SUNDHEDSDATA-
STYRELSEN

OIOSAML Attribute Profiles for Healthcare (OIOSAML-H) 1.0.1

1. Document History

Version	Initials	Changes
1.0	CHG	First published version
1.0.1	CHG	Updated to be based on OIOSAML 2.1.0 (removed certificate attributes) Added global UUID attribute

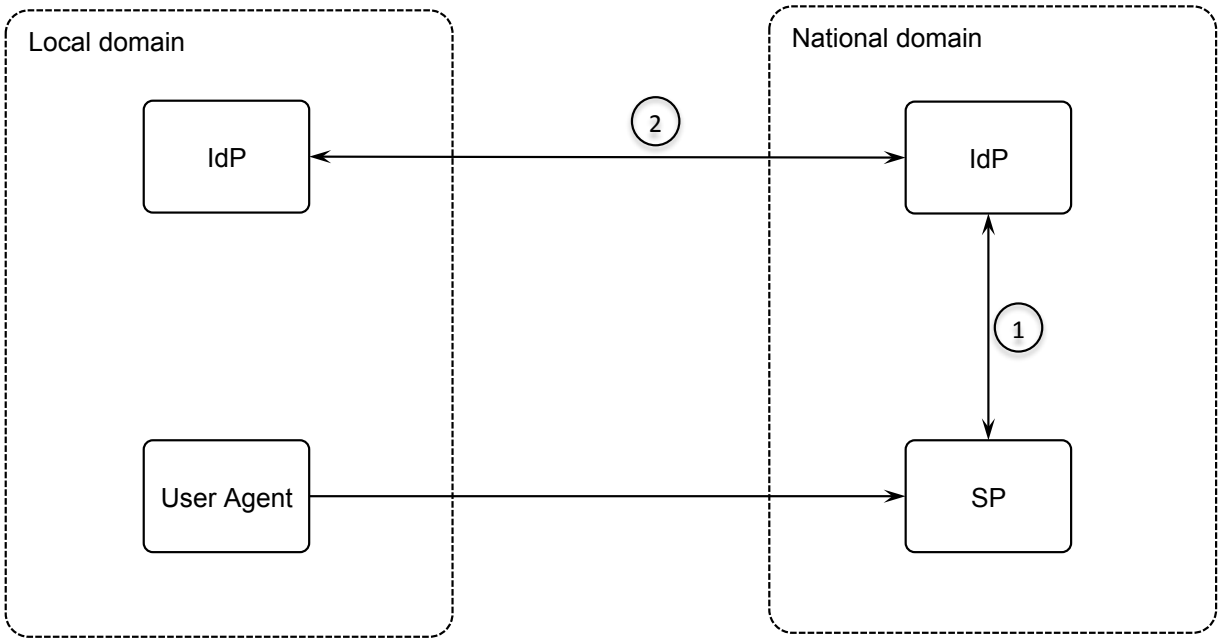
2. Introduction

This document contains attribute profiles for OIOSAML (see [OIO-WEBSSO]) for use within the Danish healthcare sector.

The scope of these profiles is Web browser Single-Sign-On (SSO) within the healthcare sector.

The intended scope of the *OIOSAML Identity Assertion Profile for Healthcare* are assertions that are issued by an Identity Provider (IdP) and consumed by a Service Provider (SP), illustrated as '1' in the figure below.

On the other hand, the intended scope of the *OIOSAML Attribute Assertion Profile for Healthcare* are assertions that are used to transfer attributes from one Identity Provider to another, illustrated as '2' in the figure below.



Example figure illustrating the intended use of OIOSAML-H profiles (non-normative)

Both profiles build on the OIOSAML attribute profiles defined in chapter 7 and 8 in [OIO-WEBSSO] and thus MUST adhere to the rules stated in [OIO-WEBSSO]. Specifically, all assertions MUST be encrypted.

(Later editions may extend this document's scope to include assertions for identity-based web services.)

3. OIOSAML Identity Assertion Profile for Healthcare

This OIOSAML profile defines a set of healthcare specific attributes, builds on attributes from the OCES attribute profile and defines encoding rules for optional privileges and security tokens.

3.1. Healthcare specific attributes

This profile extends the core OIOSAML Authentication Assertion profile with attributes from the OCES attribute profile and attributes that are specific to the healthcare sector.

The following table summarizes all attributes used in this profile. Deviations in mandatoriness from the original attribute definitions are marked as **bold**.

Certificate-related attributes that were removed in OIOSAML 2.1.0 have been marked with ~~strikethrough~~.

Name	Friendly Name	Category	Mandatory
urn:oid:2.5.4.4	surName	Core	Yes
urn:oid:2.5.4.3	CommonName	Core	Yes
urn:oid:0.9.2342.19200300.100.1.1	Uid	Core	Yes
urn:oid:0.9.2342.19200300.100.1.3	Email	Core	Yes
dk:gov:saml:attribute:AssuranceLevel		Core	Yes
dk:gov:saml:attribute:SpecVer		Core	Yes
~~dk:gov:saml:attribute:UniqueAccountKey~~		~~Core~~	~~No~~
urn:liberty:disco:2006-08:DiscoveryEPR		Core	No
~~urn:oid:2.5.4.5~~	~~serialNumber~~	~~OCES~~	**~~No~~**
urn:oid:2.5.4.10	organizationName	OCES	Yes
~~urn:oid:2.5.4.11~~	~~organizationUnit~~	~~OCES~~	~~No~~
~~urn:oid:2.5.4.12~~	~~Title~~	~~OCES~~	~~No~~
~~urn:oid:2.5.4.16~~	~~postalAddress~~	~~OCES~~	~~No~~
~~urn:oid:2.5.4.65~~	~~Pseudonym~~	~~OCES~~	~~No~~
~~dk:gov:saml:attribute:IsYouthCert~~		~~OCES~~	**~~No~~**
~~urn:oid:1.3.6.1.4.1.1466.115.121.1.8~~	~~userCertificate~~	~~OCES~~	~~No~~
dk:gov:saml:attribute:PidNumberIdentifier		OCES	No
dk:gov:saml:attribute:CprNumberIdentifier		OCES	**Yes**
dk:gov:saml:attribute:CvrNumberIdentifier		OCES	Yes
dk:gov:saml:attribute:RidNumberIdentifier		OCES	**No**
dk:healthcare:saml:attribute:SpecVer		OIOSAML-H	Yes
dk:healthcare:saml:attribute:UserAuthorizations		OIOSAML-H	No
dk:healthcare:saml:attribute:HasUserAuthorization		OIOSAML-H	No
dk:gov:saml:attribute:Privileges_intermediate	Privileges	OIO-BPP	No

3.1.1. Specification Version

The mandatory `SpecVer` attribute is used to denote the version of OIOSAML-H this assertion adheres to. The current value is 'OIOSAML-H-1.0'.

Example (non-normative):

```
<!-- The current version of the employed healthcare attribute profile -->
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
      Name="dk:healthcare:saml:attribute:SpecVer">
  <saml:AttributeValue xsi:type="xs:string">OIOSAML-H-1.0</saml:AttributeValue>
</saml:Attribute>
```

3.1.2. User Authorizations

The optional `UserAuthorizations` attribute contains the list of healthcare authorizations the user has been granted by the Department of Health.

All of the user's authorizations SHOULD be included in the attribute. If necessary, the SP consuming the assertion should thus let the user choose which authorization to employ.

The healthcare professional's authorizations MUST be encoded according to the following custom 'User Authorization Profile 1.0' defined by the normative XML schema below:

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:uap="urn:dk:healthcare:saml:user_authorization_profile:1.0"
        targetNamespace="urn:dk:healthcare:saml:user_authorization_profile:1.0">
    <element name="UserAuthorizationList" type="uap:UserAuthorizationListType"/>
    <complexType name="UserAuthorizationListType">
        <sequence>
            <element ref="uap:UserAuthorization" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
    </complexType>
    <element name="UserAuthorization" type="uap:UserAuthorizationType"/>
    <complexType name="UserAuthorizationType">
        <sequence>
            <element ref="uap:AuthorizationCode"/>
            <element ref="uap:EducationCode"/>
            <element ref="uap:EducationType"/>
        </sequence>
    </complexType>
    <element name="AuthorizationCode" type="xsd:string"/>
    <element name="EducationCode" type="xsd:string"/>
    <element name="EducationType" type="xsd:string"/>
</schema>
```

XML schema for User Authorization Profile 1.0

The <uap:UserAuthorizationList> contains a sequence of <uap:UserAuthorization> elements that each contain three elements that MUST conform to the following requirements:

- The <uap:AuthorizationCode> element MUST contain the unique identifier that identifies a healthcare professional's granted authorization. Authorization codes are managed by the Department of Health and consist of a 5-digit code, which is a mixture of letters and numbers.

- The <uap:EducationCode> element MUST contain the 4 digits code that specifies the education of the authorized healthcare professional.

- The <uap:EducationType> element MUST contain a textual representation of <uap:EducationCode> in Danish.

Both the <uap:EducationCode> and <uap:EducationType> element MUST only contain the values defined and maintained by the Department of Health [EDU-AUTREG].

The currently used values are listed below (non-normative).

User Education Code	User Education Type
4498	Optiker
5015	Tandplejer
5151	Fysioterapeut
5152	Social- og sundhedsassistent
5153	Ergoterapeut

5155	Fodterapeut
5158	Radiograf
5159	Bioanalytiker
5166	Sygeplejerske
5175	Jordemoder
5176	Kontaktlinseoptiker
5176	Optometrist
5265	Kiropraktor
5431	Tandplejer
5432	Klinisk tandtekniker
5433	Tandlæge
5451	Klinisk diætist
7170	Læge
9495	Bandagist
A511	Osteopat
B511	Behandlerfarmaceut
C511	Ambulancebehandler

An empty `<uap:UserAuthorizationList>` element means that the person who is identified by the assertion does not have any healthcare authorization.

The `<uap:UserAuthorizationList>` element MUST be embedded as base64 encoded string.

Example (non-normative):

```
<!-- User Authorizations from the Department of Health -->
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
      Name="dk:healthcare:saml:attribute:UserAuthorizations">
  <saml:AttributeValue xsi:type="xs:string">
     [base64-encoded authorizations]
  </saml:AttributeValue>
</saml:Attribute>
```

Where `[base64-encoded authorizations]` is formatted as follows prior to being base64 encoded (non-normative example):

```
<?xml version="1.0" encoding="UTF-8"?>
<uap:UserAuthorizationList xmlns:uap="urn:dk:healthcare:saml:user_authorization_profile:1.0">
    <uap:UserAuthorization>
        <uap:AuthorizationCode>341KY</uap:AuthorizationCode>
        <uap:EducationCode>7170</uap:EducationCode>
        <uap:EducationType>Læge</uap:EducationType>
    </uap:UserAuthorization>
    <uap:UserAuthorization>
        <uap:AuthorizationCode>7AD6T</uap:AuthorizationCode>
        <uap:EducationCode>5433</uap:EducationCode>
        <uap:EducationType>Tandlæge</uap:EducationType>
    </uap:UserAuthorization>
</uap:UserAuthorizationList>
```

3.1.3. HasUserAuthorization

The `HasUserAuthorization` attribute reflects whether the person denoted by this assertion has been granted a healthcare authorization by the Department of Health. Allowed attribute values are `true` and `false`.

Example (non-normative):

```
<!-- Whether the user has a User Authentication Code from the Department of Health -->
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
      Name="dk:healthcare:saml:attribute:HasUserAuthorization">
  <saml:AttributeValue xsi:type="xs:string">true</saml:AttributeValue>
</saml:Attribute>
```

3.2. Mandatory attributes from OIOSAML

Besides the mandatory core OIOSAML attributes the following attributes from the OCES Attribute Profile are mandatory in this profile.

- `dk:gov:saml:attribute:CprNumberIdentifier`
- `dk:gov:saml:attribute:CvrNumberIdentifier`
- `urn:oid:2.5.4.10 (organizationName)`

3.3. Privilege attributes

The assertion MAY contain a set of privileges for the user identified by the assertion.

Privileges MUST be encoded according to the rules defined in [OIOSAML-BPP].

Delegated privileges from one user to another can be expressed as described in [OIOSAML-BPP]. Furthermore, to be able to designate the delegating user by his or her healthcare authorization (instead of his or her cpr-number) this profile introduces the following healthcare specific `Scope` URI for healthcare authorizations:

```
urn:dk:healthcare:saml:userAuthorization:AuthorizationCode:AAAAA:EducationCode:EEEE
```

In the above URI `AAAAA` MUST be set to the delegating user's healthcare authorization code and `EEEE` MUST be set to the corresponding education code.

The following non-normative example illustrates a case where the subject of the assertion has been granted to act on behalf of a doctor (education code '7170') with authorization code '341KY' for the two listed privileges:

```
<?xml version="1.0" encoding="UTF-8"?>
<bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile">
 <PrivilegeGroup
Scope="urn:dk:healthcare:saml:userAuthorization:AuthorizationCode:341KY:EducationCod
e:7170">
  <Privilege>urn:dk:fmk:medicine_ordination</Privilege>
  <Privilege>urn:dk:fmk:renew_prescription</Privilege>
 </PrivilegeGroup>
</bpp:PrivilegeList>
```

In order to express privileges a user has within an organization identified by its "yder-nummer"[1], this specification defines the following `Scope` URN, where `<yderNumber>`

[1] A number for health professional providers in Denmark managed by the Danish regions under the agreements between "Regionernes Lønnings/- og Takstnævn" and the provider ("Ydernes") negotiation organizations, see https://sundhedsdatastyrelsen.dk/da/registre-og-services/om-de-nationale-sundhedsregistre/personoplysninger-og-sundhedsfaglig-beskaeftigelse/yderregisteret .

MUST refer to ID of the organization within the "yderregister" and the optional `:regionCode:<regionCode>` part MAY be used to denote the region, the "yder"-organization belongs to.

```
urn:dk:healthcare:saml:yderNumberIdentifier:<yderNumber>(:regionCode:<regionCode>)
```

The following notation MAY be used to format `<Privilege>` elements, in order to express that the user has the role identified by `<roleCode>` and corresponding `<roleName>` within the specified "yder"-organization.

```
urn:dk:healthcare:saml:yder:roleCode:<roleCode>:roleName:<roleName>
```

Example illustrating a user with relations to two "yder"-organizations:

```
<bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
  <PrivilegeGroup Scope="urn:dk:healthcare:saml:yderNumberIdentifier:18244:regionCode:81">
    <Privilege>urn:dk:healthcare:saml:yder:roleCode:1A:roleName:Ansat læge (§20 stk
1)</Privilege>
  </PrivilegeGroup>
  <PrivilegeGroup Scope="urn:dk:healthcare:saml:yderNumberIdentifier:58541:regionCode:83">
    <Privilege>urn:dk:healthcare:saml:yder:roleCode:23:roleName:Vikar</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

3.4. Security token

The OIOSAML OCES Attribute Profile defines an optional `DiscoveryEPR` attribute that may be used to include a security token (see section 7.3.12 in [OIO-WEBSSO]).

This profile specifies how to include a SOSI IDCard (as defined in [DGWS]) as security token in the `DiscoveryEPR` attribute.

Consult [LIB-DISCO] for details on the `DiscoveryEPR` attribute.

If the included security token is a SOSI IDCard version 1.0.1 then the following rules must be followed:

- The `ServiceType` element contained in the `DiscoveryEPR` attribute MUST have its value set to

  `dk:sosi:1-0-1`

- If the above defined healthcare attribute `HasAuthorizationCode` is included in the assertion its value MUST correspond to the respective attribute in the SOSI IDCard, more specifically:
  - The `HasAuthorizationCode` attribute MUST be set to `true` if the SOSI IDCard `medcom:UserAuthorizationCode` attribute is set.
- Attributes defined in the OCES Attribute Profile MUST match their corresponding attributes in the SOSI IDCard, that is:
  - The `dk:gov:saml:attribute:CprNumberIdentifier` attribute MUST match the SOSI IDCards `medcom:UserCivilRegistrationNumber` attribute.

- The `dk:gov:saml:attribute:CvrNumberIdentifier` attribute MUST match the SOSI IDCards `medcom:CareProviderID` attribute if the later has its `NameFormat` set to `medcom:cvrnumber`.
- The `urn:oid:2.5.4.10` attribute (that is 'organizationName') MUST match the SOSI IDCards `medcom:CareProviderName` attribute.

Example (non-normative):

```
<saml:Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue>
    <wsa:EndpointReference>
      <wsa:Address>http://sosi.dk/sts</wsa:Address>
      <wsa:Metadata>
        <disco:Abstract>A SOSI idcard</disco:Abstract>

        <disco:ServiceType>dk:sosi:1-0-1</disco:ServiceType>

        <disco:ProviderID>http://sosi.dk/sts</disco:ProviderID>
        <disco:SecurityContext>
          <disco:SecurityMechID>urn:liberty:security:2006-08:TLS:SAMLV2</disco:SecurityMechID>
            <sec:Token usage="urn:liberty:security:tokenusage:2006-08:SecurityToken">

              <!-- Here comes the SOSI IDCard -->
              <saml:Assertion IssueInstant="2015-05-07T12:38:33Z" Version="2.0" id="IDCard">

                    . . .

             </saml:Assertion>

          </sec:Token>
        </disco:SecurityContext>
      </wsa:Metadata>
    </wsa:EndpointReference>
  </saml:AttributeValue>
</saml:Attribute>
```

4. OIOSAML Attribute Assertion Profile for Healthcare

This OIOSAML profile defines a set of healthcare specific attributes, builds on attributes from the OCES attribute profile and defines encoding rules for optional privileges.

4.1. Healthcare specific attributes

This profile extends the OIOSAML Authentication Assertion Profile with attributes from the OCES attribute profile and attributes that are specific to the healthcare sector.

The following table summarizes all attributes used in this profile. Deviations in mandatoriness from the original attribute definitions are marked as **bold**.

Certificate-related attributes that were removed in OIOSAML 2.1.0 have been marked with ~~strikethrough~~.

Name	Friendly Name	Category	Mandatory
urn:oid:2.5.4.4	surName	Core	Yes
urn:oid:2.5.4.3	CommonName	Core	Yes
urn:oid:0.9.2342.19200300.100.1.1	Uid	Core	Yes
urn:oid:0.9.2342.19200300.100.1.3	Email	Core	Yes
dk:gov:saml:attribute:AssuranceLevel		Core	Yes
dk:gov:saml:attribute:SpecVer		Core	Yes
~~dk:gov:saml:attribute:UniqueAccountKey~~		~~Core~~	~~No~~
urn:liberty:disco:2006-08:DiscoveryEPR		Core	No
dk:gov:saml:attribute:CprNumberIdentifier		OCES	**Yes**
dk:gov:saml:attribute:CvrNumberIdentifier		OCES	Yes
dk:gov:saml:attribute:RidNumberIdentifier		OCES	No
urn:oid:2.5.4.10	organizationName	OCES	Yes
dk:healthcare:saml:attribute:SpecVer		OIOSAML-H	Yes
dk:healthcare:saml:attribute:EncryptedOIOSamlAssertion		OIOSAML-H	No
dk:gov:saml:attribute:Privileges_intermediate	Privileges	OIO-BPP	No
https://data.gov.dk/model/core/eid/professional/uuid/persistent	Global UUID	OIOSAML-3	No

4.1.1. Specification Version

This profile requires assertion to include the mandatory `SpecVer` attribute as in the above OIOSAML Identity Assertion Profile for Healthcare, see section 3.1.1.

4.1.2. Encrypted OIOSAML assertion

The optional `EncryptedOIOSamlAssertion` attribute contains an encrypted OIOSAML assertion (possibly with an embedded SOSI IDCard or other security token) for the user. The OIOSAML assertion MUST be included in base64 encoded form and MUST be encrypted under a public key for the consuming part.[2]

Example (non-normative):

```
<!-- Encrypted OIOSAML assertion -->
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
      Name="dk:healthcare:saml:attribute:EncryptedOIOSamlAssertion">
  <saml:AttributeValue xsi:type="xs:string">
     [base64-encoded encrypted assertion]
  </saml:AttributeValue>
</saml:Attribute>
```

[2] Future versions of this specification aim to converge the `EncryptedOIOSamlAssertion` and the `DiscoveryEPR` attributes from this specification's two profiles into one attribute such that security tokens are embedded in the same way in both profiles.

Where `[base64-encoded encrypted assertion]` is a base64 encoded SAML `Encrypted-Assertion` element (non-normative example):

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:EncryptedAssertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                     Type="http://www.w3.org/2001/04/xmlenc#Element">
  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
    <xenc:CipherData>
     <xenc:CipherValue>DRct ... Yg==</xenc:CipherValue>
    </xenc:CipherData>
   </xenc:EncryptedKey>
  </ds:KeyInfo>
  <xenc:CipherData>
   <xenc:CipherValue>Q0Rq ... KSme</xenc:CipherValue>
  </xenc:CipherData>
 </xenc:EncryptedData>
</saml:EncryptedAssertion>
```

4.1.3. Identifier attributes (RID and UUID)

The `dk:gov:saml:attribute:RidNumberIdentifier` from [OIOWEB-SSO] and/or the globally unique `https://data.gov.dk/model/core/eid/professional/uuid/persistent` attribute from [OIOSAML-3] (with the value assigned by 'NemLog-in Erhvervsadministration') should be included to support unique user account identification.

Furthermore, including both attributes can be used to facilitate automatic user account migration.

4.2. Subject encoding

The NameID element for the assertion's Subject MUST be encoded as `X509SubjectName`.

Example (non-normative):

```
<saml:Subject>
 <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
   C=DK,O=20688092,CN=Hans Jensen,Serial=123abc456
 </saml:NameID>
   . . .
</saml:Subject>
```

4.3. Mandatory attributes from OIOSAML

Besides the mandatory core OIOSAML attributes the following attributes from the OCES Attribute Profile are mandatory in this profile (Exactly as in the above OIOSAML Identity Assertion Profile for Healthcare).

- `dk:gov:saml:attribute:CprNumberIdentifier`
- `dk:gov:saml:attribute:CvrNumberIdentifier`
- `urn:oid:2.5.4.10 (organizationName)`

4.4. Privilege attributes

The assertion MAY contain a set of privileges for the user identified by the assertion.

Privileges MUST be encoded according to the rules defined in [OIOSAML-BPP].

If privileges are delegated from user to another, the delegating user MAY be identified by his or her healthcare authorization as described in section 3.3 of the above OIOSAML Identity Assertion Profile for Healthcare.

5. Compatibility with other profiles and frameworks

Both the *OIOSAML Identity Assertion Profile for Healthcare* and the *OIOSAML Attribute Assertion Profile for Healthcare* are designed to be compatible with the OIOSAML WebSSO and the KOMBIT SAML set of profiles, see [OIO-WEBSSO] and [KOMBIT-SAML].

6. References

DGWS	Den Gode Web-Service version 1.0.1 http://www.medcom.dk/wm110731
EDU-AUTREG	Education codes for healthcare professionals in Denmark http://autregwebservice.sst.dk/autregservice.asmx/GetAllProfessionGroups
IDWS-H	OIOIDWS for Healthcare Token Profile for Identity Tokens 1.0 https://digitaliser.dk/resource/766172
KOMBIT-SAML	Bilag 2A - Beskrivelse af sikkerhedsmodellen i Rammearkitekturen https://share-komm.kombit.dk/P024/Delte%20dokumenter/Bilag%202A.%20Beskrivelse%20af%20sikkerhedsmodellen%20i%20Rammearkitekturen%20version%201.4%20-%206.%20marts%202015.pdf
LIB-DISCO	Liberty ID-WSF Discovery Service Specification 2.0 http://projectliberty.org/liberty/content/download/875/6201/file/liberty-idwsf-disco-svc-v2.0.pdf
OIOSAML-BPP	OIOSAML Basic Privilege Profile 1.0.1 https://www.digitaliser.dk/resource/2377872/artefact/OIOSAMLBasicPrivilegeProfile1_0_1.pdf?artefact=true&PID=2377876
OIO-WEBSSO	OIO Web SSO Profile V2.1.0 https://www.digitaliser.dk/resource/5833271
OIOSAML-3	OIOSAML Web SSO Profile 3.0.3 https://www.digitaliser.dk/resource/6508977

7. Appendix A: OIOSAML Identity Assertion Profile for Healthcare example

Listed below is a non-normative example of an OIOSAML-H token adhering to the OIOSAML Identity Assertion Profile for Healthcare (with included SOSI IDCard).

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:disco="urn:liberty:disco:2006-08" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:sec="urn:liberty:security:2006-08" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" ID="_5323b570-2b94-48c2-8981-d900e2ec2f96" IssueInstant="2015-05-27T10:02:17Z"
Version="2.0">
 <saml:Issuer>Test STS</saml:Issuer>
 <ds:Signature Id="OCESSignature">
  <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="#_5323b570-2b94-48c2-8981-d900e2ec2f96">
    <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/xmldsig#sha1"/>
    <ds:DigestValue>hJeFB5zsJGgJGgYlbpgz1DJIeVQ=</ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>h1 . . . </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:X509Data>
    <ds:X509Certificate>MI . . . </ds:X509Certificate>
   </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">C=DK,O=NETS
DANID A/S // CVR:30808460,CN=TU GENEREL MOCES M CPR gyldig,Serial=CVR:30808460-
RID:42634739</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <saml:SubjectConfirmationData NotOnOrAfter="2015-05-27T10:07:17Z"
Recipient="http://sundhed.dk/saml/SAMLAssertionConsumer"/>
  </saml:SubjectConfirmation>
 </saml:Subject>
 <saml:Conditions NotBefore="2015-05-27T10:02:17Z" NotOnOrAfter="2015-05-27T11:02:17Z">
  <saml:AudienceRestriction>
   <saml:Audience>http://sundhed.dk</saml:Audience>
  </saml:AudienceRestriction>
 </saml:Conditions>
 <saml:AuthnStatement AuthnInstant="2015-05-27T09:57:16Z" SessionIndex="_5323b570-2b94-48c2-
8981-d900e2ec2f96">
  <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml:AuthnContextClass
Ref>
  </saml:AuthnContext>
 </saml:AuthnStatement>
 <saml:AttributeStatement>
  <saml:Attribute FriendlyName="surName" Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">Dampf</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute FriendlyName="CommonName" Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">Hans Dampf</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute FriendlyName="email" Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string"/>
  </saml:Attribute>
  <saml:Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">3</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
```

```
   <saml:AttributeValue xsi:type="xs:string">DK-SAML-2.0</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">30808460</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute FriendlyName="organizationName" Name="urn:oid:2.5.4.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">Lægehuset på bakken</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">1111111118</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">42634739</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:healthcare:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">OIOSAML-H-1.0</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:healthcare:saml:attribute:UserAuthorizations"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">RS391 . . . </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="dk:healthcare:saml:attribute:HasUserAuthorization"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <saml:AttributeValue xsi:type="xs:string">true</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue>
    <wsa:EndpointReference>
     <wsa:Address>http://sosi.dk/sts</wsa:Address>
     <wsa:Metadata>
      <disco:Abstract>A SOSI idcard</disco:Abstract>
      <disco:ServiceType>dk:sosi:1-0-1</disco:ServiceType>
      <disco:ProviderID>http://sosi.dk/sts</disco:ProviderID>
      <disco:SecurityContext>
       <disco:SecurityMechID>urn:liberty:security:2006-08:TLS:SAMLV2</disco:SecurityMechID>
       <sec:Token usage="urn:liberty:security:tokenusage:2006-08:SecurityToken">
        <saml:Assertion IssueInstant="2015-05-27T09:57:16Z" Version="2.0" id="IDCard"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
         <saml:Issuer>TheSOSILibrary</saml:Issuer>
         <saml:Subject>
          <saml:NameID Format="medcom:other">SubjectDN={SERIALNUMBER=CVR:30808460-RID:42634739
+ CN=TU GENEREL MOCES M CPR gyldig, O=NETS DANID A/S // CVR:30808460,
C=DK},IssuerDN={CN=TRUST2408 Systemtest VIII CA, O=TRUST2408,
C=DK},CertSerial={1276276143}</saml:NameID>
          <saml:SubjectConfirmation>
           <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key</saml:ConfirmationMethod>
           <saml:SubjectConfirmationData>
            <ds:KeyInfo>
             <ds:KeyName>OCESSignature</ds:KeyName>
            </ds:KeyInfo>
           </saml:SubjectConfirmationData>
          </saml:SubjectConfirmation>
         </saml:Subject>
         <saml:Conditions NotBefore="2015-05-27T09:57:16Z" NotOnOrAfter="2015-05-
28T09:57:16Z"/>
         <saml:AttributeStatement id="IDCardData">
          <saml:Attribute Name="sosi:IDCardID">
           <saml:AttributeValue>ftMpXpQ9+hZARZMz9uqIeA==</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:IDCardVersion">
           <saml:AttributeValue>1.0.1</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:IDCardType">
           <saml:AttributeValue>user</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute Name="sosi:AuthenticationLevel">
           <saml:AttributeValue>4</saml:AttributeValue>
          </saml:Attribute>
         </saml:AttributeStatement>
```

```
          <saml:AttributeStatement id="UserLog">
           <saml:Attribute Name="medcom:UserCivilRegistrationNumber">
            <saml:AttributeValue>1111111118</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:UserGivenName">
            <saml:AttributeValue>Hans</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:UserSurName">
            <saml:AttributeValue>Dampf</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:UserRole">
            <saml:AttributeValue>7170</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:UserAuthorizationCode">
            <saml:AttributeValue>341KY</saml:AttributeValue>
           </saml:Attribute>
          </saml:AttributeStatement>
          <saml:AttributeStatement id="SystemLog">
           <saml:Attribute Name="medcom:ITSystemName">
            <saml:AttributeValue>IT-System</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:CareProviderID" NameFormat="medcom:cvrnumber">
            <saml:AttributeValue>30808460</saml:AttributeValue>
           </saml:Attribute>
           <saml:Attribute Name="medcom:CareProviderName">
            <saml:AttributeValue>Lægehuset på bakken</saml:AttributeValue>
           </saml:Attribute>
          </saml:AttributeStatement>
          <ds:Signature id="OCESSignature">
           <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="#IDCard">
             <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/xmldsig#sha1"/>
             <ds:DigestValue>mi0rk+JSFF6mnW1ybUL4sJz3MnM=</ds:DigestValue>
            </ds:Reference>
           </ds:SignedInfo>
           <ds:SignatureValue>Uc  . . . </ds:SignatureValue>
           <ds:KeyInfo>
            <ds:X509Data>
             <ds:X509Certificate>MII . . . </ds:X509Certificate>
            </ds:X509Data>
           </ds:KeyInfo>
          </ds:Signature>
         </saml:Assertion>
        </sec:Token>
       </disco:SecurityContext>
      </wsa:Metadata>
     </wsa:EndpointReference>
    </saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
 </saml:Assertion>
```

Appendix B: OIOSAML Attribute Assertion Profile for Healthcare example

Listed below is a non-normative example of an OIOSAML-H token adhering to the OIOSAML Attribute Assertion Profile for Healthcare.

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_5a49e560-5312-4237-8f32-
2ed2b58cfcf7" IssueInstant="2015-03-27T09:23:13.461Z" Version="2.0">
 <Issuer>Korsbæk Kommune STS</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="#_5a49e560-5312-4237-8f32-2ed2b58cfcf7">
    <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/xmldsig#sha1"/>
    <ds:DigestValue>5EGTkJwo1RWRXAzyemxPNDiIwQ1=</ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>jfsos . . .
  </ds:SignatureValue>
  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
   <ds:X509Data>
    <ds:X509Certificate>MII . . .
    </ds:X509Certificate>
   </ds:X509Data>
  </KeyInfo>
 </ds:Signature>
 <Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
   C=DK,O=13529031,CN=Lise Christiansen,Serial=123abc456
  </NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <SubjectConfirmationData InResponseTo="_0a644321-4795-491a-ad0c-37d5d4b03e6f"
                            NotOnOrAfter="2015-03-27T09:24:13.461Z"
                           Recipient="https://saml.nsf.dk"/>
  </SubjectConfirmation>
 </Subject>
 <Conditions NotBefore="2015-03-27T09:23:13.461Z" NotOnOrAfter="2015-03-27T09:24:13.461Z">
  <AudienceRestriction>
   <Audience>https://saml.nsf.dk</Audience>
  </AudienceRestriction>
 </Conditions>
 <AuthnStatement AuthnInstant="2015-03-27T08:55:18.385Z" SessionIndex="_5a49e560-5312-4237-
8f32-2ed2b58cfcf7">
  <AuthnContext>

<AuthnContextClassRef>element:urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContextCla
ssRef>
  </AuthnContext>
 </AuthnStatement>
 <AttributeStatement>
  <Attribute Name="urn:oid:2.5.4.4" FriendlyName="surName"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>Christiansen</AttributeValue>
  </Attribute>
  <Attribute Name="urn:oid:2.5.4.3" FriendlyName="CommonName"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>Lise Christiansen</AttributeValue>
  </Attribute>
  <Attribute Name="urn:oid:0.9.2342.19200300.100.1.1" FriendlyName="Uid"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>lisech</AttributeValue>
  </Attribute>
  <Attribute Name="urn:oid:0.9.2342.19200300.100.1.3" FriendlyName="email"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>lisech@korsbaek-kommune.dk</AttributeValue>
  </Attribute>
  <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>2</AttributeValue>
```

```
  </Attribute>
  <Attribute Name="dk:gov:saml:attribute:SpecVer"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>DK-SAML-2.0</AttributeValue>
  </Attribute>
  <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>13529031</AttributeValue>
  </Attribute>
  <Attribute Name="dk:gov:saml:attribute:CprNumberIdentifier"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>2107831372</AttributeValue>
  </Attribute>
  <Attribute Name="dk:healthcare:saml:attribute:SpecVer"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>OIOSAML-H-1.0</AttributeValue>
  </Attribute>
  <Attribute Name="dk:healthcare:saml:attribute:EncryptedOIOSamlAssertion"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>Xs34 . . .</AttributeValue>
  </Attribute>
  <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate" FriendlyName="Privileges"
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
   <AttributeValue>3EZi . . .</AttributeValue>
  </Attribute>
 </AttributeStatement>
</Assertion>
```