20 November 2017 Version 1.0

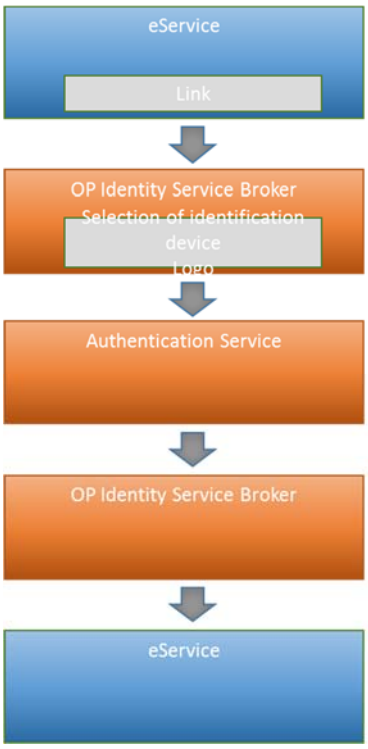
OP Identity Service Broker

Contents

Author	Mailing address	Street address	Telephone	Email/Internet
OP Corporate Bank plc	P.O.Box 308 00013 OP	Gebhardinaukio 1 Helsinki	010 252 010	op.fi

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 the identification broker service provider. The eService requiring Identity Provider Services can thereby obtain from OP the various strong identification devices created with a single contract.



The eService must add a link into its service requiring identity verification that lead to OP Identity Service Broker. A call must be built into the link using the SAML2 interface.

The user interface for OP Identity Service Broker contains the identification service providers available in Luottamusverkosto described in op.fi under the OP Identity Service Broker page. The Identity Service is selected from the logo.

Authentication takes place in the authentication service chose by the customer.

The broker service returns the customer authentication to the eService. If authentication is unsuccessful, an error is returned to the eService.

The eService receives to authenticated person's details, or, in the case of an error, and error code.

OP Identity Service Broker replaces current TUPAS authentication service contracts that nevertheless remain in force and may be used for strong authentication until the end of the transition period in September 2019. After this deadline, the TUPAS interface will no longer meet the legal requirements for strong electronic credentials.

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.viestintavirasto.fi/attachments/maaraykset/MPS_72_2016.pdf.

OP Identity Service Broker is based on the SAML2 interface specification. For a more detailed description of the interface, see below in the appendix (Appendix 1). We handle only Finnish authentication credentials on the service. An identification event that contains optional attributes is handled as if no optional attributes are involved.

OP Identity Service Broker may also be used in the TUPAS interface when TUPAS is still valid. For instructions about the TUPAS interface, see the TUPAS service page on op.fi. If the service has been first used on the TUPAS interface, whenever you want to change the interface to SAML2, you must first be in touch with us by email to verkkopainikkeet@op.fi.

Use of OP Identity Service Broker requires that a contract has been made at a Group member bank and that user conditions have been accepted. Once accepted, the Identity Service system is implemented as described herein.

2 Software requirements

2.1 User interface

OP Identity Service Broker has a web-based responsive user interface. The user interface is offered as a full-page service and it is no longer available as a version that can be embedded into the eService. The user interface is available in Finnish, Swedish and English.

2.2 Supported browsers

OP Identity Service Broker 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 eService and OP Identity Service Broker the purpose for which the eService 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 the eService's 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

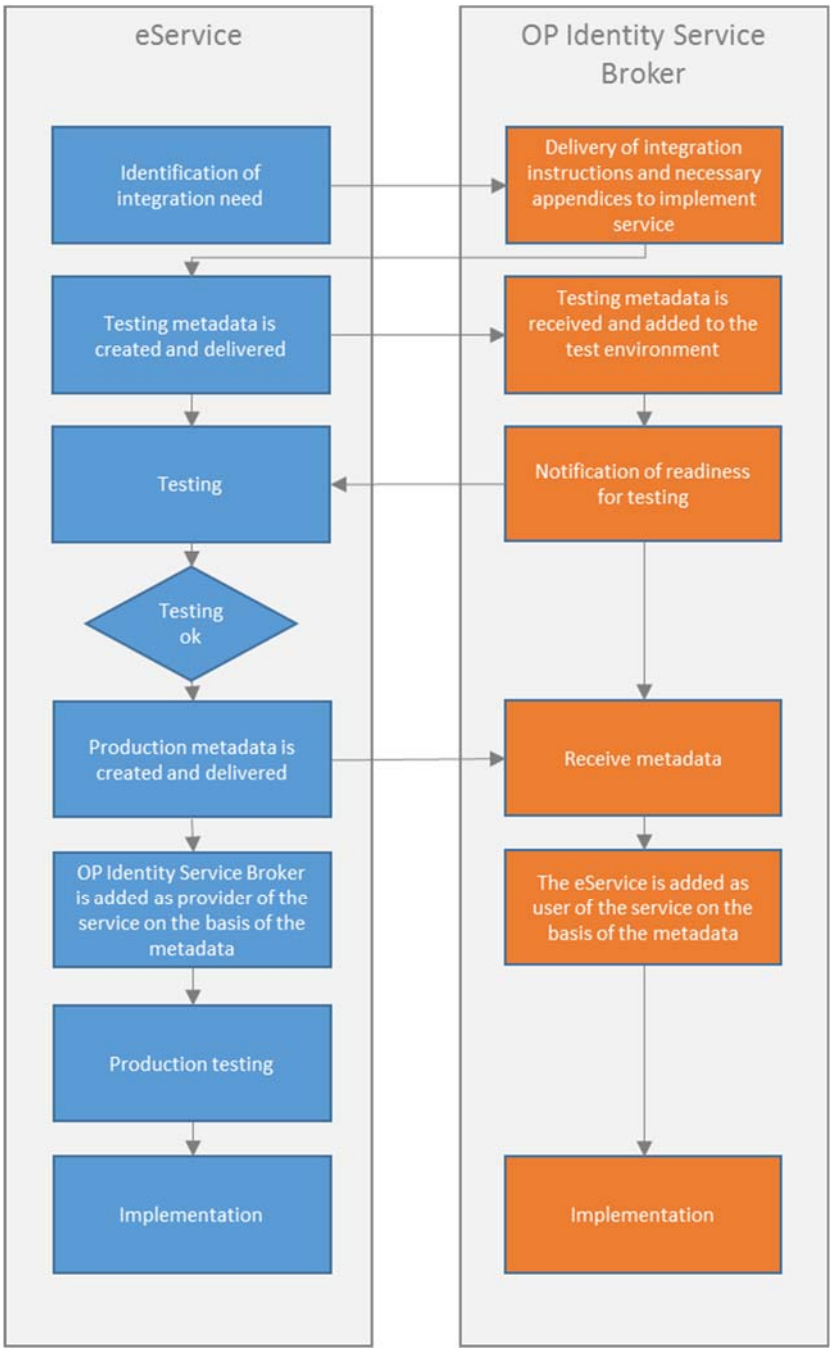
The following changes require a change in the contract:

- Addition or removal of the chaining of strong electronic credentials or weak electronic credentials
- Addition of restriction on the use of identification devices
- Removal of restriction on the use of identification devices

OP will notify if new providers of strong authentication providers are added to OP Identity Service Broker.

4 Implementation phases

The metadata and certificates used in the service are exchanged between OP Identity Service Broker and the eService once an agreement has been made. 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 Tunnistuspalvelu ja OP Tunnistuksen välityspalvelun 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 eService 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 Tunnistuspalvelu ja OP Tunnistuksen välityspalvelun 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 customer must send their own SAML2 metadata filled in as specified in Appendix 1. The appropriately filled form and metadata 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). PartnerId specifies the eService and the Service Broker's purpose of use. 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 eService's duty to keep track of its certificate's validity and to get a new one in time.
The recommended period of validity for a certificate is two years. The eService 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 the use of two certificates simultaneously, meaning that the old and new certificates can be used at the same time.

4.4 Testing the Identity Service Broker

Testing between OP Identity Service Broker and the eService takes place in a test 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 test certificate. For testing purposes, customers must send the SAML2 metadata used in the testing by encrypted email. Implementation of the test environment follows the implementation stages detailed in Chapter 4.

In the OP Identity Service Broker, only OP Identity Provider Service has been in the test.

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 Information required for testing

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

- Download certificate, signature certificate for OP Identity Service Broker
- Download metadata, signature certificate for OP Identity Service Broker

The URL for testing the OP Identity Service Broker is:

saml-idp.testid-broker.op.fi/FIM/sps/BrokerIdP/saml20/login

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

<md:EntityDescriptor mlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="**https:// saml-idp.testid-broker.op.fi/FIM/sps/BrokerIdP/saml20/login**">

4.5 Production verification

Production must be verified by logging through the OP Identity Service Broker by means of credentials provided by an identification device provider belonging to Luottamusverkosto.

5 Contact information

For questions regarding the Identity Service Broker, please phone

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

In contractual matters, please contact your own bank branch.

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

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 spefication.

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.

By using the Identity service broker, the service provider need to make only one integration to be able to utilize many different identity providers. The Identity Providers which are utilized by the identity service broker can be reached by the service providers via the identity service broker provided by OP. Service provider can be integrated for Identity service broker by using SAML 2.0 - interfaces.

When requesting authentication by using OP's Identity Service Broker, SAML AuthnRequst message needs to be sent. This message requests an authentication from the service to which it is sent. The user is forwarded into Identity service broker for to choose which Identity provider they want to use for authentication. On completion of the authentication process, a new SAML Response is created by OP Identity service broker, and the message is sent back to the requesting service. The SAML Response will be connected to the SAML Request message in the identity service broker. SAML Response includes information on whether the authentication process was successful with the needed identity information on the 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 on how SAML-message is moved in each of HTTP-methods.

Service can request authentication from OP's Identity service broker by sending an AuthnRequest message with a return destination by using user's browsers POST-method.

OP's Identity Service Broker will forward the authentication request for the wanted authentication process, after which OP 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 service provider can start using OP Identity Service Broker.

All connections are protected by TLS 1.2 or newer. This means that all request and response messages will be transmitted using HTTPS-connections. OP's Identity Service Broker will make requests by using HTTPS protocol.

All SAML-messages are signed to ensure on the sender, integrity of the message and that the message is unaltered. 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 Identity Service Broker.

2.1 Certificates

OP SAML 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 MUST be signed, and parties MUST not accept messages that are not signed, or where the verification of the signature fails. In these cases the receiving parties MUST respond with an error message.

2.2 Partner profile

To be able to make the integration, OP Identity service broker 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 explained

Specific metadata should be exchanged between the service provider and OP Identity Service Broker for the integration to work. The partner profiles are created by 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 the elements and attributes of metadata are presented in a table. This metadata represents the metadata which SP will provide for OP's Identity service broker.

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...WiHUsogetpcqg0qNk=		
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...WiHUsogetpcqg0qNk=	MJST	
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 to OP's Identity service broker. OP's Identity service broker will receive the SAML AuthnRequest message and will forward the user to the wanted Identity Provider for authentication.

SAML AuthnRequest messages must be signed, and OP Identity service broker will not accept messages that are not signed, or where the verification of the signature fails. 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 must 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 substantial (ftn.ficora.fi/2017/loa2) is supported.

OP Identity service broker 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 and IsPassive attributes have to be set true.

2.3.1 SAML Destination

The SAML 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	FIMREQ_5dad53-...d5fe94ad373	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	A Boolean value. If "true", the identity provider and the user agent itself MUST NOT visibly take control of the user interface from the requester and interact with the presenter in a noticeable fashion.

		IssueInstant	Required	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	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	A URI reference that identifies a SAML protocol binding to be used when returning the <Response> message.
		Version	MUST	2.0	States the version of SAML message (Here 2.0)
	<saml:Issuer		MUST	URL	ID of the responding service. References to the EntityID attribute in metadata. URL-format.
		Format		urn:oasis:names:tc:SAML:2.0:nameid-format:entity	
2	<ds:Signature>		MUST		<ds:Signature> is defined in [XMLDSig]
		Id		uuid5dad54-015b-...cd5fe94ad373	
3	<ds:SignedInfo>				
4	<ds:CanonicalizationMethod>				
		Algorithm		http://www.w3.org/2001/10/xml-exc-c14n#	SAML implementations SHOULD use Exclusive Canonicalization [Excl-C14N].
4	<ds:SignatureMethod>		MUST		
		Algorithm	MUST	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	
4	<ds:Reference>		MUST		The signature must include a single <ds:Reference> containing the ID attribute value (URI) of the <samlp:AuthnRequest> element
		URI	MUST	URI="#FI94-ad373"	
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 saml ds	
5	<ds:DigestMethod				
		Algorithm		http://www.w3.org/2001/04/xmlenc#sha256	
5	<ds:DigestValue>			Kza18Y86fHR...7Ar0lZmNr/u4	
3	<ds:SignatureValue>		MUST	fw6SmTb0ZMAhQrCNuncCbXzlaz2NLjZSdd5qsPmL7PJUs4ad...+0XYfwnsEjMFzBWnrCFKr4VgVtRa6WufkOuSSt8oll66X9JHdYNLHWI+Hwq/jY7Y=	
3	<ds:KeyInfo>				
4	<ds:X509Data>		MUST		
5	<ds:X509Certificate>		MUST	MIICOTCCAaKgAwIBAgIEWlH8jzANBgkqhkiG9w0BAQUFADBLMQsw CQYDVQQGE...	
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.
		Format	MUST	urn:oasis:names:tc:SAML:2.0:nameidformat:transient	It MUST be set to urn:oasis:names:tc:SAML:2.0:nameid-format:transient. A Boolean value used to indicate whether the identity provider is allowed, in the course of fulfilling the request, to create a new identifier to represent the principal.
		SPNameQualifier	Optional	URL	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.MUST use Finnish levels (ftn.ficora).	In FTN there are not yet loa3 level services. So all will be loa2.
3	<saml:AuthnContextClassRef>		MUST	http://ftn.ficora.fi/2017/loa2	

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_5dad53-...-cd5fe94ad373"
IsPassive="false"
IssueInstant="2017-03-24T12:49:50Z"
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="uuid5dad54-...cd5fe94ad373">
<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="#FIMREQ_5dad--cd5fe94ad373">
<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 saml ds"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>Kza...ANr/u4=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>fw6SmTbOZMAhQrCNuncCbXzlaz2NLjZSd...HdYNLHWI+Hwq/jY7Y=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICOTCCAaKgAw...UrV6kGNPfQNm8hDy</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:RequestedAuthnContext>
<saml:AuthnContextClassRef>http://ftn.ficora.fi/2017/loa2</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

2.4 SAML response

Identity service broker will forward the successfully authenticated SAML message containing user identity or forward/send an 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 (ftn.ficora).

2.4.1 Response validations

OP 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 Identity service broker 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.

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 indicationg the address to which this response has been sent.
		ID	FIMRSP_5e02de-015b...96ec11413afd	MUST	An unique ID for a SAML message.
		InResponseTo	FIMREQ_5dbd2a-0...a4e95c10e08c	MUST	The ID of the requesting 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-...-8d56-96ec11413afd	MUST	An unique ID for a signature.
3	<ds:SignedInfo>			MUST	
4	<ds:CanonicalizationMethod>				
		Algorithm			Method how canonicalization is done.
4	<ds:SignatureMethod>			MUST	
		Algorithm		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		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>				
		xmlns:xc14n	http://www.w3.org/2001/10/xml-exc-c14n		
		PrefixList	samlp xs saml xsi ds		
5	<ds:DigestMethod				

		Algorithm	http://www.w3.org/2001/04/xmlenc#sha256		
5	<ds:DigestValue>		MFeyJca... Z0=		
3	<ds:SignatureValue>		Yu1rkbRtYf4Zih1UD...mUp5Ful8g7UfPA==	MUST	
3	<ds:KeyInfo>			MUST	XML Signature defines usage of the <ds:KeyInfo> element.
4	<ds:X509Data>			MUST	
5	<ds:X509Certificate>			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 – *The request succeeded*	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#		
		Id	uuid5e59b0-015b-1038-8cd3-b2459bb9f3a9		
		Type	http://www.w3.org/2001/04/xmlenc#Element		
4	<EncryptionMethod>			MUST	Encryption method. Need to use aes-256.
		Algorithm	http://www.w3.org/2001/04/xmlenc#aes256-cbc	MUST	
4	<ds:KeyInfo>				
5	<EncryptedKey>			MUST	
		Id	uuid5e59b0-...-8cd3-b2459bb9f3a9	MUST	
6	EncryptionMethod			MUST	
		Algorithm	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	MUST	Key transport algorithm.
6	<ds:KeyInfo>				
7	<ds:KeyName>				Name og the key
6	<CipherData>			MUST	The CipherData is a mandatory element that provides the encrypted data.
7	<CipherValue>		Ob6JUy7ekGsGXREZH5UPA...Vkqo2qPZCCAfNQd/MQ=		The actual encrypted data is the value of this element.
4	<CipherData>				
5	<CipherValue>		Uf63y3x1AEGXZQ1nXzujUpUdME0....ffljg97boZufdjUwsc2fpb8=		
<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-uuid5e02d5-015b-1548-...96ec11413afd	MUST	
		IssueInstant	2017-03-24T12:50:12Z	MUST	
		Version	2.0		
3	<saml:Issuer>		http://...	MUST	
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity	MUST	
3	<ds:Signature>			MUST	
		Id	uuid5e02d7...-bba1-96ec11413afd	MUST	
4	<ds:SignedInfo>			MUST	
5	<ds:CanonicalizationMethod				
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#		
5	<ds:SignatureMethod			MUST	
		Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	MUST	
5	<ds:Reference			MUST	
		URI	#Assertion-uuid5e02d5-0...-96ec11413afd	MUST	
6	<ds:Transforms>				
7	<ds:Transform				
		Algorithm	http://www.w3.org/2000/09/xmldsig#enveloped-signature	MUST	
7	<ds:Transform				
		Algorithm	http://www.w3.org/2001/10/xml-exc-c14n#	MUST	
8	<xc14n:InclusiveNamespaces				
		xmlns:xc14n	http://www.w3.org/2001/10/xml-exc-c14n#	MUST	
		PrefixList	xs saml xsi		
6	<ds:DigestMethod>				
		Algorithm	http://www.w3.org/2001/04/xmlenc#sha256		
6	<ds:DigestValue>		rtyLMiX...IxPsll8=		
4	<ds:SignatureValue>		FdVPaDfigTMOt/fd13AtStlYQeoZqjsa+k... zfWu3mkLX7urYQv+Q+QLU	MUST	
4	<ds:KeyInfo>			MUST	

5	<ds:X509Data>			MUST	
6	<ds:X509Certificate>			MUST	
3	<saml:Subject>			MUST	
4	<saml:NameID>		uuid5e0257-...-a6b7-96ec11413afd	MUST	
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	MUST	
		NameQualifier	http://...	MUST	
		SPNameQualifier	http://...		
4	<saml:SubjectConfirmation>			MUST	
		Method	urn:oasis:names:tc:SAML:2.0:cm:bearer	MUST	
	<saml:SubjectConfirmationData>				
		InResponseTo	FIMREQ_5dbd2a-...-a693-a4e95c10e08c	MUST	The InResponseTo attribute need to be present and its value need to 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>				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
		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>			MUST	
		AuthnInstant	2017-03-24T12:50:12Z	MUST	
		SessionIndex	uuid5dbdcb-...-a538-96ec11413afd	MUST	
		SessionNotOnOrAfter	2017-03-24T13:50:12Z	MUST	
4	<saml:AuthnContext>		MUST specify the exact authentication assurance level.MUST use Finnish levels (ftn.ficora).	MUST	In FTN there are not yet loa3 level services. So all will be loa2.
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 *http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier - PersonIdentifier (not supported)* 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://..."
ID="FIMRSP_5e59af-015b...-b2459bb9f3a9"
InResponseTo="FIMREQ_5dad53-015b-...-cd5fe94ad373"
IssueInstant="2017-03-24T12:50:35Z"
Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
http://...
</saml:Issuer>
<ds:Signature Id="uuid5e59b0-015b-...-b2459bb9f3a9">
<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_5e59af-...-b2459bb9f3a9">
<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/xmlenc#sha256"/>
<ds:DigestValue>+WtCkp79b09Dkl+p6wDHrmvX3io=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>Yu1rkbRtYf4Zih1UD...iDqOTpAgyLkQMoR5mUp5Ful8g7UfPA==</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDKDCCAhCgAwIBAgIHYy80b86VKTANBgkqhkiG9w0BAQUFADBDMQswCQYD...ZQiD0bfHRsvlf0EA=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>

```
<saml:EncryptedAssertion>
<EncryptedData
xmlns="http://www.w3.org/2001/04/xmlenc#"
Id="uuid5e59b0-015b-...-b2459bb9f3a9"
Type="http://www.w3.org/2001/04/xmlenc#Element">
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
<ds:KeyInfo>
<EncryptedKey
Id="uuid5e59b0-015b-...-b2459bb9f3a9">
<EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
<ds:KeyInfo>
<ds:KeyName>KeyName
</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue>Ob6JUy7ekGsGXREZH5UPA...Vkqo2qPZCCAfNQd/MQ=
</CipherValue>
</CipherData>
</EncryptedKey>
</ds:KeyInfo>
<CipherData>
<CipherValue>Uf63y3x1AEGXZQ1nXzujUpUdME0....ffljg97boZufdjUwsc2fpb8=</CipherValue>
</CipherData>
</EncryptedData>
</saml:EncryptedAssertion>
</samlp:Response>
```

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

```
<saml:Assertion ID="Assertion-uuid5e599e-...-b2459bb9f3a9" IssueInstant="2017-03-24T12:50:35Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://...</saml:Issuer>
<ds:Signature Id="uuid5e599f-015b-...-b2459bb9f3a9">
<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="#Assertion-uuid5e599e...-ab5b-b2459bb9f3a9">
<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="xs saml xsi"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>mEFQfcGkhB...riTN6jacSjvA=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>IPFSfT1/oyVR/casuPE6DTjmy1579+/yuy5s5ZQeLsLvJZep3PhD...1A8vz3UGxoTymow==</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDKDCCAhCgAwIBAgIHYy80b86VKTANBgkqhkiG9....XzBXg3EZxZB0ksTNZQiD0bfHRsvlf0EA=</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://...>
</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
```

<saml:SubjectConfirmationData InResponseTo="FIMREQ_5dad53-015b...-cd5fe94ad373" NotOnOrAfter="2017-03-24T12:51:35Z" Recipient="http://..."/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions
NotBefore="2017-03-24T12:40:35Z"
NotOnOrAfter="2017-03-24T12:51:35Z">
<saml:AudienceRestriction>
<saml:Audience>http://...>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement
AuthnInstant="2017-03-24T12:50:35Z"
SessionIndex="uuid5daf0c-015b-...b2459bb9f3a9"
SessionNotOnOrAfter="2017-03-24T13:50:34Z">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</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.

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:metadata	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/xmlenc#rsa-oaep-mgf1p"/>
</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>