eIDAS SAML Message Format

Version 1.0

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 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.

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-Services MUST publish all their supported attributes as `<saml:Attribute>` elements in the `<md:IDPSSODescriptor>` element according to [SAML2Meta].

eIDAS-Services MUST publish its highest supported Level of Assurance as entity attribute according to [MetaAttr] in the `<md:Extension>` element. The `NameFormat` of the including `<saml:AttributeValue>` 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 2.1.1). 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 5.3) 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.

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 ProviderName to indicate the actual service provider filing the authentication request. <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 MUST limit the value of the Comparison attribute of <saml2p:RequestedAuthnContext> to "minimum".

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>.

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:

http://eidas.europa.eu/LoA/low
http://eidas.europa.eu/LoA/substantial
http://eidas.europa.eu/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].

4 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.

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="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">

<xs:element name="SPType" type="SPTypeType"/>

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

5.2 <eidas:RequestedAttributes>

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

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema
      xmlns="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">
<xs:element  name="RequestedAttributes"  type="eidas:RequestedAttributesType"
/>
      <xs:complexType name="RequestedAttributesType">
      <xs:sequence>
      <xs:element            minOccurs="0"            maxOccurs="unbounded"
ref="eidas:RequestedAttribute"/>

      </xs:sequence>

      </xs:complexType>

</xsd:schema>
```

5.3 <eidas:RequestedAttribute>

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

```
<?xml version="1.0" encoding="UTF-8"?>

<xsd:schema

      xmlns="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">

<complexType name="RequestedAttributeType">

      <sequence>

      <element   ref="eidas:AttributeValue"   type="anyType"   minOccurs="0"
maxOccurs="unbounded"/>

      </sequence>

      <attribute name="Name" type="string" use="required"/>

      <attribute name="NameFormat" type="anyURI" use="required"/>

      <attribute name="FriendlyName" type="string" use="optional"/>

      <anyAttribute namespace="##other" processContents="lax"/>

      <attribute name="isRequired" type="boolean" use="optional"/>

</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"
         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/2001/04/xmldsig-more#rsa-sha256"/>
          <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/2001/04/xmldsig-more#rsa-sha256"/>
      </md:Extensions>
    <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="false"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <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>
        <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes 256-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"
        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: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”
  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/2001/04/xmldsig-more#rsa-sha256”/>
        <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>MIIDPWA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  <md:Extensions>
    <mdattr:EntityAttributes">
       <saml2:Attribute
           Name="http://eidas.europa.eu/LoA"
           NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
           <saml2:AttributeValue>
             http://eidas.europa.eu/LoA/high
           </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/2001/04/xmldsig-more#rsa-sha256”/>
  </md:Extensions>
    <md:IDPSSODescriptor WantAuthnRequestsSigned=”true”
      protocolSupportEnumeration=”urn:oasis:names:tc:SAML:2.0:protocol“>
      <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>
        <EncryptionMethod Algorithm=“http://www.w3.org/2009/xmlenc11#aes 256-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: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-service.eu</md:OrganizationURL>
  </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"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:eidas="http://eidas.europa.eu/saml-
extensions">
  <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-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/2000/09/xmldsig#rsa- sha1"/>
      <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#sha1"/>
        <ds:DigestValue>EFe8x1Gvm5RVmrBaWM5RrQm81xk=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>SaO8==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>nEPz==</ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </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/2001/04/xmldsig-more#rsa-sha256"/>
   <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#Content">
   <xenc:EncryptionMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
   <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-1_5"/>
     <ds:KeyInfo>
      <ds:KeyValue>
       <ds:RSAKeyValue>
        <ds:Modulus>vOD </ds:Modulus>
        <ds:Exponent>AQAB </ds:Exponent>
       </ds:RSAKeyValue>
      </ds:KeyValue>
     </ds:KeyInfo>
     <xenc:CipherData>
      <xenc:CipherValue>MDTq </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="_47482789069732322d02d825c9a2fafa" IssueInstant="2015-04-30T19:27:20.159Z"
  Version="2.0" xmlns:saml2="urn:oasis:names:tc:saml2:2.0: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>
```

```xml
         <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 languageID="en-GR" xsi:type="eidas:CurrentFamilyNameType">
         Ωνάσης
      </saml2:AttributeValue>
      <saml2:AttributeValue eidas:Transliterated="true" xsi:type="eidas:CurrentFamilyNameType">
         Onasis
      </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 languageID="en-GB" 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>
```

7 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

[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/