SUNDHEDSDATA-
STYRELSEN

OIO Healthcare WS-Trust profile

Version 1.0

1 Introduction

This document defines requirements for using WS-Trust within the Danish Healthcare Sector.

This specification does not stand for itself. The reader is thus expected to have knowledge about [OIO-WST-11].

1.1 Notation

This specification uses schema documents conforming to W3C XML Schema [Schema1] and normative text to describe the syntax and semantics of XML-encoded SAML assertions and protocol messages. In cases of disagreement between the SAML profile schema documents and schema listings in this specification, the schema documents take precedence. Note that in some cases the normative text of this specification imposes constraints beyond those indicated by the schema documents.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 [RFC2119].

```
Example code listings appear like this.
```

2 WS Trust profile

The OIO Healthcare WS-Trust follows the OIO-WS-Trust profile [OIO-WST-11], unless specifically noted.

The profile defines thus how to exchange a bootstrap token (issued by an IdP) to another token, that can be used to get access to an actual service.

2.1 Claims

When exchanging a bootstrap token to another token, the service consumer MAY provide claims with values to the STS.

2.1.1 Claims dialect

To specify desired attribute values in the requested token the `Dialect` attribute on a `<Claims>` element MAY be set to `http://docs.oasis-open.org/wsfed/authorization/200706/authclaims`, see [WS-FED], which supports both simple string values and structured values.

The URI attribute MUST be the set to the name of the specified attribute.

Example:

```
<wst:Claims xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">

   <auth:ClaimType Uri="dk:gov:saml:attribute:CprNumberIdentifier">
      <auth:Value>2512484916</auth:Value>
   </auth:ClaimType>

</wst:Claims>
```

3 Requesting a SOSI idcard

When the requested token is a SOSI idcard a value for the in [DGWS] mandatory `medcom:ITSystemName` attribute MUST be provided as WS-Trust claim as specified above.

Example:

```
<wst:Claims xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">

   <auth:ClaimType Uri="medcom:ITSystemName">
      <auth:Value>Korsbæk Kommunes omsorgssystem</auth:Value>
   </auth:ClaimType>

   <!-- Optional claims -->

</wst:Claims>
```

Optionally the request MAY include values as WS-Trust claims for the [DGWS] attributes `medcom:UserAuthorizationCode` or `medcom:UserRole` in order to specify a user's healthcare authorization or role (national role or education code) within the SOSI federation.

Example (claiming a healthcare authorization):

```
<wst:Claims xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">

   <!-- Mandatory "medcom:ITSystemName" claim -->
   <auth:ClaimType Uri="medcom:ITSystemName">
      <auth:Value>Region Vestjyllands EPJ</auth:Value>
   </auth:ClaimType>

   <auth:ClaimType Uri="medcom:UserAuthorizationCode">
      <auth:Value>ZXCVB</auth:Value>
   </auth:ClaimType>

</wst:Claims>
```

Example (claiming an education code):

```
<wst:Claims xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">

   <!-- Mandatory "medcom:ITSystemName" claim -->
   <auth:ClaimType Uri="medcom:ITSystemName">
      <auth:Value>Region Vestjyllands EPJ</auth:Value>
   </auth:ClaimType>

   <auth:ClaimType Uri="medcom:UserRole">
      <auth:Value>7170</auth:Value>
   </auth:ClaimType>

</wst:Claims>
```

Example (claiming a national role):

```
<wst:Claims xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">

   <!-- Mandatory "medcom:ITSystemName" claim -->
   <auth:ClaimType Uri="medcom:ITSystemName">
      <auth:Value>Korsbæk Kommunes audiologisystem</auth:Value>
   </auth:ClaimType>

   <auth:ClaimType Uri="medcom:UserRole">
      <auth:Value>urn:dk:healthcare:national-federation-role:AudiologiMedarbR4
      </auth:Value>
   </auth:ClaimType>

</wst:Claims>
```

4 References

Reference	Description
[DGWS]	Den Gode Web-Service 1.0.1 https://www.medcom.dk/standarder/webservice-standarder/den-gode-webservice
[RFC2119]	Key words for use in RFCs to indicate requirement levels. https://www.ietf.org/rfc/rfc2119.txt
[OIO-WST-11]	OIO WS-Trust Profile V1.1 https://www.digitaliser.dk/resource/3457606