eIDAS SAML Message Format

Version 1.3

31 August 2019

eIDAS Technical Specifications

Document created by:

eIDAS eID Technical Subgroup

Document adopted by:

eIDAS Cooperation Network

DOCUMENT HISTORY

Version	Date	Adopted by	Short Description of Changes
1.0	26 January 2016	eIDAS Cooperation Network	/
1.1	16 December 2016	eIDAS Cooperation Network	Various updates
1.2	27 September 2019	eIDAS Cooperation Network	• Use of non-notified eID schemes • Identification of Relying parties • Fixes in attributes profiles and cryptographic requirements • Improvements in metadata handling

NOTE: As specified in the *Opinion No. 3/2023 of the Cooperation Network on version 1.3 of the eIDAS Technical specifications* **version 1.3** of the eIDAS technical specifications is limited to the documents included in **version 1.2 plus eIDAS Common Attributes v1**

Table of Contents

.

1. Introduction

The eIDAS interoperability framework including its national entities (eIDAS-Connector and eIDAS-Service) need to exchange messages including personal and technical attributes to support cross-border identification and authentication processes. For the exchange of messages, the use of the SAML 2.0 specifications has been agreed in the eIDAS technical subgroup and is laid down in the eIDAS Interoperability Architecture.

Since the eIDAS interoperability architecture should use widely used standards, the following SAML-based profiles are taken into utmost account in this paper:

- Kantara Initiative eGovernment Implementation Profile of SAML V2.0 [SAMLeGov2.0]
- STORK 2.0 D4.4 First version of Technical Specifications for the cross border Interface [STORK]

1.1. Definitions

Terms used throughout this document are defined in [eIDAS Interoperability Architecture]. In addition, when referring to SAML technology, an eIDAS-Service can be seen as SAML identity provider (IdP) and an eIDAS-Connector as a SAML service provider (SP).

The following references are used in this document:

- Elements and attributes of the SAML 2.0 Protocol namespace of [SAML2Core] will be prefixed by "`saml2p:`", e.g. `<saml2p:Respone>`
- Elements and attributes of the SAML 2.0 Core namespace of [SAML2Core] will be prefixed by "`saml2:`", e.g. `<saml2:NameID>`
- Elements and attributes of the SAML 2.0 Metadata namespace of [SAML2Meta] will be prefixed by "`md:`", e.g. `<md:EntityDescriptor>`
- Elements and attributes of the Metadata Extension for Entity Attributes [MetaAttr] will be prefixed by "`mdattr:`", e.g. `< mdattr:EntityAttributes>`
- Elements and attributes of the XML Digital Signature Syntax namespace of [XML-DSig] will be prefixed by "`ds:`", e.g. `<ds:X509Certificate>`
- Elements and attributes of this specification and the eIDAS SAML Attribute Profile [eIDAS-Attr-Profile] will be prefixed by "`eidas:`", e.g. `<eidas:SPType>`

1.2. KEY WORDS

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119]. The key word "CONDITIONAL" is to be interpreted as follows:

CONDITIONAL: The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

2. eIDAS Message Format

The following sub-sections specify the message format of exchanged metadata or SAML AuthnRequest and Response messages to be exchanged between eIDAS-Nodes. This document considers sign-on use cases only and thus neglects logout use cases. For SAML elements and attributes not explicitly discussed in this specification the SAML WebSSO-Profile [SAML2Prof] MUST be referred to. Metadata trust management is specified in [eIDAS-Interop-Architecture] and thus not explicitly discussed here. However, in most use cases defined in [eIDAS-Interop-Architecture] the metadata document MUST be properly signed according to [eIDAS-Interop-Architecture].

2.1. METADATA

This section defines basic requirements for the support and use of SAML metadata between different SAML entities and eIDAS-Nodes, respectively. The format for an aggregated list of the different metadata locations across Member States covering one or more eIDAS-Nodes is specified in Appendix A.

2.1.1.Metadata Format

The root element of SAML metadata MUST be `<md:EntitiesDescriptor>` or – if only a single entity is covered – `<md:EntityDescriptor>`. The root element MUST contain the attribute `validUntil`. The `cacheDuration` attribute MAY be included. For a single entity, the attribute `EntityID` in a `<md:EntityDescriptor>` element MUST be a HTTPS URL pointing to the location of its published metadata..

SAML metadata of eIDAS-Services MUST contain a `<md:IDPSSODescriptor>` element whereas SAML metadata of eIDAS-Connectors MUST contain a `<md:SPSSODescriptor>` element. SAML metadata of both eIDAS-Services and eIDAS-Connectors SHOULD NOT contain `<SingleLogoutElementService>`, `<ArtifactResolutionService>` or `<ManageNameIDService>` elements. The `<md:IDPSSODescriptor>` element MUST contain the attribute `WantAuthnRequestsSigned` set to "true" to indicate the requirement of a signed `<saml2p:AuthnRequest>`. The `<md:SPSSODescriptor>` element MUST contain the attribute `AuthnRequestsSigned` set to "true" to indicate that transmitted `<saml2p:AuthnRequest>` messages are signed.

Implementations MUST support and use the `<md:KeyDescriptor>` element and the `<ds:X509Certificate>` element for the inclusion of X.509 Certificates used for SAML communication. Support for other key representations, and for other mechanisms for credential

distribution, is OPTIONAL. The `usage` attribute of the `<md:KeyDescriptor>` element MUST be present.

The supported name identifier formats SHOULD be indicated in the `<saml2:NameIDFormat>` element in the respective SAML metadata.

The default `AssertionConsumerServiceIndex` and the default `AttributeConsumingServiceIndex` SHOULD be indicated by the attribute `isDefault` set to "true" within SAML Metadata.

Human readable information of the organization operating the eIDAS-Node SHOULD be indicated by the `<md:Organization>` element. At least the elements `<md:OrganizationName>`, `<md:OrganizationDisplayName>`, and `<md:OrganizationURL>` SHOULD be provided.

In addition, SAML metadata SHOULD contain contact information for support and for a technical contact. SAML metadata SHOULD contain both a `<md:ContactPerson>` element with a `contactType` value of "support" and a `<md:ContactPerson>` element with a `contactType` value of "technical". The `<md:ContactPerson>` elements SHOULD contain at least one `<md:EmailAddress>`.

eIDAS-Nodes MUST publish their cryptographic capabilities with regards to XML Signature and XML Encryption in their SAML metadata according to [eIDAS-Crypto] and [SAML2AlgSup]. Entities MAY use this information for automatic negotiation of algorithms.

eIDAS-Nodes SHOULD publish information about the implemented eIDAS protocol version as well as information about which product/software and version is used by the node. These informations MUST be published as entity attribute according to [MetaAttr] in the `<md:Extension>` element. The attributes and names are defined in Section 3.4.

If an eIDAS Service requires the RequesterID (see. Section 2.4.1) for identification of non-public relying parties, it SHALL indicate this via a flag in the SAML metadata. These information MUST be published as entity category attribute according to [ECATSAML2] in the `<md:Extension>` element. The attribute and name is defined in Section 3.5.

eIDAS-Services MUST publish all their supported attributes as `<saml:Attribute>` elements in the `<md:IDPSSODescriptor>` element according to [SAML2Meta]. Depending on the implementation and deployment of eIDAS-Services, this can result in the publication of a union of supported attributes.

eIDAS-Services MUST publish all supported Level of Assurance as entity attribute according to [MetaAttr] in the `<md:Extension>` element. The `NameFormat` of the including `<saml:Attribute>` MUST be set to "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" and the `Name` value MUST be set to

“urn:oasis:names:tc:SAML:attribute:assurance-certification” according to [SAML2IA].

2.2. NAME IDENTIFIERS

This section defines the treatment of identifiers to be used in a cross-border context.

eIDAS-Node implementations MUST support the following SAML 2.0 name identifier formats [SAML2Core]:
`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
`urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
Support for other formats is OPTIONAL.

2.3. ATTRIBUTES

This section discusses the handling and inclusion of attributes into exchanged messages.

2.3.1.Attribute Support

eIDAS-Services MUST support at least all mandatory attributes as specified in [eIDAS-Attr-Profile]. Optional attributes of [eIDAS-Attr-Profile] SHOULD be supported. Other optional attributes beyond the ones defined in [eIDAS-Attr-Profile] MAY be supported. Attributes not defined in [eIDAS-Attr-Profile] MAY require bilateral agreement on acceptance between eIDAS-Connector and eIDAS-Service.

2.3.2.Requesting Attributes

Requesting attributes by an eIDAS-Connector from an eIDAS-Service MUST be carried out dynamically by including them in a `<saml2p:AuthnRequest>`. Only attributes that are published in the SAML metadata of the eIDAS-Service can be requested by an eIDAS-Connector (see Section 0). Attributes requested that are not supported by an eIDAS-Service MUST be ignored by the eIDAS-Service.

Attributes MUST be requested as `<eidas:RequestedAttributes>` (see Section 5.2) according to [STORK]. `<eidas:RequestedAttributes>` MUST be included in the `<saml2p:Extensions>` element of the SAML AuthnRequest. For every requested attribute the eIDAS-Connector includes a `<eidas:RequestedAttribute>` (see Section 5.4) element within the `<eidas:RequestedAttributes>` element. For attributes requested and being mandatory according to the eIDAS minimum data sets and [eIDAS-Attr-Profile] the attribute `isRequired` of `<eidas:RequestedAttribute>` MUST be set to “true”. For all optional attributes according to the

eIDAS minimum data sets and [eIDAS-Attr-Profile] the attribute `isRequired` of `<eidas:RequestedAttribute>` MUST be set to "false". When requesting a minimum data set, at least all attributes defined as mandatory within this minimum data set MUST be requested. At least one minimum data set MUST be requested in each `<saml2p:AuthnRequest>`.

2.3.3.Responding Attributes

Attributes are delivered in `<saml2:Attribute>` elements within one `<saml2:AttributeStatement>` included in one SAML assertion. `<saml2:AttributeValue>` elements within the eIDAS context are defined in [eIDAS-Attr-Profile].

`<saml2:AttributeValue>` elements SHOULD be strings. XML content should be base64-encoded. Attributes MUST NOT contain empty values.

Single encrypted attributes using `<saml2:EncryptedAttribute>` MUST NOT be used.

Note: For representation cases (e.g. a natural person representing a legal person) the SAML response MAY contain attributes of a representative not requested as `<eidas:RequestedAttributes>` (see section 2.8 of the sibling specification [eIDAS-Attr-Profile]).

2.4. SAML PROTOCOL MESSAGE CONTENT

This section gives details on the exchanged SAML protocol messages between eIDAS-Nodes and the underlying transport mechanisms. SAML bindings for transporting SAML protocol messages are defined in [eIDAS-Interop-Architecture].

2.4.1.SAML AuthnRequest

eIDAS-Connectors SHOULD NOT provide `AssertionConsumerServiceURL`. If included, the eIDAS-Service MUST compare the value with the SAML metadata element `<md:AssertionConsumerService>` using case-sensitive string comparison and issue an error if the value does not match.

eIDAS-Connectors SHOULD NOT use `ProtocolBinding`.

eIDAS-Connectors MUST support `ForceAuthn`. `ForceAuthn` MUST be set to "true".

eIDAS-Connectors MUST support `isPassive`. `isPassive` SHOULD be set to "false".

`AttributeConsumingServiceIndex` MAY be included.

eIDAS-Connectors SHOULD use `RequesterID` to indicate the actual relying party filing the

authentication request. When present, the `RequesterID` MUST be guaranteed to be unique at least within the Connector of the Member State where the request originates from.

Implementation Note: Under article 7.f of the eIDAS Regulation Member States may define terms of access for non-public sector relying parties. As identification of the relying party through `RequesterID` is a typical requirement of such terms, implementers of eIDAS-Connectors shall consult the separate specification document for non-public sector relying parties[1] to make sure that such requirements are fulfilled, as the eIDAS-Service might reject requests otherwise.

`<saml2p:NameIDPolicy>` SHOULD be used to indicate the requested name identifier format.

`<saml2p:RequestedAuthnContext>` SHALL be used to indicate the requested eIDAS Levels of Assurance. Implementations MUST support the eIDAS Levels of Assurance (LoA) as defined in Section 3.2. eIDAS-Connectors SHOULD request a specific LoA that is defined in Section 3.2. eIDAS-Connectors requesting a LoA of a notified eID MUST limit the value of the Comparison attribute of `<saml2p:RequestedAuthnContext>` to "minimum".

Note: To support reuse of eIDAS-Node infrastructure for non-notified eID schemes, Member States MAY support other URIs as Authentication Context without any obligation for a receiving Member State to request and thus accept such non-notified eIDs. Receiving Members States need to be aware that this is meant only as an interoperability measure and that a non-notified eID does not claim any guarantees for assurance or does not claim any sending Member State liability. In case of requesting a LoA of a non-notified eID, the `Comparison` attribute of `<saml2p:RequestedAuthnContext>` MUST be set to “exact” and the eIDAS-Connector MUST include any LoA URI (for notified and non-notified eID) that are acceptable in a response assertion. eIDAS-Service implementations MUST support all `<saml2p:AuthnRequest>` child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations MUST fully support the options enumerated above.

SAML AuthnRequest messages MUST be signed according to [eIDAS-Interop-Architecture].

2.4.2.SAML Response

The status of the SAML response MUST be indicated using the `<saml2p:Status>` element providing at least one `<saml2p:StatusCode>`.

[1] Available at Terms of access to notified eID schemes for non-public sector - Identification of relying parties (https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Terms+of+access+to+notified+eID+schemes+for+non-public+sector+-+Identification+of+relying+parties)

The <saml2:Subject> element of the assertions issued by an eIDAS-Service MUST contain a <saml2:NameID> element. Details of the <saml2:NameID> are defined in Section 3.1.

The elements <saml2:AuthnContext> and <saml2:AuthnContextClassRef> MUST contain a URI describing an eIDAS LoA according to Section 3.2.

A SAML assertion MUST include at least the attributes requested as mandatory (indicated in the SAML authentication request by the attribute isRequired="true"), otherwise the SAML response MUST include an appropriate error message. The NameFormat value of a <saml2:Attribute> MUST be urn:oasis:names:tc:SAML:2.0:attrname-format:uri. The attributes and names are defined in Section 3.3. SAML response messages MUST be signed and SAML assertions MAY be signed according to [eIDAS-Interop-Architecture]. SAML assertions MUST be encrypted according to [eIDAS-Interop-Architecture].

3. Attribute Definitions

In this section, a basic set of attributes is defined.

3.1. Name Identifier

It is RECOMMENDED to use a person identifier of [eIDAS-Attr-Profile] as name identifier.

3.2. Levels of Assurance

The following URIs are valid and indicate a notified eID:
http://eidas.europa.eu/LoA/low
http://eidas.europa.eu/LoA/substantial
http://eidas.europa.eu/LoA/high

Note: To support reuse of eIDAS-Node infrastructure for non-notified eID schemes, Member States MAY support other URIs. Such non-notified eIDs MUST NOT use an "http://eidas.europa.eu/LoA/" prefix. The following URIs indicate a situation where the sending Member State claims to, in principle, meeting requirements defined as eIDAS Levels of Assurances, but as the eID means was not notified, there are no guarantees whatsoever (see section 2.4.1 on receiving side processing of such cases):

http://eidas.europa.eu/NotNotified/LoA/low
http://eidas.europa.eu/NotNotified/LoA/substantial
http://eidas.europa.eu/NotNotified/LoA/high

3.3. eIDAS Attributes

The complete list of attributes supported by the eIDAS minimum data sets are defined in [eIDAS-Attr-Profile].

3.3.1.Additional Attributes

Exchange of further additional attributes between eIDAS-Connector and eIDAS-Service MAY be supported. Additional attribute definitions are out-of-scope of this specification and of [eIDAS-Attr-Profile].

3.4. eIDAS-Node deployment version

These attributes contain parameters specifying information about the deployed version of an eIDAS-node in the form of an eIDAS-Connector or an eIDAS-Service. The attributes are added to that entity's

<md:EntityDescriptor> element using the <mdattr:EntityAttributes> extension element defined in [MetaAttr]. The entity attributes are placed in a metadata <Extensions> element as a child element to the <EntityDescriptor> element of this eIDAS-Node. The NameFormat of the including <saml:Attribute> MUST be set to "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" two SAML attribute names are defined:

http://eidas.europa.eu/entity-attributes/protocol-version

http://eidas.europa.eu/entity-attributes/application-identifier

The defined attributes, when present, MUST contain a non-empty attribute containing a string value as follows. To indicate multi-protocol support, the attribute MAY have multiple values.

Entity Attribute	**Description**
protocol-version	The version of the official eIDAS protocol implemented by this eIDAS-Node. E.g. “1.2” or two string values with “1.1” and “1.2” **Note:** This version number does not represent the version of individual specifications, but rather a common version number assigned to the eIDAS technical specifications set.
application-identifier	An arbitrary identifier of the software vendor / software identifier/ software version in the form “vendor name”:“software identifier”:”{major-version}.{minor-version}[.{patch-version}]” **Example:** CEF:eIDAS-ref:2.0 **Note:** Detailed information about formatting software vendor and software identifier values are defined in the guidelines for versioning.

3.5. REQUESTERID FOR NON-PUBLIC SECTOR RELYING PARTIES

If an eIDAS Service requires the RequesterID (see. Section 2.4.1) for identification of non-public relying parties, it SHALL indicate this via a flag in the SAML metadata. The flag is added as an entity category attribute [ECATSAML2] to the entity's <md:EntityDescriptor> element using the <mdattr:EntityAttributes> extension element defined in [MetaAttr]. The entity category attribute is placed in a metadata <Extensions> element as a child element to the <EntityDescriptor> element of this eIDAS Service.

The defined flag, when present in entity category attribute, MUST contain a non-empty <saml2:AttributeValue> element containing a string value defined as:

http://eidas.europa.eu/entity-attributes/termsofaccess/requesterid

4. Additional Information

4.1. Private/Public Sector SP

For indicating whether an authentication request is made by a private sector or public sector SP, the defined element <eidas:SPType> (See Section 5.1) MUST be present either in the <md:Extensions> element of SAML metadata or in the <saml2p:Extensions> element of a <saml2p:AuthnRequest>. If the SAML metadata of an eIDAS-Connector contains a <eidas:SPType> element, SAML authentication requests originating at that eIDAS-Connector MUST NOT contain a <eidas:SPType> element. The <eidas:SPType> element can contain the values “public” or “private” only.

4.2. Node Country

For indicating which Member State or international organisation is responsible for an eIDAS-Node (serving this Member State’s eID means, this Member State’s or international organisation’s relying parties, respectively), the element <eidas:NodeCountry> (see Section 5.2) MUST be present in the <md:Extensions> element of SAML metadata. In detail, if the eIDAS-Node acts as a eIDAS-Service, the <eidas:NodeCountry> MUST be present in the <md:Extensions> element of the <md:IDPSSODescriptor>. If the eIDAS-Node acts as a eIDAS-Connector, the <eidas:NodeCountry> MUST be present in the <md:Extensions> element of the <md:SPSSODescriptor>.

The SAML authentication request MUST NOT contain a <eidas:NodeCountry> element. The value of the <eidas:NodeCountry> element MUST be the Nationality Code of the SP country or international organization[2] in ISO 3166-1 alpha-2 format.

[2] e.g. ‚EU‘ for European Institutions; ‚EU‘ has been exceptionally reserved by ISO 3166”

5. Definition of specific message format elements

This section provides definitions on specific eIDAS message formats elements.

5.1. <EIDAS:SPTYPE>

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
      xmlns:eidas="http://eidas.europa.eu/saml-extensions"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://eidas.europa.eu/saml-extensions"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified"
      version="1">

   <xsd:element name="SPType" type="eidas:SPTypeType"/>

   <xsd:simpleType name="SPTypeType">
      <xsd:restriction base="xsd:string">
         <xsd:enumeration value="public"/>
         <xsd:enumeration value="private"/>
      </xsd:restriction>
   </xsd:simpleType>
</xsd:schema>
```

5.2. <EIDAS:SERVICECOUNTRY>

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
      xmlns:eidas="http://eidas.europa.eu/saml-extensions"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://eidas.europa.eu/saml-extensions"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified"
      version="1">

   <xsd:element name="NodeCountry" type="eidas:NodeCountryType"/>

   <xsd:simpleType name=" NodeCountryType ">
      <xsd:restriction base="xsd:string">
         <xsd:pattern value="[A-Z][A-Z]"/>
      </xsd:restriction>
```

```
   </xsd:simpleType>
</xsd:schema>
```

5.3. <EIDAS:REQUESTEDATTRIBUTES>

This attribute and its definition has been taken over from [STORK]. For details on its definition the STORK specification [STORK] is referred to.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
      xmlns:eidas="http://eidas.europa.eu/saml-extensions"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://eidas.europa.eu/saml-extensions"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified"
      version="1">

      <xsd:element name=" RequestedAttributes"
                  type="eidas:RequestedAttributesType" />

      <xsd:complexType name="RequestedAttributesType">
         <xsd:sequence>
            <xsd:element minOccurs="0" maxOccurs="unbounded"
                        ref="eidas:RequestedAttribute"/>
         </xsd:sequence>
      </xsd:complexType>
</xsd:schema>
```

5.4. <EIDAS:REQUESTEDATTRIBUTE>

This attribute and its definition has been taken over from [STORK]. For details on its definition the STORK specification [STORK] is referred to.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
      xmlns:eidas="http://eidas.europa.eu/saml-extensions"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://eidas.europa.eu/saml-extensions"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified"
      version="1">

   <xsd:element name="RequestedAttribute"
                type="eidas:RequestedAttributeType"/>

   <xsd:complexType name="RequestedAttributeType">
      <xsd:sequence>
```

```
         <xsd:element name=" AttributeValue" type="xsd:anyType"
                      minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="Name" type="xsd:string" use="required"/>
      <xsd:attribute name="NameFormat" type="xsd:anyURI" use="required"/>
      <xsd:attribute name="isRequired" type=" xsd:boolean" use="required"/>
      <xsd:attribute name="FriendlyName" type="xsd:string" use="optional"/>
      <xsd:anyAttribute namespace="##other" processContents="lax"/>
   </xsd:complexType>
</xsd:schema>
```

6. Message Format Examples

In the following, samples for SAML Metadata and exchanged SAML messages are provided.

6.1. eIDAS-Connector SAML-Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:eidas="http://eidas.europa.eu/saml-extensions"
   xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   ID="_9ebc8854ec7f701da9749e87a801e5f2"
   entityID="https://eidas-connector.eu"
   validUntil="2015-05-24T19:30:26.624Z">
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
            <ds:Reference URI="#_9ebc8854ec7f701da9749e87a801e5f2">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>t2DvNbFynxqsLoF4BfJPIvauBrSeVDjBCPBHulKYh4g=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>G34==</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MIID==</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
        <md:Extensions>
          <eidas:SPType>public</eidas:SPType>
          <alg:DigestMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <alg:SigningMethod MinKeySize="256"
                  Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
          <alg:SigningMethod MinKeySize="3072" MaxKeySize="4096"
                  Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
          <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
                                   xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml2:Attribute Name="http://eidas.europa.eu/entity-attributes/protocol-version"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
              <saml2:AttributeValue xsi:type="xs:string"
                                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                  1.1
              </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="http://eidas.europa.eu/entity-attributes/application-identifier"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
              <saml2:AttributeValue xsi:type="xs:string"
                                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                 CEF:eIDAS-ref:2.0
              </saml2:AttributeValue>
            </saml2:Attribute>             </mdattr:EntityAttributes>
```

```
        </md:Extensions>
    <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:Extensions>
          <eidas:NodeCountry>EU</eidas:NodeCountry>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
          <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
              <ds:X509Certificate>MIID==</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
              <ds:X509Certificate>MIID==</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
          <md:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes256-gcm"/>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://eidas-connector.eu/post"
            index="0"
            isDefault="true"/>
    </md:SPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="en">eIDAS Connector</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="en">eIDAS Connector</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="en">https://eidas-connector.eu</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:Company>eIDAS Connector Operator</md:Company>
        <md:GivenName>John</md:GivenName>
        <md:SurName>Doe</md:SurName>
        <md:EmailAddress>john.doe@eidas-connector.eu</md:EmailAddress>
        <md:TelephoneNumber>+43 123456</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

6.2. eIDAS-Service SAML Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:eidas="http://eidas.europa.eu/saml-extensions"
    xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    ID="_9ebc8854ec7f701da9749e87a801e5f2"
    entityID="https://eidas-service.eu"
    validUntil="2015-05-24T19:30:26.624Z">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
```

```
        <ds:Reference URI="#_9ebc8854ec7f701da9749e87a801e5f2">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                  PrefixList="xs"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>t2DvNbFynxqsLoF4BfJPIvauBrSeVDjBCPBHulKYh4g=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>G34==</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIDPWA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
                             xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      <saml2:Attribute Name="http://eidas.europa.eu/entity-attributes/protocol-version"
                       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
        <saml2:AttributeValue xsi:type="xs:string"
                              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
          1.1
        </saml2:AttributeValue>
      </saml2:Attribute>
        <saml2:Attribute Name="http://eidas.europa.eu/entity-attributes/application-identifier"
                         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
          <saml2:AttributeValue xsi:type="xs:string"
                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            CEF:eIDAS-ref:2.0
          </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute
            Name="urn:oasis:names:tc:SAML:attribute:assurance-certification"
            NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
          <saml2:AttributeValue>
            http://eidas.europa.eu/LoA/high
          </saml2:AttributeValue>
          <saml2:AttributeValue>
            http://eidas.europa.eu/LoA/substantial
          </saml2:AttributeValue>
          <saml2:AttributeValue>
            http://eidas.europa.eu/LoA/low
          </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="http://macedir.org/entity-category"
                         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
          <saml2:AttributeValue>
            http://eidas.europa.eu/entity-attributes/termsofaccess/requesterid
          </saml2:AttributeValue>
        </saml2:Attribute>
    </mdattr:EntityAttributes>
    <alg:DigestMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <alg:SigningMethod MinKeySize="256"
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
    <alg:SigningMethod MinKeySize="3072" MaxKeySize="4096"
```

```
                Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
    </md:Extensions>
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
      <md:Extensions>
        <eidas:NodeCountry>EU</eidas:NodeCountry>
      </md:Extensions>
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>MIID==</ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://eidas-service.eu/post"/>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://eidas-service.eu/redirect"/>
      <saml2:Attribute
        FriendlyName="PersonIdentifier"
        Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      </saml2:Attribute>
      <saml2:Attribute
        FriendlyName="FamilyName"
        Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      </saml2:Attribute>
      <saml2:Attribute
        FriendlyName="FirstName"
        Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      </saml2:Attribute>
      <saml2:Attribute
        FriendlyName="DateOfBirth"
        Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      </saml2:Attribute>
    </md:IDPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">eIDAS Service</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">eIDAS Service</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en"> “https://eidas-connector.eu”
  </md:Organization>
  <md:ContactPerson contactType="technical">
    <md:Company>eIDAS Service Operator</md:Company>
    <md:GivenName>John</md:GivenName>
    <md:SurName>Doe</md:SurName>
    <md:EmailAddress>john.doe@eidas-service.eu</md:EmailAddress>
    <md:TelephoneNumber>+43 123456</md:TelephoneNumber>
  </md:ContactPerson>
</md:EntityDescriptor>
```

6.3. SAML AUTHNREQUEST

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest
    Destination="https://eidas-service.eu/post"
    ID="_171ccc6b39b1e8f6e762c2e4ee4ded3a" IssueInstant="2015-04-30T19:25:14.273Z" Version="2.0"
    ForceAuthn="true"
    IsPassive="false"
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:eidas="http://eidas.europa.eu/saml-extensions"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://eidas-connector.eu
  </saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
      <ds:Reference URI="#_171ccc6b39b1e8f6e762c2e4ee4ded3a">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
        <ds:DigestValue>EFe8x1Gvm5RVmrBaWM5RrQm81xk=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>SaO8==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIDPWA==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Extensions>
    <eidas:SPType>public</eidas:SPType>
    <eidas:RequestedAttributes>
      <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
      <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
      <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
      <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
    </eidas:RequestedAttributes>
  </saml2p:Extensions>
  <saml2p:NameIDPolicy AllowCreate="true"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
  <saml2p:RequestedAuthnContext Comparison="minimum">
    <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        http://eidas.europa.eu/LoA/high
    </saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

6.4. SAML RESPONSE

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://eidas-connector.at/post"
```

```
    ID="_5a15625de8618920748123042db52367"
    InResponseTo="_171ccc6b39b1e8f6e762c2e4ee4ded3a"
    IssueInstant="2015-04-30T19:27:20.159Z"
    Version="2.0"
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://eidas-service.eu</saml2:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"/>
    <ds:Reference URI="#_5a15625de8618920748123042db52367">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ec:InclusiveNamespaces PrefixList="xs"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>t5V4hqAh4Nxjd49H/rC+N9tN/dNHBNuCOco1v1GYfFc=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>GX2==</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>MIIDPWA==</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
<saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</saml2p:Status>
<saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Id="encrypted-data-0-1152532362-41467517-23174"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod
        Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey Id="encrypted-key-1-1152532362-41467527-29158-c0">
        <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        </xenc:EncryptionMethod>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIIDPWA==</ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>MDTqUNbO8Wd</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>NhUqASe+jJ0BHqTX4sayQLz7qUNbO8Wdj9qEI4wm+9Mbml3Agfjluw==
      </xenc:CipherValue>
    </xenc:CipherData>
```

```
    </xenc:EncryptedData>
  </saml2:EncryptedAssertion>
</saml2p:Response>
```

6.5. SAML ASSERTION

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="_474827890697323 22d02d825c9a2fafa" IssueInstant="2015-04-30T19:27:20.159Z"
    Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:eidas="http://eidas.europa.eu/attributes/naturalperson">
  <saml2:Issuer Format="urn:oasis:names:tc:saml2:2.0:nameid-format:entity">
      https://eidas-service.eu
  </saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:saml2:2.0:nameid-format:persistent"
      > ES/AT/02635542Y </saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:saml2:2.0:cm:bearer">
      <saml2:SubjectConfirmationData InResponseTo="_171ccc6b39b1e8f6e762c2e4ee4ded3a"
        NotOnOrAfter="2015-04-30T19:32:20.157Z"
        Recipient="https://eidas-connector.eu/post"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2015-04-30T19:27:20.159Z" NotOnOrAfter="2015-04-30T19:32:20.157Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://eidas-connector.eu/post</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2015-04-30T19:27:20.159Z"
    SessionIndex="_5eeb319253e2d7d125e3dcc72806209a">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/high</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
  <saml2:Attribute
    FriendlyName="PersonIdentifier"
    Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
    NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:PersonIdentifierType">
      ES/AT/02635542Y
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute
    FriendlyName="FamilyName"
    Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:CurrentFamilyNameType">
      Onasis
    </saml2:AttributeValue>
    <saml2:AttributeValue LatinScript="false" xsi:type="eidas:CurrentFamilyNameType">
      Ωνάσης
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute
    FriendlyName="FirstName"
    Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
    NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:CurrentGivenNameType">
```

```
            Sarah
        </saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute
        FriendlyName="DateOfBirth"
        Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
        NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
        <saml2:AttributeValue xsi:type="eidas:DateOfBirthType">
            1970-05-28
        </saml2:AttributeValue>
    </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

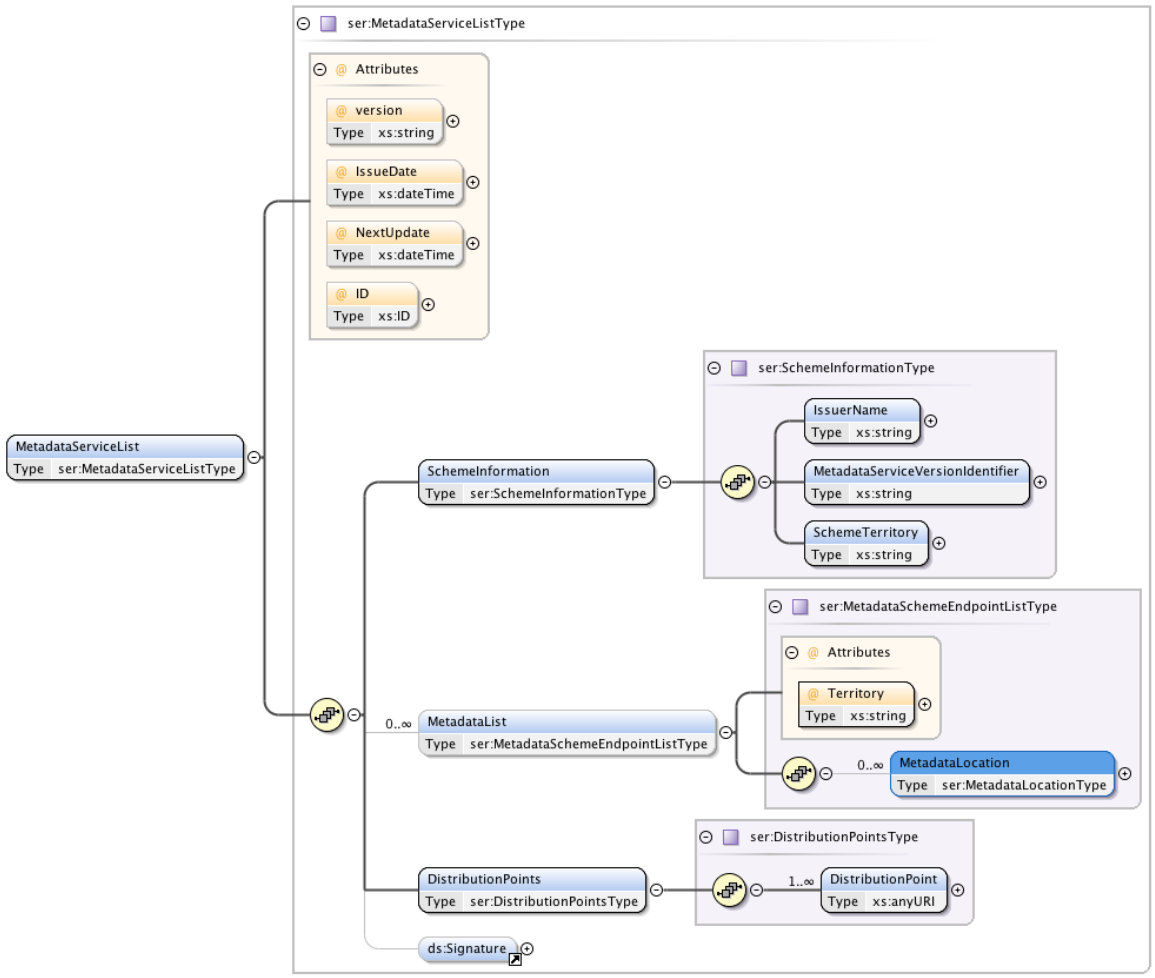
Appendix A Metadata Aggregator Format

The purpose of this section is to provide a consolidated list of the different metadata locations across Member States covering one or more endpoints. This list may be cryptographically signed, but integrity of the metadata is ensured through a signature on each metadata document that can be retrieved at any specified location.

The following cases have been taken into account:

- MSs with one connector and one proxy (the 'classical' eIDAS-Node case),
- MSs with no proxy (the middleware case, middleware-services do not need publicly available metadata),
- MSs with some or many connectors (decentralised).

This format is inspired by what has been done for trusted list in eSignature.



A.1 List of THE list, MS-based

A.1.1 Sample with one country

This sample is an example of a single country's information as it can be enclosed in the list.

```
<ser:MetadataServiceList xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:ser="http://eidas.europa.eu/metadata/servicelist"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
version="1.0" IssueDate="2006-05-04T18:13:51.0" NextUpdate="2006-05-04T18:13:51.0"
ID="ID001">
   <ser:SchemeInformation>
      <ser:IssuerName>IssuerName</ser:IssuerName>
      <ser:SchemeIdentifier> https://eidas.example.com/metadatalist/Scheme01</ser:SchemeIdentifier>
      <ser:SchemeTerritory>BE</ser:SchemeTerritory>
   </ser:SchemeInformation>
   <ser:MetadataList Territory="BE">
      <ser:MetadataLocation Location="https://eidas.example.com/node1/metadata">
         <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/Connector"
                       EntityID="https://eidas.example.com/node1"/>
      </ser:MetadataLocation>
      <ser:MetadataLocation Location="https://eidas.example.com/node2/metadata">
         <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/ProxyService"
                       EntityID="https://eidas.example.com/node2"/>
      </ser:MetadataLocation>
   </ser:MetadataList>
   <ser:DistributionPoints>
      <DistributionPoint>http://www.example.com/distributionpoint1</DistributionPoint>
   </ser:DistributionPoints>
</ser:MetadataServiceList>
```

A.1.2 Sample of list covering the different cases

```
<ser:MetadataServiceList xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:ser="http://eidas.europa.eu/metadata/servicelist"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
version="1.0" IssueDate="2006-05-04T18:13:51.0" NextUpdate="2006-05-04T18:13:51.0"
ID="ID001">
   <ser:SchemeInformation>
      <ser:IssuerName>IssuerName</ser:IssuerName>
      <ser:SchemeIdentifier> https://eidas.example.com/metadatalist/Scheme01</ser:SchemeIdentifier>
      <ser:SchemeTerritory>EU</ser:SchemeTerritory>
   </ser:SchemeInformation>
   <!-- Country with several locations for signle entities -->
   <ser:MetadataList Territory="BE">
      <ser:MetadataLocation Location="https://eidas.example.com/node1/metadata">
         <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/Connector"
                       EntityID="https://eidas.example.com/node1"/>
      </ser:MetadataLocation>
      <ser:MetadataLocation Location="https://eidas.example.com/node2/metadata">
         <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/ProxyService"
                       EntityID="https://eidas.example.com/node2"/>
      </ser:MetadataLocation>
   </ser:MetadataList>
   <!-- Country with one location for multiple specified entities -->
   <ser:MetadataList Territory="AT">
      <ser:MetadataLocation Location="https://eidas.example.com/node3and4/metadata">
         <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/Connector"
```

```
                        EntityID="https://eidas.example.com/node3"/>
        <ser:Endpoint EndpointType="http://eidas.europa.eu/metadata/ept/ProxyService"
                        EntityID="https://eidas.example.com/node4"/>
      </ser:MetadataLocation>
  </ser:MetadataList>
  <!-- Country with one location for multiple unspecified entities -->
  <ser:MetadataList Territory="SE">
      <ser:MetadataLocation Location="https://eidas.example.com/senodes/metadata"/>
  </ser:MetadataList>
  <ser:DistributionPoints>
      <DistributionPoint>http://www.example.com/distributionpoint1 </DistributionPoint>
      <DistributionPoint>http://www.example.com/distributionpoint2</DistributionPoint>
  </ser:DistributionPoints>
  <ds:Signature>
    …
  </ds:Signature>
</ser:MetadataServiceList>
```

A.2 LIST SCHEMA

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema version="1.0" attributeFormDefault="unqualified" elementFormDefault="qualified"
 targetNamespace="http://eidas.europa.eu/metadata/servicelist"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:ser="http://eidas.europa.eu/metadata/servicelist"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

 <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
  schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd"/>

 <xs:annotation>
  <xs:documentation>
   Document identifier: eidas-metadata-servicelist-1.0
  </xs:documentation>
 </xs:annotation>

 <xs:element name="MetadataServiceList" type="ser:MetadataServiceListType"/>

 <xs:complexType name="MetadataServiceListType">
  <xs:annotation>
   <xs:documentation>
    The MetadataServiceListType is the root type for representing a metadata service list. It holds
    scheme information, metadata locations for each member state and optionally distribution point(s).
   </xs:documentation>
  </xs:annotation>
  <xs:sequence>
   <xs:element name="SchemeInformation" type="ser:SchemeInformationType"/>
   <xs:element name="MetadataList" type="ser:MetadataSchemeEndpointListType" minOccurs="0"
    maxOccurs="unbounded"/>
   <xs:element name="DistributionPoints" type="ser:DistributionPointsType"/>
   <xs:element ref="ds:Signature" minOccurs="0"/>
  </xs:sequence>
  <xs:attribute name="Version" type="xs:string" use="required">
   <xs:annotation>
    <xs:documentation>
     The version of a metadata service list.
    </xs:documentation>
   </xs:annotation>
```

```
  </xs:attribute>
  <xs:attribute name="IssueDate" type="xs:dateTime" use="required">
    <xs:annotation>
      <xs:documentation>
        Issuance time for a metadata service list.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>
  <xs:attribute name="NextUpdate" type="xs:dateTime">
    <xs:annotation>
      <xs:documentation>
        Time when the next metadata service list will be published.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>
  <xs:attribute name="ID" type="xs:ID">
    <xs:annotation>
      <xs:documentation>
        The unique ID for a metadata service list.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>

<xs:complexType name="SchemeInformationType">
  <xs:annotation>
    <xs:documentation>
      Scheme information about a published metadata service list, where the publisher
      and territory are included.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="IssuerName" type="xs:string"/>
    <xs:element name="SchemeIdentifier" type="xs:anyURI"/>
    <xs:element name="SchemeTerritory" type="xs:string"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="MetadataSchemeEndpointListType">
  <xs:annotation>
    <xs:documentation>
      Defines the metadata location(s) for a specific member state (territory).
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element type="ser:MetadataLocationType" name="MetadataLocation" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Territory" type="xs:string" use="required"/>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

<xs:complexType name="DistributionPointsType">
  <xs:annotation>
    <xs:documentation>
      A list of distribution points. URLs from where the metadata service list can be downloaded.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="DistributionPoint" type="xs:anyURI" minOccurs="1" maxOccurs="unbounded"/>
```

```
  </xs:sequence>
 </xs:complexType>

 <xs:complexType name="MetadataLocationType">
  <xs:sequence>
   <xs:element name="Endpoint" type="ser:MsEndpointType" minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
     <xs:documentation>
      A list of eIDAS endpoints (nodes) for the current location.
     </xs:documentation>
    </xs:annotation>
   </xs:element>
   <xs:element ref="ds:KeyInfo" minOccurs="0">
    <xs:annotation>
     <xs:documentation>
      Key material (usually a certificate) that should be used to verify the signature
      of the downloaded metadata for this metadata location.
     </xs:documentation>
    </xs:annotation>
   </xs:element>
  </xs:sequence>
  <xs:attribute name="Location" type="xs:anyURI" use="required">
   <xs:annotation>
    <xs:documentation>
     The URL from where the metadata for the endpoint(s) can be obtained.
    </xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
 </xs:complexType>

 <xs:complexType name="MsEndpointType">
  <xs:annotation>
   <xs:documentation>
    Defines a member state "endpoint" (eIDAS node).
   </xs:documentation>
  </xs:annotation>
  <xs:attribute name="EndpointType" type="xs:anyURI" use="required">
   <xs:annotation>
    <xs:documentation>
     The type of endpoint. Currently defined URI:s are:
      http://eidas.europa.eu/metadata/ept/ProxyService for an eIDAS Proxy Service, and,
      http://eidas.europa.eu/metadata/ept/Connector for an eIDAS Connector.
    </xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:attribute name="EntityID" type="xs:anyURI" use="required">
   <xs:annotation>
    <xs:documentation>
     The SAML entityID of the endpoint. For an eIDAS connector this is the entityID for
     the SP-part of the node, and for an eIDAS Proxy Service this is the entityID for the
     IdP-part of the node.
    </xs:documentation>
   </xs:annotation>
  </xs:attribute>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
 </xs:complexType>
</xs:schema>
```

A.3 DESCRIPTION OF LIST-ELEMENTS

The main element `MetadataServiceList` holds the following attributes and elements.

Attributes

Name	Content
Version	The version of this metadata list (e.g. 0.9)
IssueDate	The time when this list was issued
NextUpdate	The time when an update of this list will be available
ID	An ID element supporting a signature over this list

Elements

Name	Content
SchemeInformation	Information about the issuer of this list and how the list was created
MetadataList	One or more lists of metadata locations for one or more territories
DistributionPoints	One or more locations where this list, and future updates of this list can be obtained.
Signature	An optional signature of the list

A.3.1 SchemeInformation

The `SchemeInformation` element holds the following elements

Name	Content
IssuerName	A descriptive name of the issuer of this list
SchemeIdentifier	An Identifier of the Scheme used to generate this list
SchemeTerritory	The territory covered by this list.

A.3.2 MetadataList

The `MetadataList` element holds the following attributes and elements

Attributes

Name	Content
Territory	The territory covered by metadata locations found in this element
##any	Extension point for locally defined attributes

Elements

Name	Content
MetadataLocation	Zero or more MetadataLocation elements, each specifying a location where metadata can be retrieved. This element MAY also specify: • Zero or more endpoints that are covered by the metadata found at the specified location. • Zero or more certificates or public keys that can be used to validate the signature on the metadata found at specified location.

The specified `SchemeIdentifier` may further identify requirements on presence of endpoint elements as well as certificates or keys for signature validation.

Each endpoint element contains the following attributes

Name	Content
EndpointType	A URI specifying the endpoint type
EntityID	The EntityID of the endpoint
##any	Extension point for locally defined attributes

Valid values of the `EndpointType` URI are:

EndpointType	URI
Connector	TBD
ProxyService	TBD

A.3.3 DistributionPoints

The `DistributionPoints` element holds the following elements

Name	Content
DistributionPoint	A location where this list, and future updates of this list can be obtained.

References

[eIDAS-Attr-Profile] eIDAS SAML Attribute Profile

[eIDAS-Crypto] eIDAS Cryptographic requirements for the Interoperability Framework

[eIDAS-Interop-Architecture] eIDAS Interoperability Architecture

[eIDAS-Interop-IA] eIDAS Interoperability Framework Implementing Act

[ECATSAML2] RFC8409, The Entity Category Security Assertion Markup Language (SAML) Attribute Types, August 2018, https://tools.ietf.org/html/rfc8409

[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.pdf

[MetaIOP] 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

[SAMLeGov2.0] eGovernment Implementation Profile of SAML V2.0 (2010) http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf

[SAML2IA] OASIS Committee Specification, SAML V2.0 Identity Assurance Profiles Version 1.0, November 2010, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf

[SAML2AlgSup] Metadata Profile for Algorithm Support Version 1.0, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-v1.0-cs01.pdf

[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

[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

[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

[STORK] D4.4 First version of Technical Specifications for the cross border Interface https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=6&cid=64

[XML-DSig] XML Digital Signature, http://www.w3.org/TR/xmldsig-core/

eIDAS SAML Message Format - Version 1.2

2019 – 31 pages