



# WS:Security



# Table of Contents

**WS:Security** ..... 1



## WS:Security

Den centrale Soap Header i IDWS opslaget er ws:security elementet som bl.a. skal indeholde en SAML Assertion der identificerer personen der udfører opslaget via et Attribute element. Der findes gode eksempler på opbygningen af elementet i [Liberty Alliance Basic Profile Soap Binding specifikationen](#).

```
<saml2:Attribute FriendlyName="CprNumberIdentifier"
Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml2:AttributeValue>2512484916</saml2:AttributeValue>
</saml2:Attribute>
```

Security elementet skal desuden indeholde to signaturer, en for selve SAML Assertion og en for dokumentet som refererer alle de øvrige headers.

Wsu:Id attributten er påkrævet.

Bemærk at selvom man benytter en anden Trust metode end den beskrevet i pkt 1 [her](#), bør man lave en SAML Assertion med holder-of-key - og så sørge for derudover at få etableret trust via en af de øvrige understøttede trust metoder.

XML eksempel på Security element:

```
<wsse:Security
xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:NS1="http://schemas.xmlsoap.org/soap/envelope/"
xmlns="http://schemas.xmlsoap.org/soap/envelope/" NS1:mustUnderstand="1">
  <wsu:Timestamp
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_b28b7d3e-ea8b-4151-b7f1-26a5c6d0c412">
    <wsu:Created>2014-09-21T19:52:16.125Z</wsu:Created>
    <wsu:Expires>2014-09-21T20:02:16.125Z</wsu:Expires>
  </wsu:Timestamp>
  <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
ID="_c191c238-041f-4976-8a5d-868f6f3ccf7e"
IssueInstant="2014-09-21T19:57:15.309Z" Version="2.0">
    <saml2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameidformat:entity">https://sts.sundhed.dk</saml2: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/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#_c191c238-041f-4976-8a5d-868f6f3ccf7e">
          <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/2000/09/xmlsig#sha1" />
<ds:DigestValue>OByI8xL+3DbmIoJPwfoLSZMFrXM=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>***BASE64 SignatureValue for Assertion
element***</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:KeyValue>
            <ds:RSAKeyValue>
                <ds:Modulus>***BASE64 Modulus***</ds:Modulus>
                <ds:Exponent>AQAB</ds:Exponent>
            </ds:RSAKeyValue>
        </ds:KeyValue>
    </ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">C=DK,0=Ingen organisatorisk tilknytning</saml2:NameID>
    <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
        <saml2:SubjectConfirmationData
NotOnOrAfter="2014-09-22T03:57:15.309Z" Recipient="https://fmk">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>***BASE64
CERT***</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </saml2:SubjectConfirmationData>
    </saml2:SubjectConfirmation>
</saml2:Subject>
    <saml2:Conditions NotBefore="2014-09-21T19:57:15.309Z"
NotOnOrAfter="2014-09-22T03:57:15.309Z">
        <saml2:AudienceRestriction>
            <saml2:Audience>https://fmk</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AttributeStatement>
        <saml2:Attribute FriendlyName="SpecVer"
Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue>DK-SAML-2.0</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute FriendlyName="AssuranceLevel"
Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml2:AttributeValue>3</saml2:AttributeValue>

```

```

        </saml2:Attribute>
        <saml2:Attribute FriendlyName="CprNumberIdentifier"
Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue>2512484916</saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="_cad9fec6-d78c-4e93-971d-c298c80d1c52">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#_90e86943-a8b9-4674-b1be-400f1f5fdb80">
            <ds:Transforms>
                <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>NJooSjGnx4ch+bYD+raSFnJK3aM=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_337c5d0d-a5bd-4e7b-9f3a-918a01f98c79">
            <ds:Transforms>
                <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>/AcypI+frSy+wwS5QMhb40+ScsI=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_dad96bc7-7c82-4738-a3c4-78c58b502395">
            <ds:Transforms>
                <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                    <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd" />
                </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>BBebPUGVZ0vEENrxdiIleuvpsLA=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
</ds:Signature>

```

```

    </ds:Reference>
    <ds:Reference URI="#_d6ff9c04-b1c2-4622-b97f-98094cdf89ef">
      <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
<ds:DigestValue>efIb7T7jynPWgwz06a00u1ltiyo=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#_6d46bd38-7d11-4f65-8a11-d79269edffdb">
        <ds:Transforms>
          <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
<ds:DigestValue>Kj/WHDmy1wXAaQYgdSBw/ja0jEA=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#_7d7be81f-0812-4111-964d-14d9b2882c9c">
          <ds:Transforms>
            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
<ds:DigestValue>74hWBRQhvy9sLxAMHInvhXbtD0g=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="#_b28b7d3e-ea8b-4151-b7f1-26a5c6d0c412">
            <ds:Transforms>
              <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <InclusiveNamespaces
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
<ds:DigestValue>BmtLW4tqtUgT80Q1fi362sS2t0o=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
<ds:SignatureValue>Nk7QvKND8E8cFtcj8re1MGwtAZrLCJvgw2ahKTgqLxcQUzT+0gVxBX2+/

```

```

Ifu1zG1z2ne8LssP5EP
ak0FSJX5qs06u/Vc5e+a1q+3o9mitQ66przWRz2KUKF80Tr3pUuuz3ThjkEqnueDBVx8kt90260x
c7QpmGEK9gH5s
Npb6Ld7PuryCbkWvdZf2gKpqSnI02oTuiicQtLZYKg5/IL2ICDJPwd1wIpVbCuyYtN6v/06iWwBL
XesWiWwD3XeAt9ZD
EdvGY34KilWjCac8FY5S4EpSXrfLGTSwCax1EGKANdLZ+k+U+VnF9qhtklETrt/Rhf3zLY/0EBHT
NTXee0Grg==</ds:SignatureValue>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference
xmlns:wss1="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1
.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurit
y-utility-1.0.xsd"
xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecuri
ty-secext-1.0.xsd"
wss1:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profil
e-1.1#SAMLV2.0" wsu:Id="_fcd711cfc396-4440-9bd9-3de674ad3247">
    <wsse:KeyIdentifier
ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#S
AMLID">_c191c238-041f-4976-8a5d-868f6f3ccf7e</wsse:KeyIdentifier>
    </wsse:SecurityTokenReference>
    </ds:KeyInfo>
  </ds:Signature>
</wsse:Security>

```

From:  
<http://wiki.fmk-teknik.dk/> -  
**Fælles Medicinkort - Dokumentation**

**Permanent link:**  
[http://wiki.fmk-teknik.dk/fmk:ddv:1.4.0:idws\\_ws\\_security](http://wiki.fmk-teknik.dk/fmk:ddv:1.4.0:idws_ws_security)

**Last update: 2026-03-06 08:53**

