn:oid:2.5.4.4">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="CommonName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="urn:oid:2.5.4.3">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Uid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:0.9.2342.19200300.100.1.1">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Mail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:0.9.2342.19200300.100.1.3">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="serialNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="urn:oid:2.5.4.5">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
```

```
            <saml2:Attribute FriendlyName="userCertificate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Certificate issuer attribute"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:2.5.29.29">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:CprNumberIdentifier">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:UniqueAccountKey">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Privileges"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:Privileges_intermediate">
              <saml2:AttributeValue
xsi:type="xs:string">PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48YnBwOlByaXZpb
GVnZUxpc3Qg
eG1sbnM6eHNpPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaGVtYS1pbnN0YW5jZSIgeG1s
bnM6YnBwPSJodHRwOi8vaXRzdC5kay9vaW9zYW1sL2Jhc2ljX3ByaXZpbGVnZV9wcm9maWxlIj48
UHJpdmlsZWdlR3JvdXAgU2NvcGU9InVybjpkazpnb3Y6c2FtbDpDdnJOdW1iZXJJZGVudGlmaWVy
OjEwMjEzMjMxIj48UHJpdmlsZWdlPmh0dHBzOi8vbm9ybXByaXYxLnBoPC9Qcml2aWxlZ2U+PC9Q
cml2aWxlZ2VHcm91cD48L2JwcDpQcml2aWxlZ2VMaXN0Pg==</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:IsYouthCert">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="PidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:PidNumberIdentifier">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Postal address"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:2.5.4.16">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="Title"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:2.5.4.12">
```

```
            <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="Organization unit"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:2.5.4.11">
            <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
          </saml2:Attribute>
        </saml2:AttributeStatement>
      </saml2:Assertion>
    </wst14:ActAs>
    <wsp:AppliesTo>
      <wsa:EndpointReference>
        <wsa:Address>https://saml.WSPSUAll.env</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>
  </wst:RequestSecurityToken>
 </S11:Body>
</S11:Envelope>
```

Commented [A4]: Base64 decoded bootstrap token issued by Nemlogin. Can be sent encoded as received by Nemlogin and is only decoded here to illustrate contents

Commented [A5]: Entityid of the WSP to get an identity token for

4.3.2 Response envelope example (decrypted)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="messageid">uuid:ee4e62b5-e930-4b09-9777-
67bb5308c45c</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesto">uuid:40ffa8d6-c575-4f38-8204-
8a5d541d5e59</wsa:RelatesTo>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec_timestamp">
        <wsu:Created>2015-03-19T09:06:17.580Z</wsu:Created>
        <wsu:Expires>2015-03-19T17:06:17.580Z</wsu:Expires>
      </wsu:Timestamp>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
```

```
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
             <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
           </Reference>
           <Reference URI="#messageid">
             <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
             </Transforms>
             <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
             <DigestValue>bBLo2guR70AN36ap5Qk8k6qIxfI=</DigestValue>
           </Reference>
           <Reference URI="#relatesto">
             <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
             </Transforms>
             <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
             <DigestValue>xxCvtfcbPZPULgiIxGPx82yQ+Bw=</DigestValue>
           </Reference>
           <Reference URI="#sec_timestamp">
             <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
             </Transforms>
             <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
             <DigestValue>05bwXa4Lh6tQJAQtJKGx2G71584=</DigestValue>
           </Reference>
           <Reference URI="#body">
             <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
             </Transforms>
             <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
             <DigestValue>SvowhgBcd4P+ttLJ/ovOlv7ZjIc=</DigestValue>
           </Reference>
         </SignedInfo>
<SignatureValue>hJYbPDB3Xz/TVtSQ6lPy3OitonNYhmKk/FQLkHKA4oim1mFPgg8k2SnfUnMYXrn3qbOTyT
bUOaocNviqxog7t4qWN/Gx6CAxfeefCwbnwMigtXI+5ZuM496EhDoFEpZgEKnqkh7CJkvs261a7y+RwKHuswYx
rw/16kqwlBkXmBTjvU0ODW4gjX6kSLkIpwmqpPpb3bC6PMUO5Dy1eKRXRy92gtg1p8MzX/V3PHVUX0mn77M+yP
3+WUai0ZUK0+50ncsF3mdBo7a/Ge/CrDHiNw3OoGESEZusFMn/R8HVd6HOSA+dm+D7YZBVnyT2m9vZVx/S/KQM
I+oQsk70mUlijQ==</SignatureValue>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
```

```
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
      <RequestSecurityTokenResponse Context="urn:uuid:9cefa774-2922-4a49-afbe-
d7d81fb11d79">
        <TokenType />
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <Address>https://saml.WSPSUAll.env</Address>
          </EndpointReference>
        </AppliesTo>
        <RequestedSecurityToken>
          <Assertion ID="_2b439124-f8c0-448a-bc77-ca7968824aec" IssueInstant="2015-03-
19T09:06:17.580Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://bootstrap.sts.nemlog-in.dk/</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
                <ds:Reference URI="#_2b439124-f8c0-448a-bc77-ca7968824aec">
                  <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<ds:DigestValue>80eHENpwgGId8PQSguWsPAeORd1+DwGqIF/uD9E4LBs=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
<ds:SignatureValue>o7+u6lxbH5x9J6UaH/qyTcL+GvhgoSXLxGcW/qXujyOhlCv0+XHEce6gDFIngR/w/CG
Riv7EjZSsG18o9cU3JNSEm0DO4GtfoCyuyCPw2fXMOKFODcfGf8AWnVhPJuG9E/LgBJQNZsbME4YyA3Rk1Vcs4
+R3J51PrRiWKojnteEGlX3fSH/3vfhDTX3wvDuf+rVM2vX2Kx89bQRNyEEPuOeMidRZ1CTciGRA3m1W12eN3MB
o7sDPKsK9od+w/mnnb+AEJwQ5/JhRNA/pJp2XfaFrDcubFlWM3mcdhu9j2Y8vAwffQuKnZLMBw4LCAXYGm7ofv
bnNrrTvndwC/G3/bQ==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
<X509Certificate>MIIGFTCCBP2gAwIBAgIETBI9xjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTE0MDE
zMDEwMjkzN1oXDTE3MDEzMDEwMjgyM1owgYQxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUjAlBgNVBAUTHkNWUjoyMTA5MzEwNi1GSUQ6MTMzNjQ2NzA5MjUwNzApBgNVBAMMIktGT0J
TIC0gQURGUyAoZnVua3Rpb25zY2VydGlmaWthdCkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpu
3eSu0HkpTrawmmtaeBezZL7NnNno/L4fIWXXawxUcIfcnqSp5ZKpjBm4mzeRRwqkYlOn0WfROeqMgOCXRnNnRd
+I2aWWSWIMPYVGVZqT2/MQPo2UvDZ2Z/j4xyQDUx7L+l6elsq7IDGfSvzwrE/qU98Zr3bm3HvbUTK5F4ZE2w4R
eB2UU2QJowDUrdMNmoQ57Bx7UOobqwlNb3VYVwYwdgoJwQik+Jonm8/i4mNeKnGstYTZuEJTOr1LG0T3QOrqJM
Y8COYvIuTy14nC+cZAcSV4nWCnZ3MzTX6CohkzBG87W3BiPH9BDrjoGyilwhCorjgoFMkuIWgzgv2MDMjAgMBA
```


Commented [A6]: EntityId of the WSP this identity token is valid for

AGjggLIMIICxDAOBgNVHQ8BAf8EBAMCBLAwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8
vb2NzcC5zeXN0ZW10ZXN0OC50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL2YuY
WlhLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARM
wggEPBg0rBgEEAYH0UQIEBgQCMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb
3NpdG9yeTCByQYIKwYBBQUHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZ
yYSBkZW5uZSBDQSB1ZHN0ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuNC4yLiBEYW5JR
CB0ZXN0IGNlcnRpZmljYXRlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjE
uMzEzMTMuMi40LjYuNC4yLjCBqwYDVR0fBIGjMIGgMDqgOKA2hjRodHRwOi8vY3JsLnN5c3RlbXRlc3Q4LnRyd
XN0MjQwOC5jb20vc3lzdGVtdGVzdDguY3JsMGKgYKBepFwwWjELMAkGA1UEBhMCREsxEjAQBgNVBAoMCVRSVVN
UMjQwODElMCMGA1UEAwwcVFJVU1QyNDA4IFN5c3RlbXRlc3QgVklJSSBDQTEQMA4GA1UEAwwHQ1JMMTY2MDAfB
gNVHSMEGDAWgBSWGzYTOyIpwj355/mT68bLPhJfBDAdBgNVHQ4EFgQUseDu/uyKIUjTMu4ktOz/qCJ9cEYwCQY
DVR0TBAIwADANBgkqhkiG9w0BAQsFAAOCAQEAWfWB2H/B1R8m0/qWSsZTD7fMoPpNVzyK8gDJBATZnxqZYKYdq
qC93DmstKuVrVdVao1H8rUXb6UrcTgHWzvsbFIlM6zqXU5lmljypkn9+8NZrw2ttxbZ1MyB8uCOcQ2Eaj5Fyfa
QTr6HVWQDE0/9QzObtiaNweKv4DVTF+JBgCj4S8KE9wvqB66QPfrACGY8pVizHIVMgokMu6cqSULcQ4tKRFSPG
nac2d0DqllZkn+pxmD1dw6BUgh0SQ1ijfhl5TnVpVBAuvjIbpFD6rhuETDE6u9GECo5OCoqxksFbc4nfOPE7u6
A1zqWrGso2rTZ1ryIZWnjebcZ1BceEDZRYw==</X509Certificate>

Commented [A7]: Certificate used to sign the message. Do not verify signature with embedded certificates.

```
            </X509Data>
          </KeyInfo>
        </ds:Signature>
        <Subject>
          <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</NameID>
          <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
            <SubjectConfirmationData a:type="KeyInfoConfirmationDataType"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance">
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>

<X509Certificate>
```

MIIGIDCCBQigAwIBAgIETAV1TzANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEyMDE
xMjE0MTQwNloXDTE2MDExMjE0MTM1MlowdjELMAkGA1UEBhMCREsxKjAoBgNVBAoMIcOYa29ub21pc3R5cmVsc
2VuIC8vIENWUjoxMDIxMzIzMTE7MBcGA1UEAwwQTW9ydGVuIE1vcnRlbnNlbjAgBgNVBAUTGUNWUjoxMDIxMzI
zMS1SSUQ6OTM5NDc1NTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXxgVHipGqErG8xLbYqxmPv
yZzh1aBK4th2YaiIbRyZfSO3gOxhWs+XR3JLOrVMgKxERYGD4fTnNfWU7TpYaTO8pnXEx2+bV2ohIzcyavQYW2
1KMgcp1psWr6wv5IuF0Ykhydv9OOqJRouBh4oHJwvBjVJQLDw0L+d6bJ/DjW+tHWtuWMyPUKZRjQf6dWIA45pk
LH8mcFNztxGIOZHvlqH7IiPHc73KKqxmig/vvdUCVI15MADeCsQQ8ds0Aw7uFJiytROF/5wD0jJOZHJToBLvtQ
d8UShEtL6TSiEchi2ZVPf/tJmiRriQQNHQy/sWEPlnkt2HZxRkuPNzt1GeMVBAgMBAAGjggLiMIIC3jAOBgNVH
Q8BAf8EBAMCA/gwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcC5zeXN0ZW10ZXN
0OC50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL20uYWlhLnN5c3RlbXRlc3Q4L
nRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARMwggEPBg0rBgEEAYH0UQI
EBgIFMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb3NpdG9yeTCByQYIKwYBB
QUHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZyYSBkZW5uZSBDQSB1ZHN
0ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41LiBEYW5JRCB0ZXN0IGNlcnRpZmljY
XRlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi4
1LjAYBgNVHREEETAPgQ1qZWxmQG5uaXQuY29tMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzd
GVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBA
GA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDD
AdDUkwxMTI0MB8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTv7aQGa8L1qrrstR8

```
ItB9Lz0RT/zAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQA0Pd04cFScEKoZgug3x+GBFoYzDgYBZR/dS
JexU3N9+e5wTgwterC9Ykk3BTV4VlBl6NFUjP9TPqOZaCkqTdWlXruy0wNKvMNGacVZJhS91baTW3ZnNIhAE5x
5gDxvsjuRVc0xZvyAhT7jkp4J62haMoDt+pRsZoDcVCN0KuLWL+Lh5efaB9vSCMsyKUjXf9A/F21nhBiNsECsW
jNXyt2/igbTuYCST12dTCpHs+sDEAnaZlTJa2B/CMUPo15niVLFuOWCPPyxurUZfB3bK/9qdHT60JvaVezwAAm
CWYEW7CW4AAGKDPMDG1qsRxFgaObB3bd5zCbnJkW/SNhg8/lc</X509Certificate>
                    </X509Data>
                  </KeyInfo>
                </SubjectConfirmationData>
              </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2015-03-19T09:06:17.580Z" NotOnOrAfter="2015-03-
19T17:06:17.580Z">
              <AudienceRestriction>
                <Audience>https://saml.WSPSUAll.env</Audience>
              </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
              <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="SpecVer">
                <AttributeValue>DK-SAML-2.0</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="AssuranceLevel">
                <AttributeValue>2.0</AttributeValue>
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="surName">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CommonName">
                <AttributeValue>Morten Mortensen</AttributeValue>
              </Attribute>
              <Attribute Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="uid">
                <AttributeValue>CVR:10213231-RID:93947552</AttributeValue>
              </Attribute>
             <Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="mail">
                <AttributeValue>MortenMortensen@kfobs.dk</AttributeValue>
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.5"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="serialNumber">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
```

Commented [A8]: Certificate used to sign the requestmessage as SubjectConfirmation has been set to holder-of-key

```
            <Attribute Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="userCertificate">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.29.29"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Certificate issuer attribute">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CprNumberIdentifier">
              <AttributeValue>0711550068</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UniqueAccountKey">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Privileges">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="IsYouthCert">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:PidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="PidNumberIdentifier">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="organizationName">
              <AttributeValue>Økonomistyrelsen // CVR:10213231</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:UserAdministratorIndicator"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserAdministratorIndicator">
              <AttributeValue>0</AttributeValue>
```

```
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:SENumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="SENumberIdentifier">
                <AttributeValue>66662222</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CVRnumberIdentifier">
                <AttributeValue>10213231</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="RidNumberIdentifier">
                <AttributeValue>93947552</AttributeValue>
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.65"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="OCES
Pseudonym">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
            </AttributeStatement>
          </Assertion>
        </RequestedSecurityToken>
        <wst:RequestedAttachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedAttachedReference>
        <wst:RequestedUnattachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedUnattachedReference>
        <Lifetime>
          <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-19T09:06:17.58Z</Created>
          <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-19T17:06:17.58Z</Expires>
        </Lifetime>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </S11:Body>
</S11:Envelope>
```

Commented [A9]: Asserted attributes

4.4 Local token scenario

In this scenario the user identity is proofed by a bootstrap token that is obtained from WSC's local STS, ie. an STS external to Nemlog-in, hosted by the WSC organization itself (local STS policy) or, if so set up in CSS, another organization (local IDP policy).

Request and response messages are described in detail in [STS-RULES].

4.4.1 Request example local STS

In the request example below https://sts.wsc1.dkdev is used as an issuer to create the message and https://saml.nnit001.dmz.inttest as the WSP to issue an identity token for. The issuer must be created specifically for your organization should you need to test this scenario.

```
POST https://securetokenservice.nemlog-in.dk/SecurityTokenService.svc HTTP/1.1
SOAPAction: http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
Content-Type: text/xml;charset=utf-8
Host: securetokenservice.nemlog-in.dk
Content-Length: [length]

<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-
trust/200802" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="msgid">uuid:af73276c-3ad2-4182-88e3-
4daf50c76305</wsa:MessageID>
    <wsa:To wsu:Id="to">https://local.sts.nemlog-in.dk/</wsa:To>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec-ts">
        <wsu:Created>2015-03-20T08:56:39Z</wsu:Created>
        <wsu:Expires>2015-03-30T08:56:39Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken wsu:Id="sec-binsectoken" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMT
AwOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBD
VlI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZPQ0
VTIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/Z
nSGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0ZP
7mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2sG
XfZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvIED
```

Commented [A10]: Local token scenario

```
7cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAwEA
AaOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly
9vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5h
aWEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEz
CCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBv
c2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZn
JhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklE
IHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS
4zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1
c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1
QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8G
A1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRFtYa8Wnp3jGC8dDwriSfl24GfpDAJBg
NVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vlgY
W2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330LO
SBtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J51
T8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsAHp
NTrcdunHgvCliJaiCK/J2CnH5XmpntX9fn</wsse:BinarySecurityToken>
```

Commented [A11]: Certificate used to sign the request

```
      <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="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>NrdtWxaigbkMffHPgKCAMndq0hRMvsKQSkNelmS5cAE=</DigestValue>
          </Reference>
          <Reference URI="#msgid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>ntTwpaO9a63lYBBjFCaPVUL3h/Wc0BMftgDd2feQnwg=</DigestValue>
          </Reference>
          <Reference URI="#to">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>sMhjXKoKEa8DfxKVk7tu0ZpijaHwgihAElBouQMVIs0=</DigestValue>
          </Reference>
          <Reference URI="#sec-ts">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>cVWOc8oRtzwZkPUpbjy7OIqJcBKUJJBDLDXQtAHIMpU=</DigestValue>
          </Reference>
          <Reference URI="#sec-binsectoken">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>BreEB9lOvyk0TDSxVt4vkiu8sTbbXKCmfcHaEJIV8f0=</DigestValue>
          </Reference>
```

```
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>ueqWu5v0zy4yzRhR1LYk8kzdk3D7hcue0Bbj5X5l0iY=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>q7vwRmUJ5mkw6W70QQqhGk1k2i00FMc1D8IHQVX89Cr3caHdwOGE60iuuNbp6RMRvqnDEP
rvMRaFcQoQUeL4Hcx6n/gAOqEsqYm/iu1oZft2rhYHdGa3sQVbhhPB7XsnwWFrCFEpy/JtGeTMBfQPfqilxpnv
N+9bzSoAuSKNq/kc1tTRawsg8nlW6EYQ8DHAwjBHiPj2zFg0FUQxRdKPG9+y9cuWiEeu7CYVGsGNQn4HSilNJb
8408SQ6Cj2b/QphkZL84+5ZV1EU1KiX5G1jFy90ZBG3x5Pja1HpM7fcwH9SUkN94HvctHGF5+87MBarbut9CSP
wl/VypSRGkBRbQ==</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#sec-binsectoken" />
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <wst:RequestSecurityToken Context="urn:uuid:c3f0de51-fa70-4373-9ecf-92965394a6d8">
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wst14:ActAs>
        <saml2:Assertion ID="_941598e8-6c34-4b98-9a57-cde8f6531452"
IssueInstant="2015-03-20T08:56:39.1Z" Version="2.0">
          <saml2:Issuer>https://sts.wsc1.test</saml2:Issuer>
          <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="#_941598e8-6c34-4b98-9a57-cde8f6531452">
                <Transforms>
                  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<DigestValue>k9NJN6wtzIq54E/ng7uyNjkpGvNen60FhqZJ83FSPfI=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>PzYPOF8OXi4kHR2COfC0NJAzCsk8qrXlSLGfnwtUVC/SgCRStzzWT8Bwd9KU2yxRNHwtrX
ISfv5JIb0NfctjE7vl366wgWI6VrK/HY2+bCSTwalqrhB37cOd9ofkUJOnxBEHdNGfF5YGMMUcdkUJPwuRmFxf
VHIprrCdQdBWbL8QgDM9IM/Lg7vbVm3IpQZ3Svb8AcQE+pUjW5A+d4Lgd2Gy7USb8+EQnFh9HqYQwRW4li1G25
wkMzM/3iHiJDD+Tz9Kem3isIYT4KY4GXhedc+S6INa5OIMIZ8jKq8rQyWqjMWU+yX+hZEEPPA7LV15s2cnKaB2
h82bSrFsT7kNJw==</SignatureValue>
          </Signature>
          <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</saml2:NameID>
```

Commented [A12]: Subjectname to issue identity token for

```
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-
of-key">
              <saml2:SubjectConfirmationData
xsi:type="saml2:KeyInfoConfirmationDataType">
                <ds:KeyInfo>
                  <ds:X509Data>

<ds:X509Certificate>MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESz
ESMBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEz
MTAwOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLy
BDVlI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZP
Q0VTIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM
/ZnSGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0
ZP7mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2
sGXfZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvI
ED7cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAw
EAAaOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6
Ly9vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi
5haWEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIB
EzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZX
Bvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIg
ZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbk
lEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQu
MS4zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudH
J1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJV
U1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB
8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRFtYa8Wnp3jGC8dDwriSfl24GfpDAJ
BgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vl
gYW2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330
LOSBtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J
51T8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsA
HpNTrcdunHgvCliJaiCK/J2CnH5XmpntX9fn</ds:X509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
              </saml2:SubjectConfirmationData>
            </saml2:SubjectConfirmation>
          </saml2:Subject>
          <saml2:Conditions NotBefore="2015-03-20T08:56:39.1Z" NotOnOrAfter="2015-03-
20T16:56:39.1Z">
            <saml2:AudienceRestriction>
              <saml2:Audience>https://local.sts.nemlog-in.dk/</saml2:Audience>
            </saml2:AudienceRestriction>
          </saml2:Conditions>
          <saml2:AttributeStatement>
            <saml2:Attribute FriendlyName="ProductionUnitIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:ProductionUnitIdentifier">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="SeNumberIndentifie"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:SENumberIdentifier">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:AssuranceLevel">
              <saml2:AttributeValue xsi:type="xs:string">True</saml2:AttributeValue>
```

Commented [A13]: Certificate used to sign the request message since SubjectConfirmation is set to holder-of-key

```
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:SpecVer">
              <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
            </saml2:Attribute>
          </saml2:AttributeStatement>
        </saml2:Assertion>
      </wst14:ActAs>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>https://saml.nnit001.dmz.dkdev</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

Commented [A14]: Entityid of the WSP to issue identity token for

4.4.2 Response envelope example local STS (decrypted)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="messageid">uuid:95a3219f-079f-407b-b14a-
c511ea25d8da</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesto">uuid:af73276c-3ad2-4182-88e3-
4daf50c76305</wsa:RelatesTo>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec_timestamp">
        <wsu:Created>2015-03-20T08:57:20.010Z</wsu:Created>
        <wsu:Expires>2015-03-20T16:57:20.010Z</wsu:Expires>
      </wsu:Timestamp>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
          </Reference>
          <Reference URI="#messageid">
            <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>PzeO7vMcton9klub2j/AHElgOmI=</DigestValue>
          </Reference>
          <Reference URI="#relatesto">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>5R2m6yiD0DStzkwbmdK0zlK9aIk=</DigestValue>
          </Reference>
          <Reference URI="#sec_timestamp">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>NdIhX7CfyjRMmkbN5Cqo1vLJXNs=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>zMOQ+z07XwwIC9W4nj5k3iDIMog=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>HU3ue73OZupo2CYrxXZ+VOx72PWpH94X+ma65MuDWDSFhFVrgRIOM2IXGUe10WXilcZpoX
6LIzStcpc14WZOuO43z0Dl5xpi4VC0BycAT75PjX1I+D8Sdw3o+L/Gs23M9c4lNUf7U+Mt+s0zu1ide98P2cXO
CCQfAZ6Y/KGrE98Ie5QOy8kLP0qT4JqZI972Nw4A6arkmjLT2NzsHxuQrX/tuF/rZjdkr7Imr8gojioMbKINEU
PSU7L4E97vrtHNJh2Dy92g/VqHC3OFg4Ib6ERyfmWqzPk027Js4OQgI0hyqu472mzEfdBN8NlSo9IelqTUaGCJ
OrB8OeMTzhRdQg==</SignatureValue>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
      <RequestSecurityTokenResponse Context="urn:uuid:c3f0de51-fa70-4373-9ecf-
92965394a6d8">
        <TokenType />
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <Address>https://saml.nnit001.dmz.dkdev</Address>
          </EndpointReference>
        </AppliesTo>
        <RequestedSecurityToken>
          <Assertion ID="_d360e5b5-a558-411e-a417-9097b9e84033" IssueInstant="2015-03-
20T08:57:20.010Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

Commented [A15]: Entityid of the WSP this identitytoken is issued for

```
            <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://local.sts.nemlog-in.dk/</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
                <ds:Reference URI="#_d360e5b5-a558-411e-a417-9097b9e84033">
                  <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<ds:DigestValue>Hc5MpIhMWiRF6T01+/qe6n1LjM8CZFA5xtUpmjafNqk=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>

<ds:SignatureValue>WapxF8RcJdMxndZIESjdH3pWGS0Efr+VVvV5KrAG/IkT/fA9gQqLQxhPQN5sDkWGeNe
kWeuMuAe12f1JIhbhYhByL7r89z/R0O64CEVIs+nxXDMoBNwoKPL8VXvPlaIANzNudgT4kbGaMN1R25r1fbQEO
XUIPJn53iDGXcUcWyXNHDULgQzD1G+kSsdRsaUAM22mJNPT+beP1kC114NFyNJ9B1Lh5okXKmZxOfFRMq9Zvby
zYWILmIBI3XbgmUeBpXep1Ft7yZsBZAkTPC4+URGXRoHVTI3sSLohmTKrge/mE0wsNxNL402hvuEAh8Ccl+27E
/zJyW20Xn8xIrZKeQ==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>

<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSSjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MDUwMVoXDTE2MTAwOTE5MDM0OFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NTk3MjQwMzQwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQxIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKG1O
mrGwc+bU6MbI9kyHRjFwkkkloNbwH0M7oV2o5mbTzX+bqiow2lRihyKTm0xtKkXC1sKCPjj9aOjhiN/jDYTBG/
bUeMSuIpvryl83VW0HhjXQFIfe1flR9gBDEdzd4fYVHcbnJNMeMLFb/rdnXCADzPcmsy5w0QxOnrPbGHwzPE0N
2QO/NzS+tz61EWfLGnt9WhOKuD/gur16PVtyWrJ9/bxRGGTyQ06FAp12z+OZ5MGmCXNmi1BDeJzC5kMMbkyN7e
JUCLkXDiWqXoeypCumr68TU4+r/1GvumZTPZW/qRCNpUci96e8ZJrFVrHWlKcnqvYvU+JHey5QXu89ecCAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTqfHRtduHEfrO0lhFT0ou/HItjATAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQC0LTDB/5B0cepHuOG8QBGrH+ARIhJE/ZDl1bi5Z3R7OdBBSR2W2
QiB4GKsZC9qS1jNheK7o7/RCqg+w0U7p5W6+xdAsd5dYwidzMxSJa1lLSovoxFyvfFPK9nU+yaozrciasScylp
mio7AnzWJ26HotU+REoNW9vaeLFIEnQnqbJmpVlBG0Cm7pa4tR8ULC1SQjJTmJXMzNU0JdHb7nDyzYW4sK+40t
4sEGlUfj8eo8oE9l3HMM2I6POaipXSK42s5IG6bOOmbWWqQ57wgJ8qB7YanDu+9hFHje88xrRTl2R2dWfjbS7R
6kB9uS/DojjoA7A1dTx2hGC5qRNobRYlM</X509Certificate>
                </X509Data>
              </KeyInfo>
            </ds:Signature>
```

Commented [A16]: Certificate used to sign the response. Do not verify signature with embedded certificates.

```
            <Subject>
              <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</NameID>
              <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
                <SubjectConfirmationData a:type="KeyInfoConfirmationDataType"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance">
                  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <X509Data>

<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/Zn
SGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0ZP7
mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2sGX
fZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvIED7
cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRftYa8Wnp3jGC8dDwriSfl24GfpDAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vlgYW
2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330LOS
BtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J51T
8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsAHpN
TrcdunHgvCliJaiCK/J2CnH5XmpntX9fn</X509Certificate>
                    </X509Data>
                  </KeyInfo>
                </SubjectConfirmationData>
              </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2015-03-20T08:57:20.010Z" NotOnOrAfter="2015-03-
20T16:57:20.010Z">
              <AudienceRestriction>
                <Audience>https://saml.nnit001.dmz.dkdev</Audience>
              </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
              <Attribute Name="dk:gov:saml:attribute:ProductionUnitIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="ProductionUnitIdentifier">
                <AttributeValue />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:SENumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="SeNumberIndentifie">
                <AttributeValue />
              </Attribute>
```

Commented [A17]: Certificate used to sign the request message since SubjectConfirmation is set to holder-of-key

```
            <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="AssuranceLevel">
              <AttributeValue>True</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="SpecVer">
              <AttributeValue />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="surName">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CommonName">
              <AttributeValue>Morten Mortensen</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="uid">
              <AttributeValue>CVR:10213231-RID:93947552</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="mail">
              <AttributeValue>MortenMortensen@kfobs.dk</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.5"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="serialNumber">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="userCertificate">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.29.29"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Certificate issuer attribute">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UniqueAccountKey">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Privileges">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
```

```
            <Attribute Name="dk:gov:saml:attribute:IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="IsYouthCert">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:PidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="PidNumberIdentifier">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="organizationName">
              <AttributeValue>Økonomistyrelsen // CVR:10213231</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:UserAdministratorIndicator"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserAdministratorIndicator">
              <AttributeValue>0</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CVRnumberIdentifier">
              <AttributeValue>10213231</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="RidNumberIdentifier">
              <AttributeValue>93947552</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.65"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="OCES
Pseudonym">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
          </AttributeStatement>
        </Assertion>
      </RequestedSecurityToken>
      <wst:RequestedAttachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
        <wsse:SecurityTokenReference>
          <wsse:Reference URI="#encryptedassertion" />
        </wsse:SecurityTokenReference>
      </wst:RequestedAttachedReference>
      <wst:RequestedUnattachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
        <wsse:SecurityTokenReference>
          <wsse:Reference URI="#encryptedassertion" />
        </wsse:SecurityTokenReference>
      </wst:RequestedUnattachedReference>
```

Commented [A18]: Asserted attributes

```
        <Lifetime>
          <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T08:57:20.01Z</Created>
          <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T16:57:20.01Z</Expires>
        </Lifetime>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </S11:Body>
</S11:Envelope>
```

4.4.3 Request example local IDP

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-
trust/200802" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="msgid">uuid:f2243dbd-3e58-4032-8a2c-
89474b9e5c6b</wsa:MessageID>
    <wsa:To wsu:Id="to">https://local.sts.nemlog-in.dk/</wsa:To>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec-ts">
        <wsu:Created>2015-03-20T09:04:26Z</wsu:Created>
        <wsu:Expires>2015-03-30T09:04:26Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken wsu:Id="sec-binsectoken" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMT
AwOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBD
VlI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZPQ0
VTIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/Z
nSGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0ZP
7mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2sG
XfZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvIED
7cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAwEA
AaOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly
```

Commented [A19]: Local token case

9vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5h
aWEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEz
CCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBv
c2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZn
JhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklE
IHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS
4zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1
c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1
QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8G
A1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRFtYa8Wnp3jGC8dDwriSfl24GfpDAJBg
NVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vlgY
W2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330LO
SBtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J51
T8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsAHp
NTrcdunHgvCliJaiCK/J2CnH5XmpntX9fn

```
      <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="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>NrdtWxaigbkMffHPgKCAMndq0hRMvsKQSkNelmS5cAE=</DigestValue>
          </Reference>
          <Reference URI="#msgid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>V09c9Qe8xqWvVXJLeWhGI0oa1+wf9Ji/dRyMzHpcDSg=</DigestValue>
          </Reference>
          <Reference URI="#to">
          <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>sMhjXKoKEa8DfxKVk7tu0ZpijaHwgihAElBouQMVIs0=</DigestValue>
          </Reference>
          <Reference URI="#sec-ts">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
```

```
          <DigestValue>IrS/aAyD6HzebEZVuM2TO4BhOOU8aCHFKQXnSsXlzQI=</DigestValue>
        </Reference>
        <Reference URI="#sec-binsectoken">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>BreEB9lOvyk0TDSxVt4vkiu8sTbbXKCmfcHaEJIV8f0=</DigestValue>
        </Reference>
        <Reference URI="#body">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>e4ZBdV2ZgDRpUlHYvCznGQG/hFca/nz1b+N3qYPSqKk=</DigestValue>
        </Reference>
      </SignedInfo>
<SignatureValue>HM/n2dsLwJiJIdirTwxlBwxyZYj04JW9/cH1SmYxQyokQwcfoGMA7mgbL/fMz/BxFG40/A
TWD5XFP1QilFs+4fNzaX8llGZpCyEXh6VPWqXOk3dE2+oT6z6HANQRS0Ax513XRNkDRqDJLZavcEHU8c7O9lJG
Q3eCehtx4U9nHRmEu7OreueQOGB6z1hpDGn3km5BsykGYuSFZgDTK+gF+pCUrU8fNGJ6asu4SYnQRumKS8p0b8
bXKPXAyXxBUfzQs9nhlgkvMEEhshs059vOIVgQ3vw5UP6KnW+0a1/sw+F29QOVrpplZX0BYIuuDrKe84uHKqwN
c2nLhEwwEq3MCQ==</SignatureValue>
      <KeyInfo>
        <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
          <o:Reference URI="#sec-binsectoken" />
        </o:SecurityTokenReference>
      </KeyInfo>
    </Signature>
  </wsse:Security>
</S11:Header>
<S11:Body wsu:Id="body">
  <wst:RequestSecurityToken Context="urn:uuid:502e6d53-d2fb-46fc-afa8-24c8c43623cd">
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
    <wst14:ActAs>
      <saml2:Assertion ID="_09659fea-6c62-4eb4-b65f-789ba396e4ca"
IssueInstant="2015-03-20T09:04:26.1Z" Version="2.0">
        <saml2:Issuer>https://sts.wsc1.test</saml2:Issuer>
        <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="#_09659fea-6c62-4eb4-b65f-789ba396e4ca">
              <Transforms>
                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
```

signature" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<DigestValue>lE63Z24+rwT2XKovXtaYBoByWG3L0lwesdJqsUDa8gg=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>dw7EH6kclc0/xxCPv0QTZSBu6faKPlj8WI6+dHpy16jRb4a6Af+iaHWHy9Ll/bQ7OUrtM9
hAazGirB2xw1gvnPOBAefTjxMh4w6pfWqs61hlCY6svJIhcovq93DOdz1E5B6/Zv9XrGTX8iVMHoBS144gKIhM
lFKARfVzlC+yptZcfXuldHf9aBSnOBtIWLdaSMvfUccQva90oOjwb8p/6O9mC4r5nxdKgyg/GYjkwQ9Uvhn5Ev
orityTURD+oxRauO5V3JGzIuCK7mMBVnyi9QSNKIBEpsCmpxnnGojgUYrURSoCLIvMOESPkLuoKiWvGW1cKE2j
eaBt9WkIepyOpw==</SignatureValue>
</Signature>
<saml2:Subject>
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-
of-key">
<saml2:SubjectConfirmationData
xsi:type="saml2:KeyInfoConfirmationDataType">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESz
ESMBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEz
MTAwOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLy
BDVlI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZP
Q0VTIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM
/ZnSGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0
ZP7mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2
sGXfZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvI
ED7cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAw
EAAaOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6
Ly9vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi
5haWEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIB
EzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZX
Bvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIg
ZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbk
lEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQu
MS4zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudH
J1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJV
U1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB
8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRFtYa8Wnp3jGC8dDwriSfl24GfpDAJ
BgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vl
gYW2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330
LOSBtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J
51T8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsA
HpNTrcdunHgvCliJaiCK/J2CnH5XmpntX9fn</ds:X509Certificate>
</ds:X509Data>

```
              </ds:KeyInfo>
            </saml2:SubjectConfirmationData>
          </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2015-03-20T09:04:26.1Z" NotOnOrAfter="2015-03-
20T17:04:26.1Z">
          <saml2:AudienceRestriction>
            <saml2:Audience>https://local.sts.nemlog-in.dk/</saml2:Audience>
          </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AttributeStatement>
          <saml2:Attribute FriendlyName="ProductionUnitIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:ProductionUnitIdentifier">
            <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="SeNumberIndentifie"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:SENumberIdentifier">
            <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:AssuranceLevel">
            <saml2:AttributeValue xsi:type="xs:string">True</saml2:AttributeValue>
          </saml2:Attribute>
          <saml2:Attribute FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="dk:gov:saml:attribute:SpecVer">
            <saml2:AttributeValue xsi:type="xs:string"></saml2:AttributeValue>
          </saml2:Attribute>
        </saml2:AttributeStatement>
      </saml2:Assertion>
    </wst14:ActAs>
    <wsp:AppliesTo>
      <wsa:EndpointReference>
        <wsa:Address>https://saml.nnit001.dmz.dkdev</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>
  </wst:RequestSecurityToken>
 </S11:Body>
</S11:Envelope>
```

Commented [A20]: Mandatory audience for both local STS and IDP policies. For the latter additional audiences are allowed

4.4.4 Response envelope example local IDP (decrypted)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
```

```
1.0.xsd">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="messageid">uuid:6a30340d-37d6-4b06-bf23-
ed8ce500feab</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesto">uuid:f2243dbd-3e58-4032-8a2c-
89474b9e5c6b</wsa:RelatesTo>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec_timestamp">
        <wsu:Created>2015-03-20T09:04:46.256Z</wsu:Created>
        <wsu:Expires>2015-03-20T17:04:46.256Z</wsu:Expires>
      </wsu:Timestamp>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
          </Reference>
          <Reference URI="#messageid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>uCXhfwzmKLctxTEUFIkXQ49Gq3c=</DigestValue>
          </Reference>
          <Reference URI="#relatesto">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>FZhXB+BSpXWxXIEhgtpNhK0oTcg=</DigestValue>
</Reference>
          <Reference URI="#sec_timestamp">
            <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>eQY5cdqEBXcQU4uEB4+zEfEUr9c=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>p9fH1dnXThhomMxcm7xZ4KJe5p4=</DigestValue>
</Reference>
        </SignedInfo>
<SignatureValue>YqDIO35dNEmzP8j7375Nj/dZLHnTwr0iFb9zhe2aPRopbBPXAIGzvofW43si41FXkrkxlb
XlZDnWeKCFY4zahEINVp2hvRV1VCf7UgE+MfFYtF9u8ksaLXKRyq96Yw1YnM237HUDSH8eAtYP4/0u4yQwvtfg
6jSkm89nEkm6WBVVBZKyVE1cr87ltrAdDRPFILyoxYWo1NWjVGnWPyTFKRx2lmBoTn3Pdb3DFqXffPB7HgI7BR
Sclbx6MJK1zPc1CvvC4ZK8Fj6SYZ2JnXUAf96e46K4BOy9UK+f+oixEjPCByIJy611nc59+UJdd28sJydXm7bE
xSmdWpkIAjoOng==</SignatureValue>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
      <RequestSecurityTokenResponse Context="urn:uuid:502e6d53-d2fb-46fc-afa8-
24c8c43623cd">
        <TokenType />
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <Address>https://saml.nnit001.dmz.dkdev</Address>
</EndpointReference>
        </AppliesTo>
        <RequestedSecurityToken>
          <Assertion ID="_cc909803-e214-459c-842d-67915512f655" IssueInstant="2015-03-
20T09:04:46.256Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://local.sts.nemlog-in.dk/</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
                <ds:Reference URI="#_cc909803-e214-459c-842d-67915512f655">
```

```
                <ds:Transforms>
                  <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>
<ds:DigestValue>V/0KsXEEEuSF/qC8K6Q2sCzGjbfQB4KUBLccuxeSoC4=</ds:DigestValue>
</ds:Reference>
              </ds:SignedInfo>
<ds:SignatureValue>WwBbPMuPObjJYfXI3uMTgZd5471mI7A3r4dzeSqUNEA57BYA1gO5Azkxlts2P9Lwhip
J/2XQD2oecugaQNCg7THTMavctZHj+hJyRz+Ww8fujHnxChysaKBMi53lTydWkwYWizkAHJ2lmJKMBxSsAXK93
C+FjW5Bi9V+kjV8dA3Mde1wtSbhMxx7HW6BZsjQ79axyBKIbEx1E4aTeMlnEeR7XyAozT01JRso/4eMF6KYbX6
FZHOJLPblgeiMqOxNbdqCMolfbTTPmjvUp7w+EI/bgRamP/bGgLOD5UlukB/pVlaB1orKXew46SMZr//PftyCZ
WtcjbD81U2vPJzyhw==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSSjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MDUwMVoXDTE2MTAwOTE5MDM0OFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NTk3MjQwMzQwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQxIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKG1O
mrGwc+bU6MbI9kyHRjFwkkkloNbwH0M7oV2o5mbTzX+bqiow2lRihyKTm0xtKkXC1sKCPjj9aOjhiN/jDYTBG/
bUeMSuIpvryl83VW0HhjXQFIfe1flR9gBDEdzd4fYVHcbnJNMeMLFb/rdnXCADzPcmsy5w0QxOnrPbGHwzPE0N
2QO/NzS+tz61EWfLGnt9WhOKuD/gur16PVtyWrJ9/bxRGGTyQ06FAp12z+OZ5MGmCXNmi1BDeJzC5kMMbkyN7e
JUCLkXDiWqXoeypCumr68TU4+r/1GvumZTPZW/qRCNpUci96e8ZJrFVrHWlKcnqvYvU+JHey5QXu89ecCAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTqfHRtduHEfrO0lhFT0ou/HItjATAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQC0LTDB/5B0cepHuOG8QBGrH+ARIhJE/ZDl1bi5Z3R7OdBBSR2W2
QiB4GKsZC9qS1jNheK7o7/RCqg+w0U7p5W6+xdAsd5dYwidzMxSJa1lLSovoxFyvfFPK9nU+yaozrciasScylp
mio7AnzWJ26HotU+REoNW9vaeLFIEnQnqbJmpVlBG0Cm7pa4tR8ULC1SQjJTmJXMzNU0JdHb7nDyzYW4sK+40t
4sEGlUfj8eo8oE9l3HMM2I6POaipXSK42s5IG6bOOmbWWqQ57wgJ8qB7YanDu+9hFHje88xrRTl2R2dWfjbS7R
6kB9uS/DojjoA7A1dTx2hGC5qRNobRYlM</X509Certificate>
                </X509Data>
              </KeyInfo>
            </ds:Signature>
            <Subject>
              <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
```

```
Mortensen,Serial=CVR:10213231-RID:93947552</NameID>
            <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
              <SubjectConfirmationData a:type="KeyInfoConfirmationDataType"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance">
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                  <X509Data>
<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSTDANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MTMzM1oXDTE2MTAwOTE5MTIzOFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NDkxOTY0MzEwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQyIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM/Zn
SGcUTb5QEGNoYbRo9ivhyhvWh0Wpqjxd034T5J6q2sGyRhmj+t/U0ED0fvqMSPYRO1ovaeLpT++lNz08EG0ZP7
mek5eUeyQlBZseAe8ZUKFSUXfNvYvo/x/inVxePCTBwPvYVUP1ap/V4dRcz/Y1e5+qjrweWuZJ1Yct1KqW2sGX
fZTEBFdsiTVlxAiLwcM9KVthV+rUB3dqtu1FvVO0TOQJLxzD7eP6ObF1gRGG14kG0fknrKcPvq35OyFluvIED7
cykHfedVeAZP3DY3dgrsWaKi8ztlIUHH5avIq5hKm6JCcYzrB6LaX6aG0GMFMZ9R/Mw9alUxTvak//K0CAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBRFtYa8Wnp3jGC8dDwriSfl24GfpDAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQDKHXvqqw7V4gKLcd0WRmivpyupIsxJsfB9oqjVGOOHJXr7vlgYW
2bkMjUpSy6WLTd+686ZjLh1E1FWCwqw1rwI8/BlxX62fT8j79EDamJLBAvUXOYNL1drG33lH7vZK90ri330LOS
BtOy9EOm+7v/lKwdYbgHYDgFub+htYiB4RofkiVKhzgdwHV9WjMcKUQ99hWhHww4thy1RoxEjPXZLMkSG8J51T
8+GW0DGzXI8l7Pc0nKcn5PN6ydoC+ErTTgsAEMW2qq+N7G+Hs/E7IZ9HLGJ3EvPvborHqQwElh7WEOq8OsAHpN
TrcdunHgvCliJaiCK/J2CnH5XmpntX9fn</X509Certificate>
                  </X509Data>
                </KeyInfo>
              </SubjectConfirmationData>
            </SubjectConfirmation>
          </Subject>
          <Conditions NotBefore="2015-03-20T09:04:46.256Z" NotOnOrAfter="2015-03-
20T17:04:46.256Z">
            <AudienceRestriction>
              <Audience>https://saml.nnit001.dmz.dkdev</Audience>
            </AudienceRestriction>
          </Conditions>
          <AttributeStatement>
            <Attribute Name="dk:gov:saml:attribute:ProductionUnitIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="ProductionUnitIdentifier">
              <AttributeValue />
            </Attribute>
```

Commented [A21]: Always holder-of-key for local IDP policy

Commented [A22]: WSC certificate refereced for the local IDP policy

```
            <Attribute Name="dk:gov:saml:attribute:SENumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="SeNumberIndentifie">
              <AttributeValue />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="AssuranceLevel">
              <AttributeValue>True</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="SpecVer">
              <AttributeValue />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="surName">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CommonName">
              <AttributeValue>Morten Mortensen</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="uid">
              <AttributeValue>CVR:10213231-RID:93947552</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="mail">
              <AttributeValue>MortenMortensen@kfobs.dk</AttributeValue>
            </Attribute>

            <Attribute Name="urn:oid:2.5.4.5"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="serialNumber">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="userCertificate">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.29.29"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Certificate issuer attribute">
              <AttributeValue a:nil="true"
```

```
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UniqueAccountKey">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Privileges">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="IsYouthCert">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:PidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="PidNumberIdentifier">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="organizationName">
                <AttributeValue>Økonomistyrelsen // CVR:10213231</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:UserAdministratorIndicator"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserAdministratorIndicator">
                <AttributeValue>0</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CVRnumberIdentifier">
<AttributeValue>10213231</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="RidNumberIdentifier">
                <AttributeValue>93947552</AttributeValue>
              </Attribute>
              <Attribute Name="urn:oid:2.5.4.65"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="OCES
```

```
Pseudonym">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
            </AttributeStatement>
          </Assertion>
        </RequestedSecurityToken>
        <wst:RequestedAttachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedAttachedReference>
        <wst:RequestedUnattachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedUnattachedReference>
        <Lifetime>
          <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T09:04:46.256Z</Created>
          <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T17:04:46.256Z</Expires>
        </Lifetime>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </S11:Body>
</S11:Envelope>
```

4.5 Signature scenario

In this scenario the "user identity" is proofed by the signing of the request to Nemlog-in STS. The scenario which exists in an Identity policy and a System policy variant contains no bootstrap tokens.

Request and response messages are described in detail in [STS-RULES].

4.5.1 Request example ("Identity" / MOCES certificate)

```
POST https://securetokenservice.nemlog-in.dk/SecurityTokenService.svc HTTP/1.1
SOAPAction: http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
```

```
Content-Type: text/xml;charset=utf-8
Host: securetokenservice.nemlog-in.dk
Content-Length: [length]


<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-
trust/200802" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="msgid">uuid:541a1974-13e5-4d36-a6c5-
f71d0605b275</wsa:MessageID>
    <wsa:To wsu:Id="to">https://signature.sts.nemlog-in.dk/</wsa:To>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec-ts">
        <wsu:Created>2015-03-20T08:02:23Z</wsu:Created>
        <wsu:Expires>2015-03-30T08:02:23Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken wsu:Id="sec-binsectoken" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIGIDCCBQigAwIBAgIETAV1TzANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEyMD
ExMjE0MTQwNloXDTE2MDExMjE0MTM1MlowdjELMAkGA1UEBhMCREsxKjAoBgNVBAoMIcOYa29ub21pc3R5cmVs
c2VuIC8vIENWUjoxMDIxMzIzMTE7MBcGA1UEAwwQTW9ydGVuIE1vcnRlbnNlbjAgBgNVBAUTGUNWUjoxMDIxMz
IzMS1SSUQ6OTM5NDc1NTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXxgVHipGqErG8xLbYqxmP
vyZzh1aBK4th2YaiIbRyZfSO3gOxhWs+XR3JLOrVMgKxERYGD4fTnNfWU7TpYaTO8pnXEx2+bV2ohIzcyavQYW
21KMgcp1psWr6wv5IuF0Ykhydv9OOqJRouBh4oHJwvBjVJQLDw0L+d6bJ/DjW+tHWtuWMyPUKZRjQf6dWIA45p
kLH8mcFNztxGIOZHvlqH7IiPHc73KKqxmig/vvdUCVI15MADeCsQQ8ds0Aw7uFJiytROF/5wD0jJOZHJToBLvt
Qd8UShEtL6TSiEchi2ZVPf/tJmiRriQQNHQy/sWEPlnkt2HZxRkuPNzt1GeMVBAgMBAAGjggLiMIIC3jAOBgNV
HQ8BAf8EBAMCA/gwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcC5zeXN0ZW10ZX
N0OC50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL20uYWlhLnN5c3RlbXRlc3Q4
LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARMwggEPBg0rBgEEAYH0UQ
IEBgIFMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb3NpdG9yeTCByQYIKwYB
BQUHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZyYSBkZW5uZSBDQSB1ZH
N0ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41LiBEYW5JRCB0ZXN0IGNlcnRpZmlj
YXRlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi
41LjAYBgNVHREEETAPgQ1qZWxmQG5uaXQuY29tMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lz
dGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMB
AGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQD
DAdDUkwxMTI0MB8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTv7aQGa8L1qrrstR
8ItB9Lz0RT/zAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQA0Pd04cFScEKoZgug3x+GBFoYzDgYBZR/d
SJexU3N9+e5wTgwterC9Ykk3BTV4VlBl6NFUjP9TPqOZaCkqTdWlXruy0wNKvMNGacVZJhS91baTW3ZnNIhAE5
x5gDxvsjuRVc0xZvyAhT7jkp4J62haMoDt+pRsZoDcVCN0KuLWL+Lh5efaB9vSCMsyKUjXf9A/F21nhBiNsECs
WjNXyt2/igbTuYCST12dTCpHs+sDEAnaZlTJa2B/CMUPo15niVLFuOWCPPyxurUZfB3bK/9qdHT60JvaVezwAA
mCWYEW7CW4AAGKDPMDG1qsRxFgaObB3bd5zCbnJkW/SNhg8/lc</wsse:BinarySecurityToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
```

Commented [A23]: Signature scenario

Commented [A24]: Moces certificate used to sign the message

```
          <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="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>NrdtWxaigbkMffHPgKCAMndq0hRMvsKQSkNelmS5cAE=</DigestValue>
          </Reference>
          <Reference URI="#msgid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>dBMMqthBFSaQDgkdW4gE99QbqbyiS/9BbMk3pO/CWS4=</DigestValue>
          </Reference>
          <Reference URI="#to">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>VRjscE+sMXYwGdFXLwczBVCnXdPBwx7vm800+bGCrQw=</DigestValue>
          </Reference>
          <Reference URI="#sec-ts">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>Za45FgPz/Ayqtbhxa0QC4P26P0ev+0S/hVyzK8KvAic=</DigestValue>
          </Reference>
          <Reference URI="#sec-binsectoken">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>gC0rvFzqTwR4HgCX5liQ6AnQuriSEQw9PUZlHDD9nn0=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>y5x5ngzpwCabqA7/8KPzuIUmk2Au/ovaCBrHPimVbGY=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>OEfmkHRk/wESKHFhlktNM85Mpkn7pcGGq0SrTDBul6ix52tDr7nUIlq3sWSRmpdTtb6Bkn
IWarQ2CLkckzhy4tMYIrvARA1x1cMvUGOCsqevTTbZl7zhcLgZVUsykM6wRwnmF9QGRJZ9dOBPVXqhlHSAT7RU
6jL8/IHbNI/wo71h7NYYM1X8xLyfXJIpxAfj2o0Th+WVvluu04Li8KTJ/2kYzgtXPC2dMByfRb2EyjGuT2NUF0
Eab8KyqFfoUW5dUu1uZt+afSWpqor8ALvnKhpEy0ij62gXUAmlhscz06QSkEIv4+VBYRzEfXwyAcl+Lro82q0u
39/O+A1qv2NT4Q==</SignatureValue>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#sec-binsectoken" />
          </o:SecurityTokenReference>
```

```
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <wst:RequestSecurityToken Context="urn:uuid:705515c8-54d0-4336-9c28-d05f30093125">
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>https://saml.nnit001.dmz.dkdev</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

Commented [A25]: EntityId to issue identity token for

4.5.2 Response envelope example local STS ("Identity" / MOCES certificate) (decrypted)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="messageid">uuid:6f89d3ae-0fad-4c5d-925c-
60e9240e6a13</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesto">uuid:541a1974-13e5-4d36-a6c5-
f71d0605b275</wsa:RelatesTo>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec_timestamp">
        <wsu:Created>2015-03-20T08:03:13.429Z</wsu:Created>
        <wsu:Expires>2015-03-20T16:03:13.429Z</wsu:Expires>
      </wsu:Timestamp>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#action">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
          </Reference>
          <Reference URI="#messageid">
            <Transforms>
```

```
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>YFINY7VV9KL8xD8uiyOanefFjFI=</DigestValue>
          </Reference>
          <Reference URI="#relatesto">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>08Ji4Y2kwdfhjWbs5tYB4eUkoS0=</DigestValue>
          </Reference>
          <Reference URI="#sec_timestamp">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>jSPcIsNzQaUWI7EnZG5EMlkDt7s=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>J2sdhxiII1poBx33sQTtd2bs4AM=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>YIN1SzPV/ThEewqVTY9nLdE1RwhqyPQ7PxZznZRHgEvyvquIMnjGGoQ28fc8UouU4LFqSc
czMoxDqSzYz6izT4RJ9YbGAYDHZOyg7ItioaWSLk7VQ9pwbQFSv/nT2+6fangc3+qzGdPhLDLevwPTFmKi272i
KeBmVgSeD06JROx9K+gV1BfVr7qj7JQ0gEl82Zprk62tQ7weXhDuGaLqtmqeif4gXJtz7jAwlwEItUt1EHsZ0V
mgZ2piR3HH9+o/i/tRv6Zsscp1mzhqfRMNdqlXyNxZktYA2GAJCN+aFn1hDti6U/0KX39AZVafEnOv+6u7LUwE
wSrSZNtJzgW2tA==</SignatureValue>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
      <RequestSecurityTokenResponse Context="urn:uuid:705515c8-54d0-4336-9c28-
d05f30093125">
        <TokenType />
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <Address>https://saml.nnit001.dmz.dkdev</Address>
          </EndpointReference>
        </AppliesTo>
        <RequestedSecurityToken>
          <Assertion ID="_284fff56-38b7-470a-96d3-961a43a38b5b" IssueInstant="2015-03-
20T08:03:13.429Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

Commented [A26]: Entityid of the WSP this identity token is issued for

```
            <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://signature.sts.nemlog-in.dk/</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
                <ds:Reference URI="#_284fff56-38b7-470a-96d3-961a43a38b5b">
                  <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>

<ds:DigestValue>P5Nez2ge68csaXnrFsvc/AAsywWMcRY0e6RlVLnXG7Q=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
<ds:SignatureValue>AVt5zPLJvgUA8oOsjqCk1z0pu/V0s/10o7guZugGJkyLdX7zl8pr1Gk1xTQazb9FSDL
Hpvdo4RJ5bYJSq73gaslQIWWXOcoVvS5UuNQ/v/NPx8h4/x9uR5xsGQDEXi6U8TbLq/VTamh0uYbHBQqaJIPst
KqnijJy8FZJRBtQWazJMVa1ccmH1zrostkYGFVGTfRiwTTVw3nGOcDGN0b6HFkh21gKr0RKFJw+UUDpeghU4ap
pdTMjVlgpMMqYnwvxeEi+oJRtgOKJWX9Q2iYJ+YXeuuljiOFeMCNAKszewAjXz6jowGRaM6wJzYSaYBYqpJ6Ng
+nMCt634XTAivrcwA==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSSjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MDUwMVoXDTE2MTAwOTE5MDM0OFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NTk3MjQwMzQwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQxICAhmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKG1O
mrGwc+bU6MbI9kyHRjFwkkkloNbwH0M7oV2o5mbTzX+bqiow2lRihyKTm0xtKkXC1sKCPjj9aOjhiN/jDYTBG/
bUeMSuIpvryl83VW0HhjXQFIfe1flR9gBDEdzd4fYVHcbnJNMeMLFb/rdnXCADzPcmsy5w0QxOnrPbGHwzPE0N
2QO/NzS+tz61EWfLGnt9WhOKuD/gur16PVtyWrJ9/bxRGGTyQ06FAp12z+OZ5MGmCXNmi1BDeJzC5kMMbkyN7e
JUCLkXDiWqXoeypCumr68TU4+r/1GvumZTPZW/qRCNpUci96e8ZJrFVrHWlKcnqvYvU+JHey5QXu89ecCAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTqfHRtduHEfrO0lhFT0ou/HItjATAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQC0LTDB/5B0cepHuOG8QBGrH+ARIhJE/ZDl1bi5Z3R7OdBBSR2W2
QiB4GKsZC9qS1jNheK7o7/RCqg+w0U7p5W6+xdAsd5dYwidzMxSJa1lLSovoxFyvfFPK9nU+yaozrciasScylp
mio7AnzWJ26HotU+REoNW9vaeLFIEnQnqbJmpVlBG0Cm7pa4tR8ULC1SQjJTmJXMzNU0JdHb7nDyzYW4sK+40t
4sEGlUfj8eo8oE9l3HMM2I6POaipXSK42s5IG6bOOmbWWqQ57wgJ8qB7YanDu+9hFHje88xrRTl2R2dWfjbS7R
6kB9uS/DojjoA7A1dTx2hGC5qRNobRYlM</X509Certificate>
                </X509Data>
              </KeyInfo>
            </ds:Signature>
            <Subject>
```

Commented [A27]: Certificate used to sign the response. Do not verify signature with embedded certificates.

```
            <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Økonomistyrelsen // CVR:10213231,CN=Morten
Mortensen,Serial=CVR:10213231-RID:93947552</NameID>
            <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
          </Subject>
          <Conditions NotBefore="2015-03-20T08:03:13.429Z" NotOnOrAfter="2015-03-
20T16:03:13.429Z">
            <AudienceRestriction>
              <Audience>https://saml.nnit001.dmz.dkdev</Audience>
            </AudienceRestriction>
          </Conditions>
          <AttributeStatement>
            <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="SpecVer">
              <AttributeValue>DK-SAML-2.0</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="AssuranceLevel">
              <AttributeValue>2.0</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="surName">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CommonName">
              <AttributeValue>Morten Mortensen</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="uid">
              <AttributeValue>CVR:10213231-RID:93947552</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="mail">
              <AttributeValue>MortenMortensen@kfobs.dk</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.5"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="serialNumber">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="userCertificate">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.29.29"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Certificate issuer attribute">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
```

Commented [A28]: Subjectname extracted from the certificate used to sign the request

```
            <Attribute Name="dk:gov:saml:attribute:UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UniqueAccountKey">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Privileges">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="IsYouthCert">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:PidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="PidNumberIdentifier">
              <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="organizationName">
              <AttributeValue>Økonomistyrelsen // CVR:10213231</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:ProductionUnitIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="ProductionUnitIdentifier">
              <AttributeValue>1003388503</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:UserAdministratorIndicator"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="UserAdministratorIndicator">
              <AttributeValue>0</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:SENumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="SENumberIdentifier">
              <AttributeValue>66662222</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CVRnumberIdentifier">
              <AttributeValue>10213231</AttributeValue>
            </Attribute>
            <Attribute Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="RidNumberIdentifier">
              <AttributeValue>93947552</AttributeValue>
            </Attribute>
            <Attribute Name="urn:oid:2.5.4.65"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="OCES
Pseudonym">
```

```
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
            </AttributeStatement>
          </Assertion>
        </RequestedSecurityToken>
        <wst:RequestedAttachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedAttachedReference>
        <wst:RequestedUnattachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedUnattachedReference>
        <Lifetime>
          <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T08:03:13.429Z</Created>
          <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T16:03:13.429Z</Expires>
        </Lifetime>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </S11:Body>
</S11:Envelope>
```

Commented [A29]: Issued attributes

4.5.3 Request example ("System" / FOCES/VOCES certificate)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-
trust/200802" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">

  <S11:Header>

    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
```

```
    <wsa:MessageID wsu:Id="msgid">uuid:e5bda526-5923-4d78-a4d7-
534a3e6d1b5a</wsa:MessageID>
    <wsa:To wsu:Id="to">https://signature.sts.nemlog-in.dk/</wsa:To>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec-ts">
        <wsu:Created>2015-03-20T08:05:49Z</wsu:Created>
        <wsu:Expires>2015-03-30T08:05:49Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken wsu:Id="sec-binsectoken" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-
1.0#Base64Binary">MIIGGTCCBQGgAwIBAgIEUw+gETANBgkqhkiG9w0BAQsFADBHMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSQwIgYDVQQDDBtUUlVTVDI0MDggU3lzdGVtdGVzdCBYSVggQ0EwHhcNMTUwMT
IxMTgwNDQ0WhcNMTgwMTIxMTgwNDA5WjCBhzELMAkGA1UEBhMCREsxITAfBgNVBAoMGE5OSVQgQS9TIC8vIENW
UjoyMTA5MzEwNjFVMCAGA1UEBRMZQ1ZSOjIxMDkzMTA2LUZJRDo1OTQ3ODA5MTAxBgNVBAMMKktGT0JTLVRFU1
QtRk9DRVMtMDU5ICHmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AIQlH94vHdHGtq1o1DFRvQYmmsitJxbI5PyIJQXoFPIGbjon7A9+tgR/Nt5mF2X2aGh1Ouw8kfLnetVsoifG0Y
OGyp2rKzEqTsU4Emxw4Myj4FwDG06xkYuxiBKKkB6won86RXr3QvRed28vAkDSEniFGIabXRxlVv/HWASEJIEo
+yqFnVOmmqSBh9RIQ5i/JpJUhJdZ2M988O10RuNo2SIRrJ2/Mv+FLtlSlJLa4IgedQ936ATEOheNOLsVNLOMww
qfvWv3im+RWqBTVktYqWnB7qmM8oBJSBxRSe4gJ+PQfQ4s37BK+5/NSmrV8WnNqoFrxsV9SRMwhUavGxI4mA0C
AwEAAaOCAsowggLGMA4GA1UdDwEB/wQEAwIDuDCBlwYIKwYBBQUHAQEEgYowgYcwPAYIKwYBBQUHMAGGMGh0dH
A6Ly9vY3NwLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBHBggrBgEFBQcwAoY7aHR0cDov
L2YuYWlhLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3N5c3RlbXRlc3QxOS1jYS5jZXIwggEgBgNVHSAEgg
EXMIIBEzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNv
bS9yZXBvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2
F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIu
IERhbklEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi
4xLjQuMS4zMTMxMy4yLjQuNi40LjIuMIGqBgNVHR8EgaIwgZ8wPKA6oDiGNmh0dHA6Ly9jcmwuc3lzdGVtdGVz
dDE5LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDE5LmNybDBfoF2gW6RZMFcxCzAJBgNVBAYTAkRLMRIwEAYDVQ
QKDAlUUlVTVDI0MDgxJDAiBgNVBAMMG1RSVVNUMjQwOCBTeXN0ZW10ZXN0IFhJWCBDQTEOMAwGA1UEAwwFQ1JM
MjIwHwYDVR0jBBgwFoAUzAJVDOSBdK8gVNURFFeckVI4f6AwHQYDVR0OBBYEFNc41PG/agTmqzigwWuFpNkf8z
f3MAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBADnssIGIxgIPwgfgLjxuOYPVchS5W68JeQOoljGhEGJY
/9sao8HvTLiJCPSwJ0SuyPJUu6/b6r1Q0ATGwk1fmCEjDQidyOAg2Lsn1sDix+Nbf+CxvtI2F1gIx7IasExBDJ
gsCOsozCDdoHBaPbAqhrj/pu0tp+rcHA/tG3DAsyHSlbZBYmO3QyKn7+GVIikEi2sSnwvaT95fRUUvf4ur2n9s
l1gIfXqbPliWgAiHeAn8u9FzjvIZmbOOt3yuzf3tr6ZREB3Emp6spHWmlERNeiHFSrZIIGk/kDYLYC8Oza4sNe
FmIGVUaReidHGGVA3IMACfJCVLqGBG6VyZaJHPVhs=</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="#action">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
```

Commented [A30]: Signature case

Commented [A31]: Signing certificate of type VOCES or FOCES for System policy

```
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>NrdtWxaigbkMffHPgKCAMndq0hRMvsKQSkNelmS5cAE=</DigestValue>
        </Reference>
        <Reference URI="#msgid">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>DGrhNDOP5WVXHv32syDFjz/EvkwX9fUho0E4Z7Ng858=</DigestValue>
        </Reference>
        <Reference URI="#to">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>VRjscE+sMXYwGdFXLwczBVCnXdPBwx7vm800+bGCrQw=</DigestValue>
        </Reference>
        <Reference URI="#sec-ts">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>OKCzjbMTQzBTl+Du4FO+7uqIx6rn4HX0ztPoPqWUiK4=</DigestValue>
        </Reference>
        <Reference URI="#sec-binsectoken">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>Q2VuF5Ly9NMqX3gnkPXEb4CP6iIIUl8iIf20CptoUNY=</DigestValue>
        </Reference>
        <Reference URI="#body">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
          <DigestValue>AkcsxCYOD/d3ts/9xR5kL+thdatMMTteK6pwMj1tQdg=</DigestValue>
        </Reference>
      </SignedInfo>
<SignatureValue>Ki2+KJk83cE1RAiH113n40CTv/yDsm/U/gXmGt0pnZveW7hAu65YiGVH5M71NArRVs5k6J
+u4u8je1EdBe09s3Jbb9xtoK/1Oth13Ny+o3PBwDN/KvbO6yFH+B3Z1HxhS/SP0NqcwT/rgxW2uT+zpVvyOgd2
Iv5tg7rU77yaGbl3FRWrFfCwdmf4GPkzAMV4rnjIgJPpFRsPO0mZc56wLqlw/+eHrHGFMYcIiLVASfHzrxL8ww
30dC0S1dNmFbTpvQ/kVft/PJU6j22Hbj6csPcVYYlN7MRv1f91j/b2mpkR1FCG6cPe/GMtrIr81qyvFyZ0SIQ3
78++RWtBGPfmog==</SignatureValue>
      <KeyInfo>
```

```
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
            <o:Reference URI="#sec-binsectoken" />
          </o:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <wst:RequestSecurityToken Context="urn:uuid:9f4e1596-7d81-4af5-8334-99d3d1bc169f">
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>https://saml.nnit001.dmz.dkdev</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

4.5.4 Response envelope example (“System” / FOCES/VOCES certificate) (decrypted)

```
<S11:Envelope xmlns:S11="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
  <S11:Header>
    <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID wsu:Id="messageid">uuid:38753c46-9a4f-4559-9bd6-
ac0d7625e9e6</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesto">uuid:e5bda526-5923-4d78-a4d7-
534a3e6d1b5a</wsa:RelatesTo>
    <wsse:Security S11:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="sec_timestamp">
        <wsu:Created>2015-03-20T08:05:52.871Z</wsu:Created>
        <wsu:Expires>2015-03-20T16:05:52.871Z</wsu:Expires>
      </wsu:Timestamp>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></CanonicalizationMethod>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></SignatureMethod>
          <Reference URI="#action">
```

```
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
          </Reference>
          <Reference URI="#messageid">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>hF7C+AMXxUURhrOLdjsKxO9bEF4=</DigestValue>
          </Reference>
          <Reference URI="#relatesto">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>Akm30KBGu0EG53Tz5PtNW9YeWS8=</DigestValue>
          </Reference>
          <Reference URI="#sec_timestamp">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>df1/tn25bpbOJeBIqiyoPKln6d0=</DigestValue>
          </Reference>
          <Reference URI="#body">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"></Transform>
            </Transforms>
            <DigestMethod
```

```
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
            <DigestValue>w7mwHz+Hzxj95VQSBobpcpRmHdY=</DigestValue>
          </Reference>
        </SignedInfo>
<SignatureValue>ZECtXNhsoDF2Cq2/vx9plfXJ8O72FiJOGg1nf64WKQS0aYuQoH3yweCZaHJ3hDisSGEEgn
iCHGcCIbLQ2CNW0POPBk47ZqOZo0LEgZamO093z3Z8SgmTGR3UHNMfGYxItBG/AAM4R5T3Rp82dKiSHPNTGn3l
4fUt+2rPf3ZQNzS7T57sW53yMC+im2Q0pufJ6THyThr4sF8+CuUvMJQEx7urqIzPOwCdRjgNUfHGpJJvn5QFXG
8mnf0/MBea2qHFfFjwAZ0qHlu4WnQkUqQPqsUsZahS8NV5maaN+mncDDbah1FaSi66PUxxVtEsu5R4nQUKx0qe
xjR7byjsOzUgSQ==</SignatureValue>
      </Signature>
    </wsse:Security>
  </S11:Header>
  <S11:Body wsu:Id="body">
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
      <RequestSecurityTokenResponse Context="urn:uuid:9f4e1596-7d81-4af5-8334-
99d3d1bc169f">
        <TokenType />
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
          <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
            <Address>https://saml.nnit001.dmz.dkdev</Address>
          </EndpointReference>
        </AppliesTo>
        <RequestedSecurityToken>
          <Assertion ID="_10fbef57-875f-4e91-b477-76308c247772" IssueInstant="2015-03-
20T08:05:52.871Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://signature.sts.nemlog-in.dk/</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
                <ds:Reference URI="#_10fbef57-875f-4e91-b477-76308c247772">
                  <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
/>
<ds:DigestValue>MdcOES5VZSD6slE4wq6U6OqKdhvKz5lJ5b3JTm5OJk4=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
<ds:SignatureValue>T52l7YL7Sm1rMQsMsNrdnphh+rF43mdXoEcWiQOXVm0YAbvjs98AcclVX1FKrAjvyKP
Iaj0makE5EiqK68UFNb6l/hvLt7SmYclydojT0PZxIKHIU+RYnnexqxVr6HekEYDgek0GrivwFZBzO67jyx6h3
TdcZZ3Of2UAzHFG23BvMv2d/8YNWtYd7e/hMKUlictoUQpGznDo9ZEyNnITHflkh+Bt+YY5kuXMEmEzhfQH4S5
7sSbEzSrfPx+Jp+OG6m3Ytp/JlD6ZG/424ugXPD7ohPs1UPVYgLATKWMJEC847OKrjqfxYmbPBTIRNVuT9StqX
```

```
vRqcvbcewQWad9A1Q==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
<X509Certificate>MIIGFDCCBPygAwIBAgIETBGSSjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wOTE5MDUwMVoXDTE2MTAwOTE5MDM0OFowgYMxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUTAgBgNVBAUTGUNWUjoyMTA5MzEwNi1GSUQ6NTk3MjQwMzQwLQYDVQQDDCZOTklUIEZPQ0V
TIGNlcnQxICHmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKG1O
mrGwc+bU6MbI9kyHRjFwkkkloNbwH0M7oV2o5mbTzX+bqiow2lRihyKTm0xtKkXC1sKCPjj9aOjhiN/jDYTBG/
bUeMSuIpvryl83VW0HhjXQFIfe1flR9gBDEdzd4fYVHcbnJNMeMLFb/rdnXCADzPcmsy5w0QxOnrPbGHwzPE0N
2QO/NzS+tz61EWfLGnt9WhOKuD/gur16PVtyWrJ9/bxRGGTyQ06FAp12z+OZ5MGmCXNmi1BDeJzC5kMMbkyN7e
JUCLkXDiWqXoeypCumr68TU4+r/1GvumZTPZW/qRCNpUci96e8ZJrFVrHWlKcnqvYvU+JHey5QXu89ecCAwEAA
aOCAsgwggLEMA4GA1UdDwEB/wQEAwIDuDCBlAYIKwYBBQUHAQEEgYcwgYQwOwYIKwYBBQUHMAGGL2h0dHA6Ly9
vY3NwLnN5c3RlbXRlc3Q4LnRydXN0MjQwOC5jb20vcmVzcG9uZGVyMEUGCCsGAQUFBzAChjlodHRwOi8vZi5ha
WEuc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzC
CAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc
2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJ
hIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEI
HRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4
zMTMxMy4yLjQuNi40LjIuMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdGVtdGVzdDgudHJ1c
3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1Q
yNDA4MSUwIwYDVQQDDBxUUlVTVDI0MDggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDAdDUkwxNjM0MB8GA
1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTqfHRtduHEfrO01hFT0ou/HItjATAJBgN
VHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQC0LTDB/5B0cepHuOG8QBGrH+ARIhJE/ZDl1bi5Z3R7OdBBSR2W2
QiB4GKsZC9qS1jNheK7o7/RCqg+w0U7p5W6+xdAsd5dYwidzMxSJa1lLSovoxFyvfFPK9nU+yaozrciasScylp
mio7AnzWJ26HotU+REoNW9vaeLFIEnQnqbJmpVlBG0Cm7pa4tR8ULC1SQjJTmJXMzNU0JdHb7nDyzYW4sK+40t
4sEGlUfj8eo8oE9l3HMM2I6POaipXSK42s5IG6bOOmbWWqQ57wgJ8qB7YanDu+9hFHje88xrRTl2R2dWfjbS7R
6kB9uS/DojjoA7A1dTx2hGC5qRNobRYlM</X509Certificate>
                </X509Data>
              </KeyInfo>
            </ds:Signature>
            <Subject>
              <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://sts.wsc3.test</NameID>
              <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
                <SubjectConfirmationData a:type="KeyInfoConfirmationDataType"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance">
                  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <X509Data>
<X509Certificate>MIIGGTCCBQGgAwIBAgIEUw+gETANBgkqhkiG9w0BAQsFADBHMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSQwIgYDVQQDDBtUUlVTVDI0MDggU3lzdGVtdGVzdCBYSVggQ0EwHhcNMTUwMTI
xMTgwNDQ0WhcNMTgwMTIxMTgwNDA5WjCBhzELMAkGA1UEBhMCREsxITAfBgNVBAoMGE5OSVQgQS9TIC8vIENWU
joyMTA5MzEwNjFVMCAGA1UEBRMZQ1ZSOjIxMDkzMTA2LUZJRDo1OTQ3ODA5MTAxBgNVBAMMKktGT0JTLVRFU1Q
tRk9DRVMtMDU5IChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
IQlH94vHdHGtq1o1DFRvQYmmsitJxbI5PyIJQXoFPIGbjon7A9+tgR/Nt5mF2X2aGh1Ouw8kfLnetVsoifG0YO
Gyp2rKzEqTsU4Emxw4Myj4FwDG06xkYuxiBKKkB6won86RXr3QvRed28vAkDSEniFGIabXRxlVv/HWASEJIEo+
yqFnVOmmqSBh9RIQ5i/JpJUhJdZ2M988O10RuNo2SIRrJ2/Mv+FLtlSlJLa4IgedQ936ATEOheNOLsVNLOMwwq
fvWv3im+RWqBTVktYqWnB7qmM8oBJSBxRSe4gJ+PQfQ4s37BK+5/NSmrV8WnNqoFrxsV9SRMwhUavGxI4mA0CA
```


Commented [A32]: Entity format for the System policy

Commented [A33]: EntityId for the WSC

Commented [A34]: SubjectConfirmation Method always holder-of-key for the System Policy

wEAAaOCAsowggLGMA4GA1UdDwEB/wQEAwIDuDCBlwYIKwYBBQUHAQEEgYowgYcwPAYIKwYBBQUHMAGGMGh0dHA
6Ly9vY3NwLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBHBggrBgEFBQcwAoY7aHR0cDovL
2YuYWlhLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3N5c3RlbXRlc3QxOS1jYS5jZXIwggEgBgNVHSAEggE
XMIIBEzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvb
S9yZXBvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F
0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuI
ERhbklEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4
xLjQuMS4zMTMxMy4yLjQuNi40LjIuMIGqBgNVHR8EgaIwgZ8wPKA6oDiGNmh0dHA6Ly9jcmwuc3lzdGVtdGVzd
DE5LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDE5LmNybDBfoF2gW6RZMFcxCzAJBgNVBAYTAkRLMRIwEAYDVQQ
KDAlUUlVTVDI0MDgxJDAiBgNVBAMMG1RSVVNUMjQwOCBTeXN0ZW10ZXN0IFhJWCBDQTEOMAwGA1UEAwwFQ1JMM
jIwHwYDVR0jBBgwFoAUzAJVDOSBdK8gVNURFFeckVI4f6AwHQYDVR0OBBYEFNc41PG/agTmqzigwWuFpNkf8zf
3MAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBADnssIGIxgIPwgfgLjxuOYPVchS5W68JeQOoljGhEGJY/
9sao8HvTLiJCPSwJ0SuyPJUu6/b6r1Q0ATGwk1fmCEjDQidyOAg2Lsn1sDix+Nbf+CxvtI2F1gIx7IasExBDJg
sCOsozCDdoHBaPbAqhrj/pu0tp+rcHA/tG3DAsyHSlbZBYmO3QyKn7+GVIikEi2sSnwvaT95fRUUvf4ur2n9sl
1gIfXqbPliWgAiHeAn8u9FzjvIZmbOOt3yuzf3tr6ZREB3Emp6spHWmlERNeiHFSrZIIGk/kDYLYC8Oza4sNeF
mIGVUaReidHGGVA3IMACfJCVLqGBG6VyZaJHPVhs=</X509Certificate>

Commented [A35]: The certificate for the WSC for the System policy. Note this structure is different from the Identity policy Response.

```
                    </X509Data>
                  </KeyInfo>
                </SubjectConfirmationData>
              </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2015-03-20T08:05:52.871Z" NotOnOrAfter="2015-03-
20T16:05:52.871Z">
              <AudienceRestriction>
                <Audience>https://saml.nnit001.dmz.dkdev</Audience>
              </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
              <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" FriendlyName="SpecVer">
<AttributeValue>DK-SAML-2.0</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="AssuranceLevel">
                <AttributeValue>2.0</AttributeValue>
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="Privileges">
                <AttributeValue a:nil="true"
xmlns:a="http://www.w3.org/2001/XMLSchema-instance" />
              </Attribute>
              <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
FriendlyName="CVRnumberIdentifier">
                <AttributeValue>21093106</AttributeValue>
              </Attribute>
            </AttributeStatement>
```

```
          </Assertion>
        </RequestedSecurityToken>
        <wst:RequestedAttachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedAttachedReference>
        <wst:RequestedUnattachedReference xmlns:wst="http://docs.oasis-open.org/ws-
sx/ws-trust/200512">
          <wsse:SecurityTokenReference>
            <wsse:Reference URI="#encryptedassertion" />
          </wsse:SecurityTokenReference>
        </wst:RequestedUnattachedReference>
        <Lifetime>
          <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T08:05:52.871Z</Created>
          <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2015-03-20T16:05:52.871Z</Expires>
        </Lifetime>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </S11:Body>
</S11:Envelope>
```

5 Reference

Reference	Description
[STS-RULES]	Security Token Service DS – Processing rules https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-STS-Processing%20rules.pdf
[CSS – USERMANUAL]	CSS User manual http://digitaliser.dk/resource/2561041
[DanIDVocesGyldig.p12]	DanId Voces test certificate used for the test WSP https://test-nemlog-in.dk/Testportal/certifikater/DanIDVocesGyldig.p12
[IntegrationTestSigning.cer]	Integration test signing certificate https://test-nemlog-in.dk/Testportal/certifikater/IntegrationTestSigning.zip
[ProductionSigning.cer]	Production signing certificate https://test-nemlog-in.dk/Testportal/certifikater/ProductionSigning.zip
[OIOIDWS]	OIO Identity-based Web Services v1.0.1a http://digitaliser.dk/resource/526486
[SOAP11]	Simple Object Access Protocol (SOAP) 1.1 http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

6 Change log

Date	Version	Description of Changes	Initials
2014-03-19	0.1	Document created	AxPe
2014-04-02	0.2	Document updated	AxPe
2014-04-03	1.0	Approved by DIGST	AxPe
2014-04-22	1.1	Added reference to "ECHO" test service	AxPe
2014-10-30	1.2	Section "3.2 Binding" updated to include SOAP version. Request examples updated with http headers	TMLN
2015-03-20	1.3	Document updated with new Request – Response examples and descriptions of new scenarios.	TRq