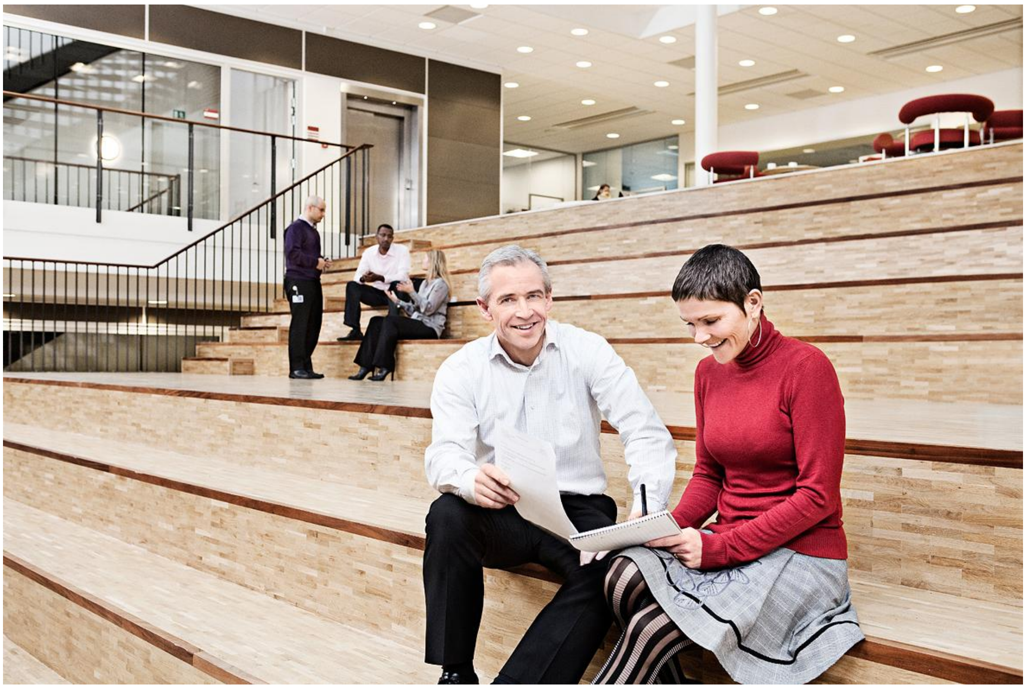


Digitaliseringsstyrelsen

Nemlog-in

Nemlog-in STS

Version: 1.2

ID: 32309

2014-10-30

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].

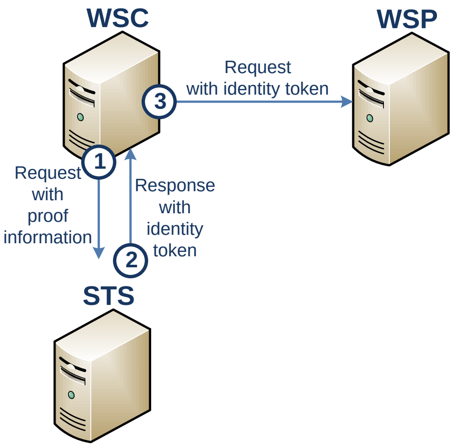
The document consists of the following sections:

- 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.

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.
- 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.

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:b3f7fda3-047e-4ecc-80ee-
7cf2a15e2b28</wsa:MessageID>
    <wsa:To wsu:Id=”to”>Error! Hyperlink reference not valid.>
    <wsse:Security mustUnderstand=”1”>
      <wsu:Timestamp wsu:Id=”sec-ts”>
        <wsu:Created>2014-03-19T15:42:08Z</wsu:Created>
        <wsu:Expires>2014-03-29T15:42:08Z</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”>MIIGJTCCBQ2gAwIBAgIETBGQPTANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzES
MBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMT
AwODEwMzA1OVoXDTE2MTAwODEwMjkzNVowgZQxCzAJBgNVBAYTAkRLMSowKAYDVQQKDCHDmGtvbm9taXN0eXJl
bHNlbiAvLyBDVlI6MTAyMTMyMzExWTAgBgNVBAUTGUNWUjoxMDIxMzIzMS1GSUQ6MTA5NTA3MjEwNQYDVQQDDC
7DmGtvbm9taXN0eXJlbHNlbiBGT0NFUzEgKGZ1bmt0aW9uc2NlcnRpZmlrYXQpMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAjA9FNMAzxS62VXKL2CbVQiEIP4aBEJzH5mbIJ500JCX/BQnTjqwB58nfrn46kywpA2
iD0twmaF5J5T7v1xryN+uhvuP4B5G2E/Ydirb4fM71pw0Ur0bxByYd2jbtRUMAaQxParXQNvuo9M8TgVpvGTAS
dCvN8H0zHwrBAGj4P+Ehl94rZaDlT1np75cQLEccbHQer55Fg542NljNe8X7E6a1pRfbsI1eK7YtJDMj5pXhSr
Ko8G1vCPhOurkJoVNgiUVD6PnPH+eq4FkfidTx93lYvagTDeDAkk0qWIxU4a859StEjgU16e5hTDQG9srpM5Y6
RK55ACG8njw72o1V7wIDAQABo4ICyDCCAsQwDgYDVR0PAQH/BAQDAgO4MIGUBggrBgEFBQcBAQSBhzCBhDA7Bg
grBgEFBQcwAYYvaHR0cDovL29jc3Auc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwRQYIKwYB
BQUHMAKGOWh0dHA6Ly9mLmFpYS5zeXN0ZW10ZXN0OC50cnVzdDI0MdguY29tL3N5c3RlbXRlc3Q4LWNhLmNlcj
CCASAGA1UdIASCARcwggETMIIBDwYNKwYBBAGB9FECBAYEAjCB/TAvBggrBgEFBQcCARYjaHR0cDovL3d3dy50
cnVzdDI0MdguY29tL3JlcG9zaXRvcnkwgckGCCsGAQUFBwICMIG8MAwWBURhbklEMAMCAQEagatEYW5JRCB0ZX
N0IGNlcnRpZmlrYXRlciBmcmEgZGVubmUgQ0EgdWRzdGVkZXMgdW5kZXIgT0lEIDEuMy42LjEuNC4xLjMxMzEz
LjIuNC42LjQuMi4gRGFuSUQgdGVzdCBjZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5kZX
```

Comment [A1]: Bootstrap scenario

```
IgT0lEIDEuMy42LjEuNC4xLjMxMzEzLjIuNC42LjQuMi4wgasGA1UdHwSBozCBoDA6oDigNoY0aHR0cDovL2Ny
bC5zeXN0ZW10ZXN0OC50cnVzdDI0MdguY29tL3N5c3RlbXRlc3Q4LmNybDBioGCgXqRcMFoxCzAJBgNVBAYTAk
RLMRIwEAYDVQQKDAlUUlVTVDI0MDgxJTAjBgNVBAMMHFRSVVNUMjQwOCBTeXN0ZW10ZXN0IFZJSUkgQ0ExEDAO
BgNVBAMMB0NSTDE2MzMwHwYDVR0jBBgwFoAUlhs2EzsiKcI9+ef5k+vGyz4SXwQwHQYDVR0OBBYEFE66Ft1BtS
J7FwAC6lIOWhrLnxLyMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBAEVQAp1vujR5nPDpHy0D52KspmF4
yDkbmixPzh/eroSwqBnUFONPMAIz70/+NogwGxPy4H6odMlRwEoHwy67cVCejKMdaNT69JEFxqe+ZQZzj70B+V
rtsMnSAPFJrgopukHoCjHEmOR2/sSoPgY6N2MUFM15KC0zHiNMWFUIMbuhawEP3kMSTUe85XSQXU8yMZv50zjG
0Kdtu/pudb2jYLYLwB/RREk1qa9wWuHvBGNzw/ZHZMZFnUsormbFEI7+0jFDsMqBEad+Mtu5IpVLd1VWnLJF6L
It1bXmUihVhjuZcPho8AsQpw1vOYifNyOfvNHEUk6x18P+KyOWkcA12U8=</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/2000/09/xmldsig#rsa-sha1” />
          <Reference URI=”#action”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>3cXAhlhZH22NiSh7AttxKxBap7Q=</DigestValue>
          </Reference>
          <Reference URI=”#msgid”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>pWQAcXZ9y9ivwfqQQo8bXWx647E=</DigestValue>
          </Reference>
          <Reference URI=”#to”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>NpjeF+QxtVh1evyCgU75tqu5MrI=</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/2000/09/xmldsig#sha1” />
            <DigestValue>3yFxXAnEUrxFf/8EnUCSkGttl7Y=</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/2000/09/xmldsig#sha1” />
            <DigestValue>ee1qFWDiXfdE9X6JlPD8sjfCJec=</DigestValue>
          </Reference>
          <Reference URI=”#body”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>7Duk89GNbUPkGVPgzuO+V2eTrwk=</DigestValue>
          </Reference>
        </SignedInfo>
```

Comment [A2]: Certificate used to sign the request

```
<SignatureValue>EmKPlLT8PIEM8eIPPOk3YnB0qvTJGQp/mA6bQOBXDSWq3uihvTniLF56WL17chJafJsiJC
J43untS5JHRJCCugyJQ3Kuuqfvu0+WwLihO53/f+90lBQmBKlJGZO38kROhlwISjTyeycKTD0jOhUWFxzY+nQD
l/qQYZmxAhR0lnpgJXZswoEg9DhEBZOpFT8woQPOY83SNQvYl4p1EbqQz01ntRfOzpOf1yW9qntNatnYuWElhp
jwoSRnzaQTWYbe9QaWz4vTO7lrkeBFXkpXeFxni9apdNO43nlMLh7chZj1yl/slB7v/fUFVYlWfJoAcFY5XSyD
JfGn+mSNpPiGUQ==</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:fa8babae-74ad-4971-94f1-9840f7cb97cc”>
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wst14:ActAs>
        <saml2:Assertion ID=”af0de510-8a7f-49b3-a3d4-f31c698f9537” IssueInstant=”2014-
03-19T15:42:08.8Z” Version=”2.0”>
          <saml2:Issuer>Error! Hyperlink reference not valid.>
          <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/2000/09/xmldsig#rsa-sha1”
/>
              <Reference URI=”#af0de510-8a7f-49b3-a3d4-f31c698f9537”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>pyeNIAABDsFpEkxHzX3+4kn/f3U=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>D9ZWuJOG1PoiATBOOQ48J33+SV0Ul1VTlZnW9FNQyprvkipNrOH0u7qd0BhhJfDrXYk7cE
Rw27NQ/N5dpYa4xrjHDlO7GDMrHK4j83HTN6tYK68QDr08qYuVg10k2NbuvLLW62pH3C/LUVTjhmDhHmh2CZ2t
9HD04IQ/McDKlgCnzJYAuDs3JUUGMaz7YWXgVG/kPZ4yFT0L7yvpbSVjM+ZZ9CjSLOdiaBj08v75N88BmRMp6+
6BTd/OqpHcC0s91Bz4Tqc+mi20ItqhtHKpDvdhF3/t3K32hTW405omVvotJMOw/UteaEKSibGb95sEEPPe7xlw
OMxGEsBEU6qhuA==</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>MIIGJTCCBQ2gAwIBAgIETBGQPTANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESz
ESMBAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEz
```

Comment [A3]: Subject that logged into Nemlogin

```
MTAwODEwMzA1OVoXDTE2MTAwODEwMjkzNVowgZQxCzAJBgNVBAYTAkRLMSowKAYDVQQKDCHDmGtvbm9taXN0eX
JlbHNlbiAvLyBDVlI6MTAyMTMyMzExWTAgBgNVBAUTGUNWUjoxMDIxMzIzMS1GSUQ6MTA5NTA3MjEwNQYDVQQD
DC7DmGtvbm9taXN0eXJlbHNlbiBGT0NFUzEgKGZ1bmt0aW9uc2NlcnRpZmlrYXQpMIIBIjANBgkqhkiG9w0BAQ
EFAAOCAQ8AMIIBCgKCAQEAjA9FNMAzxS62VXKL2CbVQiEIP4aBEJzH5mbIJ500JCX/BQnTjqwB58nfrn46kywp
A2iD0twmaF5J5T7v1xryN+uhvuP4B5G2E/Ydirb4fM71pw0Ur0bxByYd2jbtRUMAaQxParXQNvuo9M8TgVpvGT
ASdCvN8H0zHwrBAGj4P+Ehl94rZaDlT1np75cQLEccbHQer55Fg542NljNe8X7E6a1pRfbsI1eK7YtJDMj5pXh
SrKo8G1vCPhOurkJoVNgiUVD6PnPH+eq4FkfidTx93lYvagTDeDAkk0qWIxU4a859StEjgU16e5hTDQG9srpM5
Y6RK55ACG8njw72o1V7wIDAQABo4ICyDCCAsQwDgYDVR0PAQH/BAQDAgO4MIGUBggrBgEFBQcBAQSBhzCBhDA7
BggrBgEFBQcwAYYvaHR0cDovL29jc3Auc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwRQYIKw
YBBQUHMAKGOWh0dHA6Ly9mLmFpYS5zeXN0ZW10ZXN0OC50cnVzdDI0MDguY29tL3N5c3RlbXRlc3Q4LWNhLmNl
cjCCASAGA1UdIASCARcwggETMIIBDwYNKwYBBAGB9FECBAYEAjCB/TAvBggrBgEFBQcCARYjaHR0cDovL3d3dy
50cnVzdDI0MDguY29tL3JlcG9zaXRvcnkwgckGCCsGAQUFBwICMIG8MAwWBURhbklEMAMCAQEagatEYW5JRCB0
ZXN0IGNlcnRpZmlrYXRlciBmcmEgZGVubmUgQ0EgdWRzdGVkZXMgdW5kZXIgT0lEIDEuMy42LjEuNC4xLjMxMz
EzLjIuNC42LjQuMi4gRGFuSUQgdGVzdCBjZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5k
ZXIgT0lEIDEuMy42LjEuNC4xLjMxMzEzLjIuNC42LjQuMi4wgasGA1UdHwSBozCBoDA6oDigNoY0aHR0cDovL2
NybC5zeXN0ZW10ZXN0OC50cnVzdDI0MDguY29tL3N5c3RlbXRlc3Q4LmNybDBioGCgXqRcMFoxCzAJBgNVBAYT
AkRLMRIwEAYDVQQKDAlUUlVTVDI0MDgxJTAjBgNVBAMMHFRSVVNUMjQwOCBTeXN0ZW10ZXN0IFZJSUkgQ0ExED
AOBgNVBAMMB0NSTDE2MzMwHwYDVR0jBBgwFoAUlhs2EzsiKcI9+ef5k+vGyz4SXwQwHQYDVR0OBBYEFE66Ft1B
tSJ7FwAC6lIOWhrLnxLyMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBAEVQAp1vujR5nPDpHy0D52Kspm
F4yDkbmixPzh/eroSwqBnUFONPMAIz70/+NogwGxPy4H6odMlRwEoHwy67cVCejKMdaNT69JEFxqe+ZQZzj70B
+VrtsMnSAPFJrgopukHoCjHEmOR2/sSoPgY6N2MUFM15KC0zHiNMWFUIMbuhawEP3kMSTUe85XSQXU8yMZv50z
jG0Kdtu/pudb2jYLYLwB/RREk1qa9wWuHvBGNzw/ZHZMZFnUsormbFEI7+0jFDsMqBEad+Mtu5IpVLd1VWnLJF
6Lit1bXmUihVhjuZcPho8AsQpw1vOYifNyOfvNHEUk6x18P+KyOWkcA12U8=</ds:X509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
              </saml2:SubjectConfirmationData>
            </saml2:SubjectConfirmation>
          </saml2:Subject>
          <saml2:Conditions NotBefore=”2014-03-19T15:42:08.8Z” NotOnOrAfter=”2014-03-
19T23:42:08.8Z”>
            <saml2:AudienceRestriction>
              <saml2:Audience>Error! Hyperlink reference not valid.>
            </saml2:AudienceRestriction>
          </saml2:Conditions>
          <saml2:AttributeStatement>
            <saml2:Attribute NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-
format:basic” Name=”dk: urname :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: urname :saml:attribute:SpEntityId”>
              <saml2:AttributeValue xsi:type=”xs:string”>Error! Hyperlink reference
not valid.>
            </saml2:Attribute>
          </saml2:AttributeStatement>
        </saml2:Assertion>
      </wst14:ActAs>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>Error! Hyperlink reference not valid.>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

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

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

4.3.2 Response envelope example (decrypted)

```
<s:Envelope xmlns:s=”http://schemas.xmlsoap.org/soap/envelope/”>
  <s:Body>
    <S11: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” xmlns:S11=”http://schemas.xmlsoap.org/soap/envelope/”>
      <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:4233013c-a5c2-4f76-8d01-
d1bb05748a20</wsa:MessageID>
        <wsa:To wsu:Id=”relatesto”>uuid:7116fb59-9999-49c5-8812-3454d1e6da88</wsa:To>
        <wsse:Security mustUnderstand=”1”>
          <wsu:Timestamp wsu:Id=”sec_timestamp”>
            <wsu:Created>2014-03-19T15:53:35.677Z</wsu:Created>
            <wsu:Expires>2014-03-19T23:53:35.677Z</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#” />
              <SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1”
/>
              <Reference URI=”#action”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
              </Reference>
              <Reference URI=”#messageid”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>rpWy0Yec6gj9AOHIyXstM3rtRRU=</DigestValue>
              </Reference>
              <Reference URI=”#relatesto”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>z+qW7tLlhRcQYX3devjrfDwkue8=</DigestValue>
              </Reference>
              <Reference URI=”#sec_timestamp”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>SpavL5iUpQ8+PJS2kdZLoDjcgyQ=</DigestValue>
              </Reference>
              <Reference URI=”#body”>
```

```
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>8lkSQhIg9u+uGg+UlNlO77c5pBY=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>nzpn0lrLpv5cv8fAx2dWWhRp4v5KNxq/gkoYh64+D93cflFpd/VUPuELUQF8W1x7AMaFrT
fC+xHEhQnevLWYbu39lY+MWGNB0gaVK7PzsVwnqXnO9UV8okqDRgPfgDPRSGLlmvxUWSn3aXFx4TeujY/sJOqU
ObK1HpDXI+/Kis3hSIQkZFq4a9ussnRxEy3wuxTOfnxXPT6CFnj4B51DlH0vcRE6gT5OATr0SyxFyJKVnuQCWf
ckir4I4CX+rZ47QNVc045URD497sTteolSargio1LqBabCrF/lkNCvJ545phVr45NIY+lPLgLPueO8EXSMJtnk
4IEUQo0K9Ch6Fw==</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:ab217ef6-2a61-4081-83ae-
f0f7788017a6”>
            <TokenType />
            <AppliesTo xmlns=”http://schemas.xmlsoap.org/ws/2002/12/policy”>
              <EndpointReference xmlns=”http://www.w3.org/2005/08/addressing”>
                <Address>Error! Hyperlink reference not valid.>
              </EndpointReference>
            </AppliesTo>
            <RequestedSecurityToken>
              <Assertion ID=”_8e8ed6cb-0fd7-41a3-b6f3-478e0b4a1c76”
IssueInstant=”2014-03-19T15:53:35.677Z” Version=”2.0”
xmlns=”urn:oasis:names:tc:SAML:2.0:assertion”>
                <Issuer Format=”urn:oasis:names:tc:SAML:2.0:nameid-
format:entity”>Error! Hyperlink reference not valid.>
                <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=”#_8e8ed6cb-0fd7-41a3-b6f3-478e0b4a1c76”>
                      <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>YgzcHkR4Wqvjij6V1kllU+yd6/nxIZhkMVk/aM3G4CE=</ds:DigestValue>
                    </ds:Reference>
                  </ds:SignedInfo>

<ds:SignatureValue>o7v7Nms7j7Z6zE8POXV6RLZGd71BttiWztDAipHAZAroJUiD6qIpxRaaW5HfALp0Z7i
d/uEQmgrYPcGfQpYla6QJIJaw1ijxtQYWQPh4giYIbXarFfeM4Bo5TMMJt8H6zCThIxboVvHwwSCzrSyIW4ecr
lghag+niRpRrkS7QhgB/FWM6Wlluq224PDOkYlp6BfZl4GxVNL2cJQrJxHpMGrBWEkymsas43wUYmR5X71EvKE
```

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

```
ZniYOBZPV8TecY2+ya3IxIqGG7y0wB2qMW/9LhXBFYU4kiVBv6Dv77tSM2uGnj5XgYf4b2OoyLcHKKnY0BEIk/
+tcFvHrXhaGwfu7YA==</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
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>
                    </X509Data>
                  </KeyInfo>
                </ds:Signature>
                <Subject>
                  <NameID Format=”urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent”>C60OISuKWxuZZb38U2Kwow==</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>MIIGJTCCBQ2gAwIBAgIETBGQPTANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEzMTA
wODEwMzA1OVoXDTE2MTAwODEwMjkzNVowgZQxCzAJBgNVBAYTAkRLMSowKAYDVQQKDCHDmGtvbm9taXN0eXJlb
HNlbiAvLyBDVlI6MTAyMTMyMzExWTAgBgNVBAUTGUNWUjoxMDIxMzIzMS1GSUQ6MTA5NTA3MjEwNQYDVQQDDC7
DmGtvbm9taXN0eXJlbHNlbiBGT0NFUzEgKGZ1bmt0aW9uc2NlcnRpZmlrYXQpMIIBIjANBgkqhkiG9w0BAQEFA
AOCAQ8AMIIBCgKCAQEAjA9FNMAzxS62VXKL2CbVQiEIP4aBEJzH5mbIJ500JCX/BQnTjqwB58nfrn46kywpA2i
D0twmaF5J5T7v1xryN+uhvuP4B5G2E/Ydirb4fM71pw0Ur0bxByYd2jbtRUMAaQxParXQNvuo9M8TgVpvGTASd
CvN8H0zHwrBAGj4P+Ehl94rZaDlT1np75cQLEccbHQer55Fg542NljNe8X7E6a1pRfbsI1eK7YtJDMj5pXhSrK
o8G1vCPhOurkJoVNgiUVD6PnPH+eq4FkfidTx93lYvagTDeDAkk0qWIxU4a859StEjgU16e5hTDQG9srpM5Y6R
K55ACG8njw72o1V7wIDAQABo4ICyDCCAsQwDgYDVR0PAQH/BAQDAgO4MIGUBggrBgEFBQcBAQSBhzCBhDA7Bgg
rBgEFBQcwAYYvaHR0cDovL29jc3Auc3lzdGVtdGVzdDgudHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwRQYIKwYBB
QUHMAKGOWh0dHA6Ly9mLmFpYS5zeXN0ZW10ZXN0OC50cnVzdDI0MdguY29tL3N5c3RlbXRlc3Q4LWNhLmNlcjC
CASAGA1UdIASCARcwggETMIIBDwYNKwYBBAGB9FECBAYEAjCB/TAvBggrBgEFBQcCARYjaHR0cDovL3d3dy50c
nVzdDI0MdguY29tL3JlcG9zaXRvcnkwgckGCCsGAQUFBwICMIG8MAwWBURhbklEMAMCAQEagatEYW5JRCB0ZXN
0IGNlcnRpZmlrYXRlciBmcmEgZGVubmUgQ0EgdWRzdGVkZXMgdW5kZXIgT0lEIDEuMy42LjEuNC4xLjMxMzEzL
```

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

Comment [A8]: Since the WSP uses persistent identifiers the subject name has been translated

```
jIuNC42LjQuMi4gRGFuSUQgdGVzdCBjZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5kZXI
gT0lEIDEuMy42LjEuNC4xLjMxMzEzLjIuNC42LjQuMi4wgasGA1UdHwSBozCBoDA6oDigNoY0aHR0cDovL2Nyb
C5zeXN0ZW10ZXN0OC50cnVzdDI0MdguY29tL3N5c3RlbXRlc3Q4LmNybDBioGCgXqRcMFoxCzAJBgNVBAYTAkR
LMRIwEAYDVQQKDAlUUlVTVDI0MDgxJTAjBgNVBAMMHFRSVVNUMjQwOCBTeXN0ZW10ZXN0IFZJSUkgQ0ExEDAOB
gNVBAMMB0NSTDE2MzMwHwYDVR0jBBgwFoAUlhs2EzsiKcI9+ef5k+vGyz4SXwQwHQYDVR0OBBYEFE66Ft1BtSJ
7FwAC6lIOWhrLnxLyMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBAEVQAp1vujR5nPDpHy0D52KspmF4y
DkbmixPzh/eroSwqBnUFONPMAIz70/+NogwGxPy4H6odMlRwEoHwy67cVCejKMdaNT69JEFxqe+ZQZzj70B+Vr
tsMnSAPFJrgopukHoCjHEmOR2/sSoPgY6N2MUFM15KC0zHiNMWFUIMbuhawEP3kMSTUe85XSQXU8yMZv50zjG0
Kdtu/pudb2jYLYLwB/RREk1qa9wWuHvBGNzw/ZHZMZFnUsormbFEI7+0jFDsMqBEad+Mtu5IpVLd1VWnLJF6LI
t1bXmUihVhjuZcPho8AsQpw1vOYifNyOfvNHEUk6x18P+KyOWkcA12U8=</X509Certificate>
                        </X509Data>
                      </KeyInfo>
                    </SubjectConfirmationData>
                  </SubjectConfirmation>
                </Subject>
                <Conditions NotBefore=”2014-03-19T15:53:35.677Z” NotOnOrAfter=”2014-
03-19T23:53:35.677Z”>
                  <AudienceRestriction>
                    <Audience>Error! Hyperlink reference not valid.>
                  </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:2.5.29.29”
NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:basic”
FriendlyName=”Certificate issuer attribute”>
                    <AttributeValue>CN=TRUST2408 Systemtest VIII CA, O=TRUST2408,
C=DK</AttributeValue>
                  </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=”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>
                  <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>
            <Lifetime>
```

Comment [A9]: Certificate used to sign the requestmessage as SubjectConfirmation has been set to holder-of-key

Comment [A10]: Asserted attributes

```
       <Created xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2014-03-19T15:53:35.677Z</Created>
       <Expires xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">2014-03-19T23:53:35.677Z</Expires>
      </Lifetime>
     </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
   </S11:Body>
  </S11:Envelope>
 </s:Body>
</s:Envelope>
```

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 hosted by the WSC organization itself.

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

4.4.1 Request example

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:bfd8c8de-ddf6-44e4-b89d-
de467b380d83</wsa:MessageID>
  <wsa:To wsu:Id="to">Error! Hyperlink reference not valid.>
  <wsse:Security mustUnderstand="1">
   <wsu:Timestamp wsu:Id="sec-ts">
```

Comment [A11]: Local token scenario

```
        <wsu:Created>2014-03-19T16:08:01Z</wsu:Created>
        <wsu:Expires>2014-03-29T16:08:01Z</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”>MIIE3TCCBEagAwIBAgIEQDhRhTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJESzEM
MAoGA1UEChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMB4XDTEzMDExNTE1MTM1MV
oXDTE1MDExNTE1NDM1MVowgZIxCzAJBgNVBAYTAkRLMSEwHwYDVQQKExhOTklUIEEvUyAvLyBDVlI6MjEwOTMx
MDYxYDAlBgNVBAUTHkNWUjoyMTA5MzEwNi1GSUQ6MTM1ODI2MzY0Otk3NDA3BgNVBAMUMNhrb25vbWlzdHlyZW
xzZW4gU3lzdGVtIDUxIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uVq1GdHBsznydpLe2fDvibnFaSq/lCEDoaynJqfbguBaiXkkDJkO9EjmfXh9UgdUj1dx8IM5t5FpidflzUX1FN
iDVaQpoMeDASTN5VhtTHvUZdTGSL8YdKk6Yio+9r3tjSkOdsroXElYpHsjXUBpD2xDXrr52h2m2m3LwhQyMS8C
AwEAAaOCApAwggKMMA4GA1UdDwEB/wQEAwIDuDArBgNVHRAEJDAigA8yMDEzMDExNTE1MTM1MVqBDzIwMTUwMT
E1MTU0MzUxWjBGBggrBgEFBQcBAQQ6MDgwNgYIKwYBBQUHMAGGKmh0dHA6Ly90ZXN0Lm9jc3AuY2VydGlmaWth
dC5kay9vY3NwL3N0YXR1czCCAQMGA1UdIASB+zCB+DCB9QYJKQEBAQEBAQEDMIHnMC8GCCsGAQUFBwIBFiNodH
RwOi8vd3d3LmNlcnRpZmlrYXQuZGsvcmVwb3NpdG9yeTCBswYIKwYBBQUHAgIwgaYwChYDVERDMAMCAQEagZdU
REMgVGVzdCBDZXJ0aWZpa2F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjEuMS4xLjEuMS
4xLjEuMS4zLiBUREMgVGVzdCBDZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5kZXIgT0lE
IDEuMS4xLjEuMS4xLjEuMS4xLjMuMIGXBgNVHR8EgY8wgYwwV6BVoFOkUTBPMQswCQYDVQQGEwJESzEMMAoGA1
UEChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMQ4wDAYDVQQDEwVDUkwzNjAxoC+g
LYYraHR0cDovL3Rlc3QuY3JsLm9jZXMuY2VydGlmaWthdC5kay9vY2VzLmNybDAfBgNVHSMEGDAWgBQcmAlHGk
w4uRDFBClb8fROgGrMfjAdBgNVHQ4EFgQUK/UQPKT7so1BLwlx70j+a2UB0RUwCQYDVR0TBAIwADAZBgkqhkiG
9n0HQQAEDDAKGwRWNy4xAwIDqDANBgkqhkiG9w0BAQUFAAOBgQAMY0oYNddMesTY2J4QiD85f/I2PZPDxPLiNZ
nvkKjRW0cSbnMofjhioF4nkFPycuMdALveYzBoGAwj6c/1c260uex6OaUYBkcqXnkwNvFuU86rBIr0cvr78kdN
0UB2P9D2fnB0cyazjvBpeq/NM7j0WP4kgmuo8kCBr68Fc8PX3w==</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/2000/09/xmldsig#rsa-sha1” />
          <Reference URI=”#action”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>3cXAhlhZH22NiSh7AttxKxBap7Q=</DigestValue>
          </Reference>
          <Reference URI=”#msgid”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>hJKU+61aLXghUlAArd/Vzv7895k=</DigestValue>
          </Reference>
          <Reference URI=”#to”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>Zq8Hj7tkR7arE2GaC1O0rGPMOWU=</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/2000/09/xmldsig#sha1” />
```

Comment [A12]: Certificate used to sign the request

```
            <DigestValue>8cVtRKb+5Os69UoKSi3kjWZ7D1o=</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/2000/09/xmldsig#sha1” />
            <DigestValue>e5x5O1qT2vNlrU0xzBoxop27eMc=</DigestValue>
          </Reference>
          <Reference URI=”#body”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>9rHHTL23Lvy/aKnJcwH74ECRaTw=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>Xic/OuZOFRykaGHBXq5YlRcursUE+jRI5PM/nQ/Ec5gKDKQUk2pww2mexArQtiR/7by7ar
u2WoHkT+x6c40SjDUPhK1Fmy9PGcP5xYM76Hs+ipgc/KrG9BumU14r+jKcz074KfUvnzs3vlH+Ryxwe43FpaFs
/ez4PTOPuWUQITM=</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:2e6ae0af-de22-4256-a417-30f2e659de22”>
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wst14:ActAs>
        <saml2:Assertion ID=”_db1e4ff1-66be-445e-a45b-f10de717430b”
IssueInstant=”2014-03-19T16:08:01.6Z” Version=”2.0”>
          <saml2:Issuer>Error! Hyperlink reference not valid.>
          <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/2000/09/xmldsig#rsa-sha1”
/>
              <Reference URI=”#_db1e4ff1-66be-445e-a45b-f10de717430b”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>Om3kP8fKr5/gJqOV3IgEnQZ4G9I=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>W/2eNTMW8gb2J3DkgBQtInRV4BvvYh+o/cFBdh6dg83sRYDg1foBIiR4aIQZX8SkehGFLS
hSkLucv3Z+zxX4j1Z3PVQyJFRhd0r97QWffXES+trP70Y0LLzLsx+49q47f+NmLHUG5+wt7gH4Vu4LXIF/Sain
Y5QxPW1Lfs+mNpY=</SignatureValue>
          </Signature>
```

Comment [A13]: EntityId of the bootstrap token issuer

```
          <saml2:Subject>
            <saml2:NameID Format=”urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName”>C=DK,O=NNIT A/S // CVR:21093106,CN=Rex
Holm,Serial=CVR:21093106-RID:71591761</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>MIIE3TCCBEagAwIBAgIEQDhRhTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJESz
EMMAoGA1UEChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMB4XDTEzMDExNTE1MTM1
MVoXDTE1MDExNTE1NDM1MVowgZIxCzAJBgNVBAYTAkRLMSEwHwYDVQQKExhOTklUIEEvUyAvLyBDVlI6MjEwOT
MxMDYxYDAlBgNVBAUTHkNWUjoyMTA5MzEwNi1GSUQ6MTM1ODI2MzY0Otk3NDA3BgNVBAMUMNhrb25vbWlzdHly
ZWxzZW4gU3lzdGVtIDUxIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgY
EAuVq1GdHBsznydpLe2fDvibnFaSq/lCEDoaynJqfbguBaiXkkDJkO9EjmfXh9UgdUj1dx8IM5t5FpidflzUX1
FNiDVaQpoMeDASTN5VhtTHvUZdTGSL8YdKk6Yio+9r3tjSkOdsroXElYpHsjXUBpD2xDXrr52h2m2m3LwhQyMS
8CAwEAAaOCApAwggKMMA4GA1UdDwEB/wQEAwIDuDArBgNVHRAEJDAigA8yMDEzMDExNTE1MTM1MVqBDzIwMTUw
MTE1MTU0MzUxWjBGBggrBgEFBQcBAQQ6MDgwNgYIKwYBBQUHMAGGKmh0dHA6Ly90ZXN0Lm9jc3AuY2VydGlmaW
thdC5kay9vY3NwL3N0YXR1czCCAQMGA1UdIASB+zCB+DCB9QYJKQEBAQEBAQEDMIHnMC8GCCsGAQUFBwIBFiNo
dHRwOi8vd3d3LmNlcnRpZmlrYXQuZGsvcmVwb3NpdG9yeTCBswYIKwYBBQUHAgIwgaYwChYDVERDMAMCAQEagZ
dUREMgVGVzdCBDZXJ0aWZpa2F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjEuMS4xLjEu
MS4xLjEuMS4zLiBUREMgVGVzdCBDZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5kZXIgT0
lEIDEuMS4xLjEuMS4xLjEuMS4xLjMuMIGXBgNVHR8EgY8wgYwwV6BVoFOkUTBPMQswCQYDVQQGEwJESzEMMAoG
A1UEChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMQ4wDAYDVQQDEwVDUkwzNjAxoC
+gLYYraHR0cDovL3Rlc3QuY3JsLm9jZXMuY2VydGlmaWthdC5kay9vY2VzLmNybDAfBgNVHSMEGDAWgBQcmAlH
Gkw4uRDFBClb8fROgGrMfjAdBgNVHQ4EFgQUK/UQPKT7so1BLwlx70j+a2UB0RUwCQYDVR0TBAIwADAZBgkqhk
iG9n0HQQAEDDAKGwRWNy4xAwIDqDANBgkqhkiG9w0BAQUFAAOBgQAMY0oYNddMesTY2J4QiD85f/I2PZPDxPLi
NZnvkKjRW0cSbnMofjhioF4nkFPycuMdALveYzBoGAwj6c/1c260uex6OaUYBkcqXnkwNvFuU86rBIr0cvr78k
dN0UB2P9D2fnB0cyazjvBpeq/NM7j0WP4kgmuo8kCBr68Fc8PX3w==</ds:X509Certificate>
                  </ds:X509Data>
                </ds:KeyInfo>
              </saml2:SubjectConfirmationData>
            </saml2:SubjectConfirmation>
          </saml2:Subject>
          <saml2:Conditions NotBefore=”2014-03-19T16:08:01.6Z” NotOnOrAfter=”2014-03-
20T00:08:01.6Z”>
            <saml2:AudienceRestriction>
              <saml2:Audience>Error! Hyperlink reference not valid.>
            </saml2:AudienceRestriction>
          </saml2:Conditions>
          <saml2:AttributeStatement>
            <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”>3</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”>DK-SAML-
2.0</saml2:AttributeValue>
            </saml2:Attribute>
          </saml2:AttributeStatement>
        </saml2:Assertion>
      </wst14:ActAs>
      <wsp:AppliesTo>
```

Comment [A14]: Subjectname to issue identity token for

Comment [A15]: Certificate used to sign the request message since SubjectConfirmation is set to holder-of-key

```
        <wsa:EndpointReference>
          <wsa:Address>Error! Hyperlink reference not valid.>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

Comment [A16]: Entityid of the WSP to issue identity token for

4.4.2 Response envelope example (decrypted)

```
<s:Envelope xmlns:s=”http://schemas.xmlsoap.org/soap/envelope/”>
  <s:Body>
    <S11: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” xmlns:S11=”http://schemas.xmlsoap.org/soap/envelope/”>
      <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:cf6a69ae-20c3-40fc-beb4-
b4b274c39a84</wsa:MessageID>
        <wsa:To wsu:Id=”relatesto”>uuid:bfd8c8de-ddf6-44e4-b89d-de467b380d83</wsa:To>
        <wsse:Security mustUnderstand=”1”>
          <wsu:Timestamp wsu:Id=”sec_timestamp”>
            <wsu:Created>2014-03-19T16:08:07.562Z</wsu:Created>
            <wsu:Expires>2014-03-20T00:08:07.562Z</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#” />
              <SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1”
/>
              <Reference URI=”#action”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
              </Reference>
              <Reference URI=”#messageid”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>M1Uyo3CixVdha1FCCKAua4DgMUs=</DigestValue>
              </Reference>
              <Reference URI=”#relatesto”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>33utWzlUPTxPqPR+C2Z1FvQcVlE=</DigestValue>
              </Reference>
              <Reference URI="#sec_timestamp">
                <Transforms>
                  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <DigestValue>oG1qch310TXYT8lGFR0QDWUmdDQ=</DigestValue>
              </Reference>
              <Reference URI="#body">
                <Transforms>
                  <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <DigestValue>Sb0GCThFJH84H5K0/ihmjizH+hA=</DigestValue>
              </Reference>
            </SignedInfo>

<SignatureValue>VtF8HjHx1QqoUuB5fUWtF0h8y4D9h8d7dEFEsgE78mivxPf+GNbsgMz+RD4YM9MJ6r6doO
DFqHOKKCJ7O2DDUp/olKm0arcmF1kC4bvKoCEj97vApFUsnxY+ZPBFOhOHl0gbW3WyvFQuyzU7ToRTLQisps/J
PlG4Cs/EFZAFZ0MKrs7h9i0v8oTuJ2PuhEJMYbqKHUeaWwh3N0ZGmd0sEv4TqiMXmsvKzgQ5g1kwxYvb6o+WCb
kFkGfneH0+M/VCcQLczYwyLTEqh7AW3q6egAiQreDO6KoUHHwkH4ngG5oOPa7HyBsk6cmnAdJhSZUzpPJXbYts
boXn9ojS0r/iXw==</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:2e6ae0af-de22-4256-a417-
30f2e659de22">
            <TokenType />
            <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2002/12/policy">
              <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
                <Address>Error! Hyperlink reference not valid.>
              </EndpointReference>
            </AppliesTo>
            <RequestedSecurityToken>
              <Assertion ID="_d9e47a96-01b4-4a44-9f98-338f19180ad2"
IssueInstant="2014-03-19T16:08:07.562Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
                <Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">Error! Hyperlink reference not valid.>
                <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="#_d9e47a96-01b4-4a44-9f98-338f19180ad2">
                      <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>
```

Comment [A17]: Entityid of the WSP this identitytoken is issued for

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

<ds:DigestValue>MuG0Rnzy+CGAIt6Mo5xua3P0s9b1qm2EbzSzhrpScyk=</ds:DigestValue>
                    </ds:Reference>
                  </ds:SignedInfo>

<ds:SignatureValue>Pm4dDJEPTlcW5M3UDVvIdJ5rqzG6uR+p0+KzU1OAAyp3Q/7H8yv4LVArMKlQK08BheV
UBbvDjrxpBKDbcfHAhXZw7JoWnjlmyJqr16FhrNtngEmwdYyyO79pVFo3KCRBHjylFFHuL86KWdKnYgOpgTHRc
r3rl1/o8fjEmpsQonzjkd9ozeFd/Zur5itpulLeSgVyCM+QWAO3ht5xMMVVuWRJI4h+vLNzQfoeDNulfi7u1r4
pismlYpPgbDaT+IYZMVweE+zWgLCtPKPMLqwlaKXLo2prCiWtwH2Sxpb7UPVpy7cJO7nSiqTj3Fzlohvh+Jw4x
okCeQ8sfNzCWIiRmQ==</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
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>
                    </X509Data>
                  </KeyInfo>
                </ds:Signature>
                <Subject>
                  <NameID Format=”urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent”>XJjNlz2VteP+w4iqFZ3dyw==</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>MIIE3TCCBEagAwIBAgIEQDhRhTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJESzEMM
AoGA1UEChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMB4XDTEzMDExNTE1MTM1Mvo
XDTE1MDExNTE1NDM1MVowgZIxCzAJBgNVBAYTAkRLMSEwHwYDVQQKExhOTklUIEEvUyAvLyBDVlI6MjEwOTMxM
DYxYDAlBgNVBAUTHkNWUjoyMTA5MzEwNi1GSUQ6MTM1ODI2MzY0Otk3NDA3BgNVBAMUMNhrb25vbWlzdHlyZWx
zZW4gU3lzdGVtIDUxIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAu
```

Comment [A18]: Certificate used to sign the response. Do not verify signature with embedded certificates.

```
Vq1GdHBsznydpLe2fDvibnFaSq/lCEDoaynJqfbguBaiXkkDJkO9EjmfXh9UgdUj1dx8IM5t5FpidflzUX1Fni
DVaQpoMeDASTN5VhtTHvUZdTGSL8YdKk6Yio+9r3tjSkOdsroXElYpHsjXUBpD2xDXrr52h2m2m3LwhQyMS8CA
wEAAaOCApAwggKMMA4GA1UdDwEB/wQEAwIDuDArBgNVHRAEJDAigA8yMDEzMDExNTE1MTM1MVqBDzIwMTUwMTE
1MTU0MzUxWjBGBggrBgEFBQcBAQQ6MDgwNgYIKwYBBQUHMAGGKmh0dHA6Ly90ZXN0Lm9jc3AuY2VydGlmaWthd
C5kay9vY3NwL3N0YXR1czCCAQMGA1UdIASB+zCB+DCB9QYJKQEBAQEBAQEDMIHnMC8GCCsGAQUFBwIBFiNodHR
wOi8vd3d3LmNlcnRpZmlrYXQuZGsvcmVwb3NpdG9yeTCBswYIKwYBBQUHAgIwgaYwChYDVERDMAMCAQEagZdUR
EMgVGVzdCBDZXJ0aWZpa2F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjEuMS4xLjEuMS4
xLjEuMS4zLiBUREMgVGVzdCBDZXJ0aWZpY2F0ZXMgZnJvbSB0aGlzIENBIGFyZSBpc3N1ZWQgdW5kZXIgT0lEI
DEuMS4xLjEuMS4xLjEuMS4xLjMuMIGXBgNVHR8EgY8wgYwwV6BVoFOkUTBPMQswCQYDVQQGEwJESzEMMAoGA1U
EChMDVERDMSIwIAYDVQQDExlUREMgT0NFUyBTeXN0ZW10ZXN0IENBIElJMQ4wDAYDVQQDEwVDUkwzNjAxoC+gL
YYraHR0cDovL3Rlc3QuY3JsLm9jZXMuY2VydGlmaWthdC5kay9vY2VzLmNybDAfBgNVHSMEGDAWgBQcmAlHGkw
4uRDFBClb8fROgGrMfjAdBgNVHQ4EFgQUK/UQPKT7so1BLwlx70j+a2UB0RUwCQYDVR0TBAIwADAZBgkqhkiG9
n0HQQAEDDAKGwRWNy4xAwIDqDANBgkqhkiG9w0BAQUFAAOBgQAMY0oYNddMesTY2J4QiD85f/I2PZPDxPLiNZn
vkKjRW0cSbnMofjhioF4nkFPycuMdALveYzBoGAwj6c/1c260uex6OaUYBkcqXnkwNvFuU86rBIr0cvr78kdN0
UB2P9D2fnB0cyazjvBpeq/NM7j0WP4kgmuo8kCBr68Fc8PX3w==</X509Certificate>
                        </X509Data>
                      </KeyInfo>
                    </SubjectConfirmationData>
                  </SubjectConfirmation>
                </Subject>
                <Conditions NotBefore=”2014-03-19T16:08:07.562Z” NotOnOrAfter=”2014-
03-20T00:08:07.562Z”>
                  <AudienceRestriction>
                    <Audience>Error! Hyperlink reference not valid.>
                  </AudienceRestriction>
                </Conditions>
                <AttributeStatement>
                  <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=”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: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=”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>
                  <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>
```

Comment [A19]: Certificate used to sign the request message since SubjectConfirmation is set to holder-of-key

Comment [A20]: Asserted attributes

```
            <Lifetime>
              <Created xmlns=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd”>2014-03-19T16:08:07.562Z</Created>
              <Expires xmlns=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd”>2014-03-20T00:08:07.562Z</Expires>
            </Lifetime>
          </RequestSecurityTokenResponse>
        </RequestSecurityTokenResponseCollection>
      </S11:Body>
    </S11:Envelope>
  </s:Body>
</s:Envelope>
```

4.5 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.

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

4.5.1 Request example

```
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:843e7250-bd66-43c1-a033-
1fcbf171fb79</wsa:MessageID>
    <wsa:To wsu:Id=”to”>Error! Hyperlink reference not valid.>
    <wsse:Security mustUnderstand=”1”>
      <wsu:Timestamp wsu:Id=”sec-ts”>
        <wsu:Created>2014-03-19T16:30:54Z</wsu:Created>
        <wsu:Expires>2014-03-29T16:30:54Z</wsu:Expires>
      </wsu:Timestamp>
```

Comment [A21]: Signature scenario

```
      <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>
          <CanonicalizationMethod Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#”
/>
          <SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1” />
          <Reference URI=”#action”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>3cXAhlhZH22NiSh7AttxKxBap7Q=</DigestValue>
          </Reference>
          <Reference URI=”#msgid”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>NvtEuEg8pJizRfQYeOuaSeSlhls=</DigestValue>
          </Reference>
          <Reference URI=”#to”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>ss1+nV/baeyPJ/37viSjsyXRlzo=</DigestValue>
          </Reference>
          <Reference URI=”#sec-ts”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
```

Comment [A22]: Moces certificate used to sign the message

```
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>DW99ilEe95p4lxJYtQ7zi71kdJo=</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/2000/09/xmldsig#sha1” />
            <DigestValue>zBUY+nRlcI7i2tPGuMdySQ+61RQ=</DigestValue>
          </Reference>
          <Reference URI=”#body”>
            <Transforms>
              <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#” />
            </Transforms>
            <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
            <DigestValue>yAdTWdcsjfKpfrLVOASy6ns9ZnY=</DigestValue>
          </Reference>
        </SignedInfo>

<SignatureValue>0Lzuj8QqwpY0o2AW5k8O88jGtP9ENJck2NC+rVJGyRF/sVyGI78kIQbpABUEkoh17eEuTd
ouEmY0EEUjD61RoDXY2HKWTRiR566SekJqco+p1e5NWxgqoFMW9Ovaf7z40zfrTvRzh94GSPzHWjAQT3Dy77ui
+Llb2ESXLic4c8tDWHRfbmX1Afd3iL9YLbysObGDNvnWBv0qOHI3t+WoihtIbo/T3uiOmxk8FgGepza8Trvo6P
gKsYmxcDxNpNdMrWirC4h4XhSinZblBi7twtQYdiwRlYhjWmxHkeYh1k4xEvP6HQOcUGc8fVSSVf0qVyNBlRcx
MfgbGDf+cSvDZQ==</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:8592b8cc-8403-4fcd-bbdc-2edeff7233ea”>
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>Error! Hyperlink reference not valid.>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
    </wst:RequestSecurityToken>
  </S11:Body>
</S11:Envelope>
```

Comment [A23]: EntityId to issue identity token for

4.5.2 Response envelope example (decrypted)

```
<s:Envelope xmlns:s=”http://schemas.xmlsoap.org/soap/envelope/”>
  <s:Body>
    <S11: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” xmlns:S11=”http://schemas.xmlsoap.org/soap/envelope/”>
```

```
      <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:387df9d7-9cd4-4dce-9631-
4a454382ccc2</wsa:MessageID>
        <wsa:To wsu:Id=”relatesto”>uuid:843e7250-bd66-43c1-a033-1fcbf171fb79</wsa:To>
        <wsse:Security mustUnderstand=”1”>
          <wsu:Timestamp wsu:Id=”sec_timestamp”>
            <wsu:Created>2014-03-19T16:31:16.530Z</wsu:Created>
            <wsu:Expires>2014-03-20T00:31:16.530Z</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#” />
              <SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1”
/>
              <Reference URI=”#action”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>1hj8fpM7T5rcOsNRPpnxA3p3AkM=</DigestValue>
              </Reference>
              <Reference URI=”#messageid”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>feXCrOA4kTVaJymWshnvvJ5ojgY=</DigestValue>
              </Reference>
              <Reference URI=”#relatesto”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>TdErp5Ev8aUIm+N9uLyOBmzy0NA=</DigestValue>
              </Reference>
              <Reference URI=”#sec_timestamp”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>Exf1NzNZ8HjiIWBufFQI2YXVto4=</DigestValue>
              </Reference>
              <Reference URI=”#body”>
                <Transforms>
                  <Transform Algorithm=”http://www.w3.org/2000/09/xmldsig#enveloped-
signature” />
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1” />
                <DigestValue>JhZNRBfxT1gCLZH0dFNUTLf7a+I=</DigestValue>
              </Reference>
            </SignedInfo>
```

```
<SignatureValue>lpj1z5i3/BTMgyM+NyUs2g7A6HckfY9estZrUFVT5fcb7L2tbhg5KafUu7fDaROkxRVMxn
3YLqCiEEQcvrfdbMYBsBqpM1vWFkn8uCH8ViHc/gFCAzFuJJ8HnrEbUtJI7dCpp48UDJPMpQaxlKV6mgsfXAQ1
YmLTsGCqTA2/BtfnkhujUBm8I7XfHe6QianEDMu994XQqLUV+SMt38/xnTX/MHICVweY2KwFT7phtSVwGqkV9c
IEwKDZUhhzLL0dFV2N6ziQ5m8tY4S9mtvXgtHMbkj3JF1J/kxXA982PpjVu9Czc1bkOeDN42by0YS+70J/uj61
bPHA4CfndgoZvw==</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:8592b8cc-8403-4fcd-bbdc-
2edeff7233ea”>
            <TokenType />
            <AppliesTo xmlns=”http://schemas.xmlsoap.org/ws/2002/12/policy”>
              <EndpointReference xmlns=”http://www.w3.org/2005/08/addressing”>
                <Address>Error! Hyperlink reference not valid.>
              </EndpointReference>
            </AppliesTo>
            <RequestedSecurityToken>
              <Assertion ID=”_f93c8d3e-a0ff-4ad9-b796-f6a0d5582442”
IssueInstant=”2014-03-19T16:31:16.530Z” Version=”2.0”
xmlns=”urn:oasis:names:tc:SAML:2.0:assertion”>
                <Issuer Format=”urn:oasis:names:tc:SAML:2.0:nameid-
format:entity”>Error! Hyperlink reference not valid.>
                <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=”#_f93c8d3e-a0ff-4ad9-b796-f6a0d5582442”>
                      <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>Ug/4DYRgen0PFKKxBpzzjPL0YRNo/8Zuub183/Od8RQ=</ds:DigestValue>
                    </ds:Reference>
                  </ds:SignedInfo>

<ds:SignatureValue>FY1qcmJjbdGsdfs/xKkLA3FxTkUN4/Jxs53H72dVpSW9Cx0oYem9VtFzlh7uLhRGfl8
+Ok31eJBKJannjkxfQtIjk4SepnGnPyjkW7fsYzBcCBFh7UwM0wdyQPq1t0YPMDz+mpSua5LqeoBY1nIK0Q4n3
ofyRVrb4LejMV24m92jWCX+JmvyOsORL+2eQFu2orb7uJyQUD/XYBebDS2tbbXjL4Svj2SQU2nvs6Rf71K2Ufn
YI+DfDvXkJzctx72GQ+2pUfiiRnjdmx74IbHcFh1zIkT5cVD/BCwQWp4fLbhOo3Ou0Wahf5J8Z1kVfpYaJ50iJ
4dtBPtUGl2esQ8i2A==</ds:SignatureValue>
                  <KeyInfo xmlns=”http://www.w3.org/2000/09/xmldsig#”>
                    <X509Data>

<X509Certificate>MIIGFTCCBP2gAwIBAgIETBI9xjANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESM
BAGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTE0MDE
zMDEwMjkzN1oXDTE3MDEzMDEwMjgyM1owgYQxCzAJBgNVBAYTAkRLMSEwHwYDVQQKDBhOTklUIEEvUyAvLyBDV
lI6MjEwOTMxMDYxUjAlBgNVBAUTHkNWUjoyMTA5MzEwNi1GSUQ6MTMzNjQ2NzA5MjUwNzApBgNVBAMMIktGT0J
```

Comment [A24]: Entityid of the WSP this identity token is issued for

```
TIC0gQURGUyAoZnVua3Rpb25zY2VydGlmaWthdCkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpu
3eSu0HkpTrawmmtaeBezZL7NnNno/L4fIWXXawxUcIfcnqSp5ZKpjBm4mzeRRwqkYlOn0WfROeqMgOCXRnNnRd
+I2aWWSWIMPYVGVZqT2/MQPo2UvDZ2Z/j4xyQDUx7L+l6elsq7IDGfSvzwrE/qU98Zr3bm3HvbUTK5F4ZE2w4R
eB2UU2QjowDUrdMNmoQ57Bx7UoobqwlNb3VYVwYwdgoJwQik+Jonm8/i4mNeKnGstYTZuEJTOr1LG0T3QOrqJM
Y8COYvIuTy14nC+cZAcSV4nWCnZ3MzTX6CohkzBG87W3BiPH9BdrjoGyilwhCorjgoFMkuIWgzgv2MDMjAgMBA
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>
                    </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:bearer”
/>
                </Subject>
                <Conditions NotBefore=”2014-03-19T16:31:16.530Z” NotOnOrAfter=”2014-
03-20T00:31:16.530Z”>
                  <AudienceRestriction>
                    <Audience>Error! Hyperlink reference not valid.>
                  </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=” urname”>
                    <AttributeValue />
                  </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”>
```

Comment [A25]: Certificate used to sign the response. Do not verify signature with embedded certificates.

Comment [A26]: Subjectname extracted from the certificate used to sign the request

```
                     <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>4C05754F</AttributeValue>
                   </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>MIIGIDCCBQigAwIBAgIETAV1TzANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESMB
AGA1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMB4XDTEyMDEx
MjE0MTQwNloXDTE2MDExMjE0MTM1MlowdjELMAkGA1UEBhMCREsxKjAoBgNVBAoMIcOYa29ub21pc3R5cmVsc2
VuIC8vIENWUjoxMDIxMzIzMTE7MbcGA1UEAwwQTW9ydGVuIE1vcnRlbnNlbjAgBgNVBAUTGUNWUjoxMDIxMzIz
MS1SSUQ6OTM5NDc1NTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXxgVHipGqErG8xLbYqxmPvy
Zzh1aBK4th2YaiIbRyZfSO3gOxhWs+XR3JLOrVMgKxERYGD4fTnNfWU7TpYaTO8pnXEx2+bV2ohIzcyavQYW21
KMgcp1psWr6wv5IuF0Ykhydv9OoqJRouBh4oHJwvBjVJQLDw0L+d6bJ/DjW+tHWtuWMyPUKZRjQf6dWIA45pkL
H8mcFNztxGIOZHvlqH7IiPHc73Kkqxmig/vvdUCVI15MADeCsQQ8ds0Aw7uFJiytROF/5wD0jJOZHJToBLvtQd
8UshEtL6TsiEchi2ZVPf/tJmiRriQQNHQy/sWEPlnkt2HzxRkuPNzt1GeMVBAgMBAAGjggLiMIIC3jAOBgNVHQ
8Baf8EBAMCA/gwgZQGCCsGAQUFBwEBBIGHMIGEMDsGCCsGAQUFBzABhi9odHRwOi8vb2NzcC5zeXN0ZW10ZXN0
OC50cnVzdDI0MdguY29tL3Jlc3BvbmRlcjBFBggrBgEFBQcwAoY5aHR0cDovL20uYWlhLnN5c3RlbXRlc3Q4Ln
RydXN0MjQwOC5jb20vc3lzdGVtdGVzdDgtY2EuY2VyMIIBIAYDVR0gBIIBFzCCARMwggEPBg0rBgEEAYH0UQIE
BgIFMIH9MC8GCCsGAQUFBwIBFiNodHRwOi8vd3d3LnRydXN0MjQwOC5jb20vcmVwb3NpdG9yeTCByQYIKwYBBQ
UHAgIwgbwwDBYFRGFuSUQwAwIBARqBq0RhbklEIHRlc3QgY2VydGlmaWthdGVyIGZyYSBkZW5uZSBDQSB1ZHN0
ZWRlcyB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41LiBEYW5JRCB0ZXN0IGNlcnRpZmljYX
RlcyBmcm9tIHRoaXMgQ0EgYXJlIGlzc3VlZCB1bmRlciBPSUQgMS4zLjYuMS40LjEuMzEzMTMuMi40LjYuMi41
LjAYBgNVHREEETAPgQ1qZWxmQG5uaXQuY29tMIGrBgNVHR8EgaMwgaAwOqA4oDaGNGh0dHA6Ly9jcmwuc3lzdG
VtdGVzdDgudHJ1c3QyNDA4LmNvbS9zeXN0ZW10ZXN0OC5jcmwwYqBgoF6kXDBaMQswCQYDVQQGEwJESzESMBAG
A1UECgwJVFJVU1QyNDA4MSUwIwYDVQQDDBxUUlVTVDI0MdggU3lzdGVtdGVzdCBWSUlJIENBMRAwDgYDVQQDDA
dDUkwxMTI0MB8GA1UdIwQYMBaAFJYbNhM7IinCPfnn+ZPrxss+El8EMB0GA1UdDgQWBBTv7aQGa8L1qrrstR8I
tB9Lz0RT/zAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQA0Pd04cFScEKoZgug3x+GBFoYzDgYBZR/dSJ
exU3N9+e5wTgwterC9Ykk3BTV4VlBl6NFUjP9TpqOZaCkqTdWlXruy0wNKvMNGacVZJhS91baTW3ZnNIhAE5x5
gDxvsjuRVc0xZvyAhT7jkp4J62haMoDt+pRsZoDcVCN0KuLWL+Lh5efaB9vSCMsyKUjXf9A/F21nhBiNsECsWj
NXyt2/igbTuYCST12dTCpHs+sDEAnaZlTJa2B/CMUPo15niVLFuOWCPPyxurUZfB3bK/9qdHT60JvaVezwAAmC
WYEW7CW4AAGKDPMDG1qsRxFgaObB3bd5zCbnJkW/SNhg8/lc</AttributeValue>
                   </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>CN=TRUST2408 Systemtest VIII CA, O=TRUST2408,
C=DK</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: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>
                </AttributeStatement>
              </Assertion>
            </RequestedSecurityToken>
            <Lifetime>
              <Created xmlns=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd”>2014-03-19T16:31:16.53Z</Created>
              <Expires xmlns=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd”>2014-03-20T00:31:16.53Z</Expires>
            </Lifetime>
```

Comment [A27]: Issued attributes

```
          </RequestSecurityTokenResponse>
        </RequestSecurityTokenResponseCollection>
      </S11:Body>
    </S11:Envelope>
  </s:Body>
</s: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