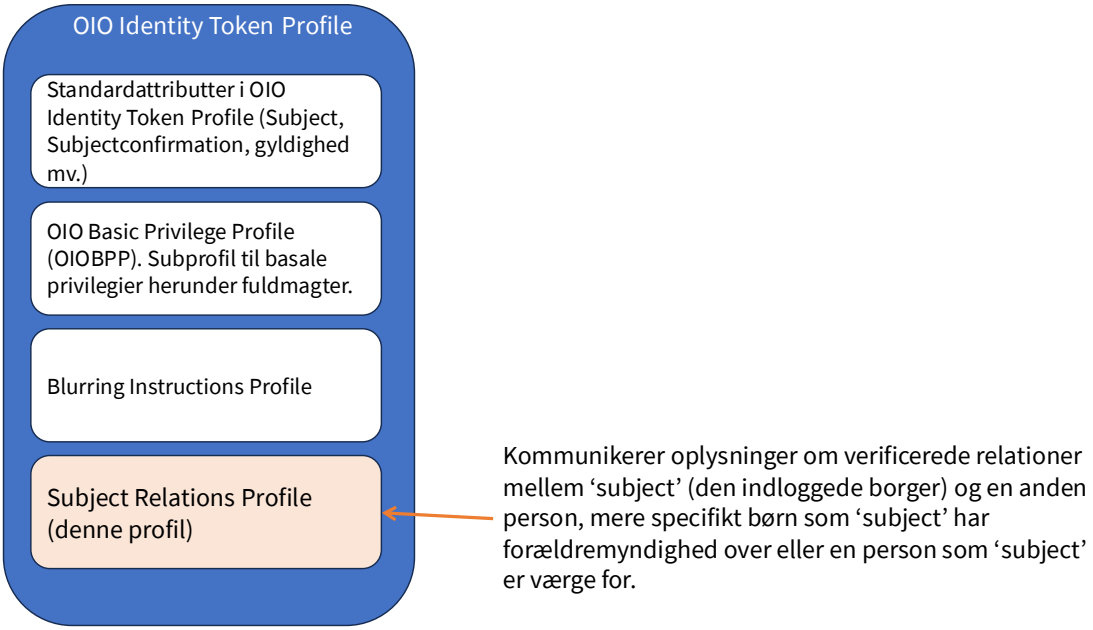
# OIOITP Subject Relations Profile 1.0

## 1. Dokumenthistorik

| Version | Dato | Initialer | Ændringer |
|---|---|---|---|
| 0.1 | 10.01.2024 | JRI | Draft. |
| 0.2 | 15.01.2024 | JRI | Efter CHG review |
| 0.31 | 17.01.2024 | JRI | Efter ASHA, JFQ review. CPR nu med OID |
| 1.0 | 18.01.2024 | Anni | Final |
| | | | |

## 2. Introduktion

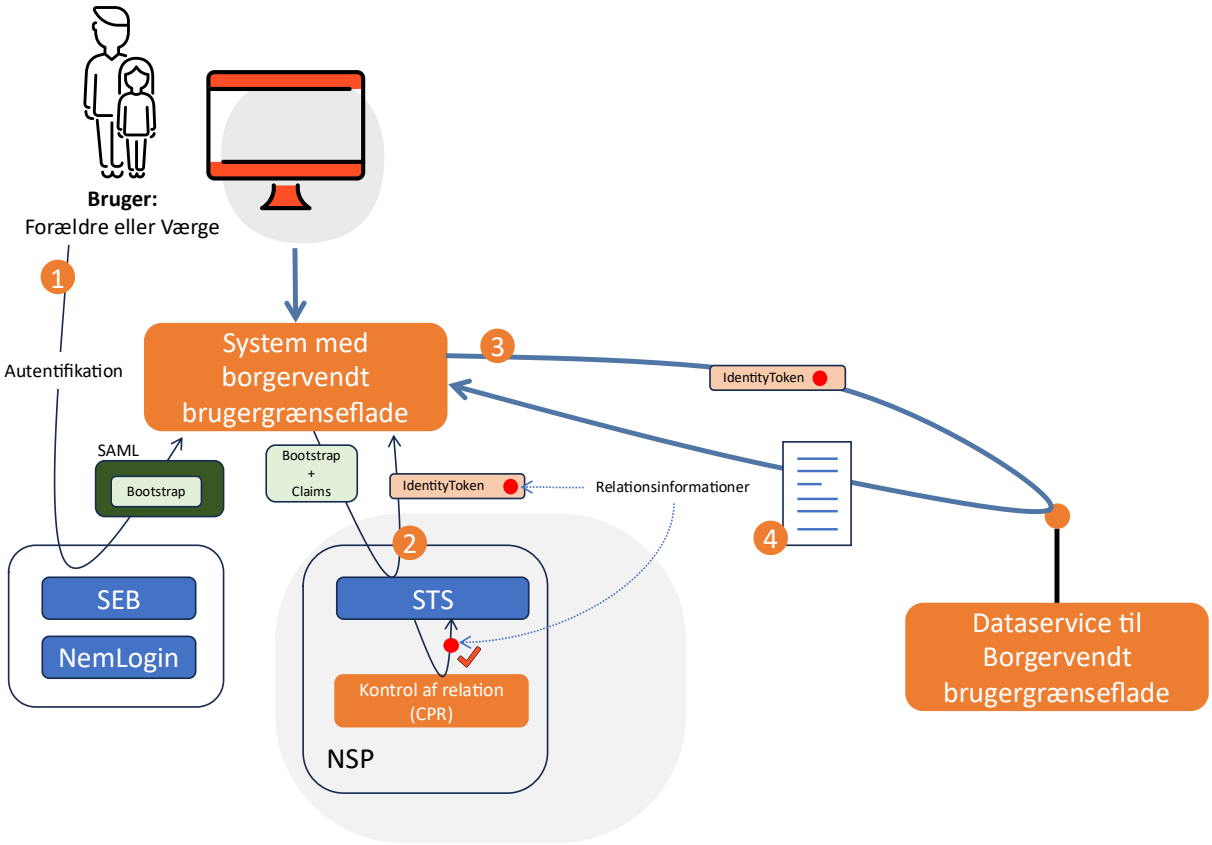
Dette dokument specificerer hvorledes relationer mellem forældremyndighedsindehavere og børn hhv. værger og personer under værgemål skal udtrykkes som SAML attributter i OIO Identity Token Profile [OIOITP][1].




**Figur 1: Profilen er en subprofil til OIO Identity Token Profile og har til hensigt at regulere, hvorledes værge- og forældremyndighedsrelationer udtrykkes som SAML attributter.**

Profilen skal anvendes i omveksling af Bootstrap tokens hhv. JWT tokens til OIO SAML Identity Tokens. Scopet er således kald af identitetsbaserede web services[2] i en sikker Borger-login kontekst (mere specifikt i respons fra trin 2 i Figur 2 nedenfor).

[1] https://digst.dk/media/28186/oio-saml-profile-for-identity-tokens-v12.pdf. Bemærk, sundhedsområdet anvender stadig version 1.0, men det har ingen betydning for denne profil.
[2] https://digst.dk/it-loesninger/standarder/oio-identity-based-web-services-12-oio-idws/. Bemærk, sundhedsområdet anvender stadig version 1.0, men det har ingen betydning for denne profil.




**Figur 2: Profilen regulerer indholdet af relationsinformationer i Identity Tokens (rød prik i trin 2 i figuren), her eksemplificeret gennem et SAML login flow (kunne også være et Open ID Connect flow). Den person der er relationer til udtrykkes pt. via CPR-numre og kontrolleres gennem CPR-registret.**

## 2.1. Overordnede krav

### 2.1.1. Krav: Skal kommunikere verificeret forældremyndighedsrelation.

Profilen skal sikre, at det er muligt at kommunikere, at der findes en verificeret forældremyndighedsrelation mellem 'subject' (forælderen) og barnet, der er angivet som claim i omvekslingsforespørgslen. Hvis relationen ikke kan verificeres hos en autoritativ kilde eller med fornøden sikkerhed, må der ikke udstedes en billet.

### 2.1.2. Krav: Skal kommunikere verificeret værgerelation.

Profilen skal sikre, at det er muligt at kommunikere, at der findes en verificeret værgerelation mellem 'subject' (værgen) og personen der er i værgemål (angivet som claim i omvekslingsforespørgslen). Hvis relationen ikke kan verificeres hos en autoritativ kilde eller med fornøden sikkerhed, må der ikke udstedes en billet.

### 2.1.3. Krav: Skal være en ægte subprofil til OIO Identity Token Profile

Profilen skal være en ægte subprofil til et element i OIO Identity Token Profile og skal ses som et supplement (en søsterprofil) til OIO Basic Privilege Profile.

### 2.1.4. Krav: Skal encodes som Base64 og indlejres i SAML token (identity token)

Det resulterende XML skal i lighed med OIOBPP indlejres i Identity Tokenet som en base64 encoded streng som SAML attribut med navn `urn:dk:health-care:saml:attribute:SubjectRelations`.

### 2.1.5. Attributten må kun være til stede, hvis der er claims om relationer

Attibutten `urn:dk:healthcare:saml:attribute:SubjectRelations` må kun være til stede, hvis der i omvekslingskaldet er mindst et claim om relation.

### 2.1.6. Attributten skal afspejle claims 1-til-1

Hvis der er angivet N claims i omvekslingskaldet skal der være præcis N unikke verificerede relationer i `SubjectRelations`.

## 2.2. Notationskonventioner

Flg. danske nøgleord følger [RFC 2119]

- "SKAL" og "MÅ KUN" svarer til SHALL eller MUST
- "SKAL IKKE" og "MÅ IKKE" svarer til SHALL NOT eller MUST NOT
- "KRÆVET" svarer til REQUIRED
- "BØR" svarer til SHOULD
- "BØR IKKE" svarer til SHOULD NOT
- "KAN" og "MÅ" svarer til "MAY"

Denne specifikation bruger en notationskonvention kendt som "Pseudo-schemas", der er en [BNF][3] konvention til at beskrive attributter og elementer i XML:

- *'?'* markerer valgfrihed (dvs. nul eller én forekomst),
- *'*' markerer* nul eller flere forekomster,
- *'+' markerer én eller flere forekomster*,
- *'[' og ']' bruges til at danne grupper*,
- '|' repræsenterer valg.
- Attributter får per konvention tilegnet en værdi, der matcher den datatype, som attributten repræsenterer.
- Elementer med ikke-kompleks indhold tilegnes per konvention en værdi, der matcher indholdet i elementets normative XML schema.
- Brugen af {any} indikerer forekomsten af et vilkårligt element (<xs:any/>).
- Brugen af @{any} indikerer forekomsten af en vilkårlig attribut (<xs:anyAttribute/>).

```
<!-- Pseudo-schema eksempel -->
<element
     required_attribute_of_type_QName="xs:QName"
     optional_attribute_of_type_string="xs:string"? >
   <required_element />
   <optional_element /> ?
   <one_or_more_of_these_elements /> +
   [ <choice_1 /> | <choice_2 /> ] *
</element>
```

### 2.2.1. XML Namespaces

| Prefix | Namespace |
|---|---|
| xsd | http://www.w3.org/2001/XMLSchema |
| srp | urn:dk:healthcare:saml:subject_relations_profile:1.0 |

[3] http://en.wikipedia.org/wiki/Backus–Naur_Form

# 3. OIOITP Subject Relations Profile

## 3.1. Profilspecifikke elementer og attributter

| Name | Mandatory |
|---|---|
| srp:SubjectRelations | Yes |
| srp:VerifiedRelation | Yes |
| srp:VerifiedRelation:attribute:relationType | Yes |
| srp:VerifiedRelation:attribute:relatedPersonID | Yes |
| srp:VerifiedRelation:attribute:relatedPersonIDType | Yes |
| | |
| | |

## 3.2. XML Schema inkl. beskrivelse af elementer og attributter

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:srp="urn:dk:healthcare:saml:subject_relations_profile:1.0"
   attributeFormDefault="unqualified"
   elementFormDefault="qualified"
   targetNamespace="urn:dk:healthcare:saml:subject_relations_profile:1.0">

   <xs:element name="SubjectRelations">
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="srp:VerifiedRelation"
               maxOccurs="unbounded"
               minOccurs="1"
            />
         </xs:sequence>
      </xs:complexType>
   </xs:element>

   <xs:element name="VerifiedRelation">
      <xs:complexType>
         <xs:attribute name="relationType" type="srp:relationTypeAttribute" use="required" />
         <xs:attribute name="relatedPersonID" type="xs:string" use="required" />
         <xs:attribute name="relatedPersonIDType"
                       type="srp:personIDTypeAttribute" use="required" />
      </xs:complexType>
   </xs:element>

   <xs:simpleType name="relationTypeAttribute">
      <xs:restriction base="xs:string">
         <xs:enumeration value="wardCustodyHolder" /> <!-- Fuld værge -->
         <xs:enumeration value="partlyWardCustodyHolder" /> <!-- Delvis værge -->
         <xs:enumeration value="parentalCustodyHolder"/> <!—Forældremyndighed -->
      </xs:restriction>
   </xs:simpleType>

   <xs:simpleType name="personIDTypeAttribute">
      <xs:restriction base="xs:string">
         <xs:enumeration value="URN:OID:1.2.208.176.1.2" /> <!-- CPR -->
      </xs:restriction>
   </xs:simpleType>

</xs:schema>
```

**XML schema for Subject Relations Profile 1.0**

`<srp:SubjectRelations>` SKAL indeholde en liste af `<srp:VerifiedRelation>` elementer.

`<srp:VerifiedRelation>` SKAL indeholde:

- attributten **`relationType`**, der kan have følgende værdier:
  - "**`wardCustodyHolder`**", hvis 'subject' er "fuld værge"[4,5] for den, som der ønskes at handle/se på vegne af.
  - "**`partlyWardCustodyHolder`**", hvis 'subject' er "delvis værge" (se fodnoter) for den, som der ønskes at handle/se på vegne af.
  - "**`parentalCustodyHolder`**", hvis 'subject' har forældremyndighed over den, som der ønskes at handle/se på vegne af.
- Attributten **`relatedPersonID`**, der angiver ID på den person, som relationen er til.
- Attributten **`relatedPersonIDType`**, der indikerer den klassifikation, som **`relatedPersonID`** er angivet i. I denne version af profilen er følgende klassifikationer tilladt:
  - **`'URN:OID:1.2.208.176.1.2'`** når **`relatedPersonID`** er et CPR nummer.

`<srp:SubjectRelations>` SKAL indlejres i Identity Tokenet som en base64 encoded streng som SAML attribut med navn **`urn:dk:healthcare:saml:attribute:SubjectRelations`**, hvis og kun hvis, der er om relationer.

# 4. Eksempler (non-normative)

## 4.1. Eksempel – Fuld Værge

```xml
<?xml version="1.0" encoding="UTF-8"?>

<srp:SubjectRelations
   xmlns:srp="urn:dk:healthcare:saml:subject_relations_profile:1.0">

   <srp:VerifiedRelation
      relationType="wardCustodyHolder"
      relatedPersonID="0101111234"
      relatedPersonIDType="URN:OID:1.2.208.176.1.2"
   />
</srp:SubjectRelations>
```

## 4.2. Eksempel – Forældremyndighed

```xml
<?xml version="1.0" encoding="UTF-8"?>

<srp:SubjectRelations
   xmlns:srp="urn:dk:healthcare:saml:subject_relations_profile:1.0">

   <srp:VerifiedRelation
      relationType="parentalCustodyHolder"
      relatedPersonID="0101111234"
      relatedPersonIDType="URN:OID:1.2.208.176.1.2"
   />
</srp:SubjectRelations>
```

[4] https://cpr.dk/cpr-nyt/nyhedsarkiv/2019/jun/vaergemaal-og-delt-bopael

[5] https://cprservicedesk.atlassian.net/wiki/download/attachments/11436083/Udtraeksvejledning%20for%20offentlige%20brugere.pdf

### 4.3. Eksempel – Indlejring af Base64 encoded streng

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Attribute
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   Name=" urn:dk:healthcare:saml:attribute:SubjectRelations "
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

   <saml:AttributeValue xsi:type="xs:string">
      <!-- Relationer i Base64 encodet form. -->

      PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KCjxzcnA6U3ViamVjdFJlbGF0
      aW9ucwoJeG1sbnM6c3JwPSJ1cm46ZGs6aGVhbHRoY2FyZTpzYW1sOnN1YmplY3RfcmVsYXRpb25z
      X3Byb2ZpbGU6MS4wIj4KCgk8c3JwOlZlcmlmaWVkUmVsYXRpb24gCgkJcmVsYXRpb25UeXBlPSJw
      YXJlbnRhbEN1c3RvZHlIb2xkZXIiCgkJcmVsYXRlZFBlcnNvbklEPSIwMTAxMTExMjM0IgoJCXJl
      bGF0ZWRQZXJzb25JRFR5cGU9IlVSTjpPSUQ6MS4yLjIwOC4xNzYuMS4yIgoJLz4KPC9zcnA6U3Vi
      amVjdFJlbGF0aW9ucz4K

   </saml:AttributeValue>

</saml:Attribute>
```

## 5. Kompatibilitet med andre profiler

Denne profil er designet til at være et supplement til OIO Basic Privilege Profile og er en subprofil til OIO Identity Token Profile, og er dermed kompatibel med OIOSAML

# 6. Appendiks A: OIOSAML Identity Token Profile eksempel med Subject Relations Profile element

Indsættes når STS'en kan generere en sådan.