Viestintävirasto

Recommendation

212/2018 S
2018-01-26

Finnish Trust Network SAML 2.0 Protocol Profile version 1.0

FICORA Recommendation

212/2018 S

Viestintävirasto

Recommendation

212/2018 S
2018-01-26

Johdanto ja SAML rajapintasuosituksen tarkoitus

Asiakirjan nimi
Finnish Trust Network SAML 2.0 Protocol Profile version 1.0
Johdanto
Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (2009/617) 12 a §:n 2 momentin mukaan luottamusverkostoon kuuluvien tunnistuspalvelun tarjoajien on muun muassa tarjottava tekniset rajapinnat, jotka luovat edellytykset tunnistuspalveluita tarjoavien ja niitä hyödyntävien toimijoiden väliselle toiminnalle. Tämä suositus on tarkoitettu luottamusverkostoon kuuluville tunnistuspalvelun tarjoajille. Suositus määrittelee vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta annetun asetuksen (2016/169) 1 §:n mukaisen tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisen SAML 2.0 protokollaa käyttävän rajapintakuvauksen. Suosituksessa on huomioitu Viestintäviraston määräyksen 72/2016 (määräys sähköisistä tunnistus- ja luottamuspalveluista) mukaiset vähimmäistiedot, joita toimijoiden välisissä rajapinnoissa on kyettävä siirtämään, sekä määräyksessä asetetut tietoliikenteen salausvaatimukset. Suositus on laadittu yhteistyössä luottamusverkoston toimijoiden kanssa ja sen avulla toimijat voivat rakentaa yhteentoimivia järjestelmiä. Suositus on sovellettavissa myös asiointipalvelun ja luottamusverkoston välisessä rajapinnassa käytettäväksi. Yksinkertaisuuden vuoksi rajapintakuvauksessa käsitellään kuitenkin johdonmukaisesti toimintaa tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun välisessä rajapinnassa. Rajapintakuvaus on julkaistu vain englanniksi, jotta se olisi laajasti suoraan hyödynnettävissä ja jotta tulkintaeroja eri kieliversioiden välillä ei pääse syntymään. Tälle suositukselle rinnakkaisena on julkaistu vastaavan toiminnallisuuden tarjoava OpenID Connect 1.0 protokollaa käyttävä rajapintakuvaus numerolla 213/2018 S.
Avainsanat
luottamusverkosto, rajapinta, sähköinen tunnistaminen, SAML

Viestintävirasto

Recommendation

212/2018 S
2018-01-26

Inledning och syfte med SAML protokoll profil dokument

Namnet på dokumentet

Finnish Trust Network SAML 2.0 Protocol Profile version 1.0

Inledning

Enligt 12 a § 2 mom. i lagen om stark autentisering och elektroniska signaturer ska en leverantör av identifieringstjänster som hör till förtroendenätet bl.a. erbjuda tekniska gränssnitt som skapar förutsättningar för verksamheten mellan aktörerna som tillhandahåller identifieringstjänster och aktörerna som använder tjänsterna. Denna rekommendation är avsedd för de leverantörer av identifieringstjänster som hör till förtroendenätet.

Rekommendationen specificerar en gränssnittsbeskrivning för användning av SAML 2.0-protokollet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för förmedling av identifiering i enlighet med 1 § i förordningen om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016). I rekommendationen har beaktats den minimiuppsättning uppgifter som ska kunna överföras mellan aktörernas gränssnitt enligt Kommunikationsverkets föreskrift 72/2016 (föreskrift om elektroniska identifieringstjänster och betrodda elektroniska tjänster), samt kraven på trafikkryptering som anges i föreskriften.

Rekommendationen har utarbetats i samarbete med aktörerna i förtroendenätet, och med hjälp av den kan aktörerna bygga interoperabla system. Rekommendationen kan också tillämpas för användning i gränssnittet mellan ärendehanteringstjänster och förtroendenätet. För enkelhetens skull behandlas i gränssnittsbeskrivningen dock konsekvent verksamheten i gränssnittet mellan en leverantör av identifieringsverktyg och en leverantör av tjänster för identifieringsförmedling.

Gränssnittsbeskrivningen publiceras enbart på engelska för att vara direkt användbar för många och för att det inte ska bli några tolkningsskillnader mellan olika språkversioner.

Parallellt med denna rekommendation publiceras en gränssnittsbeskrivning för användning av OpenID Connect 1.0-protokollet som erbjuder motsvarande funktionalitet som SAML 2.0. Rekommendationens nummer är 213/2018 S.

Nyckelord

förtroendenät, gränssnitt, elektronisk identifiering, SAML

Contents

1 Version history of the document

1.1 Recommendation versions

The Recommendation will be supplemented and modified as necessary. In that case, the Recommendation number 212 will be maintained, but the date and the year will be changed appropriately. The modified versions of the Recommendation are listed in the following table:

Recommendation version and date	**Modifications**
Published recommendation v1.0 212/2018 S 2018-01-26	First published version

Current recommendation version is published on the FICORA website at https://www.viestintavirasto.fi/en/steeringandsupervision/guidelinesandpublications/documentsforguidelinesinterpretationsrecommendationsandreporttst.html

2 Introduction

This document defines the SAML 2.0 protocol interface for the Finnish Trust Network (FTN). Specifically this means the interface between FTN IdPs and FTN Brokers, but it is also usable between Service Providers and FTN Brokers.

2.1 About the Finnish Trust Network

The Finnish Trust Network (FTN) is a mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Trust Network delivers the following benefits:

- For citizens, the FTN delivers a sign-on experience that is familiar, fast and simple.
- For online services, the FTN removes barriers of security and complexity related to implementing strong authentication based on mutually accepted levels of assurance.

- For identity providers that issue authentication credentials, the FTN provides new opportunities to leverage the success of their credentials platform and expand credential usage.

The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model.

2.2 Audience and Scope

This profile specifies SAML2 protocol requirements for identity providers that provide authentication credentials and authorisation services within the Finnish Trust Network. This specification is intended for online service providers integrating with the FTN as Identity Providers and Identity Service Brokers.

Although this specification is worded to define only the interface between an Identity Provider and an Identity Service Broker, the same interface and attributes are also directly usable between an FTN Broker and an online Service Provider/Relying Party. It is assumed the reader is generally familiar with the SAML2 protocol.

User consent information transfer is not included in the scope of this profile. Asking for user consent when needed is the responsibility of the party needing the consent. For the typical use case of authenticating a user to a Service Provider (without enrichment) the consent is implicit and it is not necessary for the FTN Broker or IdP to separately ask for user consent for each authentication transaction.

Cross-border authentication in the EU/EEA is still work-in-progress and it may cause interoperability issues/changes that have to be taken into consideration in future versions of this document.

A sister document is published as FICORA Recommendation 213/2018 S to define a corresponding OpenID Connect 1.0 profile for the FTN.

2.3 Requirements notations

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to technically

interoperate without additional negotiation, and should be undertaken with caution.

This document uses native, eIDAS and STORK2 based abbreviations:

AP = Attribute Provider
AS = Authorisation Server
CA = Certificate Authority
CSP = Credential Service Provider, also known as Identity Provider (IDP)
FTN = Finnish Trust Network
(FTN) IdP = Identity Provider within the FTN
(FTN) Broker = Broker that handles authentication requests between Service Providers and IdPs in the FTN. The Broker MAY provide multiple interfaces for IdPs and Service Providers to integrate to.
RP = Relying Party
SP = Service Provider

2.4 References to SAML 2.0 standards and profiles

This profile extends Interoperable SAML 2.0 Web Browser SSO Deployment Profile [SAML2Int] with requirements specific for the Finnish Trust Network.

When referring to elements from the SAML 2.0 Core specification [SAML2Core], the following syntax is used:

- `<saml2p:Protocolelement>` – for elements from the SAML 2.0 Protocol namespace.
- `<saml2:Assertionelement>` – for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specifications, the following syntax is used:

- `<md:Metadataelement>` – for elements defined in SAML2Meta.
- `<mdui:Element>` – for elements defined in SAML2MetaUI.
- `<mdattr:Element>` – for elements defined in SAML2MetaAttr.

When referring to elements from the Identity Provider Discovery Service Protocol and Profile [IdpDisco], the following syntax is used:

- `<idpdisc:DiscoveryResponse>`

When referring to elements from the W3C XML Signature namespace [XMLDSig] the following syntax is used:

- `<ds:Signature>`

2.5 Single Sign On considerations

Single Sign On (SSO) authentications MUST NOT happen by chance in the FTN. All implementations MUST respect the built-in parameters in the SAML protocol that can be used to limit or forbid the (re)use of cached/SSO authentications. Separate guidelines or reports on the use of SSO within the FTN may be published later.

3 The Finnish Trust Network SAML2 profile

3.1 Metadata and trust management

Identity Providers and FTN Brokers MUST provide a SAML 2.0 Metadata document representing their entity. In this profile the metadata is only partially described.

3.2 Requirements for metadata content

3.2.1 Metadata profiles

Identity Providers and FTN Brokers that are part of the Finnish Trust Network MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].

Finnish Trust Network Assertion Consumer Service endpoints MUST be protected by TLS (see [M72notes] Part B Section 7). During a SAML protocol exchange, the relying party MUST either verify the validity of the metadata file containing the peer entity, or verify the validity of the certificate used by the peer entity for protecting the SAML exchange.

3.2.2 Other metadata content

Metadata documents provided by an Identity Provider MUST include an <md:IDPSSODescriptor> element containing all necessary <md:KeyDescriptor> and <md:SingleSignOnService> elements. Metadata MUST include <WantAuthnRequestsSigned> element with value “true”.

3.2.3 Metadata exchange

Import of multiple entities' metadata contained within an <md:EntitiesDescriptor> element MAY be supported. Metadata MUST contain a validUntil and MAY contain a cacheDuration attribute.

Metadata files MUST carry an <md:KeyDescriptor > element for the purpose of signing. It SHALL have a <ds:KeyInfo> element, which contains the used certificate.

3.2.4 Metadata verification

The Identity Providers MUST publish metadata which is signed using a certificate issued by a trusted CA as described in the service documentation. Metadata signature MUST be validated before use following instructions provided by the issuing Certificate Authority (CA).

3.3 Name identifiers

The Identity Providers and FTN Brokers MUST support the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` name identifier format as specified in [SAML2Core].

3.4 Attributes

The SAML attributes described in this section SHALL follow these requirements:

- `NameFormat` SHALL contain the value `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`
- `Name` is the URI (urn:oid or http...) described in the table. `Name` is a string without spaces or line feeds, the layout in the attribute tables is for readability
- `FriendlyName` is OPTIONAL, but if used, MUST follow the definitions below
- Latin script SHOULD be used for all attribute values. If transliteration is required from non-Latin scripts, the currently used standard of the Finnish Population Registry SHOULD be used.
- Unless otherwise specified, the attributes are encoded as UTF-8 `xsd:string`. Precomposed Unicode characters SHOULD be used when possible, instead of decomposed characters.

3.4.1 Attributes for a Natural Person

3.4.1.1 Required attributes

Note that the eIDAS technical specifications are not directly applicable within the FTN. eIDAS technical specifications should be used within the context of this document only when explicitly referred to.

Name	**FriendlyName**	**eIDAS MDS Attribute**	**Comments, Example value(s) in `Courier New`**
urn:oid: 2.5.4.4	`FamilyName`	Current Family Name	`Meikäläinen` `von Essen`

urn:oid: 1.2.246.575.1.14	`FirstNames`	Current First Names	`Matti Elmeri Valdemar`
			`Anna-Liisa Hilkka`
			(all known current first/given names, space separated)

urn:oid: 1.3.6.1.5.5.7.9.1	`DateOfBirth`	Date of Birth	`1971-06-28` (encoded as `xsd:date`)

urn:oid: 1.2.246.21	`HETU`	-	`220750-999Y`
			`141002A909X`
			(Finnish personal identity code, henkilötunnus) *

urn:oid: 1.2.246.22	`SATU`	-	`99999999D` (Finnish Unique Identification Number, sähköinen asiointitunnus) *
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	`PersonIdentifier`	Unique Identifier	`XX/YY/123456ABCDEF` (as defined by eIDAS SAML Attribute Profile [eIDASTech], subject to change) *

* One of these three attributes is mandatory, the rest are OPTIONAL to include in an assertion. It is up to the FTN Broker and IdP to agree which identifier between them is used as the mandatory attribute. The eIDAS PersonIdentifier is not expected to be commonly used nationally within the FTN, but is referred to here in case eIDAS cross-border authentication becomes relevant to the FTN.

3.4.1.2 Optional attributes

If an assertion received by an FTN Broker contains unrecognized optional attributes, the assertion SHOULD NOT be discarded solely due to the assertion containing unsupported attributes, as long as the required attributes specified above are provided. This is suggested to futureproof implementation behavior, so new attributes can be added in later versions of this recommendation in a backwards compatible manner.

Name	**FriendlyName**	**eIDAS MDS Attribute**	**Comments, Example value(s) in `Courier New`**
urn:oid: 1.2.246.575.1.3	`FamilyBirthName`	Family Name at Birth	`Möttönen` `von Essen`

urn:oid:
1.2.246.575.1.4
	`FirstBirthName`	First Names at Birth	`Matias Jalmari Valdemar`
			`Anna-Liisa Hilkka`
			(all known first/given names at birth, space separated)

urn:oid:
1.3.6.1.5.5.7.9.2
	`PlaceOfBirth`	Place of Birth	`Helsinki`
			`Kittilä Finland`
			(typically city and/or country. No specific separator is defined, but more specific areas should precede less specific areas)

urn:oid: 1.2.246.575.1.16	`CurrentAddress`	Current Address	(multiple xsd:string elements base64 encoded into one string, see eIDAS SAML Attribute Profile 2.2.9 [eIDASTech], the example below and ISA Core Location Vocabulary [ISACoreLocVoc])

urn:oid:
1.2.246.575.1.15
	`Gender`	Gender	`Male`
			`Female`
			`Not Specified`
			(string with restriction of selection to one of the three options specified above)

urn:oid:
2.5.4.42
	`GivenName`	-	`Elmeri`
			`Anna-Liisa`
			(kutsumanimi in Finnish, one of the current registered first names normally used by the person)

urn:oid:
1.2.246.575.1.18
	`AuthCachingDisabled`	-	`true`
			`false`
			(boolean (lower case), indication from the IdP/user that forbids caching of the current user authentication session (SSO), if set to true. If the attribute is not sent, the default value is false)

Example CurrentAddress encoding:

SAML attribute value:

```
PGVpZGFzOlRob3JvdWdoZmFyZT5JdMOkbWVyZW5rYXR1PC9laWRhczpUaG9yb3V
naGZhcmU+DQo8ZWlkYXM6TG9jYXRvckRlc2lnbmF0b3I+MyBBIDc1PC9laWRhcz
pMb2NhdG9yRGVzaWduYXRvcj4NCjxlaWRhczpQb3N0TmFtZT5IZWxzaW5raTwvZ
WlkYXM6UG9zdE5hbWU+DQo8ZWlkYXM6UG9zdENvZGU+MDAxODA8L2VpZGFzOlBv
c3Rjb2RlPg0KPGVpZGFzOkFkbWludW5pdEZpcnN0bGluZT5GSTwvZWlkYXM6QWR
taW51bml0Rmlyc3RsaW5lPg0K
```

The above attribute base64-decoded:

```
<eidas:Thoroughfare>Itämerenkatu</eidas:Thoroughfare>
<eidas:LocatorDesignator>3 A 75</eidas:LocatorDesignator>
<eidas:PostName>Helsinki</eidas:PostName>
<eidas:PostCode>00180</eidas:Postcode>
<eidas:AdminunitFirstline>FI</eidas:AdminunitFirstline>
```

Note that the street address has been split into two parts, `Thoroughfare` containing the street name and `LocatorDesignator` the building number and possible other details typically on the street address line. `AdminunitFirstline` contains the country code (upper case) in ISO 3166-1 alpha-2. The language of the address is not specified here, it may be in any language understood by the postal system in the specified country or area.

3.4.2 Attributes for a Legal Person

Note that including attributes of a legal person in a SAML assertion in the FTN does not in itself convey authority for the natural person being authenticated to enter into binding contracts on behalf of the legal person.

3.4.2.1 Required attributes

Note that the eIDAS technical specifications are not directly applicable within the FTN. eIDAS technical specifications should be used within the context of this document only when explicitly referred to.

Legal person attributes MUST always be accompanied by the mandatory natural person attributes of the natural person being authenticated. Optional natural person attributes MAY also be included.

Name	**FriendlyName**	**eIDAS MDS Attribute**	**Comments, Example value(s) in `Courier New`**
urn:oid: 2.5.4.10	`LegalName`	Current Legal Name	`Widget Factory Oy`
http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier	`LegalPersonIdentifier`	Uniqueness Identifier	`XX/YY/123456ABCDEF` (as defined by eIDAS SAML Attribute Profile [eIDASTech], subject to change) *
urn:oid: 1.2.246.575.1.7	`VATRegistration`	VAT Registration Number	`FI98765432` (company identifier (Y-tunnus) in EU format) *

* One of these two attributes is mandatory, the other is OPTIONAL to include in an assertion. It is up to the FTN Broker and IdP to agree which identifier between them is used as the mandatory attribute. The eIDAS LegalPersonIdentifier is not expected to be commonly used nationally within the FTN, but is referred to here in case eIDAS cross-border authentication becomes relevant to the FTN.

3.4.2.2 Optional attributes

Name	FriendlyName	eIDAS MDS Attribute	Comments, Example value(s) in `Courier New`
urn:oid: 1.2.246.575.1.6	`LegalAddress`	Current Address	(multiple xsd:string elements base64 encoded into one string, see eIDAS SAML Attribute Profile 2.3.5 [eIDASTech] and example for natural person address above)
urn:oid: 1.2.246.575.1.8	`TaxReference`	Tax Reference Number	
urn:oid: 1.2.246.575.1.9	`BusinessCodes`	Directive 2012/17/EU Identifier	
urn:oid: 1.2.246.575.1.10	`LEI`	Legal Entity Identifier (LEI)	
urn:oid: 1.2.246.575.1.11	`EORI`	Economic Operator Registration and Identification (EORI)	
urn:oid: 1.2.246.575.1.12	`SEED`	System for Exchange of Excise Data (SEED)	
urn:oid: 1.2.246.575.1.13	`SIC`	Standard Industrial Classification (SIC)	

3.5 Authentication requests

TLS MUST be used on the transport layer to protect all authentication requests and responses, i.e. all URLs the user browser requests from the IdP and the FTN Broker MUST begin with `https://`. An exception to this requirement is CRL and/or OCSP traffic. The TLS server X.509 certificates that are used to protect communication with client web browsers MUST be generally trusted by browsers (95+%). These certificates MUST be valid based on all commonly implemented validators in web browsers (certificate path to trusted root provided, certificates not expired, strong enough cryptographic primitives used, etc). The use of extended validation (EV) certificates is RECOMMENDED. eIDAS-notified IdPs may also be subject to additional security requirements based on the eIDAS regulations.

The X.509 certificates used between the IdP and FTN Brokers to sign and/or encrypt SAML Requests/Responses MAY be self-signed and do not need to be generally trusted by web browsers. But these certificates MUST always be explicitly configured/pinned as trusted for SAML use between the particular IdP and FTN Broker, even if signed by a generally trusted CA. The SAML message encryption/signing cryptosystem MUST also fulfill the cryptographic strength requirements of FICORA Regulation M72 Section 7, except for DH key exchange when it is not used.

The FTN Broker initiates SAML authentication transactions in the FTN by sending an `AuthnRequest` to the IdP using POST binding (RECOMMENDED) or Redirect binding (OPTIONAL), as agreed by the parties. The IdP returns a `Response` to the FTN Broker using POST binding. IdP-initiated unsolicited Response messages MUST be rejected.

3.5.1 Discovery

Currently the profile does not use the Identity Provider Discovery Service Protocol. If an FTN Broker plans to use a Discovery Service supporting the Identity Provider Discovery Service Protocol Profile [IdPDisco], then its metadata MUST include one or more `<idpdisc:DiscoveryResponse>` elements in the `<md:Extensions>` element of its `<md:SPSSODescriptor>` element.

3.5.2 Binding and security requirements

The endpoints at which an Identity Provider receives a `<saml2p:AuthnRequest>` message, and all subsequent exchanges with the user agent, MUST support TLS 1.2 or newer version. TLS 1.1 may only be used if the user agent is not capable of TLS 1.2 or newer (see [M72notes] Part B Section 7).

`<saml2p:AuthnRequest>` messages MUST be signed, and Identity Providers MUST NOT accept messages that are not signed, or where the verification of the signature fails. In these cases the Identity Provider MUST respond with an error message. The signature for an authentication request messages is applied differently depending on the binding. Implementations MUST support the use of SHA2-256 hash algorithm in SAML message signatures, and optionally MAY support other stronger algorithms.

A HTTP REDIRECT binding requires the signature to be applied to the URL-encoded value rather than being placed within the XML-message (see section 3.4.4.1 of [SAML2Bind]).

For the HTTP-POST binding the `<saml2p:AuthnRequest>` element MUST be signed using a `<ds:Signature>` element within the `<saml2:AuthnRequest>`.

Additional details are specified in Regulation M72.

3.5.2.1 Signing of requests

If the HTTP POST Binding is used, the signature must be an enveloped signature and applied to the `<samlp:AuthnRequest>` element and all its children. The signature must include a single `<ds:Reference>` containing the ID attribute value of the `<samlp:AuthnRequest>` element. `<ds:Signature>` is defined in [XMLDSig].

Additional details (e.g. cryptographic strength and algorithm requirements) are specified in Regulation M72.

3.5.3 Message content

The <saml2p:AuthnRequest> message issued by an FTN Broker MUST contain an AssertionConsumerServiceURL attribute identifying the desired response location. The FTN Broker MUST NOT use any other values for this attribute than those listed in its metadata record as <md:AssertionConsumerService> elements for the HTTP-POST binding (see section 4.1.6 of [SAML2Prof]).

The value of the AssertionConsumerServiceURL attribute of the <saml2p:AuthnRequest> message MUST be verified to be consistent with one of the <md:AssertionConsumerService> elements having the HTTP-POST binding found in the FTN Broker's metadata entry. If this is not the case, the request must be rejected.

Section 8.2 of [SAML2Int] specifies how comparisons between the AssertionConsumerServiceURL value and the values found in the FTN Broker's metadata should be performed.

The Destination attribute of the <saml2p:AuthnRequest> message MUST contain the URL to which the FTN Broker has instructed the user agent to deliver the request.
The <saml2p:AuthnRequest> message MUST contain a <saml2p:NameIDPolicy> element with a Format attribute set to urn:oasis:names:tc:SAML:2.0:nameid-format:transient.

The <saml2p:AuthnRequest> message MUST contain a <saml2p:RequestedAuthnContext> element. A present <saml2p:RequestedAuthnContext> element MUST specify the exact authentication assurance level. The <saml2p:RequestedAuthnContext> MUST use one or more of the URIs listed in the table below. The acronym LoA stands for Level of Assurance.

The FTN Brokers MUST request a specific level of assurance with the "exact" compare operator. The FTN Broker may request more than one level in a priority order.

The Authentication Context values relevant within the FTN are the following URIs:

AuthnContext	Meaning
http://ftn.ficora.fi/2017/loa2	Finnish level substantial (korotettu)
http://ftn.ficora.fi/2017/loa3	Finnish level high (korkea)
http://eidas.europa.eu/LoA/low	eIDAS level low
http://eidas.europa.eu/LoA/substantial	eIDAS level substantial
http://eidas.europa.eu/LoA/high	eIDAS level high

-

Use of an AuthnContext value that contains the string `eidas.europa.eu` signals that the authentication method requested/used has been successfully notified on the given level or higher to the European Commission for cross-border authentication within the EU/EEA. AuthnContext values containing the string `ftn.ficora.fi` signal that the authentication method has been approved to be a part of the FTN on the given level or higher. The eIDAS level low SHOULD NOT be used within the FTN, it is included in the table above for completeness.

In the Finnish Trust Network only levels substantial and high are used. An eIDAS level AuthnContext meets the requirements of the corresponding Finnish level, but not vice versa. If an FTN IdP receives a request from an FTN Broker for level substantial authentication (only one AuthnContext value requested), the request can also be fulfilled with a level high device/mechanism. In this case the response AuthnContext value MUST correspond to the requested level, i.e. substantial.

For **test and/or demo purposes**, the following AuthnContext values MAY be used. Authentication transactions done using these values MUST NOT be relied on for any purpose, they are only meant for testing. Attributes returned when using these AuthnContext values MUST NOT refer to a real person.

AuthnContext value **for test purposes**	Meaning
http://ftn.ficora.fi/2017/loatest2	Finnish test level substantial (korotettu)
http://ftn.ficora.fi/2017/loatest3	Finnish test level high (korkea)

Identity Providers conformant with this profile MUST support the `ForceAuthn` and `IsPassive` attributes received in `<saml2p:AuthnRequest>` messages. FTN Brokers SHOULD include the `ForceAuthn` attribute in all

<saml2p:AuthnRequest> messages and explicitly set its value to true, and not rely on its default value, when single sign on is not used/desired.

Other parameters defined by [SAML2Core] for authentication requests or agreed by the parties MAY also be used.

3.5.3.1 Request Extensions

Extensions in a <saml2p:AuthnRequest> MAY be used to carry extra information relevant to the request from the FTN Broker to the IdP. Supporting request extensions is RECOMMENDED and each extension tag is OPTIONAL to include in a request. The following extension tags have been defined:

`lg`

The user's preferred user interface language can be communicated in the request. The language is encoded and should be matched according to IETF BCP47 [BCP47] (simplest case example: two lower case ISO 639-1 letters, typically `fi`, `sv`, or `en`). The IdP MAY also use other data sources available to select the user interface language to use (e.g. Accept-Language HTTP request header) or MAY show the user a language selection dialog.

`idpid`

Lower case alphanumeric (a-z, 0-9, plus '-' acting as separator) ASCII identifier for the FTN IdP that SHOULD be used for end-user authentication. This parameter is primarily meant to be used by Service Providers to signal their Broker the IdP to use for authenticating the user, if the user has indicated the IdP service to use to the Service Provider. This makes it possible for the Broker to seamlessly transfer the user to the chosen FTN IdP, without the Broker having to display an IdP selection user interface to the end user.

The first "fi" part is constant within the FTN. The second "xyz" part in the example value is allocated by FICORA and listed in the registry of strong identification service providers [Providerlist]. The third part is OPTIONAL and MAY be used by the IdP to differentiate between their authentication services/methods. The third part value is allocated by the corresponding FTN IdP. It MUST consist of lower case alphanumeric characters only (a-z, 0-9). Maximum length of each part is 20 characters, which means the maximum length of the whole identifier including two separators is 62 characters. Example values of the whole idpid: "fi-xyz-a1bc", "fi-rst3uvw-a76f", "fi-xyz"

`clientid`

Opaque string identifier for the SAML party generating the `AuthnRequest`. The identifier is not defined further in this document and is not centrally allocated, but can be freely agreed upon by the SAML parties if needed.

`spname`

Human readable name of the Service Provider the user is authenticating to. This is carried in the request so that the IdP MAY show in its user interface the end user service being authenticated to. The name is RECOMMENDED to be in the same language as user's preferred user interface language (parameter `lg`).

`sptype`

Type of the Service Provider the user is authenticating to. This string can be either:

- `public` — services provided by the public sector
- `private` — services provided by private organizations/individuals

Example defining the requested user interface language to be Finnish, clientid to be abcdef123, requested IdP id fi-xyz-ghi, and the Service Provider requesting authentication being "Esimerkkikauppa Oy" of private type:

```
<saml2p:Extensions>
  <ftn xmlns="http://ftn.ficora.fi/2017/req_ext">
    <lg>fi</lg>
    <idpid>fi-xyz-ghi</idpid>
    <clientid>abcdef123</clientid>
    <spname>Esimerkkikauppa Oy</spname>
    <sptype>private</sptype>
  </ftn>
</saml2p:Extensions>
```

3.5.3.2 Chained authentication tokens/means creation

If this recommendation is used as the interface for creating new chained strong authentication tokens/means between two FTN IdPs, the following extra parameter is REQUIRED ("Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista" 617/2009 17 §). This parameter MUST NOT be used for any other purpose.

`chainlevel`

Presence of this parameter in an authentication request to an FTN IdP from another FTN IdP signals that this authentication is being done to issue a new chained strong authentication token/means to an end user.

The value of this parameter MUST be a URI describing the Level of Assurance (LoA) of the authentication token/means being issued. It MUST be of the same LoA level or lower than is used by the user to perform the authentication. LoA URIs that begin with `http://ftn.ficora.fi/` MUST be used exclusively. An authentication request using this parameter MUST always result in full (re)authentication, i.e. the `ForceAuthn` attribute MUST be set to `true`. The request SHOULD NOT be relayed via 3rd party FTN Brokers. If a Broker is used, the Broker MUST meet the requirements of the requested LoA. See Section 3.6.2.2 for the corresponding response attribute.

An example of a chained authentication token/means request extension for substantial level using only this extension is shown below:

```
<saml2p:Extensions>
  <ftn xmlns="http://ftn.ficora.fi/2017/req_ext">
    <chainlevel>http://ftn.ficora.fi/2017/loa2</chainlevel>
  </ftn>
</saml2p:Extensions>
```

3.6 Authentication responses

3.6.1 Security requirements

The <`saml2p:Response`> message MUST be carried over server endpoints that support and use TLS 1.2 or newer version. TLS 1.1 may only be used if the user agent is not capable of TLS 1.2 or newer (see [M72notes] Part B Section 7). When using TLS 1.3, 0-RTT data MUST NOT be used. It is RECOMMENDED to use the HTTP Strict Transport Security header (RFC 6797) in TLS servers. All <`saml2p:Response`> messages issued by the Identity Provider MUST be signed using a <`ds:Signature`> element within the <`saml2p:Response`> element. The signature MUST utilize SHA2-256 or a stronger hash function.

The entire <`saml2:Assertion`> element issued by the Identity Provider MUST be returned in an encrypted <`saml2:EncryptedAssertion`> element that is covered by the <`saml2p:Response`> signature described above. The <`saml2:EncryptedAssertion`> does not need to contain a separate embedded signature, because the whole <`saml2p:Response`> MUST be always signed.

The above in short: TLS always used in the transport layer, the SAML response message always containing a signed <`saml2p:Response`> that always contains an encrypted <`saml2:EncryptedAssertion`>.

Unsolicited <`saml2p:Response`>s MUST NOT be used.

Further security requirements are specified in Regulation M72.

3.6.2 Message content

The <saml2:Subject> element of the assertions issued by an Identity Provider MUST contain a <saml2:NameID> .

The <saml2:Subject> element MUST contain one <saml2:SubjectConfirmation> element (urn:oasis:names:tc:SAML:2.0:cm:bearer). The <saml2:SubjectConfirmation> element MUST contain a <saml2:SubjectConfirmationData> element.

The <saml2:SubjectConfirmationData> element MUST include the following:

- The InResponseTo attribute MUST be present and its value MUST match the value of the corresponding request's ID attribute
- It MUST also include a recipient attribute containing the SP assertion consumer service URL
- It MUST also include a NotOnOrAfter attribute the time at which the request expires, after which the recipient MUST discard the message.

The <saml2:Conditions> element MUST be included in the assertion. It MUST contain the attribute NotOnOrAfter in order to specify the expiration time of the assertion. A NotBefore attribute SHOULD NOT be included. All timestamps MUST be in UTC time zone (e.g. "2012-01-23T01:23:45Z"), minimum resolution 1 second. NotOnOrAfter timestamp MUST be 10 minutes or less into the future at the time of issuance. All FTN participants SHOULD be configured with a reliable UTC time source to prevent problems caused by time drift. All issued assertions MUST indicate the level of assurance (LoA) under which the assertion was issued.

An <saml2:AuthnStatement> element that includes an <saml2:AuthnContext> element that includes at least one <saml2:AuthnContextClassRef> element MUST be used.

The signature present in the <saml2p:Response> message MUST be verified. If the signature verification fails, the response MUST be discarded, the event SHOULD be logged, and an error message MAY be shown to the user. The above procedure MUST also be followed for <saml2p:Response> messages that do not contain a signature, or contain a plaintext assertion instead of an <saml2:EncryptedAssertion>.The public key being used to verify the signature MUST appear in the issuing IDP metadata (<ds:X509Certificate> or <ds:KeyValue> element under the <ds:KeyInfo> element).

3.6.2.1 Additional Security Validations

The FTN Broker MUST verify that the assertion is not used more than once, and when used, is used within its validity period (the `NotOnOrAfter` attribute in `<saml2:Conditions>` element).

Additional details are specified in Regulation M72.

3.6.2.2 Chained authentication tokens/means response attribute

This FTN IdP to FTN IdP specific response attribute is REQUIRED when creating a new chained strong authentication token/means ("Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista" 617/2009 17 §). The attribute is returned in the set of attributes specified in Section 3.4.

Name	FriendlyName	Comments
urn:oid: 1.2.246.575.1.17	`FINChainLevel`	This attribute is included in response to a Section 3.5.3.2 request. The presence of this attribute signals that the FTN IdP sending the response performed the authentication successfully in response to a `chainlevel` request extension, and that the IdP receiving the response MAY thus issue a new chained authentication token/means of the specified Level of Assurance to the end user. This attribute MUST NOT be included in a response if the authentication request did not include the `chainlevel` request extension. The value of this parameter MUST be the same Level of Assurance (LoA) URI as specified in the `chainlevel` request and the authentication of the end user MUST have been performed at the indicated LoA or higher.

3.6.3 Error responses

An Identity Provider conformant with this profile SHOULD NOT make use of any other `<saml2p:StatusCode>` values than those specified in section 3.2.2.2 of [SAML2Core].
The top-level `<saml2p:StatusCode>` value may only be one of the following error identifiers:

- `urn:oasis:names:tc:SAML:2.0:status:Requester` – The request could not be performed due to an error on the part of the FTN Broker.

- `urn:oasis:names:tc:SAML:2.0:status:Responder` – The request could not be performed due to an error on the part of the Identity Provider.

- `urn:oasis:names:tc:SAML:2.0:status:VersionMismatch` – The Identity Provider could not process the request because the version of the request message was incorrect.

If an Identity Provider displays information describing an error in its user interface, it MUST also offer ways for the end user to confirm this information (for example, by including an OK button). When the end user acknowledges the information (i.e., clicks on the OK button), the `<saml2p:Response>` message is posted back to the FTN Broker according to the HTTP POST binding [SAML2Bind].

4 Annex: Explanatory notes on Metadata and Trust management

4.1 Requirements for Metadata content

4.1.1 Metadata element explanation table

Following table provides more detailed information about metadata elements.

Element	Explanation
SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP].	For interoperability.
Participants in the Finnish Trust Network MUST use TLS 1.2 or newer for Assertion Consumer Service endpoints. During a SAML protocol exchange, the relying party MUST either verify the validity of the metadata file containing the peer entity or verify the validity of the certificate used by the peer entity for protecting the SAML exchange.	Older TLS/SSL versions are vulnerable and supporting TLS version 1.2 or newer is mandatory. See [M72] Section 7 and [M72notes] for details. [eIDASTech] document also defines acceptable algorithms and key lenghts to be used. Signature validation is always mandatory in order to guarantee communication integrity and authenticity.
MUST include an <md:IDPSSODescriptor> element	IDP service (SSO) information.
necessary <md:KeyDescriptor>	Information on used encryption / signature key.
<md:SingleSignOnService>	Binding elements, and location (http post). Mandatory entry
urn:oasis:names:tc:SAML:2.0:nameid-format:transient name identifier format as specified in [SAML2Core].	temporary (transient) identifier, not longer than 256 characters, created according to SAML standard.
metadata exchange : <md:EntitiesDescriptor>	identifies the metadata entity. entityID defines name inside this element (other options can validUntil and cacheDuration).
validUntil	Expresses the metadata ”expiry date”. This is a security feature.
cacheDuration	Expresses the maximum time the receiver should store the metadata in the cache memory, before refreshing.

4.2 Recommended cryptographic algorithms

Some XML cryptographic algorithms are listed in Table 1 for the FTN. These fulfil the encryption requirements of FICORA Regulation 72. FTN participants MUST support algorithms that are marked REQUIRED in the table.

Table 1: XML cryptographic algorithms for the FTN

URI [XMLSec]	Usage	Algorithm	Status in FTN
`http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`	Signatures, ds:SignatureMethod	RSA PKCS#1 v1.5 using SHA-256	REQUIRED
`http://www.w3.org/2001/04/xmlenc#sha256`	Digests, ds:DigestMethod	SHA-256	REQUIRED
`http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256`	Signatures, ds:SignatureMethod	ECDSA using P-256 and SHA-256	OPTIONAL
`http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p`	Key Transport	RSAES OAEP using SHA-1 and MGF1 with SHA-1	REQUIRED
`http://www.w3.org/2009/xmlenc11#rsa-oaep` `http://www.w3.org/2009/xmlenc11#mgf1sha256`	Key Transport	RSAES OAEP using SHA-256 and MGF1 with SHA-256	OPTIONAL
`http://www.w3.org/2009/xmlenc11#ECDH-ES`	Key Agreement	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement using Concat KDF	OPTIONAL
`http://www.w3.org/2009/xmlenc11#aes128-gcm`	Symmetric encryption, xenc:EncryptionMethod	AES GCM using 128-bit key	REQUIRED

RSA keys used MUST be 2048 bits or longer. Elliptic curve keys MUST be long enough to provide a symmetric key equivalent security strength of at least 112 bits (typical EC algorithm key length of 224 bits or longer). Symmetric keys MUST be 128 bits or longer. Hash algorithms used MUST have a digest size of 224 bits or longer.

Algorithms/key sizes that provide cryptographically equivalent or stronger security level than described here MAY be used. Weaker algorithms/key sizes MUST NOT be used.

References

[M72] FICORA Regulation M72/2016
https://www.viestintavirasto.fi/attachments/maaraykset/M72_2016_EN.pdf

[M72notes] Explanatory notes to FICORA Regulation M72/2016
https://www.viestintavirasto.fi/attachments/maaraykset/M72_2016_MPS_EN.pdf

[Providerlist] FICORA Register of strong identification service providers
https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus/rekisteritunnistamispalveluntarjoajista.html

[BCP47] RFC 5646 Tags for identifying Languages and RFC 4647 Matching of Language Tags, https://tools.ietf.org/html/bcp47

[RFC2119] Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997. https://www.ietf.org/rfc/rfc2119.txt

[RFC2119] Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997. https://www.ietf.org/rfc/rfc2119.txt

[SAML2Int] SAML2int profile v0.21 – SAML 2.0 Interoperability Profile. http://saml2int.org/profile/current/

[SAML2Core] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. https://www.oasis-open.org/standards#samlv2.0

[SAML v2.0 Errata 05] SAML Version 2.0 Errata 05. 01 May 2012. OASIS Approved Errata. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html

[SAML2Bind] OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. https://www.oasis-open.org/standards#samlv2.0

[SAML2Prof] OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. https://www.oasis-open.org/standards#samlv2.0

[SAML2Meta] OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. https://www.oasis-open.org/standards#samlv2.0

[SAML2Sec] Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. https://www.oasis-open.org/standards#samlv2.0

[SAML2IAP] SAML V2.0 Identity Assurance Profiles Version 1.0, 05 November 2010. https://www.oasis-open.org/standards#samlv2.0

[MetaIOP] OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009. https://www.oasis-open.org/standards#samlv2.0

[SAML2MetaUI] OASIS Draft, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, September 2010. https://www.oasis-open.org/standards#samlv2.0

[SAML2MetaAttr] OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009. https://www.oasis-open.org/standards#samlv2.0

[EntCat] The Entity Category SAML Entity Metadata Attribute Type, March 2012. http://macedir.org/entity-category/

[IdpDisco] OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008. https://wiki.oasis-open.org/security/IdpDiscoSvcProtonProfile

[STORK_2.0_D4.11] STORK 2.0 D4.11Final version of Technical Specifications for the cross border Interface, September 2015. https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174

[eIDASTech] eIDAS Technical Specifications v1.1 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID+eIDAS+profile

[RFC 2256] A Summary of the X.500(96) User Schema for use with LDAPv3, December 1997. https://www.ietf.org/rfc/rfc2256.txt

[XMLDSig] XML Signature Syntax and Processing (Second Edition) http://www.w3.org/TR/xmldsig-core/

[XMLSec] XML Security Algorithm Cross-Reference https://www.w3.org/TR/xmlsec-algorithms/

[ISACoreLocVoc] ISA Core Location Vocabulary 1.00 https://joinup.ec.europa.eu/site/core_location/xsd.html https://joinup.ec.europa.eu/site/core_location/specs.pdf