DIGITALISERINGSSTYRELSEN

OIOSAML
Local Identity Provider Profile 1.0.2

Status: Published version

Date: 18.03.2020

1 INTRODUCTION 5
1.1 PREFACE 5
1.2 USAGE SCENARIOS 6
2 NOTATION AND TERMINOLOGY 7
2.1 REFERENCES TO SAML 2.0 SPECIFICATION 7
2.2 TERMINOLOGY 7
3 COMMON REQUIREMENTS 9
3.1 GENERAL 9
3.1.1 Clock Skew 9
3.1.2 Document Type Definitions 9
3.1.3 SAML entityIDs 9
3.2 METADATA AND TRUST MANAGEMENT 10
3.2.1 Metadata Consumption and Use 10
3.2.2 Metadata Production 10
3.3 CRYPTOGRAPHIC ALGORITHMS 11
4 SP REQUIREMENTS 13
4.1 WEB BROWSER SSO 13
4.1.1 Requests 13
4.1.2 Responses 16
4.1.3 LoA check 17
4.1.4 Discovery 17
4.2 SINGLE LOGOUT 17
4.2.1 Requests 17
4.2.2 Responses 18
4.2.3 Behavioral Requirements 18
4.2.4 Logout and Virtual Hosting 19
4.3 METADATA AND TRUST MANAGEMENT 19
4.3.1 Support for Multiple Keys 19
4.3.2 Metadata Content 19
5 IDP REQUIREMENTS 21
5.1 WEB BROWSER SSO 21
5.1.1 Requests 21
5.1.2 Responses 22
5.1.3 Issuer 23
5.1.4 Subject Identifiers 23
5.1.5 Subject Confirmation 23
5.1.6 Audience Restriction 24

5.1.7 Discovery via common domain 24
5.2 SINGLE LOGOUT 25
5.2.1 Requests 25
5.2.2 Request Content 25
5.2.3 Responses 25
5.3 ATTRIBUTE QUERY 26
5.3.1 Request Message 26
5.3.2 Response Message 27
5.3.3 Error handling 27
5.4 METADATA AND TRUST MANAGEMENT 28
5.4.1 Support for Multiple Keys 28
5.4.2 Metadata Content 28
6 ATTRIBUTE PROFILES 29
6.1 GENERAL REQUIREMENTS 29
6.2 COMMON ATTRIBUTES 30
6.2.1 SpecVer attribute 30
6.2.2 BootstrapToken attribute (N/A) 30
6.2.3 Privilege attribute 30
6.2.4 Level of Assurance attribute 30
6.2.5 Identity Assurance Level attribute 30
6.2.6 Authentication Assurance Level attribute 31
6.2.7 Fullname attribute 31
6.2.8 Firstname attribute 31
6.2.9 Lastname attribute 31
6.2.10 Alias attribute 31
6.2.11 Email attribute 32
6.2.12 CPR attribute 32
6.2.13 Age attribute 32
6.2.14 CPR UUID 32
6.3 NATURAL PERSON PROFILE (N/A) 33
6.3.1 PID attribute (N/A) 33
6.4 PROFESSIONAL PERSON PROFILE 33
6.4.1 Persistent Identifier attribute (N/A) 33
6.4.2 RID number attribute (N/A) 33
6.4.3 CVR number attribute 33
6.4.4 Organization name attribute 34

6.4.5 Production unit attribute 34
6.4.6 SE Number attribute 34
6.4.7 Authorized to Represent 34
7 REFERENCES 36

1 Introduction

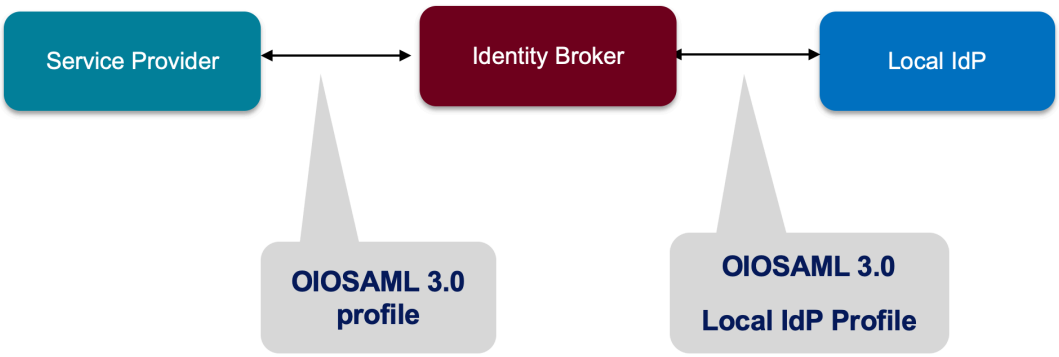
1.1 Preface

This SAML implementation profile ('OIOSAML Local IdP Profile') specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO Profile [SAML2Prof], and related profiles, are required or permitted to rely on. The document is aimed at developers and other technical resources who are involved in developing, configuring and testing implementations and the reader is assumed to be intimately familiar with the core SAML 2.0 specifications.

The OIOSAML profile is governed by the Danish Agency for Digitisation and questions surrounding the profile can be sent to: nemlogin@digst.dk. Future updates to the profile will be published at Digitaliser.dk[1] and Digst.dk where other related resources (including reference implementations of the profile) also can be found.

The current document is a sub-profile of OIOSAML 3.0.1 targeted for a special use case involving a **local Identity Provider** (or local IdP) authenticating professional users from one or more organizations towards an Identity Broker, which then brokers the identity towards the downstream Service Provider.

The use case is illustrated in the below figure:



This sub-profile inherits most requirement OIOSAML Web SSO profile 3.0 but specifies a few deviations.

All heading- and requirement numbers are kept from the original OIOSAML 3.0 profile in order to simplify comparisons and implementation. Furthermore, a few notational conventions are applied:

- Unchanged requirements from OIOSAML 3.0.1 are marked in green font.
- Requirements from OIOSAML 3.0.1 which are omitted are marked in red font, and the corresponding text is ~~striked out~~.

[1] https://www.digitaliser.dk/group/42063

- Requirements that are new or changed are marked in blue font.

1.2 Usage Scenarios

The profile is intended for use within Danish public sector federations where information about authenticated identities is communicated across organizations. The goal is to achieve standardization, interoperability, security and privacy, while enabling re-use of common implementations. OIOSAML will be the main interface for the public-sector Identity Broker in Denmark (NemLog-in3).

It should be noted, that the profile has been designed with flexibility in mind to e.g. allow individual sectors to define their own attribute profiles under OIOSAML. Thus, a delicate trade-off between interoperability and flexibility has been pursued.

2 Notation and terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`, **Datatype**, `OtherCode`. The normative requirements of this specification are individually labeled with a unique identifier in the following form: **[OIO-EXAMPLE-01]**. All information within these requirements should be considered normative unless it is set in *italic* type. Italicized text is non-normative and is intended to provide additional information that may be helpful in implementing the normative requirements.

2.1 References to SAML 2.0 specification

When referring to elements from the SAML 2.0 core specification [SAML2Core], the following syntax is used:

- `<samlp:ProtocolElement>` - for elements from the SAML 2.0 Protocol namespace.
- `<saml:AssertionElement>` - for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specification [SAML2Meta], the following syntax is used:

- `<md:MetadataElement>`

When referring to elements from the XML-Signature Syntax and Processing Version 1.1 WWWC Recommendation [XMLSig], the following syntax is used:

- `<ds:Element>`

2.2 Terminology

The abbreviations IdP and SP are used below to refer to Identity Providers and Service Providers in the sense of their usage within the SAML Browser SSO Profile and Single Logout profiles. A proxy-IdP will act in both roles i.e. as a SP towards the 'real' IdP and as IdP towards the 'real' SP.

Whether explicit or implicit, all the requirements listed in this document are meant to apply to deployments of SAML profiles and may involve explicit support for requirements by SAML-implementing software and/or supplemental support via ap-

plication code. Deployments of a Service Provider may refer to both stand-alone implementations of SAML, libraries integrated with an application, or any combination of the two. It is difficult to define a clear boundary between a Service Provider and the application/service it represents, and unnecessary to do so for the purposes of this document.

Note that all requirements for IdPs in this document should be understood as requirements for *local* IdPs, and all requirements for SPs should be understood as aimed for Identity Brokers who request authentication from the local IdP.

3 Common Requirements

This chapter includes material of general significance to both IdPs and SPs. Subsequent sections provide guidance specific to those roles.

3.1 General

3.1.1 Clock Skew

[OIO-GE-01]

Deployments MUST allow between three (3) and five (5) minutes of clock skew — in either direction — when interpreting `xsd:dateTime` values in assertions and when enforcing security policies based thereupon.

The following is a non-exhaustive list of items to which this directive applies: `NotBefore`, `NotOnOrAfter`, *and* `validUntil` *XML attributes found on*

`<saml:Conditions>`,

`<saml:SubjectConfirmationData>`,

`<samlp:LogoutRequest>`,

`<md:EntityDescriptor>`,

`<md:EntitiesDescriptor>`,

`<md:RoleDescriptor>`, *and*

`<md:AffiliationDescriptor>` *elements.*

3.1.2 Document Type Definitions

[OIO-GE-02]

Deployments MUST NOT produce any SAML protocol message that contains a Document Type Definition (DTD). Deployments SHOULD reject messages that contain them.

3.1.3 SAML entityIDs

[OIO-GE-03]

Deployments MUST be named via an absolute URI whose total length MUST NOT exceed 256 characters. To support having a well-known location from which metadata can be downloaded the Entity Identifier SHOULD be derived from the internet domain name of the Service Provider e.g.

`https://saml.[domain name]`

An entityID SHOULD be chosen in a manner that minimizes the likelihood of it changing for political or technical reasons, including for example a change to a different software implementation or hosting provider.

3.2 Metadata and Trust Management

3.2.1 Metadata Consumption and Use

[OIO-MD-01]

Deployments MUST provision their behavior in the following areas based solely on the consumption of SAML Metadata [SAML2Meta] the processing rules defined by the SAML Metadata Interoperability profile [SAML2MDIOP]:

- indications of support for Browser SSO and Single Logout profiles
- selection, determination, and verification of SAML endpoints and bindings
- determination of the trustworthiness of XML signing keys
- selection of XML Encryption keys

Metadata exchange mechanisms and establishment of trust in metadata are left to deployments to specify.

3.2.2 Metadata Production

[OIO-MD-02]

Deployments MUST have the ability to provide SAML metadata capturing their requirements and characteristics in the areas identified above in a secure fashion.

Metadata SHOULD NOT include content indicating support for profiles or features beyond the bounds of this profile.

3.2.2.1 Keys and Certificates

[OIO-MD-03]

Public keys used for signing and encryption MUST be expressed via X.509 certificates included in metadata via `<md:KeyDescriptor>` elements.

The certificates MUST be FOCES or VOCES certificates (issued under the OCES2 or OCES3 certificate policies)[2] or qualified certificates (according to the eIDAS regulation) issued to a legal person. Certificates MUST NOT be expired or revoked.

[2] https://www.nemid.nu/dk-da/om-nemid/historien_om_nemid/oces-standarden/oces-certifikatpolitikker/

[OIO-MD-04]

RSA public keys MUST be at least 2048 bits in length. At least 3072 bits is RECOMMENDED for new deployments.

[OIO-MD-05]

EC public keys MUST be at least 256 bits in length.

[OIO-MD-06]

By virtue of the profile's overall requirements, an IdP's metadata MUST include at least one signing certificate (that is, an `<md:KeyDescriptor>` with no `use` attribute or one set to `signing`), and an SP's metadata MUST include at least one signing certificate and one encryption certificate (that is, an `<md:KeyDescriptor>` with no `use` attribute or one set to `encryption`).

3.3 Cryptographic Algorithms

[OIO-ALG-01]

Deployments MUST support, and use, the following algorithms when communicating with peers in the context of this profile. Where multiple choices exist, any of the listed options may be used. The profile will be updated as necessary to reflect changes in government and industry recommendations regarding algorithm usage.

- Digest
  - http://www.w3.org/2001/04/xmlenc#sha256 [XMLEnc]
- Signature
  - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 [RFC4051]
  - http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 [RFC4051]
- Block Encryption
  - http://www.w3.org/2001/04/xmlenc#aes128-cbc [XMLEnc]
  - http://www.w3.org/2001/04/xmlenc#aes256-cbc [XMLEnc]
- Key Transport
  - http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p [XMLEnc]
  - http://www.w3.org/2009/xmlenc11#rsa-oaep [XMLEnc]

The following Block Encryption algorithms SHOULD be supported:

- http://www.w3.org/2009/xmlenc11#aes128-gcm [XMLEnc]
- http://www.w3.org/2009/xmlenc11#aes192-gcm [XMLEnc]
- http://www.w3.org/2009/xmlenc11#aes256-gcm [XMLEnc]

Note: The 'GCM' variants are more secure than the 'CBC' variants, which are allowed for backwards compatibility. The CBC variants may be deprecated in a future version of the profile.

4 SP Requirements

Note: in this profile, the SP should be understood as the central broker who requests authentication from the local Identity Provider.

4.1 Web Browser SSO

[OIO-SP-01]

SPs MUST support the Browser SSO Profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.

4.1.1 Requests

4.1.1.1 Binding

[OIO-SP-02]

The HTTP-Redirect binding [SAML2Bind] with deflate encoding MUST be used for the transmission of `<samlp:AuthnRequest>` messages.

[OIO-SP-03]

Requests MUST NOT be issued inside an HTML frame or via any mechanism that would require the use of third-party cookies by the IdP to establish or recover a session with the User Agent. This will typically imply that requests will involve a full-frame redirect, in order that the top-level window origin be associated with the IdP.

4.1.1.2 Request Content

[OIO-SP-04]

The `<samlp:AuthnRequest>` message SHOULD omit the `<samlp:NameIDPolicy>` element.

[OIO-SP-05]

The message SHOULD contain an `AssertionConsumerServiceURL` attribute and MUST NOT contain an `AssertionConsumerServiceIndex` attribute (i.e., the desired endpoint MUST be the default, or identified via the `AssertionConsumerServiceURL` attribute).

The `AssertionConsumerServiceURL` value, if present, MUST match an endpoint location expressed in the SP's metadata exactly, without requiring URL canonicalization/normalization.

As an example, the SP cannot specify URLs that include a port number (e.g., https://sp.example.com:443/acs) in its requests unless it also includes that port number in the URLs specified in its metadata, and vice versa.

4.1.1.3 *Authentication Contexts*

[OIO-SP-06]

The following `<saml:AuthnContextClassRef>` values MAY be used to request the desired [NSIS] assurance level, and if present, MUST be used with the Comparison attribute set to minimum:

```
https://data.gov.dk/concept/core/nsis/loa/Low
https://data.gov.dk/concept/core/nsis/loa/Substantial
https://data.gov.dk/concept/core/nsis/loa/High
```

Note the implicit hierarchy between these levels.

Note also that use of the above [NSIS] identifiers for LoA (Level of Assurance) requires that the implementation adheres to NSIS requirements for the given level and has been notified to the Danish Agency for Digitisation.

Example:

```
<saml2p:RequestedAuthnContext Comparison="minimum">
   <saml2:AuthnContextClassRef xmlns:saml2="urn:oa-
sis:names:tc:SAML:2.0:assertion">

https://data.gov.dk/concept/core/nsis/loa/Substantial
   </saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

Note that if the SP (i.e. identity broker) has out-of-band knowledge that the IdP implementation (e.g. Microsoft AD FS) does not support the above authentication context class references, it can be omitted, and the information provided by a RelayState parameter or some other mechanism supported by the IdP.

When using RelayState for requesting a specific LoA, the following JSON syntax SHOULD be used:

```
{
  "NSISLevelOfAssurance":
  "https://data.gov.dk/concept/core/nsis/loa/Substantial"
}
```

The JSON structure SHOULD be converted to UTF8 bytes and subsequently Base64-encoded, and the result used as the value of the RelayState. Note also, that RelayState may be used for other purposes (see [OIO-SP-07]). In this case, the combined JSON structure is Base64 encoded.

[OIO-SP-07]

The following `<saml:AuthnContextClassRef>` values MAY be used to request the desired attribute profile (see chapter 6 for attribute profiles):

```
https://data.gov.dk/eid/Person
https://data.gov.dk/eid/Professional
```

Note that if the SP (i.e. identity broker) has out-of-band knowledge that the IdP does not support this element, it can be omitted, and the information provided by a RelayState parameter or some other mechanism supported by the IdP.

When using RelayState for requesting a specific LoA, the following JSON syntax SHOULD be used:

```
{
  "IdentityType": "https://data.gov.dk/eid/Professional"
}
```

The JSON structure SHOULD be converted to UTF8 bytes and subsequently Base64-encoded, and the result used as the value of the RelayState. Note also, that RelayState may be used for other purposes (see [OIO-SP-06]).

Note: the comparison attribute mentioned above in [OIO-SP-06] does not apply to the attribute profile but only the assurance level.

4.1.1.4 Signed Requests

[OIO-SP-08]

Requests MUST be signed by the SP using a private key defined in their metadata.

Note: Since HTTP Redirect binding with DEFLATE encoding is used, the signature is located in the "Signature" query string described by this binding instead of in the request XML message.

4.1.1.5 Proxy IdPs

[OIO-SP-09]

If the SP is in fact a proxy IdP acting on behalf of another SP, the service provider SHOULD include a `<Scoping>` element in the `<AuthnRequest>` containing a `<RequesterID>` element stating the Service Provider Identity uniquely. The RequesterID MUST uniquely identify the real service provider.

Example:

```
<samlp:Scoping>
      <samlp:RequesterID>https://saml.sundhed.dk
      </samlp:RequesterID>
</samlp:Scoping>
```

Note that if the SP (i.e. identity broker) has out-of-band knowledge that the IdP does not support this element, it can be omitted, and the information provided by a RelayState parameter or some other mechanism supported by the IdP.

When using the RelayState alternative, the following JSON syntax SHOULD be used:

```
{
  "RequesterID": "https://saml.sundhed.dk"
}
```

See also RelayState usage in [OIO-SP-06] and [OIO-SP-07].

4.1.2 Responses

4.1.2.1 Binding

[OIO-SP-10]

SPs MUST support the HTTP-POST binding for the receipt of `<samlp:Response>` messages. Support for other bindings is OPTIONAL.

[OIO-SP-11]

The endpoint(s) at which an SP supports receipt of `<samlp:Response>` messages MUST be protected by TLS 1.2 or higher.

4.1.2.2 XML Encryption

[OIO-SP-12]

SPs MUST support decryption of `<saml:EncryptedAssertion>` elements. Support for other encrypted constructs is OPTIONAL.

4.1.2.3 Error Handling

[OIO-SP-13]

SPs MUST gracefully handle error responses containing `<samlp:StatusCode>` other than `urn:oasis:names:tc:SAML:2.0:status:Success`.

[OIO-SP-14]

The response to such errors MUST direct users to appropriate support resources offered by the SP.

4.1.2.4 Forced Re-Authentication

[OIO-SP-15]

SPs that include a `ForceAuthn` attribute of `true` in their requests SHOULD test the currency of the `AuthnInstant` element in the received assertions

to verify the currency of the authentication event.

4.1.3 LoA check

[OIO-SP-16]

When consuming SAML Assertions, SPs MUST check the specified [NSIS] level of assurance regardless of any LoA was set in the request. See section 6.2.4 where the attribute is defined.

Note: SPs are not guaranteed that the IdP can or will honor the requested assurance level set in the `<AuthnRequest>`.

4.1.4 Discovery

[OIO-SP-17]

~~SPs SHOULD support the Identity Provider Discovery Profile described in [SAML2Prof] which enables a Service Provider to discover which Identity Providers a principal is using with the web browser SSO profile.~~

~~*Note: The profile relies on a cookie that is written in a domain common between Identity Providers and Service Providers in a deployment. The cookie contains a list of Identity Provider identifiers and the most recently used IdP should be at the end of the list.*~~

4.2 Single Logout

[OIO-SP-18]

SPs MUST support the Single Logout Profile [SAML2Prof], as updated by the Approved Errata [SAML2Err]. The following requirements apply in the case of such support.

4.2.1 Requests

4.2.1.1 Binding

[OIO-SP-19]

The HTTP-Redirect binding [SAML2Bind] MUST be used for the transmission of (the initial) `<samlp:LogoutRequest>` messages to the IdP.

[OIO-SP-20]

SPs MUST support the HTTP-Redirect or HTTP-POST [SAML2Bind] binding for the receipt of `<samlp:LogoutRequest>` messages from the IdP, and MAY support SOAP binding.

[OIO-SP-21]

Requests MUST NOT be issued inside an HTML frame or via any mechanism that would require the use of third-party cookies by the IdP to establish or recover a session with the User Agent. This will typically imply that requests

must involve a full-frame redirect, in order that the top level window origin be associated with the IdP.

Note: The full-frame requirement is also necessary to ensure that full control of the user interface is released to the IdP.

4.2.1.2 Request Content

[OIO-SP-22]

Logout Requests MUST be signed.

[OIO-SP-23]

The `<saml:NameID>` element included in `<samlp:LogoutRequest>` messages MUST exactly match the corresponding element received from the IdP, including its element content and all XML attributes included therein.

[OIO-SP-24]

The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted[3].

4.2.2 Responses

4.2.2.1 Binding

[OIO-SP-25]

The HTTP-Redirect, HTTP-POST or SOAP binding [SAML2Bind] MUST be used for the transmission of `<samlp:LogoutResponse>` messages to the IdP.

[OIO-SP-26]

SPs MUST support the HTTP-Redirect or HTTP-POST binding [SAML2Bind] binding for the receipt of `<samlp:LogoutResponse>` messages from the IdP (to the initial request).

4.2.2.2 Response Content

[OIO-SP-27]

Responses MUST be signed.

4.2.3 Behavioral Requirements

[OIO-SP-28]

SPs MUST terminate any local session before issuing a `<samlp:LogoutRequest>` message to the IdP.

[3] Due to interoperability concerns.

Note: This ensures the safest possible result for subjects in the event that logout fails for some reason.

[OIO-SP-29]

SPs MUST NOT issue a `<samlp:LogoutRequest>` message as the result of an idle activity timeout.

Note: Timeout of a single application/service must not trigger logout of an SSO session because this imposes a single service's requirements on an entire IdP deployment. Applications with sensitivity requirements should consider other mechanisms, such as the `ForceAuthn` attribute, to achieve their goals.

4.2.4 Logout and Virtual Hosting

[OIO-SP-30]

An SP that maintains distinct sessions across multiple virtual hosts SHOULD identify itself by means of a distinct entityID (with associated metadata) for each virtual host.

Note: A single entity can have only one well-defined `<SingleLogoutService>` endpoint per binding. Cookies are typically host-based and logout cannot typically be implemented easily across virtual hosts. Unlike during SSO, a `<samlp:LogoutRequest>` message cannot specify a particular response endpoint, so this scenario is generally not viable.

4.3 Metadata and Trust Management

4.3.1 Support for Multiple Keys

The ability to perform seamless key migration depends upon proper support for consuming and/or leveraging multiple keys at the same time.

[OIO-SP-31]

SP deployments SHOULD support multiple signing certificates in IdP metadata and MUST support validation of XML signatures using a key from any of them.

[OIO-SP-32]

SP deployments SHOULD be able to support multiple decryption keys and MUST be able to decrypt `<saml:EncryptedAssertion>` elements encrypted with any configured key.

4.3.2 Metadata Content

[OIO-SP-33]

By virtue of this profile's requirements, an SP's metadata MUST contain:

- an `<md:SPSSODescriptor>` role element
  - at least one `<md:AssertionConsumerService>` endpoint element
  - at least one `<md:KeyDescriptor>` element whose `use` attribute is set to `encryption`
  - at least one `<md:KeyDescriptor>` element whose `use` attribute is set to `signing`
  - exactly one `<md:NameIDFormat>` element within their `<md:SPSSODescriptor>` element containing
    - `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
      indicating a persistent (SP-specific) identifier
  - at least one `<md:SingleLogoutService>` endpoint element

In addition, an SP's metadata SHOULD contain:

- an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

5 IdP Requirements

5.1 Web Browser SSO

[OIO-IDP-01]

IdPs MUST support the Web Browser SSO Profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.

5.1.1 Requests

5.1.1.1 Binding

[OIO-IDP-02]

IdPs MUST support the HTTP-Redirect binding [SAML2Bind] for the receipt of `<samlp:AuthnRequest>` messages.

[OIO-IDP-03]

All IdP endpoints (including at which an IdP supports receipt of `<samlp:AuthnRequest>` messages) MUST be protected by TLS 1.2 or higher.

5.1.1.2 Endpoint Verification

[OIO-IDP-04]

IdPs MUST verify the `AssertionConsumerServiceURL` supplied in an SP's `<samlp:AuthnRequest>` (if any) against the `<md:AssertionConsumerService>` elements in the SP's metadata. In the absence of such a value, the default endpoint from the SP's metadata MUST be used for the response.

When verifying the `AssertionConsumerServiceURL`, it is RECOMMENDED that the IdP perform a case-sensitive string comparison between the requested value and the values found in the SP's metadata. It is OPTIONAL to apply any form of URL canonicalization.

5.1.1.3 Signing

[OIO-IDP-05]

IdPs MUST verify the request signature according to a certificate found in SP metadata or fail the request.

[OIO-IDP-06]

IdPs MUST reject unsigned requests.

5.1.1.4 Forced Re-Authentication

[OIO-IDP-07]

IdPs MUST ensure that any response to a `<samlp:AuthnRequest>` that contains the attribute `ForceAuthn` set to `true` or `1` results in an authentication challenge that requires proof that the subject is present. If this condition is met, the IdP MUST also reflect this by setting the value of the `AuthnInstant` value in the assertion it returns to a fresh value.

If an IdP cannot prove subject presence, then it MUST fail the request and SHOULD respond to the SP with a SAML error status.

5.1.1.5 Passive Authentication

[OIO-IDP-08]

IdPs MUST understand and respect the `IsPassive` attribute on requests. If the `IsPassive` attribute is set and control of the user interface is needed to complete an authentication, the following status code MUST be returned `urn:oasis:names:tc:SAML:2.0:status:NoPassive`.

Note: The NoPassive error can occur if the IdP does not have a session with the user, if the IdP has a session but at a lower LoA than requested by the SP, or if the IdP policy requires active user consent prior to attribute release.

5.1.2 Responses

5.1.2.1 Binding

[OIO-IDP-09]

IdPs MUST support the HTTP-POST binding [SAML2Bind] for the transmission of `<samlp:Response>` messages.

5.1.2.2 Response Content

[OIO-IDP-10]

Successful responses SHOULD NOT be directly signed.

Note: Instead, Assertions are signed (see below).

[OIO-IDP-11]

Successful responses MUST contain exactly one SAML `<saml:Assertion>`, and the assertion MUST contain exactly one `<saml:AuthnStatement>` sub-element and exactly one `<saml:AttributeStatement>` sub-element. The `<saml:AttributeStatement>` sub-element MUST conform to one of the attribute profiles for natural persons or professionals as described in chapter 6 including all mandatory attributes.

All other statements MUST NOT be used.

[OIO-IDP-12]

The <saml:Assertion> within the response MUST be directly signed by the IdP.

[OIO-IDP-13]

Assertions transferred via the user agent MUST be encrypted and transmitted via a <saml:EncryptedAssertion> element. Information intended for the consumption of the SP MUST NOT be further encrypted via <saml:EncryptedID> or <saml:EncryptedAttribute> constructs.

5.1.3 Issuer

[OIO-IDP-14]

Assertions MUST contain an <Issuer> element uniquely identifying the IdP. The Format attribute MUST be omitted or have a value of

```
urn:oasis:names:tc:SAML:2.0:nameid-format:entity
```

See also section 3.1.3 on EntityIDs.

5.1.4 Subject Identifiers

[OIO-IDP-15]

Assertions MUST contain one <saml:Subject> element with a <saml:NameID> element which uniquely represents the Subject within the context of the organization (as represented by the CVR number attribute). The identifier SHOULD be unique over time.

All SAML NameID Format types excluding urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted MAY be used.

[OIO-IDP-16]

~~The <saml:NameID> identifier MUST be generated as an persistent or transient identifier by the IdP according to preferences specified in SP metadata (see section 4.3.2).~~

5.1.5 Subject Confirmation

[OIO-IDP-17]

The Subject element MUST contain at least one <SubjectConfirmation> element specifying a conformation method of urn:oasis:names:tc:SAML:2.0:cm:bearer.

The bearer `<SubjectConfirmation>` element described above MUST contain a `<SubjectConfirmationData>` element that has a Recipient attribute containing the Service Provider's assertion consumer service URL and a NotOnOrAfter attribute that limits the window during which the assertion can be delivered. It MAY contain a NotBefore attribute but the receiver is not required to process it.

5.1.6 Audience Restriction

[OIO-IDP-18]

The assertion MUST contain an `<AudienceRestriction>` including the Service Provider's unique identifier as an `<Audience>`.

5.1.7 Discovery via common domain

[OIO-IDP-19]

~~IdPs SHOULD support the Identity Provider Discovery Profile described in [SAMLProf] which enables a Service Provider to discover which Identity Providers a principal is using with the web browser SSO profile.~~

~~A cookie SHOULD be written in a domain common between Identity Providers and Service Providers in a deployment. The cookie contains a list of Identity Provider identifiers and the most recently used IdP SHOULD be at the end of the list.~~

5.2 Single Logout

[OIO-IDP-20]

IdPs MUST support the Single Logout Profile [SAML2Prof], as updated by the Approved Errata [SAML2Err], with behavior, capabilities, and options consistent with the additional constraints specified in this section.

The term "IdP session" is used to refer to the ongoing state between the IdP and its clients allowing for SSO. Support for logout implies supporting termination of a subject's IdP session in response to receiving a `<samlp:LogoutRequest>` *or upon some administrative signal.*

Note that this only involves eliminating the browser session and does not extend to an underlying session with a local domain (e.g. Kerberos).

[OIO-IDP-21]

IdPs MUST support the propagation of logout signaling to SPs using HTTP-Redirect and HTTP-POST Binding [SAML2Bind]. The binding selected for a specific SP should be based on the SP capabilities as defined in its metadata.

5.2.1 Requests

5.2.1.1 Binding

[OIO-IDP-22]

IdPs MUST support the HTTP-Redirect [SAML2Bind] binding for the receipt of (the initial) `<samlp:LogoutRequest>` message.

Note that SOAP binding is not allowed for the initial message, since the IdP would not be able to propagate the request to SPs only supporting front-channel bindings.

5.2.2 Request Content

[OIO-IDP-23]

Logout Requests MUST be signed.

[OIO-IDP-24]

The `<saml:NameID>` element in `<samlp:LogoutRequest>` messages MUST NOT be encrypted[4].

5.2.3 Responses

5.2.3.1 Binding

[OIO-IDP-25]

[4] Due to interoperability concerns.

The IdP SHOULD respond to requests using the same binding used in the request from the initiating SP.

5.2.3.2 Response Content

[OIO-IDP-26]

Logout Responses MUST be signed (with a mechanism according to the selected Binding).

[OIO-IDP-27]

The `<samlp:StatusCode>` in the response issued by the IdP MUST reflect whether the IdP session was successfully terminated.

5.3 Attribute Query

~~This chapter specifies an attribute service profile for querying attributes from an Attribute Service (often part of an Identity Provider). It is used in scenarios where a Service Provider after the initial authentication of the user needs further information e.g. in order to grant access to a resource or personalize an application. The attribute query profile can further enhance end-user privacy in scenarios where an SP initially only needs a few attributes during authentication and then later queries for more attributes if the need emerges (instead of getting all attributes that are potentially required up front).~~

[OIO-IDP-28]

~~An IdP SHOULD offer all its attributes to authorized Service Providers via a SAML `<AttributeQuery>` interface.~~

[OIO-IDP-29]

~~The SAML SOAP Binding SHOULD be used for the interface and the endpoint MUST be protected by TLS 1.2 or higher.~~

5.3.1 Request Message

[OIO-IDP-30]

~~The request message MUST contain a Consent attribute and an `<Issuer>` element matching a registered SP. The IdP SHOULD define a policy setting SP obligations regarding collection of end-user consent or other legal basis for requesting attributes.~~

[OIO-IDP-31]

~~The request message MUST uniquely identify the Subject using an identifier specified by the Attribute Service Provider.~~

[OIO-IDP-32]

~~The Attribute Service MUST verify that the request message is signed by the SP with a key corresponding to a certificate found in SP metadata.~~

5.3.2 Response Message

[OIO-IDP-33]

~~A successful response MUST be in the form of an Assertion containing exactly one attribute statement. Naming and encoding of attributes MUST be the same as specified for Web SSO, see chapter 6 for details.~~

[OIO-IDP-34]

~~A successful response MUST contain an `<Issuer>` element.~~

[OIO-IDP-35]

~~A successful response MUST NOT contain an `<AuthnStatement>` element or `<AuthzDecisionStatement>`.~~

[OIO-IDP-36]

~~The Assertion in the response MUST be signed by the IdP with a key corresponding to a certificate found in IdP metadata.~~

5.3.3 Error handling

[OIO-IDP-37]

~~If the IdP cannot identify the Subject stated in the request, it MUST return an error response with a second-level status code set to `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal`~~

[OIO-IDP-38]

~~The top-level error code SHOULD be set to "Success" if any of the requested attributes can be returned; otherwise it SHOULD be set to `urn:oasis:names:tc:SAML:2.0:status:Requester`.~~

~~If attributes are unknown, a nested status code element SHOULD be included specifying a status code of `urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue`~~

~~A sequence of `<StatusDetail>` elements SHOULD further be included, one per unknown attribute, specifying the name of the unknown attribute to the requester.~~

[OIO-IDP-39]

~~If Attributes are requested which the Attribute Service does not want to disclose to the requestor according to its attribute release policy, the Attribute Service SHOULD return a second-level status code being:~~

~~urn:oasis:names:tc:SAML:2.0:status:RequestDenied followed by a sequence <StatusDetail> elements describing the reason for not disclosing the attribute.~~

5.4 Metadata and Trust Management

5.4.1 Support for Multiple Keys

~~The ability to perform seamless key migration depends upon proper support for consuming and/or leveraging multiple keys at the same time.~~

[OIO-IDP-40]

~~IdP deployments MUST support multiple signing and encryption certificates in SP metadata and MUST support validation of signatures using a key from any of them.~~

5.4.2 Metadata Content

[OIO-IDP-41]

By virtue of this profile's requirements, an IdP's metadata MUST contain:

- an `<md:IDPSSODescriptor>` role element
  - at least one `<md:SingleSignOnService>` endpoint element
  - at least one `<md:SingleLogoutService>` endpoint element
  - at least one `<md:KeyDescriptor>` element whose use attribute is set to `signing` and
  - at least one `<md:KeyDescriptor>` element whose use attribute is set to `encryption`

In addition, an IdP's metadata MUST contain:

- an `<md:ContactPerson>` element with a `contactType` of `technical` and an `<md:EmailAddress>` element

[OIO-IDP-42]

~~If an IdP offers an AttributeQuery interface it SHOULD declare the offered attributes in metadata via an <AttributeAuthorityDescriptor> element.~~

6 Attribute profiles

This local IdP profile only deals with identities representing professional persons and their attributes. Local IdP's are not allowed to authenticate natural persons.

6.1 General requirements

[OIO-AP-01]

If an attribute is marked as Mandatory in the tables below, it MUST be present in all Assertions. Identity Providers MAY include additional attributes (e.g. sector-specific attributes).

Only a small subset of the (non-identifying) attributes are Mandatory in order to comply with the data minimization principle.

[OIO-AP-02]

~~The actual set of attributes in an Assertion SHOULD only contain attributes needed by the SP as specified in the SP metadata. An IdP MAY define policies that restrict which attributes SPs can get and it MAY ask the end-user for consent and use this for limiting the released attribute set.~~

[OIO-AP-03]

`<saml:Attribute>` elements MUST contain a NameFormat of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

This requirement ensures unique, non-conflicting naming of Attributes even in cases involving custom requirements for which no standard Attributes may exist.

[OIO-AP-04]

All attribute values SHOULD if possible be simple text strings with type `xs:string`.

It is RECOMMENDED that the content of each `<saml:AttributeValue>` element be limited to a single child text node (i.e. a simple string value) and that multiple values of an `<saml:Attribute>` be expressed as individual `<saml:AttributeValue>` elements rather than embedded in a delimited form within a single element.

Note that this refers to `<saml:AttributeValue>` elements, not `<saml:Attribute>` elements, and refers to the form of each individual value. It discourages the use of complex XML content models within the value of an Attribute. For this reason, the OIO Basic Privilege Profile base64 encodes complex attribute values.

6.2 Common attributes

This section specifies common attributes shared by subsequent attribute profiles. Note: only the 'professional' profile from OIOSAML 3.0 is supported in this profile, but the structure is kept for easy comparison.

6.2.1 SpecVer attribute

ID	https://data.gov.dk/model/core/specVersion
Description	Specifies the version of the OIOSAML profile specification - the current version is shown in example below.
Mandatory	Yes
Example	`<AttributeValue>OIO-SAML-3.0</AttributeValue>`

6.2.2 BootstrapToken attribute (N/A)

6.2.3 Privilege attribute

ID	https://data.gov.dk/model/core/eid/privilegesIntermediate
Description	Contains a base64-encoded value describing privileges assigned to the identity (see OIO Basic Privilege Profile specification [OIOBPP] for details).
Mandatory	No
Example	`<AttributeValue>AK24bWw...</AttributeValue>`

Further profiling of the privilege attribute is left to specific deployments.

6.2.4 Level of Assurance attribute

ID	https://data.gov.dk/concept/core/nsis/loa
Description	Contains the overall level of assurance of the authentication as defined by the Danish [NSIS] standard. The allowed values are 'Low', 'Substantial' and 'High'.
Mandatory	Yes
Example	`<AttributeValue>Substantial</AttributeValue>`

6.2.5 Identity Assurance Level attribute

ID	https://data.gov.dk/concept/core/nsis/ial
Description	Contains Identity Assurance Level (IAL) as defined by the Danish [NSIS] standard. The allowed values are 'Low', 'Substantial' and 'High'.
Mandatory	No

Example	`<AttributeValue>Substantial</AttributeValue>`

6.2.6 Authentication Assurance Level attribute

ID	https://data.gov.dk/concept/core/nsis/aal
Description	Contains Authenticator Assurance Level (AAL) as defined by the Danish [NSIS] standard. The allowed values are 'Low', 'Substantial' and 'High'.
Mandatory	No
Example	`<AttributeValue>High</AttributeValue>`

6.2.7 Fullname attribute

ID	https://data.gov.dk/model/core/eid/fullName
Description	Contains the full name.
Mandatory	No
Example	`<AttributeValue>Knud Erik Jensen</AttributeValue>`

6.2.8 Firstname attribute

ID	https://data.gov.dk/model/core/eid/firstName
Description	Contains the first name(s) of the identity. In case the person has multiple first names, one or more of these MUST be present. Middlenames are not allowed.
Mandatory	No
Example	`<AttributeValue>Knud</AttributeValue>`

6.2.9 Lastname attribute

ID	https://data.gov.dk/model/core/eid/lastName
Description	Contains the last name of the identity.
Mandatory	No
Example	`<AttributeValue>Jensen</AttributeValue>`

6.2.10 Alias attribute

ID	https://data.gov.dk/model/core/eid/alias

Description	Contains an alias of the identity. This attribute can be used as a display name selected by the user as an alternative to the above name attributes.
Mandatory	No
Example	`<AttributeValue>Bubber</AttributeValue>`

6.2.11 Email attribute

ID	https://data.gov.dk/model/core/eid/email
Description	Contains the email address of the identity. In cases there are multiple addresses known this attribute can be multi-valued (i.e. using multiple `<AttributeValue>` elements).
Mandatory	No
Example	`<AttributeValue>knud@jensen.dk</AttributeValue>`

6.2.12 CPR attribute

ID	https://data.gov.dk/model/core/eid/cprNumber
Description	Contains the Danish CPR number represented by 10 digits.
Mandatory	No
Example	`<AttributeValue>2702681273</AttributeValue>`

6.2.13 Age attribute

ID	https://data.gov.dk/model/core/eid/age
Description	Contains the age represented by an integer.
Mandatory	No
Example	`<AttributeValue>38</AttributeValue>`

6.2.14 CPR UUID

ID	https://data.gov.dk/model/core/eid/cprUuid
Description	Contains the central UUID for the person defined by the Danish Civil Registration Authority. This identifier is expected to replace the 10-digit CPR number.
Mandatory	No
Example	`<AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>`

6.3 Natural Person profile (N/A)

Natural person identities are not in scope within this profile.

6.3.1 PID attribute (N/A)

6.4 Professional Person profile

Identities representing professionals are described using the common attributes and the below attributes:

6.4.1 Persistent Identifier attribute (N/A)

ID	~~https://data.gov.dk/model/core/eid/professional/uuid/persistent~~
~~*Description*~~	~~Contains a UUID for the professional identity which is shared across all public sector SPs. The identifier is specific to the professional role and is **not** related to the associated natural person. The UUID MUST follow RFC 4122. This attribute is the successor to the RID attribute (see below) but is globally unique.~~
~~*Mandatory*~~	~~No~~
~~*Example*~~	~~`<AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>`~~

6.4.2 RID number attribute (N/A)

~~*ID*~~	~~https://data.gov.dk/model/core/eid/ professional/rid~~
~~*Description*~~	~~Contains the legacy RID number used in OCES infrastructure. Note: this attribute is deprecated and SPs MUST make plans for phasing out any dependencies on this.~~
~~*Mandatory*~~	~~No~~
~~*Example*~~	~~`<AttributeValue>98023728</AttributeValue>`~~

6.4.3 CVR number attribute

Note that a local IdP MUST ONLY authenticate users from organizations which have explicitly approved the IdP to authenticate their users.

ID	https://data.gov.dk/model/core/eid/professional/cvr
Description	Contains the CVR number (8 digits) of the organization related to the authentication context. Note that a professional may be associated with several organizations but only one organization is allowed per authentication context[5].

[5] I.e. the SAML Assertion only contains one relation to an organization used in the specific context.

Mandatory	Yes
Example	`<AttributeValue>20301823</AttributeValue>`

6.4.4 Organization name attribute

ID	https://data.gov.dk/model/core/eid/professional/orgName
Description	Contains the name of the organization related to the authentication context. Note that a professional may be associated with several organizations but only one organization is allowed per authentication context.
Mandatory	Yes
Example	`<AttributeValue>Digitaliseringsstyrelsen </AttributeValue>`

6.4.5 Production unit attribute

ID	https://data.gov.dk/model/core/eid/ professional/productionUnit
Description	Contains the Production Unit identifier (10 digits) which the professional is associated to within the organization related to the authentication context.
Mandatory	No
Example	`<AttributeValue>4234675432</AttributeValue>`

6.4.6 SE Number attribute

ID	https://data.gov.dk/model/core/eid/professional/seNumber
Description	Contains the SE number identifier (8 digits) which the professional is associated to within the organization related to the authentication context.
Mandatory	No
Example	`<AttributeValue>42346754</AttributeValue>`

6.4.7 Authorized to Represent

A local IdP MUST NOT include this attribute in Assertions – and it MUST be rejected by the receiving SP (Identity Broker).

~~*ID*~~	~~https://data.gov.dk/model/core/eid/professional/authorizedToRepresent~~
~~*Description*~~	~~Contains the CVR number(s) of an organization, if the professional is allowed to fully represent the organization with respect to public sec-~~

	~~tor services. In other words, the professional has a strong legal binding to the organizations[6] – the type of binding will depend on type of organization. If more organizations can be fully represented the IdP MAY include multiple <AttributeValue> elements.~~
~~*Mandatory*~~	~~No~~
~~*Example*~~	~~<AttributeValue>10346754</AttributeValue>~~

[6] This can e.g. be an authorized signatory ('tegningsberettiget') for a company (Danish 'selskab' such as IVS, ApS, A/S, P/S) or a fully responsible participant ('fuldt ansvarlig deltager') in other types of companies such as proprietorships.

7 References

- [eIDAS] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF
- [REF-ARK] Fællesoffentlig referencearkitektur for brugerstyring. https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring
- [NSIS] National Standard for Identiteters Sikringsniveauer version 2.0.1. https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/nsis-standarden/
- [OIOBPP] OIO Basic Privilege Profile. https://www.digitaliser.dk/resource/2377872
- [OIOIDWS] OIO Identity Based Web Services https://www.digitaliser.dk/resource/3457606
- [RFC2119] IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997. http://www.ietf.org/rfc/rfc2119.txt
- [RFC8174] IETF RFC 8174, Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, May 2017. http://www.ietf.org/rfc/rfc8174.txt
- [RFC4051] IETF RFC 4051, Additional XML Security Uniform Resource Identifiers, April 2005. https://www.ietf.org/rfc/rfc4051.txt
- [SAML2Core] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- [SAML2Bind] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
- [SAML2Int] SAML V2.0 Deployment Profile for Federation Interoperability. Kantara Inititive, https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
- [SAML2Prof] OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- [SAML2Meta] OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
- [X500SAMLattr] OASIS Committee Specification, SAML V2.0 X.500/LDAP Attribute Profile, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500-cs-01.pdf

- [SAML2MDIOP] OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf
- [IdPDisco] OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf
- [SAML2Err] OASIS Approved Errata, SAML Version 2.0 Errata 05, May 2012. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf
- [XMLEnc] D. Eastlake et al. XML Encryption Syntax and Processing. W3C Recommendation, April 2013. https://www.w3.org/TR/xmlenc-core1/
- [XMLSig] D. Eastlake et al. XML-Signature Syntax and Processing, Version 1.1. W3C Recommendation, April 2013. https://www.w3.org/TR/xmldsig-core1/
- [SAML2ASLO] OASIS Committee Specification, SAML V2.0 Asynchronous Single Logout Profile Extension Version 1.0, November 2012. http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.pdf
- [MetaUI] OASIS Committee Specification, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, April 2012. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/cs01/sstc-saml-metadata-ui-v1.0-cs01.pdf
- [MetaAttr] OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf