SUNDHEDSDATA-
STYRELSEN

OIOSAML Attribute Profiles for Healthcare (OIOSAML-H) 3.0

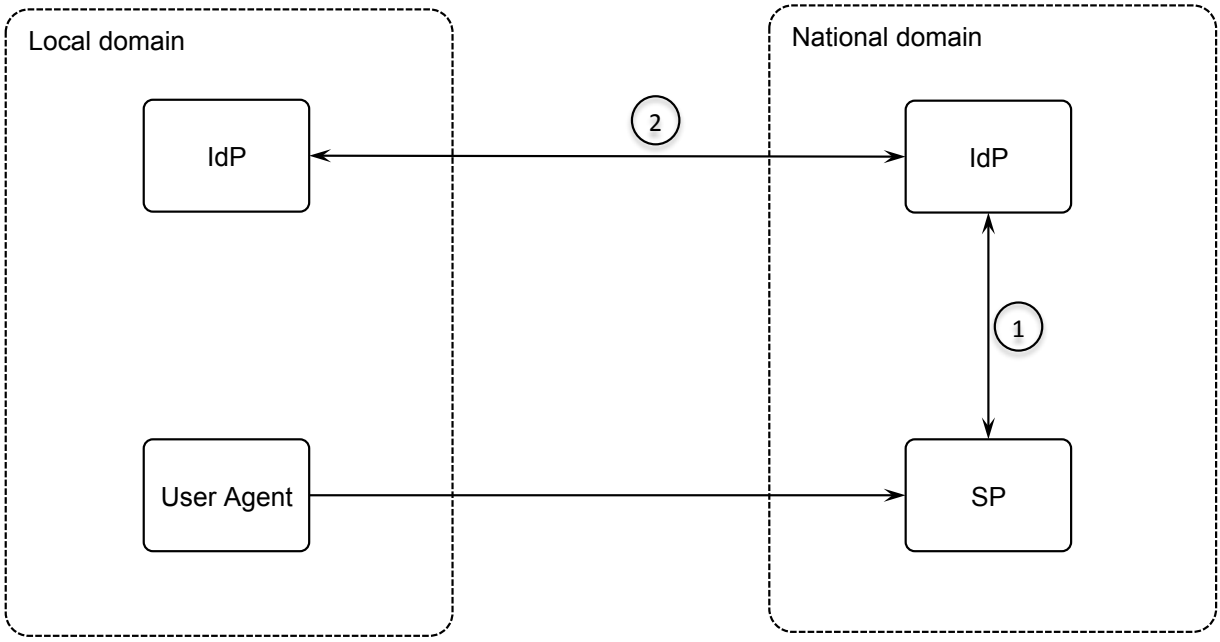
1. Document History

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
3.0	CHG	Updated to be based on OIOSAML 3.0 and OIOSAML Local IdP sub-profile

2. Introduction

This document contains attribute profiles for OIOSAML for use within the Danish healthcare sector.

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



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

The intended scope of the *OIOSAML 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 above. The *OIOSAML Assertion Profile for Healthcare* builds on

the OIOSAML attributes defined in chapter 6 in [OIO-WEBSSO] and MUST adhere to the requirements stated in [OIO-WEBSSO].

On the other hand, the intended scope of the *OIOSAML Local Assertion Profile for Healthcare* are assertions that are issued by one Identity Provider and consumed by another Identity Provider, illustrated as '2' in the figure above. The *OIOSAML Local Assertion Profile for Healthcare* builds on the OIOSAML attributes defined in chapter 6 [OIO-LOCAL-IDP] and MUST adhere to the requirements stated in [OIO-LOCAL-IDP].

3. OIOSAML Assertion Profile for Healthcare

This profile defines which attributes from OIOSAML are used within the healthcare sector and defines encoding rules for privileges employed within healthcare.

3.1. Used OIOSAML attributes

The below table lists attributes defined in [OIO-WEBSSO]. The attributes marked with ~~strikethrough~~ are not used in this profile.

Name	Mandatory
https://data.gov.dk/model/core/specVersion	Yes
https://data.gov.dk/model/core/eid/bootstrapToken	No
https://data.gov.dk/model/core/eid/privilegesIntermediate	No
https://data.gov.dk/concept/core/nsis/loa dk:gov:saml:attribute:AssuranceLevel	Yes (either one of 'loa' or 'Assurancelevel' must be included – but not both)
~~https://data.gov.dk/concept/core/nsis/ial~~	~~No~~
~~https://data.gov.dk/concept/core/nsis/aal~~	~~No~~
https://data.gov.dk/model/core/eid/fullName	No
~~https://data.gov.dk/model/core/eid/firstName~~	~~No~~
~~https://data.gov.dk/model/core/eid/lastName~~	~~No~~
~~https://data.gov.dk/model/core/eid/alias~~	~~No~~
https://data.gov.dk/model/core/eid/email	No
https://data.gov.dk/model/core/eid/cprNumber	No
~~https://data.gov.dk/model/core/eid/age~~	~~No~~
https://data.gov.dk/model/core/eid/cprUuid	No
~~https://data.gov.dk/model/core/eid/dateOfBirth~~	~~No~~
https://data.gov.dk/model/core/eid/person/pid	No
https://data.gov.dk/model/core/eid/professional/uuid/persistent	No
https://data.gov.dk/model/core/eid/professional/rid	No
https://data.gov.dk/model/core/eid/professional/cvr	Yes (for professionals)
https://data.gov.dk/model/core/eid/professional/orgName	Yes (for professionals)
~~https://data.gov.dk/model/core/eid/professional/productionUnit~~	~~No~~
~~https://data.gov.dk/model/core/eid/professional/seNumber~~	~~No~~
~~https://data.gov.dk/model/core/eid/professional/authorizedToRepresent~~	~~No~~

3.2. Encoding rules for healthcare privileges

The `https://data.gov.dk/model/core/eid/privilegesIntermediate` attribute may be used to express privileges within the healthcare sector. Thus, healthcare privileges may be included in `<PrivilegeGroup>` elements as part of the base64-encode [OIO-BPP] structure.

3.2.1. Encoding healthcare authorizations ('sundhedsfaglige autorisationer')

When a user's healthcare authorizations[1] are included in the OIO-BPP structure, the `<PrivilegeGroup>` element containing the professional's healthcare authorization:

1. MUST contain a `Scope` attribute containing the constant value

   `urn:dk:healthcare:saml:userAuthorization:National`

2. MUST NOT contain any `<Constraint>` elements
3. MUST list the professional's healthcare authorizations as `<Privilege>` elements in the form

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

[1] See https://stps.dk/da/autorisation/

where AAAAA MUST be set to the user's healthcare authorization code, EEEE MUST be set to the corresponding education code and NNNNNNNN MUST be set to the corresponding education name.

Example (non-normative):

```
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
  <PrivilegeGroup Scope="urn:dk:healthcare:saml:userAuthorization:National">
    <Privilege>urn:dk:healthcare:saml:userAuthorization:AuthorizationCode:341KY:
EducationCode:7170:EducationName:Læge</Privilege>
    <Privilege>urn:dk:healthcare:saml:userAuthorization:AuthorizationCode:7AD6T:
   EducationCode:5433:EducationName:Tandlæge</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

3.2.2. Encoding delegated privileges

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:

```
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <PrivilegeGroup Scope="urn:dk:healthcare:saml:userAuthorization:AuthorizationCode:
341KY:EducationCode:7170">
    <Privilege>urn:dk:fmk:medicine_ordination</Privilege>
    <Privilege>urn:dk:fmk:renew_prescription</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

3.2.3. Encoding roles within primary care ('yder-tilknytninger')

To express privileges a user has within an organization identified by its 'ydernummer'[2], this specification defines the following Scope URI, where <yderNumber> MUST refer to the identifier of the organization has been assigned in the 'yderregister' and the optional :regionCode:<regionCode> part MAY be used to denote the region, the 'yder'-organization belongs to[3].

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

[2] 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.

[3] The values used as <regionCode> are listed on https://www.nspop.dk/display/public/web/Yder.

The following notation MUST be used to format <Privilege> elements, to express that the user has the role identified by <roleCode> and corresponding <roleName> within the specified 'yder'-organization[4].

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

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

```
<bpp:PrivilegeList xmlns:bpp="http://digst.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>
```

3.2.4. Encoding national roles

The Danish Health Data Authority defines and maintains a set of *national roles* for healthcare professionals, see [NATIONAL-ROLES].

When a user's national roles are included in the OIO-BPP structure, the <PrivilegeGroup> element containing the professional's national roles:

1. MUST contain a Scope attribute representing the professional's organization's CVR-number
2. MUST NOT contain any <Constraint> elements
3. MUST list the professional's national roles as <Privilege> elements in the form

   ```
   urn:dk:healthcare:national-federation-role:<ROLE_NAME>
   ```

   where <ROLE_NAME> contains the actual role.

Example (non-normative):

```
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
  <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:20301823">
    <Privilege>urn:dk:healthcare:national-federation-role:PlejeAssR3</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

3.2.5. Encoding application-domain roles

Application-domain specific roles and constraints MAY be included as part of the OIO-BPP structure and MUST follow the rules defined in [OIO-BPP].

When used, the application-domain SHOULD be set in the Scope attribute in the form

```
urn:dk:healthcare:saml:application-domain:<APPLICATION_DOMAIN>
```

where <APPLICATION_DOMAIN> contains the actual application-domain.

---

[4] The values used as <roleCode> and <roleName> are also listed on https://www.nspop.dk/display/public/web/Yder.

Example (non-normative):

```
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
  <PrivilegeGroup Scope="urn:dk:healthcare:saml:application-domain:LPR-SOR">
    <Privilege>lanRet kontakt</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

Furthermore, the granted privileges MAY be restricted to organizational SOR[5]-units. When privileges are restricted to organizational SOR-units, the following two OIO-BPP `Constraint` elements MUST be specified:

1. An `urn:dk:healthcare:sorIdentifier` constraint containing a valid SOR identifier
2. An `urn:dk:healthcare:organizationalUnitRestriction` constraint containing one of the three values `UnitAndSubunits`, `SubunitsOnly` or `UnitWithoutSubunits`, with the following semantics:
    - `UnitAndSubunits`: The specified privilege(s) are valid for the specified SOR unit and all its subunits
    - `SubunitsOnly`: The specified privilege(s) are valid for all subunits of the specified SOR unit, but not the unit itself
    - `UnitWithoutSubunits`: The specified privilege(s) are valid for the specified SOR unit, but none of its subunits

Example (non-normative):

```
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
  <PrivilegeGroup Scope="urn:dk:healthcare:application-domain:DPSD">
    <Constraint Name="urn:dk:healthcare:sorIdentifier">1258941000016003</Constraint>
    <Constraint
Name="urn:dk:healthcare:organizationalUnitRestriction">UnitAndSubunits</Constraint>
    <Privilege>dpsDecentralSagsbehandler</Privilege>
    <Privilege>dpsInitialmodtager</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

3.3. Specification Version

The mandatory `https://healthcare.data.gov.dk/model/core/specVersion` attribute is used to denote the version of OIOSAML-H this assertion adheres to. The current value is 'OIOSAML-H-3.0'.

Example (non-normative):

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="https://healthcare.data.gov.dk/model/core/specVersion">
  <saml:AttributeValue xsi:type="xs:string">OIOSAML-H-3.0</saml:AttributeValue>
</saml:Attribute>
```

[5] "Sundhedsvæsenets Organisationsregister (SOR)", see https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/organisationsregistrering.

4. OIOSAML Local Assertion Profile for Healthcare

This OIOSAML profile extends [OIO-LOCAL-IDP] with healthcare specific requirements.

4.1. Used OIOSAML attributes

The below table lists attributes from [OIO-LOCAL-IDP] used in this profile and states whether they are mandatory in this profile.

Name	Mandatory
https://data.gov.dk/model/core/specVersion	Yes
https://data.gov.dk/concept/core/nsis/loa	Yes
https://data.gov.dk/model/core/eid/fullName	No
https://data.gov.dk/model/core/eid/professional/cvr	Yes
https://data.gov.dk/model/core/eid/professional/orgName	Yes
https://data.gov.dk/model/core/eid/professional/uuid/persistent	**Yes**
https://data.gov.dk/model/core/eid/privilegesIntermediate	No

4.2. Persistent identifier attribute

The persistent identifier attribute defined in OIOSAML with attribute name

`https://data.gov.dk/model/core/eid/professional/uuid/persistent`

is MANDATORY in this profile and MUST contain the global UUID for the professional identity (with the value assigned by 'NemLog-in Erhvervsadministration').

4.3. Fullname attribute

For display purposes a user's name SHOULD be provided in the

`https://data.gov.dk/model/core/eid/fullName`

attribute.

4.4. Encoding national roles for healthcare professionals

The Danish Health Data Authority defines and maintains a set of *national roles* for healthcare professionals, see [NATIONAL-ROLES].

In this profile, locally administrated national roles MAY be included in the OIOSAML assertion

`https://data.gov.dk/model/core/eid/privilegesIntermediate`

attribute. If included, a professional's locally administrated national roles MUST thus be included as part of the base64-encode [OIO-BPP] structure and adhere to the encoding rules defined in '3.2.4 Encoding national roles'.

5. References

NATIONAL-ROLES	National roles within the healthcare federation https://www.nspop.dk/pages/releaseview.action?pageId=162836066
OIO-BPP	OIOSAML Basic Privilege Profile 1.2 https://digst.dk/media/20999/oiosaml-basic-privilege-profile-1_2.pdf
OIO-WEBSSO	OIOSAML Web SSO Profile 3.0.3 https://www.digitaliser.dk/resource/6508977
OIO-WEBSSO-LEGACY	OIO Web SSO Profile V2.1.0 https://www.digitaliser.dk/resource/5833271
OIO-LOCAL-IDP	OIOSAML Local IdP Profile 1.0.2 https://www.digitaliser.dk/resource/5272559