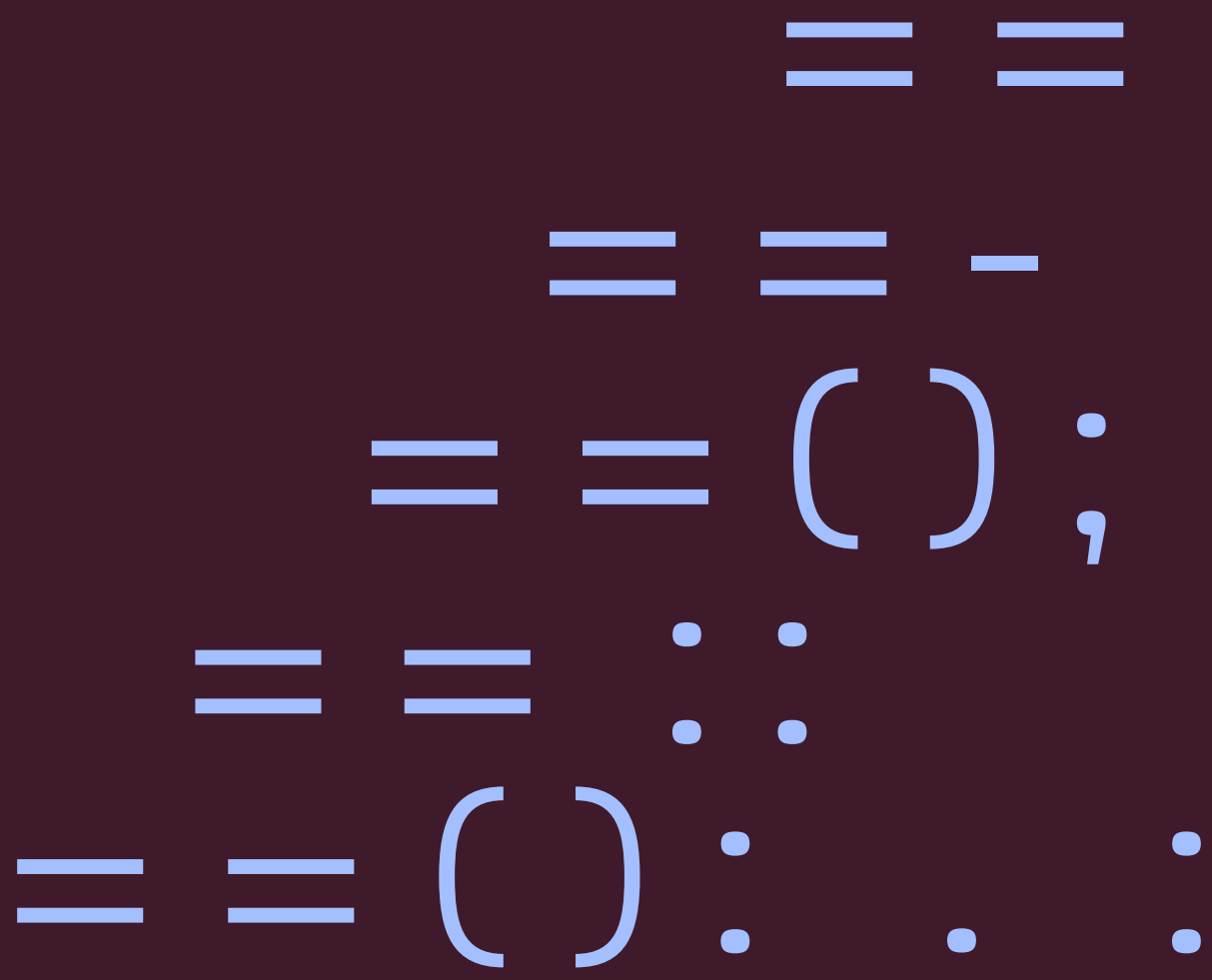
Digitaliserings-
styrelsen

Web SSO Profile 4.0.0

OIOSAML 4 profil

Høringsversion



November 24

Indhold

1. Introduction

1.1 Preface

This SAML implementation profile ('OIOSAML Web SSO 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 Digital Government and questions about the profile can be sent to nemlogin@digst.dk. Updates to the profile will be published at Digst.dk[1] where other related resources (including reference implementations of the profile) can also be found.

Version 3 of the profile was to a large degree inspired by the [SAML2Int] profile to leverage the large amount of experience put into this profile, to maximize interoperability, allow easier comparison with international profiles and ease implementation.

Version 4 adds new attribute profiles including explicit naming and handling of attribute profiles. The goal is to enable Danish service providers to easily consume multiple different types of identities via the same broker integration and further to enable identity brokers to perform orchestration of multiple up-stream IdP's in accordance with the service provider's policies and requirements. This enables an ecosystem where different service providers support different types of identities at different levels of assurance.

The requirements specified are in addition to all normative requirements of the underlying Web Browser SSO and Single Logout profiles [SAML2Prof], as modified by the Approved Errata [SAML2Err], and readers are assumed to be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

Nothing in this profile should be taken to imply that disclosing personally identifiable information, or indeed any information, is required from an Identity Provider (IdP) with respect to any particular Service Provider (SP). Such privacy considerations remain at the discretion of applicable settings, user consent, or other appropriate means in accordance with regulations and policies. However, this profile does obligate IdPs to honor certain key signals from an SP in the area of subject identification and requires successful responses to include specific SAML Attributes under certain conditions.

Note that SAML features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

[1] https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

1.2 Usage Scenarios

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

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 attempted.

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 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 application 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.

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.

[OIO-MD-04]

RSA public keys MUST be at least 3072 in length.

[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 only use the following algorithms when communicating with peers in the context of this profile. Where multiple options exist, any of the these may be used, and the chosen algorithm should be agreed upon via metadata or similar. 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]

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

    - 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]
- Key Transport
    - http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p [XMLEnc]
    - http://www.w3.org/2009/xmlenc11#rsa-oaep [XMLEnc]

Note: For block encryption 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

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 or 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 and accepted by the Danish Agency for Digitalization.

Example:

```
<saml2p:RequestedAuthnContext Comparison="minimum">

     <saml2:AuthnContextClassRefxmlns:saml2="urn:oasis:names:tc:SAML:2
.0:assertion">

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

</saml2p:RequestedAuthnContext>
```

[OIO-SP-07]

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

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

`https://data.gov.dk/eid/Person/DK/WithoutCPR`

`https://data.gov.dk/eid/Person/DK/Anonymous`

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

`https://data.gov.dk/eid/Professional/DK/Anonymous`

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

`https://data.gov.dk/eid/LegalPerson/EU`

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

Note:

- *An SP may request zero or more attribute profiles per request by including zero or more* `<saml:AuthnContextClassRef>` *elements. If more than one profile is requested and eligible, the IdP may choose which one to return based on IdP policy or out-of-band agreement with the SP.*
- *An SP or IdP is not required to support all of the above attribute profiles.*
- *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 `<AuthnRequest>` MUST contain a `ProviderName` attribute which describes the 'real' SP behind the proxy. The description MUST be user-friendly and informative such that it can be displayed in a log-in-client to inform the user about which service they are about to authenticate with. The attribute SHOULD be base64 encoded.

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] or eIDAS level of assurance regardless of any LoA was set in the request. See section 6 where the LoA attributes are 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 re-quest).

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.

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.

[3] Due to interoperability concerns

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 either
    - `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

      indicating a fresh/transient identifier per authentication or

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

indicating a persistent (SP-specific) identifier

- at least one `<md:SingleLogoutService>` endpoint element

[OIO-SP-34]

The SP's metadata SHOULD specify compliance with this profile by including the URI `https://data.gov.dk/saml/profile/oio/4` in the `protocolSupportEnumeration` attribute in `<md:SPSSODescriptor>` as shown below.

```
<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:metadata
https://data.gov.dk/saml/profile/oio/4">

…

</md:SPSSODescriptor>
```

[OIO-SP-35]

The SP's metadata SHOULD specify support for a set of attribute profiles by adding these as relevant values when requesting the attribute profile attribute. For example:

```
<md:RequestedAttribute

      Name=https://data.gov.dk/concept/core/eid/profile

      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

          <saml:AttributeValue>

              https://data.gov.dk/eid/Person/DK

          </saml:AttributeValue>

          <saml:AttributeValue>

              https://data.gov.dk/eid/Person/DK/Anonymous

          </saml:AttributeValue>

          <saml:AttributeValue>

              https://data.gov.dk/eid/Person/EU

          </saml:AttributeValue>

</md:RequestedAttribute>
```

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.

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>` subelement 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 with Format set to

urn:oasis:names:tc:SAML:2.0:nameid-format:transient or

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

as defined in [SAML2Core].

The NameID element (whether persistent or transient) SHOULD contain an **SP-specific** identifier based on a UUID following RFC 4122 as shown in the following example:

https://data.gov.dk/model/core/eid/**person**/uuid/123e4567-e89b-12d3-a456-426655440000

(if the Subject represents a natural person identity), and

https://data.gov.dk/model/core/eid/**professional**/uuid/123e4567-e89b-12d3-a456-426655440000

(if the Subject represents a professional identity; see chapter 6 for details)

So if the nameformat is "`:transient`" the UUID will be different for every authentication of the same identity, and if the nameformat is "`:persistent`" the UUID will be the same over time for all authentications requested from this SP, but other SP's will get a different UUID regardless of their choice of nameformat. If identifiers are needed which are stable across SPs, the attributes described in chapter 6 should be used as a supplement.

Example:

```
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">

https://data.gov.dk/model/core/eid/person/uuid/123e4567-e89b-12d3-
a456-426655440000

</saml:NameID>
```

[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 MAY 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.

If IdP discovery is used, 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.

[OIO-IDP-21]

IdPs MUST support the propagation of logout signaling to SPs using HTTP-Redirect, HTTP-POST and SOAP 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]

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.

[4] Due to interoperability concerns.

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 At-tribute Service SHOULD return a secondlevel 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

In addition, an IdP’s metadata MAY 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.

[OIO-IDP-43]

The IdP's metadata MAY specify compliance with this profile by including the URI `https://data.gov.dk/saml/profile/oio/4` in the `protocolSupportEnumeration` attribute in `<md:IDPSSODescriptor>.`

[OIO-IDP-44]

The IdP's metadata SHOULD specify the supported set of attribute profiles in the IDPSSODescriptor element as shown in the example below:

```
<AttributeProfile>https://data.gov.dk/eid/Person/DK</AttributeProfile>

<AttributeProfile>https://data.gov.dk/eid/Person/DK/Anonymous</Attribu
teProfile>

<AttributeProfile>https://data.gov.dk/eid/Professional/DK</AttributePr
ofile>

<AttributeProfile>https://data.gov.dk/eid/Professional/DK/Anonymous</A
ttributeProfile>

<AttributeProfile>https://data.gov.dk/eid/Person/EU</AttributeProfile>

<AttributeProfile>https://data.gov.dk/eid/Professional/EU</AttributePr
ofile>
```

6. Attribute profiles

This chapter describes attribute profiles used for communicating about identities representing natural persons and professionals. Thus, an identity (type) is represented by a set of attributes called an attribute profile. Attribute profiles are given an explicit name such that deployments can be explicit about which attribute profile they support.

Note that some attributes are found in several attribute profiles. This does not mean that the attribute values are necessarily the same 'run time' since attribute values are linked to identities and not entities. For example, if the same physical person entity is represented both as a person identity and professional identity, the run-time value of the e-mail attribute may be different with the two identities (attribute sets). However, some attribute values (e.g. name and CPR number) are linked to the entity and will be the same across the entity's identities.

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 by the SP's supported attribute profiles. 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 Attribute profiles

Having consistent and well-defined sets of attributes promotes interoperability and makes it easier to build applications. This is increasingly important when the number of identity types increases. Attribute profiles help in this regard by defining sets of attributes relevant for various types of identities and assigning explicit names (IDs) to the profiles. They enable an IdP (or broker) to declare that certain attribute profiles are supported, or an SP can request one or more identity types and easily detect the type of the returned identity and process it accordingly.

The explicitly named attribute profiles in OIO SAML are specified in table 1:

Table 1: Explicitly named attribute profiles

Identity type (friendly name)	Attribute profile ID
DK Person	https://data.gov.dk/eid/Person/DK
DK Person without CPR	https://data.gov.dk/eid/Person/DK/WithoutCPR
DK Person (anonymized)	https://data.gov.dk/eid/Person/DK/Anonymous
DK Professional	https://data.gov.dk/eid/Professional/DK
DK Professional (anonymized)	https://data.gov.dk/eid/Professional/DK/Anonymous
eIDAS person	https://data.gov.dk/eid/Person/EU
eIDAS legal person	https://data.gov.dk/eid/LegalPerson/EU
eIDAS professional	https://data.gov.dk/eid/Professional/EU

The 'DK person' and 'DK professional' profiles correspond to the two previous attribute profiles defined in OIO SAML 3.0.3 (and earlier) but with more nuances (see below). Table 2: Attribute profile definitions specifies which attributes are part of which attribute profile:

The markup in Tables 2 to 2.4 below should be interpreted as follows:

- 'M' – the attribute is Mandatory and must always be present in all assertions issued according to the attribute profile. To enable data minimization, the set of mandatory attributes is kept small.
- 'S' – the attribute must be Supported by an Identity Provider offering the attribute profile and included in an Assertion if requested by the Service Provider.
- 'O' – the attribute is Optional to support for Identity Providers, and it may be present in assertions. An Identity Provider may choose to include optional attributes according to agreement with the Service Provider (e.g. attribute contracts may be defined in SAML metadata files and exchanged between the parties).
- Blank – the attribute cannot be expected in the attribute profile.

Table 2: Attribute profile definitions

Attribute ID	DK person	DK Person without CPR	DK person (anonymized)	DK professional	DK professional (anonymized)	eIDAS natural person	eIDAS legal person	eIDAS professional
https://data.gov.dk/model/core/specVersion	M	M	M	M	M	M	M	M
https://data.gov.dk/model/core/eid/bootstrapToken	O	O	O	O	O			
https://data.gov.dk/model/core/eid/privilegesIntermediate	O	O	O	S	S			
https://data.gov.dk/concept/core/nsis/loa	M	M	M	M	M			
https://data.gov.dk/concept/core/nsis/ial	O	O	O	O	O			
https://data.gov.dk/concept/core/nsis/aal	O	O	O	O	O			
https://data.gov.dk/model/core/eid/fullName	S	S		S				
https://data.gov.dk/model/core/eid/firstName	S	O		S				
https://data.gov.dk/model/core/eid/lastName	S	O		S				
https://data.gov.dk/model/core/eid/alias			M		M			
https://data.gov.dk/model/core/eid/email	O	O		O				
https://data.gov.dk/model/core/eid/cprNumber	S		O	O		O		O
https://data.gov.dk/model/core/eid/age	S	S	O	O				
https://data.gov.dk/model/core/eid/cprUuid	S		O	O		O		O
https://data.gov.dk/model/core/eid/dateOfBirth	S	S	O					
https://data.gov.dk/model/core/eid/person/pid	O		O					
https://data.gov.dk/model/core/eid/professional/uuid/persistent				S	S			
https://data.gov.dk/model/core/eid/professional/rid				O	O			
https://data.gov.dk/model/core/eid/professional/cvr				M	M			
https://data.gov.dk/model/core/eid/professional/orgName				M	M			
https://data.gov.dk/model/core/eid/professional/productionUnit				O	O			
https://data.gov.dk/model/core/eid/professional/seNumber				O	O			
https://data.gov.dk/model/core/eid/professional/authorizedToRepresent				O				

Table 2.1: New attributes introduced in OIOSAML 4

Attribute ID	DK person	DK Person without CPR	*DK person (anonymized)*	*DK professional*	*DK professional (anonymized)*	*eIDAS natural person*	*eIDAS legal person*	*eIDAS professional*
https://data.gov.dk/concept/core/eid/profile	S	S	S	S	S	S	S	S
https://data.gov.dk/concept/core/eid/provider	O	O	O	O	O	O	O	O
https://data.gov.dk/model/core/loa	S	S	S	S	S	S	S	S
https://data.gov.dk/model/core/eidas/loa	O	O				M	M	M
https://data.gov.dk/model/core/eid/eidas/memberState	O	O				S	S	S
https://data.gov.dk/model/core/nsis/cpr_ial	O					O	O	O
https://data.gov.dk/model/core/eid/professional/isRobot				O	O			
https://data.gov.dk/model/core/eid/allowQualifiedSigning	O	O	O	O	O	O	O	O

Table 2.3: eIDAS natural person

Attribute ID	DK person	DK Person without CPR	*DK person (anonymized)*	*DK professional*	*DK professional (anonymized)*	*eIDAS natural person*	*eIDAS legal person*	*eIDAS professional*
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier						M		M*)
http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName						M		M*)
http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName						M		M*)
http://eidas.europa.eu/attributes/naturalperson/DateOfBirth						M		M*)
http://eidas.europa.eu/attributes/naturalperson/BirthName						O		O*)
http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth						O		O*)
http://eidas.europa.eu/attributes/naturalperson/CurrentAddress						O		O*)
http://eidas.europa.eu/attributes/naturalperson/Gender						O		O*)
http://eidas.europa.eu/attributes/naturalperson/Nationality						O		O*)
http://eidas.europa.eu/attributes/naturalperson/CountryOfBirth						O		O*)
http://eidas.europa.eu/attributes/naturalperson/TownOfBirth						O		O*)
http://eidas.europa.eu/attributes/naturalperson/CountryOfResidence						O		O*)
http://eidas.europa.eu/attributes/naturalperson/PhoneNumber						O		O*)
http://eidas.europa.eu/attributes/naturalperson/EmailAddress						O		O*)
http://data.europa.eu/p4s/attributes/PowerOfRepresentationScope								O

Table 2.4: eIDAS legal person

Attribute ID	DK person	DK Person without CPR	*DK person (anonymized)*	*DK professional*	*DK professional (anonymized)*	*eIDAS natural person*	*eIDAS legal person*	*eIDAS professional*
http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier							M	M
http://eidas.europa.eu/attributes/legalperson/LegalName							M	M
http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress							O	O
http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber							O	O
http://eidas.europa.eu/attributes/legalperson/TaxReference							O	O
http://eidas.europa.eu/attributes/legalperson/D-2012-17-EUIdentifier							O	O
http://eidas.europa.eu/attributes/legalperson/LEI							O	O
http://eidas.europa.eu/attributes/legalperson/EORI							O	O
http://eidas.europa.eu/attributes/legalperson/SEED							O	O
http://eidas.europa.eu/attributes/legalperson/SIC							O	O
http://eidas.europa.eu/attributes/legalperson/LegalPhoneNumber							O	O
http://eidas.europa.eu/attributes/legalperson/LegalEmailAddress							O	O

Note:

- The ‘eIDAS professional’ profile corresponds in eIDAS terms to a ‘natural person representing a legal person’.
- The Subject NameID in the Assertion provides an additional, unique identifier (not part of the AttributeStatement). This identifier is generally more privacy-friendly than most of the identifying attributes in the table above.
- Identity Provider deployments may include additional attributes if required by the Service Provider. In this case, impact on interoperability and privacy should be considered.

Note regarding the eIDAS professional profile *)

The ‘eIDAS professional’ attribute profile is modelled as a ‘natural person representing a legal’ person in the eIDAS SAML Attribute Profile specification [ESAML-AP]. This implies two things: firstly, the professional attribute profile contains attributes of both an eIDAS natural person (the representative) and an eIDAS legal person (the represented).

Secondly, the natural person attribute names (under eIDAS namespace) are amended with ‘/representative’ to indicate that the natural person represents the legal person. Thus, the attribute

- `http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier`

becomes

- `http://eidas.europa.eu/attributes/naturalperson/representative/PersonIdentifier`

6.3 Shared DK attributes

This section specifies common attributes shared by DK attribute profiles. The common attributes therefore do not have a ‘/person’ or ‘/professional’ part in their name after /eid.

6.3.1 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. Implementers should interpret version numbers using the principles of semantic versioning, see [SemVer].
Example	`<AttributeValue>https://data.gov.dk/saml/profile/oio/4.0.0/</AttributeValue>`

6.3.2 BootstrapToken attribute

ID	https://data.gov.dk/model/core/eid/bootstrapToken
Description	Contains a base64-encoded bootstrap token for identity-based web services (see [OIO IDWS] specifications).
Example	`<AttributeValue>AK24bWw...</AttributeValue>`

6.3.3 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).

Example `<AttributeValue>AK24bWw...</AttributeValue>`

6.3.4 Level of Assurance attribute

ID https://data.gov.dk/concept/core/nsis/loa

Description Contains the overall level of assurance of the authentication as de-fined by the Danish [NSIS] standard. The allowed values are 'Low', 'Substantial' and 'High'.

Example `<AttributeValue>Substantial</AttributeValue>`

6.3.5 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'.

Example `<AttributeValue>Substantial</AttributeValue>`

6.3.6 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'.

Example `<AttributeValue>High</AttributeValue>`

6.3.7 Fullname attribute

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

Description Contains the full name.

Example `<AttributeValue>Knud Erik Jensen</AttributeValue>`

6.3.8 Firstname attribute

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

Description Contains the first name(s). In case the person has multiple first names, one or more of these MUST be present. Middle names are not allowed.

Example `<AttributeValue>Knud</AttributeValue>`

6.3.9 Lastname attribute

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

Description Contains the last name.

Example `<AttributeValue>Jensen</AttributeValue>`

6.3.10 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.

Example `<AttributeValue>Bubber</AttributeValue>`

6.3.11 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).

Example `<AttributeValue>knud@jensen.dk</AttributeValue>`

6.3.12 CPR attribute

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

Description Contains the Danish CPR number for the identity represented by 10 digits.

Example `<AttributeValue>2702681273</AttributeValue>`

6.3.13 Age attribute

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

Description Contains the age of the person represented by an integer.

Example `<AttributeValue>38</AttributeValue>`

6.3.14 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.

Example `<AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>`

6.3.15 Date of Birth

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

Description Contains the date of birth in the format dd-mm-yyyy.

Example `<AttributeValue>12-11-2001</AttributeValue>`

6.4 DK Natural Person attributes

Natural person identities are described using the common attributes and the below attributes. Attributes used exclusively for natural person identities have /person in their name after the /eid part.

6.4.1 PID attribute (deprecated)

ID https://data.gov.dk/model/core/eid/person/pid

Description Contains the legacy PID number used in OCES infrastructure. Note: this attribute is deprecated and SPs MUST make plans for phasing out any dependencies on this.

Example `<AttributeValue>9802-2002-2-9142544</AttributeValue>`

6.5 DK Professional Person attributes

Identities representing DK professionals are described using the common attributes and the below attributes. Attributes used exclusively for professional person identities have /professional in their name after the /eid part.

6.5.1 Persistent Identifier attribute

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

Description Contains a UUID for the professional identity which is shared across all 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.

Example `<AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>`

6.5.2 RID number attribute (deprecated)

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.
Example	`<AttributeValue>98023728</AttributeValue>`

6.5.3 CVR number attribute

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].
Example	`<AttributeValue>20301823</AttributeValue>`

6.5.4 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.
Example	`<AttributeValue>Digitaliseringsstyrelsen</AttributeValue>`

6.5.5 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.
Example	`<AttributeValue>4234675432</AttributeValue>`

6.5.6 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.
Example	`<AttributeValue>42346754</AttributeValue>`

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

6.5.7 Authorized to Represent

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 sector 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.

Example
```
<AttributeValue>10346754</AttributeValue>
```

6.6 OIO SAML 4 common attributes

6.6.1 Attribute profile

ID https://data.gov.dk/concept/core/eid/profile

Description Contains the ID of the attribute profile that defines the identity type and the set of attributes in the attribute statement.

Example
```
<AttributeValue>https://data.gov.dk/eid/Person/DK
</AttributeValue>
```

6.6.2 Identity Provider

ID https://data.gov.dk/concept/core/eid/provider

Description Contains the name of the up-stream IdP that handled user authentication.

An Identity Provider offering this attribute must decide which values to use and document semantics of these to its Service Providers.

Examples
```
<AttributeValue>mitid</AttributeValue>
```

```
<AttributeValue>eid_gateway</AttributeValue>
```

6.6.3 Generic LoA

ID https://data.gov.dk/model/core/loa

Description Contains the generic level-of-assurance for the authentication. It can be used by service providers who do not wish to distinguish between e.g. eIDAS Substantial and NSIS Substantal but are satisfied with either of these.

[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.

The value will correspond to eIDAS and/or NSIS requirements for the stated assurance level.

Example `<AttributeValue>Substantial</AttributeValue>`

6.6.4 eIDAS LoA

ID https://data.gov.dk/model/core/eidas/loa

Description eIDAS Level of Assurance (e.g. from eID Gateway authentication)

Note: the eIDAS LoA does not cover the Danish CPR attribute which may be added to the attribute set after the eIDAS authentication which determined the LoA. For information on the 'coupling strength' of the CPR number for eIDAS persons, a separate cpr_ial attribute is used.

Example
```
<AttributeValue>http://eidas.europa.eu/LoA/substantial
</AttributeValue>
```

6.6.5 Member state

ID https://data.gov.dk/model/core/eid/eidas/memberState

Description eIDAS member state that handled user authentication encoded as ISO 3166-1 alpha-2.

Example `<AttributeValue>EL</AttributeValue>`

6.6.6 CPR IAL

ID https://data.gov.dk/model/core/nsis/cpr_ial

Description NSIS registration strength (coupling strength) for the CPR attribute when it is different from the overall registration strength given in https://data.gov.dk/model/core/nsis/ial.

The attribute is relevant when the CPR number is added to the attribute set by an intermediary (e.g. eID gateway) after eIDAS authentication in a different member state. In this case, the CPR number may not have the same level of assurance as the rest of the identity attributes.

Example `<AttributeValue>Substantial</AttributeValue>`

6.6.7 Is robot

ID https://data.gov.dk/model/core/eid/professional/isRobot

Description Indicates whether a professional user is simulated by a software robot. If the attribute is omitted it means an implied value of 'false'.

An SP can use this attribute to implement a specific logic for software robots, including blocking access.

Note: a software robot should always have a unique and separate identity, so any UUID values/identifiers should be separate from human users.

Example `<AttributeValue>true</AttributeValue>`

6.6.8 Allow Qualified Signing

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

Description Indicates whether a user has been registered at a level where a qualified signature (inluding a qualified certificate in accordance with eIDAS article 24.1) can be issued based on the attributes in the SAML Assertion.

Example `<AttributeValue>true</AttributeValue>`

6.7 eIDAS natural person attributes

See [ESAML-AP].

Note that the Latin script variant of attribute values will always be provided so Service Providers do not need to handle transliteration.

See [OOTS-TD] regarding PowerOfRepresentationScope.

6.8 eIDAS attributes for legal persons

See [ESAML-AP].

Note that the Latin script variant of attribute values will always be provided so Service Providers do not need to handle transliteration.

7. References

[eIDAS] 'EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet'

[REF-ARK] 'Fællesoffentlig referencearkitektur for brugerstyring. https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring

[NSIS] National Standard for Identiteters Sikringsniveauer 2.1. https://digst.dk/nsis/

[OIOBPP] OIO Basic Privilege Profile 1.2. https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

[OIOIDWS] OIO Identity Based Web Services https://digst.dk/it-loesninger/standarder/oio-identity-based-web-services-12-oio-idws/

[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 Initiative. 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 At-tribute 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

[ESAML-AP] ”eIDAS SAML Attribute Profile v1.4 Final”. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

[OOTS-TD] "OOTS Technical Design Documents v1.0.0". https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=706382145

[SemVer] "Semantic Versioning 2.0.0" https://semver.org/

Digitaliserings-
styrelsen