

OP Identity Provider Service

Contents

1	General description	1
2	Software requirements	1
2.1	OP logo to be used	1
2.2	User interface	1
2.3	Supported browsers	2
3	Agreement	2
3.1	Contractual changes	2
4	Implementation steps	3
4.1	OP's metadata	3
4.2	OP's signature certificate	4
4.3	Notification of metadata (profile and certificates)	4
4.4	Integration with the test environment	4
4.4.1	Data needed for the test environment	5
4.4.2	Limitations of the test environment	5
4.5	Production verification	5
5	Contact information	5
6	APPENDIX 1 OP's luottamusverkosto integration guide	6

1 General description

The Finnish Trust Network (FTN) consists of identification service providers issuing strong identification devices that are used to provide the Authentication Service, and parties acting as identification broker service providers. OP operates in the Finnish Trust Network as a strong electronic identification device provider. The service offered is OP Identity Provider Service. The service is offered through an SAML2 interface.

This description explains how OP Identity Provider Service is implemented. The description contains an interface description and sample messages (Appendix 1). Identification Service does not handle optional attributes.

Use of OP Identity Provider Service requires that the contract and user conditions have been accepted. Once accepted, the system is implemented as described herein.

The services and interfaces conform to regulation no. 72 by the Finnish Communications Regulatory Authority about electronic identification and trust services. The details of the regulation are found in <https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen>.

2 Software requirements

2.1 OP logo to be used

The Identity Service Broker must be equipped with an OP logo submitted by OP when the contract is made.

2.2 User interface

OP Identity Provider Service has a web-based responsive user interface. The user interface is available in Finnish, Swedish and English. The user interface offered by OP Identity Provider Service may not be modified and must be delivered to the customer as supplied by OP.

2.3 Supported browsers

OP Identity Provider Service works with the most commonly used browsers. We recommend that you use the latest browser version. In order for the service to work, you must allow http session cookies and JavaScript browser scripts.

The supported browsers and instructions for the use of cookies and JavaScript are found in [op.fi](#) under Use of OP eServices.

3 Agreement

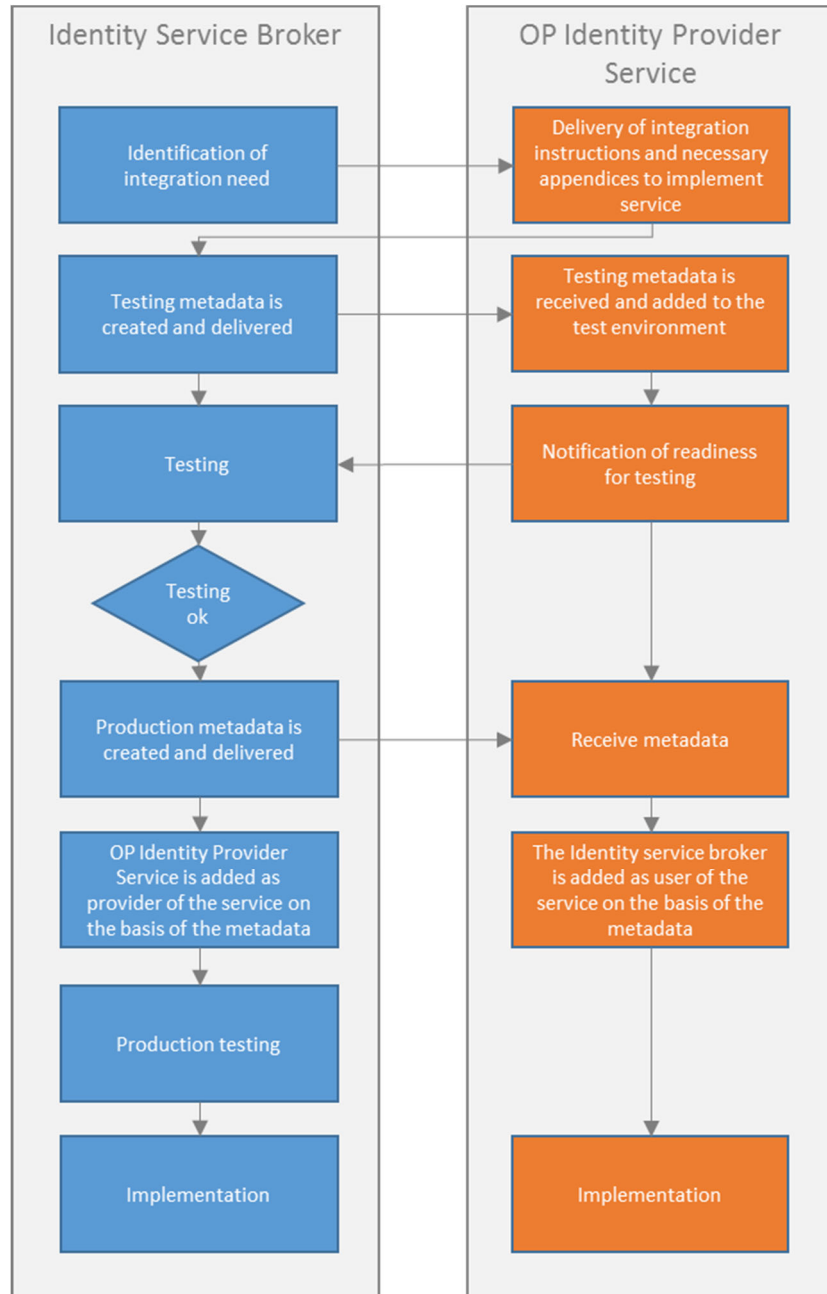
It has been decided in the agreement between the identity service broker and OP Identity Provider Service for which purpose the authentication forwarding service will use strong electronic authentication. The service can be used not only for authentication but also to chain credentials, that is, either to grant strong electronic credentials or weak credentials. These three types of use are discussed below as contract types: identity verification, chaining of strong credentials, and chaining of weak credentials.

3.1 Contractual changes

If you want to add or remove the chaining of strong electronic credentials or weak electronic credentials, the contract must be changed.

4 Implementation steps

The metadata and certificates used in the service are exchanged between OP Identity Provider Service and the owner of the authentication forwarding service. A more detailed interface description with examples is found at the end of the document, in Appendix 1.



4.1 OP's metadata

The Identity Service Broker must retrieve OP's production metadata during implementation from op.fi's page Certificate service, under 'OP Tunnistuspalvelun varmenteet ja metatiedot'. The metadata is downloaded from the following link:

- Download metadata, metadata for OP Identity Service Provider service (xml).

4.2 OP's signature certificate

OP's signature certificate is valid for two years. OP publishes a new certificate alongside the one that is expiring, and informs the Identity Service its implementation date. During the transition period, old and new certificates can be used side by side.

The Identity Service Broker must retrieve OP's signature certificate's public part from op.fi's page Certificate service, under 'OP Tunnistuspalvelun varmenteet ja metatiedot'. The certificate link is named as follows:

- Download certificate, signature certificate for OP Identity Service Provider service

4.3 Notification of metadata (profile and certificates)

OP will send, using encrypted email, the eService's technical contact person a form about data needed to start using the service. The appropriately filled form and SAML2 metadata as specified in Appendix 1 will be returned by replying to the encrypted email.

Your PartnerId must be entered in the appropriate form for each contract type (identity verification, chaining of strong credentials, and chaining of weak credentials). The PartnerId is used to specify the authentication forwarding service and the purpose of identity verification. The PartnerId must be in exactly the same format as EntityId is in the metadata.

Metadata must be sent to each contract type separately. Metadata files must be named clearly to easily know what they should be used for. Include, for example, the business ID or organisation name and the contract type extension (authentication, weak chain or strong chain). The file names are included in the above form.

It is the authentication forwarding service's duty to keep track of the certificate's validity and to get a new one in time. The recommended period of validity for a certificate is two years. The authentication forwarding service is responsible for renewing its certificate and emailing it to OP to verkkopainikkeet@op.fi. It is not necessary to send the entire metadata file. The SAML2 interface enables adding a new certificate in addition to the old certificate, meaning that the new certificate will be taken into use when the old one expires.

4.4 Integration with the test environment

Testing between OP Identity Provider Service and the integrating transmission service takes place in an environment similar to production, having the same requirements as in production. The test environment tests technical integration in the SAML2 interface and the proper functioning of metadata and the certificate. OP's test environment functions the same way as the OP Identity Provider Service, but authentication in the test environment can only be done with certain test identifiers. For testing purposes, customers must send the SAML2 metadata used in the testing by encrypted email. The test environment follows the implementation stages detailed in Chapter 4.

The following should be used in testing:

- Username: 12345678
- Password: 1234
- Key code: 1234

The following identity data will always be returned in the test environment:

- Personal identity code: 070770-905D
- Name: Väinö Tunnistus
- Date of birth: 7 July 1970

4.4.1 Data needed for the test environment

OP's test certificates and metadata can be obtained from op.fi's page Certificate service, under 'OP Tunnistuspalvelun testiympäristön varmenteet ja metatiedot'. The certificates and metadata are downloaded from links that have been names as follows:

- Download certificate, test signature certificate for OP Identity Provider Service
- Download metadata, test metadata signature certificate for OP Identity Provider Service

The URL for testing the OP Identity Provider Service is :

<https://saml-idp.test.op.fi/FIM/sps/LVASOPIDP/saml20/login>

The address used for testing is also in the OP metadata <md:EntityDescriptor> element's attribute entityID:

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://saml-idp.test.op.fi/FIM/sps/LVASOPIDP/saml20">

4.4.2 Limitations of the test environment

The test environment is intended for testing the validity of a SAML request and SAML response. This is why we do not offer interruption or error handling testing in the test environment.

4.5 Production verification

Production must be verified by logging into the OP Identity Provider Service using strong electronic credentials obtained from OP.

5 Contact information

For questions regarding the Identity Provider, please phone

- OP Corporate and Payment Services, 0100 05151 or
- send email to verkkopainikkeet@op.fi

Any changes in contact person details must be reported to OP's designated contact person.

6 APPENDIX 1 OP's luottamusverkosto integration guide

Contents

1	Terminology	7
2	SAML	7
2.1	Certificates	7
2.2	Partner profile	8
2.2.1	Metadata description	8
2.2.2	Metadata/partner profile example.....	10
2.3	SAML request.....	10
2.3.1	SAML Destination	11
2.3.2	SAML request interface description	11
2.3.3	SAML AuthnRequest message example.....	13
2.4	SAML response	14
2.4.1	Response validations	15
2.4.2	SAML Response – receive and -send destinations.....	15
2.4.3	SAML response interface description	15
2.4.4	SAML Response sample message.....	20
2.5	Error situations	23
2.6	Metadata template.....	23
2.6.1	Metadata example in xml-format	25

1 Terminology

Finnish Trust Network = FTN : The Finnish Trust Network is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. It is formed by the actors in the network who are requesting, forwarding or providing authentications.

Service Provider = SP : The service which requests authentication

Identity Provider = IdP : The service which authenticates the user

Identity Service Broker: The service which forwards the requests and responses between SP and IdP

2 SAML

Service functionality follows specification of Viestintävirasto: Finnish Trust Network SAML 2.0 Protocol Profile and SAML2 specification.

Finnish Trust Network uses SAML messages for moving identity information. SAML messages are signed and encrypted. They include all the necessary information for the authentication process.

When requesting authentication from OP's IdP, SAML AuthnRequest message needs to be sent. This message requests an authentication from the service to which it is sent. The user is forwarded into IdP's authentication process and on completion of the process, a new SAML Response is created and sent back to the requesting service. The SAML Response is connected to the SAML Request message. SAML Response includes information on whether the authentication process was successful with the needed identity information on user, which tells to the requesting service that an actual user with credentials is using the system.

In FTN SAML messages will be moved between services with POST – method of HTTP standard. SAML 2.0 standard defines the bindings of HTTP-methods, how SAML-message is moved in each of HTTP-methods.

Service can request authentication from OP's IdP by sending a AuthnRequest message with a return destination by using users browsers POST-method.

OP's IdP will do the authentication process and then OP's IdP will send the response message for the requesting service by making POST-command into the return destination described in the request.

Metadata exchange is required before the integrating service can start using OP Idp.

All connections are protected by TLS 1.2. This means that all request and response messages will be transmitted using HTTPS-connections. OP's IdP should be requested by using HTTPS protocol.

All SAML-messages are signed to ensure on the sender, the integrity of the message and that the message has not been altered. All parties need to verify the signature of the received messages.

Next, SAML messages are introduced in detail and how the messages can be utilized in FTN. The focus will be on the integration into OP's IdP.

2.1 Certificates

OP SAML Idp accepts self-signed signature certificates.

OP uses certificate generated by OP's own CA.

The TLS server X.509 certificates that are used to protect communication with client web browsers MUST be generally trusted by browsers (95+%). OP will use Symantec Class 3 EV SSL CA - G3 at least until 30.10.2023.

Signature certificates on request and response messages have to be SHA-256. In Finnish Trust Network the <saml2p:AuthnRequest> messages need to be signed, and Identity Providers will not accept messages that are not signed, or where the verification of the signature fails.

2.2 Partner profile

To be able to make the integration, OP Identity provider and the service which are going to integrate, need to exchange metadata for to create Partner Profiles. With these partner profiles, different actors can integrate into others systems and identify others for right actions in FTN.

The following information is required for the partner profile:

- Certificate
- Response URL: all URLs have to be added to the metadata so that SAML responses go into the right destination. This should be put in element <md:AssertionConsumerService> in <location> attribute.
- PartnerId: At least one ID value is required. If SP is providing also service to create new credentials then one additional partnerId value is required for weak credentials and one for strong credentials case. PartnerId is mapped to Issuer on SAML request.

2.2.1 Metadata description

Specific metadata should be exchanged between Identity Service Broker and OP IdP for the integration to work. The partner profiles are created using the exchanged metadata. Partner profiles are then used to identify different actors in FTN. This enables the integration and provides information for right handling process.

Next table will present the metadata is described in detail. This metadata represents the metadata which Identity service broker will provide for OP's IdP.

Level	Name	Attribute	Value	Required	About
0	<md:EntitiesDescriptor>			Optional	Used if multiple entities are presented for metadata. Different entities can be included inside this element.
1	<md:EntityDescriptor>			MUST	
		xmlns:md	urn:oasis:names:tc:SAML:2.0:metadata		
		entityID	http://...	MUST	This is the ID with which the partners are recognized within FTN.
2	<md:SPSSODescriptor>				
		AuthnRequestsSigned	TRUE	MUST	
		WantAssertionsSigned	TRUE	MUST	Metadata must include value <WantAuthnRequestsSigned> element with value "true".
		protocolSupportEnumeration	urn:oasis:names:tc:SAML:2.0:protocol		
3	<md:KeyDescriptor>			MUST	This includes the signing key.
		use	signing		
4	<KeyInfo>	xmlns	http://www.w3.org/2000/09/xmldsig#	MUST	Cotains relevant key information.
5	<X509Data>				
6	<X509Certificate>		MIICRzCCA...WiHUsogetpcqgOqNk=		

3	<md:KeyDescriptor			MUST	This includes the encryption key.
		use	encryption		
4	<KeyInfo				
		xmlns	http://www.w3.org/2000/09/xmldsig#		
5	<X509Data>				
6	<X509Certificate>		MIICRzCCA...WiHUsogetpcqg OqNk=	MUST	
6	<md:EncryptionMethod			MUST	Key transport algorithm.
		Algorithm	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	MUST	
3	<md:ManageNameIDService >				
		Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST		
		Location	http://...		
3	<md:NameIDFormat>		urn:oasis:names:tc:SAML:2.0:nameid-format:transient	MUST	
3	<md:AssertionConsumerService>			MUST	Describes the endpoint of the assertion.
		Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	MUST	The method for binding.
		Location	http://...	MUST	Desired response location.
		index	0		
		isDefault	TRUE		
2	<md:Organization>				The information of the organization are included in this element.
3	<md:OrganizationName >		OP		
		xml:lang	en		
3	<md:OrganizationDisplayName>		OP		
		xml:lang	en		
3	<md:OrganizationURL>				
		xml:lang	en		
2	<md:ContactPerson>				
		contactType	Technical		
3	<md:Company>		OP		The information of the company are included in this element
3	<md:GivenName/>				
3	<md:SurName/>				
3	<md:EmailAddress/>				
3	<md:TelephoneNumber />				

2.2.2 Metadata/partner profile example

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://...">
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>MIICRzCCA...WiHUsogetpcqg0qNk=</X509Certificate>
</X509Data>
</KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>MIICRzCCA...WiHUsogetpcqg0qNk=</X509Certificate>
</X509Data>
</KeyInfo>
<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
</md:KeyDescriptor>
<md:ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://...">
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://..." index="0"
isDefault="true"/>
</md:SPSSODescriptor>
<md:Organization>
<md:OrganizationName xml:lang="en">OP</md:OrganizationName>
<md:OrganizationDisplayName xml:lang="en">OP</md:OrganizationDisplayName>
<md:OrganizationURL xml:lang="en"/>
</md:Organization>
<md:ContactPerson contactType="technical">
<md:Company>OP</md:Company>
<md:GivenName/>
<md:SurName/>
<md:EmailAddress/>
<md:TelephoneNumber/>
</md:ContactPerson>
</md:EntityDescriptor>
```

2.3 SAML request

SAML AuthnRequest is an authentication request which is sent from Identity service broker to OP's IdP. OP's IdP will receive the SAML AuthnRequest message and will provide the authentication service for the user.

SAML AuthnRequest messages MUST be signed, and Identity Providers will not accept messages that are not signed, or where the verification of the signature fails. In these cases, the Identity Provider will respond with an error message. The signature for an authentication request messages is applied differently depending on the binding.

The hash algorithm used in creation of signatures in SAML messages need to be SHA-256 or stronger.

HTTP-POST binding must be signed using signature –element.

Request must have valid Issuer –value which can be found from partner profile metadata.

NameIDPolicy urn:oasis:names:tc:SAML:2.0:nameid-format:transient is supported and allowCreate –element is set false.

RequestedAuthnContext is exact and only Finnish level of authentication is supported.

OP Idp accepts only signed requests and verifies signature certificate including expiration.

AssertionConsumerServiceURL is compared to partner profile and must match one of the values on partner's metadata.

ForceAuthn attribute must be set true.

IsPassive attribute must be set false.

Supported Extensions in the <samlp:Extensions><ftn xmlns="http://ftn.ficora.fi/2017/req_ext"> are: <lg>fi</lg>, <lg>en</lg>, <lg>sv</lg>and the <spname>insert the original requestors' provided name as value here</spname>.

2.3.1 SAML Destination

The SAML request message needs a destination URL for the message to get into IdP. The destination should be put in the "Destination" attribute of the AuthnRequest message. The destination URL can be found from the metadata, provided by OP, in element <md:AssertionConsumerService> in attribute "Location".

Destination URL, where the SAML is wanted to be received, should be stated in AuthnRequest messages "AssertionConsumerServiceURL" attribute. It should also be stated in the metadata.

2.3.2 SAML request interface description

Next table will present the elements and attributes which are contained in the SAML request message.

Level	Element	Attribute	Required	Value	About
1	<saml2p:AuthnRequest>		MUST		This is the actual authentication request.
		AssertionConsumerServiceURL	MUST	URL	Desired response location URL
		Destination	MUST	URL	URL to which the Service Provider has instructed the user agent to deliver the request
		ID	MUST		An unique ID for a SAML message.
		ForceAuthn	MUST	true	A Boolean value. If "true", the identity provider MUST authenticate the presenter directly rather than rely on a previous security context. If a value is not provided, the default is "false".
		IsPassive	MUST	false	If "true", the identity provider MUST authenticate the presenter directly rather than rely on a previous security context.
		IssueInstant	MUST	YYYY-MM-DDThh:mm:ss	The creation time of the request. Must use a form of DateTime type of W3C XML Schema: "YYYY-MM-DDThh:mm:ss" encoded in UTC without time zones.

		ProtocolBinding	Optional		A URI reference that identifies a SAML protocol binding to be used when returning the <Response>.
		Version	MUST	2.0	States the version of SAML.
	<saml:Issuer		MUST	http://...	ID of the responding service. References to the EntityID attribute in metadata. URL-format.
		Format	MUST	urn:oasis:names:tc:SAML:2.0:nameid-format:entity	
2	<ds:Signature>		MUST		<ds:Signature> is defined in [XMLDSig]
		Id	MUST	uuid13303fc8-...-d7a142aeadd	
3	<ds:SignedInfo>		MUST		
4	<ds:CanonicalizationMethod>		MUST		
		Algorithm	MUST	http://www.w3.org/2001/10/xml-exc-c14n#	SAML implementations SHOULD use Exclusive Canonicalization [Excl-C14N].
4	<ds:SignatureMethod>		MUST		
		Algorithm	MUST		
4	<ds:Reference>		MUST		The signature must include a single <ds:Reference> containing the ID attribute value of the <samlp:AuthnRequest> element
		URI	MUST	#FIMREQ_d7a...aeadd	
5	<ds:Transforms>		MUST		
6	<ds:Transform>				
		Algorithm		http://www.w3.org/2000/09/xmldsig#enveloped-signature	
	<ds:Transform>				
		Algorithm		http://www.w3.org/2001/10/xml-exc-c14n#	
7	<xc14n:InclusiveNamespaces>				
		xmlns:xc14n		http://www.w3.org/2001/10/xml-exc-c14n#	
		PrefixList		samlp xs saml xsi ds	
5	<ds:DigestMethod>		MUST		
		Algorithm	MUST	http://www.w3.org/2001/04/xmenc#sha256	
5	<ds:DigestValue>		MUST	eUT...KTM8=	
3	<ds:SignatureValue>		MUST	GM...STo=	
3	<ds:KeyInfo>		MUST		
4	<ds:X509Data>		MUST		
5	<ds:X509Certificate>		MUST		

2	<saml2p:NameIDPolicy>		MUST		
		AllowCreate	MUST	false	A Boolean value used to indicate whether the identity provider is allowed in the course of fulfilling the request, to create new identifier to represent the principal. Need to be false when using urn:oasis:names:tc:SAML:2.0:nameid-format:transient in NameIDPolicy.
		Format	MUST	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	MUST be set to urn:oasis:names:tc:SAML:2.0:nameid-format:transient.
		SPNameQualifier	Optional	https://	Further qualifies an identifier with the name of a service provider or affiliation of providers. This attribute provides an additional means to federate identifiers on the basis of the relying party or parties.
2	<saml2p:RequestedAuthnContext>		MUST	MUST specify the exact authentication assurance level. Need to use Finnish level of authentication (ftn.ficora): loa2 or loa3	In FTN there are not yet loa3 services. So all will be Finnish level loa2.
3	<saml:AuthnContextClassRef>			http://ftn.ficora.fi/2017/loa2	
Extensions 1	<samlp:Extensions><ftn xmlns="http://ftn.ficora.fi/2017/req_ext">		Optional		
Extensions 2	<lg>		Optional	fi , sv, en	Relays the preferred language of the IDP UI.
Extensions 2	<spname>		Optional	String value of the original sp that stated its display value	Relays the display name of the original sp that initiated the authentication process before the broker service

2.3.3 SAML AuthnRequest message example

```

<samlp:AuthnRequest
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="http://..."
Destination="http://..."
ForceAuthn="true"
ID="FIMREQ_5dbd2a-015b...-a4e95c10e08c"
IsPassive="false"
IssueInstant="2017-03-24T12:49:54Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
http://....
</saml:Issuer>

<ds:Signature
Id="uuid5dbd2b-015b-120c-...c10e08c">
<ds:SignedInfo
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
</ds:CanonicalizationMethod>
<ds:SignatureMethod

```

```

Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">
</ds:SignatureMethod>
<ds:Reference
URI="#FIMREQ_5dbd2a-...-a4e95c10e08c">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
</ds:Transform>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<xc14n:InclusiveNamespaces
xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="samlp saml ds">
</xc14n:InclusiveNamespaces>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256">
</ds:DigestMethod>
<ds:DigestValue>OCA7kzF2...Tzew7l=
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>M6a0wC3+mjf0+fP8xCdvSQm0Bec...Bd3YQaszho0B4oTmw=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICRzCCAbCgAwIBA...xHWWiHUsogetpcqgOqNk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

<samlp:NameIDPolicy
AllowCreate="false"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" SPNameQualifier="http://...">
</samlp:NameIDPolicy>
<samlp:RequestedAuthnContext>
<saml:AuthnContextClassRef>http://ftn.ficora.fi/2017/loa2</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
</samlp:AuthnRequest>

```

2.4 SAML response

Identity provider will always respond with SAML message containing user identity or error described on SAML specification. SAML response's assertion element is returned on encrypted EncryptedAssertion –element. In addition the whole response –element is always signed.

Natural person identity contains the following attributes:

- Family name
- First name
- Date of birth
- Identifier attribute (One need to be given)
 - HETU (Finnish personal identity code)
 - SATU (Finnish electronic client identifier)
 - *Person identifier (eIDAS – not currently supported)*

Subject .element contains always NameID –element and at least one SubjectInformation –element. SubjectConfirmation –element contains one SubjectConfirmationData –element.

SubjectConfirmationData –element contains InResponseTo –element which matches request’s ID –attribute and SP assertion consumer service URL.

Also NotOnOrAfter –attribute is included on Conditions –attribute. TimeStamp is on UTC –time zone. All assertions indicate the LoA which in this case is Finnish level of authentication (ftn.ficora).

2.4.1 Response validations

The Identity Service Broker will verify that the assertion is not used more than once within its validity period through the NotOnOrAfter attribute in element.

Response is validated by using the provided certificates.

2.4.2 SAML Response – receive and –send destinations

SAML Response message needs a return destination for to direct the message into right place as it is sent for Identity Service Broker. This value will be the value of SAML AuthnRequests messages AssertionConsumerServiceURL attribute, from which OP’s IdP collects it as a destination of SAML Response message. This value should also be in the metadata, in element <md:AssertionConsumerService> in attribute “Location”, and these two values, one in SAML and other in the exchanged metadata, will be compared.

Error destination URL and cancel destination URL both need to be provided separately in technical information form. Errors and cancels from IdP will send an unsigned SAML re-sponse in the provided URL. Depending on the case, the included error code is either “AuthnFailed” or “AuthnDenied”.

2.4.3 SAML response interface description

Next table will present the elements and attributes which are included into the SAML response message.

Level	Element	Attribute	Value	Required	About
1	<samlp:Response>			MUST	
		Destination	http://...	MUST	URI reference indicating the address to which this response has been sent.
		ID	FIMRSP_5e02... 3afd	MUST	An unique ID for a SAML message.
		InResponseTo	FIMREQ_5db...10e08c	MUST	The ID of the requesters SAML message.
		IssueInstant	2017-03-24T12:50:12Z	MUST	The creation time of response message. Must use a form of DateTime type of W3C XML Sxhema: "YYYY-MM-DDThh:mm:ss" encoded in UTC without time zones.
		Version	2.0	MUST	Used SAML version.
2	<saml:Issuer>		http://...	MUST	The SAML authority that is making the claim(s) in the assertion. ID of the requesting service. References to the EntityID attribute in metadata. URL-format.
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity	MUST	
2	<ds:Signature>			MUST	An XML Signature that protects the integrity of and authenticates the issuer of the assertion.
		Id	uuid5e02df-0...8d56-96ec11413afd		An unique ID for a signature.

3	<ds:SignedInfo>			MUST	
4	<ds:CanonicalizationMethod>				
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#		
4	<ds:SignatureMethod>			MUST	
		Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	MUST	
4	<ds:Reference>			MUST	Signatures MUST contain a single <ds:Reference> containing a same-document reference to the ID attribute value of the root element of the assertion or protocol message being signed. For example, if the ID attribute value is "foo", then the URI attribute in the <ds:Reference> element MUST be "#foo".
		URI	#FIMRSP_14f7...13c563f7	MUST	
5	<ds:Transforms>			MUST	Signatures in SAML messages SHOULD NOT contain transforms other than the enveloped signature transform (with the identifier http://www.w3.org/2000/09/xmldsig#enveloped-signature) or the exclusive canonicalization transforms (with the identifier http://www.w3.org/2001/10/xml-exc-c14n# or http://www.w3.org/2001/10/xml-exc-c14n#WithComments).
6	<ds:Transform>				
		Algorithm	http://www.w3.org/2000/09/xmldsig#enveloped-signature		
6	<ds:Transform>				
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#		
7	<xc14n:InclusiveNamespaces>			MUST	
		xmlns:xc14n	http://www.w3.org/2001/10/xml-exc-c14n		
		PrefixList	samlp xs saml xsi ds		
5	<ds:DigestMethod>			MUST	
		Algorithm	http://www.w3.org/2001/04/xmenc#sha256	MUST	
5	<ds:DigestValue>		MfeyJcaK...tmZ0=	MUST	
3	<ds:SignatureValue>		UfQyvR9wTdJEo...ou3StSnx/tlbo=	MUST	
3	<ds:KeyInfo>			MUST	XML Signature defines usage of the <ds:KeyInfo> element.
4	<ds:X509Data>			MUST	
5	<ds:X509Certificate>		MIICRTCCAa6gAwIBAgIEWIHZ6...TN1QJB5QhHEr+tr	MUST	

2	<samlp:Status>			MUST	Informs the requesting service about how the authentication process went. A code representing the status of the corresponding request.
3	<samlp:StatusCode>			MUST	A code representing the status of the activity carried out in response to the corresponding request.
		Value	urn:oasis:names:tc:SAML:2.0:status:Success – <i>The request succeeded</i>	MUST	The <StatusCode> element specifies a code or a set of nested codes representing the status of the corresponding request.
2	<saml:EncryptedAssertion>			MUST	This element includes the assertion, and all information included in it, as encrypted. Encrypted assertions are intended as a confidentiality protection mechanism when the plain-text value passes through an intermediary.
3	<EncryptedData>			MUST	The encrypted content and associated encryption details.
		xmlns	http://www.w3.org/2001/04/xmlenc#	MUST	
		Id	uuid14f77024-0...a24b13c563f7	MUST	
		Type	http://www.w3.org/2001/04/xmlenc#Element	MUST	
4	<EncryptionMethod>			MUST	Encryption method. Need to use aes-256.
		Algorithm	http://www.w3.org/2001/04/xmlenc#aes256-cbc	MUST	
4	<ds:KeyInfo>			MUST	
5	<EncryptedKey>			MUST	
		Id	uuid14f77025...8f4d-a24b13c563f7	MUST	
6	EncryptionMethod			MUST	
		Algorithm	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	MUST	Key transport algorithm.
6	<ds:KeyInfo>			MUST	
7	<ds:KeyName>			MUST	Name of the key.
6	<CipherData>			MUST	The CipherData is a mandatory element that provides the encrypted data.
7	<CipherValue>		Ob6JUy7ekGsGXREZH5UPA...Vkpq2qPZCCAFNqd/MQ=	MUST	The actual encrypted data is the value of this element.
4	<CipherData>			MUST	
5	<CipherValue>		Uf63y3x1AEGXZQ1nXzujUpUdME0....ffljg97boZufdjUwsc2fpb8=	MUST	
<saml:Assertion> element is encrypted in the element <EncryptedAssertion>. Below is an example of the information in the Assertion element.					
2	<saml:Assertion>			MUST	The entire element issued by the Identity Provider MUST be returned in an encrypted element that is covered by the signature.

		ID	Assertion-...1413afd	MUST	
		IssueInstant	2017-03-24T12:50:12Z	MUST	
		Version	2.0	MUST	
3	<saml:Issuer>		http://...	MUST	
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity	MUST	
3	<ds:Signature>			MUST	
		Id	uuid5e02d7-015b...-bba1-96ec11413afd	MUST	
4	<ds:SignedInfo>			MUST	
5	<ds:CanonicalizationMethod>			MUST	
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#	MUST	
5	<ds:SignatureMethod>			MUST	
		Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	MUST	
5	<ds:Reference>			MUST	
		URI	#Assertion-...6ec11413afd	MUST	
6	<ds:Transforms>			MUST	
7	<ds:Transform>				
		Algorithm	http://www.w3.org/2000/09/xmldsig#enveloped-signature		
7	<ds:Transform>				
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#		
8	<xc14n:InclusiveNamespaces>			MUST	
		xmlns:xc14n	http://www.w3.org/2001/10/xml-exc-c14n#		
		PrefixList	xs saml xsi		
6	<ds:DigestMethod>			MUST	
		Algorithm	http://www.w3.org/2001/04/xmenc#sha256	MUST	
6	<ds:DigestValue>		rtyLMi...lxPslI8=	MUST	
4	<ds:SignatureValue>		FdVPaDfigTB3EghBTOxW8MGFs5NwylX2DiSB...	MUST	
4	<ds:KeyInfo>				
5	<ds:X509Data>				
6	<ds:X509Certificate>				
3	<saml:Subject>				
4	<saml:NameID>		uuid5e0257-...a6b7-96ec11413afd	MUST	

		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	MUST	
		NameQualifier	http://...		
		SPNameQualifier	http://...		
4	<saml:SubjectConfirmation>				
		Method	urn:oasis:names:tc:SAML:2.0:com:bearer		
	<saml:SubjectConfirmationData>			MUST	
		InResponseTo	FIMREQ_5dbd2a-...-a693-a4e95c10e08c	MUST	The InResponseTo attribute MUST be present and its value MUST match the value of the corresponding request's ID attribute.
		NotOnOrAfter	2017-03-24T12:51:12Z	MUST	NotOnOrAfter timestamp MUST be 10 minutes or less into the future at the time of issuance
		Recipient	http://...	MUST	MUST also include a recipient attribute containing the SP assertion consumer service URL
3	<saml:Conditions>			MUST	Identity service broker MUST verify that the assertion is not used more than once within its validity period through the NotOnOrAfter attribute in element
		NotBefore	2017-03-24T12:50:12Z	OPTIONAL	
		NotOnOrAfter	2017-03-24T12:51:12Z	MUST	This is the time for how long the SAML is valid. The Identity Service Broker MUST verify that the assertion is not used more than once within its validity period through the NotOnOrAfter attribute in element.
4	<saml:AudienceRestriction>				
5	<saml:Audience>		http://...		
3	<saml:AuthnStatement>				
		AuthnInstant	2017-03-24T12:50:12Z		
		SessionIndex	uuid5dbdcb-...413afd		
		SessionNotOnOrAfter	2017-03-24T13:50:12Z		
4	<saml:AuthnContext>			MUST	
5	<saml:AuthnContextClassRef>		http://ftn.ficora.fi/2017/loa2	MUST	
3	<saml:AttributeStatement>			MUST	
4	<saml:Attribute>			MUST	There can be many <saml:Attribute> elements with different information in Assertion
		Name	urn.oid:1.2.246.575.1.14	MUST	saml:AttributeValue depends on the value given for saml:Attribute Name: urn.oid:2.5.4.4 – FamilyName urn.oid:1.2.246.575.1.14 – FirstNames

					urn:oid:1.3.6.1.5.5.7.9.1 – DateOfBirth urn:oid:1.2.246.21 – HETU urn:oid:1.2.246.22 – SATU <i>http://eid.as.europa.eu/attributes/natural/person/PersonIdentifier - PersonIdentifier (not supported)</i> MUST choose one of the two last ones (HETU, SATU (personIdentifier is not supported)).
		NameFormat	urn:oasis:names:tc:SAML:2.0:attrname-format:uri	MUST	NameFormat SHALL contain the value urn:oasis:names:tc:SAML:2.0:attrname-format:uri
6	<saml:AttributeValue>		Väinö	MUST	The actual value of "Name" attribute. If Name was urn:oid:2.5.4.42 then here lies FirstName like "Matti".
		xsi:type	xs:string		

2.4.4 SAML Response sample message

```

<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
Destination="http://...login"
ID="FIMRSP_14f77059-...-a24b13c563f7"
InResponseTo="FIMREQ_14f73740...91a1-c7a31aee6a66"
IssueInstant="2017-03-28T12:50:12Z"
Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://...
</saml:Issuer>
<ds:Signature Id="uuid14f7705c-015b...a24b13c563f7">
<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="#FIMRSP_14f77059-015b-...68-a24b13c563f7">
<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#">
<xc14n:InclusiveNamespaces xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="samlp xs saml xsi ds"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmllenc#sha256"/>
<ds:DigestValue>l56zi0KE7Y9...U+R6UjtT8=
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>UfQyvR9wTdSkQ0XTBEHQzh4yflQjzJEo...ou3StC+0CdJ4CxiW3bD64Q7PSnx/tlbo=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICRTCCAa6gAwIBAgIEWIH6...TN1QJB5QhHEr+tr
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<samlp>Status>
    
```

```
<samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:StatusCode>
<saml:EncryptedAssertion>
<EncryptedData
xmlns="http://www.w3.org/2001/04/xmlenc#"
Id="uuid14f77024-015b-...-a24b13c563f7"
Type="http://www.w3.org/2001/04/xmlenc#Element">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
<ds:KeyInfo>
<EncryptedKey
Id="uuid14f77025-015b-...-a24b13c563f7">
<EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
<ds:KeyInfo>
<ds:KeyName>KeyName
</ds:KeyName>
</ds:KeyInfo>
<ds:KeyInfo>
<CipherData>
<CipherValue>Ob6JUy7ekGsA...Vkqo2qQd/MQ=
</CipherValue>
</CipherData>
</EncryptedKey>
</ds:KeyInfo>
<ds:KeyInfo>
<CipherData>
<CipherValue>Uf63y3x1AEGXZQdMEO...ffljg97c2fpb8=</CipherValue>
</CipherData>
</EncryptedData>
</saml:EncryptedAssertion>
</samlp:Response>
```

Elements and attributes which are encrypted inside *EncryptedAssertion* element:

```
<saml:Assertion
ID="Assertion-uuid5e02d5-...-96ec11413afd"
IssueInstant="2017-03-24T12:50:12Z" Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://...
</saml:Issuer>
<ds:Signature
Id="uuid5e02d7-015b-...-96ec11413afd">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
</ds:CanonicalizationMethod>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">
</ds:SignatureMethod>
<ds:Reference
URI="#Assertion-uuid5e02d5-...-8d97-96ec11413afd">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
</ds:Transform>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<xc14n:InclusiveNamespaces
xmlns:xc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="xs saml xsi">
</xc14n:InclusiveNamespaces>
```

```
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256">
</ds:DigestMethod>
<ds:DigestValue>rtyLMiXZY...LxLlxPsl8=
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>FdVPaDfigTB3EghBTOxW...xTDphn2HkQ569NM1q0xNppJPQnjQSF4zfWu3mkypevXWBkvLX7urYQv+Q+QLU=
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICRTCCAa6gAwIBAg...BgkqhkiG9w0BAQUFADBRMtr
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
NameQualifier="http://..."
SPNameQualifier="http://...">uuid5e0257-015b-...-96ec11413afd</saml:NameID>
<saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData
InResponseTo="FIMREQ_5dbd2a-...-a4e95c10e08c"
NotOnOrAfter="2017-03-24T12:51:12Z"
Recipient="http://...">
</saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions
NotBefore="2017-03-24T12:50:12Z"
NotOnOrAfter="2017-03-24T12:51:12Z">
<saml:AudienceRestriction>
<saml:Audience>http://...
</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement
AuthnInstant="2017-03-24T12:50:12Z"
SessionIndex="uuid5dbdcb-...a538-96ec11413afd"
SessionNotOnOrAfter="2017-03-24T13:50:12Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>http://ftn.ficora.fi/2017/loa2
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute
Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">Väinö
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:1.2.246.575.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">urn.oid.1.2.246.21
</saml:AttributeValue>
```

```

</saml:Attribute>
<saml:Attribute
Name="urn:oid:1.3.6.1.5.5.7.9.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">1970-07-07
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:1.2.246.575.1.2"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">070770-905D
</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">Tunnistus
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
  
```

2.5 Error situations

The authentication process can end up in error. If status is "urn:oasis:names:tc:SAML:2.0:status:Success", this means that the authentication process was successful and there is no need for error handling.

SAML protocol errors are returned immediately back to requester with SAML error message into AssertionConsumerService-URL found in request message.

Other unsuccessful events are returned to either error URL or cancel URL, depending on case. These URL-addresses are needed to be provided from integrating partner in the technical information document. These addresses are added in the profile of the requester and they are used for returning an unsigned response SAML to the provided URLs.

All recoverable errors are shown on UI with dedicated return link. User can decide to go back to service provider (in this case broker) by clicking the return link. Return link sends an unsigned SAML error response with an error code "AuthnFailed" or "AuthnDenied" into the error URL given by the Identity Service Broker.

User can cancel the identification flow by pressing the cancel button on UI. This creates an unsigned SAML response with error code "AuthnFailed" into the cancel URL given by the Identity Service Broker.

The party which receives the error SAML is responsible of how the handling and/or communication of the error.

2.6 Metadata template

Metadata xml-file should be created with the instructions and examples below. Sections that need to be completed in the template are marked with "TODO".

Level	Element	Attribute	Value	Required	About
0	<md:EntitiesDescriptor>			Optional	Used if multiple entities are presented in metadata. Different entities can be included inside this element in <md:EntityDescriptor> elements.
1	<md:EntityDescriptor>			MUST	Describes information of one specific entity (partner).

		xmlns:md	urn:oasis:names:tc:SAML:2.0:metadatas	MUST	Format
		entityID	TODO	MUST	This is the ID with which the partners are recognized within FTN. Should be in URL-format.
2	<md:SPSSODescriptor>			MUST	Includes information that is specific to service provider.
		AuthnRequestsSigned	true	MUST	Indicates whether the <samlp:AuthnRequest> messages sent by this service provider will be signed. Need to be set TRUE.
		WantAssertionsSigned	true	MUST	This implies that the assertions need to be signed.
		protocolSupportEnumeration	urn:oasis:names:tc:SAML:2.0:protocol	MUST	URI that identify the set of protocol specifications supported.
3	<md:KeyDescriptor>			MUST	This includes the signing key information
		use	signing	MUST	Declares the usage of the key. The key here is used for signing.
4	<KeyInfo>			MUST	
		xmlns	http://www.w3.org/2000/09/xmldsig#	MUST	Format
5	<X509Data>			MUST	
6	<X509Certificate>		TODO	MUST	The signing key.
3	<md:KeyDescriptor>			MUST	This includes the signing key information
		use	encryption	MUST	Declares the usage of the key. The key here is used for encryption.
4	<KeyInfo>			MUST	
		xmlns	http://www.w3.org/2000/09/xmldsig#	MUST	Format
5	<X509Data>			MUST	
6	<X509Certificate>		TODO	MUST	The encryption key.
6	<md:EncryptionMethod>			MUST	
		Algorithm	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	MUST	Key Transport algorithm.
3	<md:NameIDFormat>		urn:oasis:names:tc:SAML:2.0:nameid-format:transient	MUST	Saml-messages in FTN MUST support the urn:oasis:names:tc:SAML:2.0:nameid-format:transient name identifier format
	<md:AssertionConsumerService>			MUST	Describes the endpoint of the assertion.
		Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	MUST	The method for binding.
		Location	TODO	MUST	Desired response location in URL-format.
		index	0	MUST	Uniquely identifies multiple ACS endpoints. Here always 0 as there will be one endpoint.

		isDefault	true	MUST	Defines which is the default endpoint. Must be true for index 0 endpoint.
	<md:Organization>			MUST	The information of the organization are included in this element.
	<md:OrganizationName>		TODO	MUST	Organization name. Eg. "OP"
		xml:lang	en	MUST	Language of the name.
	<md:OrganizationDisplayName>		TODO	MUST	Name of the organization which is visible in systems.
		xml:lang	en	MUST	Language of the name.
	<md:OrganizationURL>		TODO	MUST (value optional)	Organization URL. For example "op.fi"
		xml:lang	en	MUST	Language of the url.

2.6.1 Metadata example in xml-format

```

<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="TODO">
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>TODO</X509Certificate>
</X509Data>
</KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>TODO</X509Certificate>
</X509Data>
</KeyInfo>
<md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="TODO" index="0"
isDefault="true"/>
</md:SPSSODescriptor>
<md:Organization>
<md:OrganizationName xml:lang="en">TODO</md:OrganizationName>
<md:OrganizationDisplayName xml:lang="en">TODO</md:OrganizationDisplayName>
<md:OrganizationURL xml:lang="en"/>
</md:Organization>
</md:EntityDescriptor>
    
```