OIO Healthcare Bootstrap Token Profile

Version 1.0

1 Introduction

This document defines requirements for bootstrap tokens to be used within the Danish Healthcare Sector.

In this profile, a bootstrap token is a SAML 2.0 assertion that represents a professional (contains attributes about a professional user) that can be exchanged at a Security Token Service to other tokens which in turn provide access to actual services.

This specification does not stand for itself. The reader is thus expected to be familiar with [OIO-BOOT].

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 Bootstrap token profile

A bootstrap token can be exchanged at an STS to a service/identity token, which provides access to an actual service.

2.1 Bootstrap token requirements

Healthcare bootstrap tokens MUST be valid SAML 2.0 assertions conforming to the requirements for OIO bootstrap tokens for not-collocated IdPs and STSs as defined in [OIO-BOOT] unless explicitly stated otherwise below:

- A healthcare bootstrap tokens subject element MUST contain at least one `<SubjectConfirmation>` sub-element with a confirmation method of `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`. Furthermore:
  - The element MUST be qualified with an `xsi:type` of `saml2:KeyInfoConfirmationDataType`
  - Exactly one `<ds:KeyInfo>` element MUST be included containing a `<ds:X509Data>` and a `<ds:X509Certificate>` with the X.509 certificate of the service consumer as a base64 encoded value.
- A healthcare bootstrap tokens MUST contain a *persistent* subject identifier. E.g., a locally persistent identifier or a globally persistent identifier as defined in requirement OIO-IDP-15 in [OIOSAML].

2.2 Attributes

The following attributes from [OIOSAML] and [OIOSAML-H] are employed in this profile:

Name	Source	Mandatory
`https://data.gov.dk/concept/core/nsis/loa`	OIOSAML	Yes
`https://data.gov.dk/model/core/specVersion`	OIOSAML	Yes
`https://data.gov.dk/model/core/eid/professional/uuid/persistent`	OIOSAML	Yes
`https://data.gov.dk/model/core/eid/professional/cvr`	OIOSAML	Yes
`https://data.gov.dk/model/core/eid/professional/orgName`	OIOSAML	Yes
`https://data.gov.dk/model/core/eid/privilegesIntermediate`	OIOSAML	No
`https://healthcare.data.gov.dk/model/core/specVersion`	OIOSAML-H	Yes

If included, the optional `https://data.gov.dk/model/core/eid/privilegesIntermediate` attribute MUST only be used to list a professional's national roles as defined in [OIOSAML-H].

Other attributes SHOULD NOT be included healthcare bootstraptokens adhering to this profile.

3 References

Reference	Description
[RFC2119]	Key words for use in RFCs to indicate requirement levels. https://www.ietf.org/rfc/rfc2119.txt
[OIO-BOOT]	OIO Bootstrap Token Profile V1.2 https://www.digitaliser.dk/resource/5988041
[OIOSAML]	OIOSAML Web SSO Profile 3.0.3 https://www.digitaliser.dk/resource/6508977
[OIOSAML-H]	OIOSAML Attribute Profiles for Healthcare (OIOSAML-H) 3.0