Deployment Profile for the Swedish eID Framework

ELN-0602-v1.1

Version 1.1

2014-04-22

1 Introduction 3

1.1 Requirements Notation 3

1.2 References to SAML 2.0 Standards and Profiles 3

2 Metadata and Trust Management 4

2.1 Requirements for Metadata Content 4

2.1.1 Generic 4

2.1.2 Service Providers 4

2.1.3 Identity Providers 5

2.1.4 Signature Service 5

3 Name Identifiers 7

4 Attributes 7

5 Authentication Requests 7

5.1 Discovery 7

5.2 Security Requirements 7

5.3 Message Content 7

5.4 Processing Requirements 8

5.4.1 Identity Provider User Interface 8

5.4.2 Overriding Level of Assurance 8

6 Responses 8

6.1 Security Requirements 8

6.2 Message Content 8

6.3 Error Responses 10

7 Normative References 11

8 Changes between versions 12

# Introduction

This profile specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO Profile [[SAML2Prof](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)] are required or permitted to rely on. The profile extends Interoperable SAML 2.0 Web Browser SSO Deployment Profile [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] with requirements specific for the Swedish eID-framework and specifies deployment details that are not covered in [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)].

Readers should be familiar with all relevant reference documents, and any requirements stated are not repeated unless where deemed necessary to clarify or highlight a certain issue.

This profile, like [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)], addresses the content, exchange, and processing of SAML messages, but also specifies some deployment details that go beyond that scope, such as required metadata elements.

Any SAML features specified in referenced SAML documents that are optional are out of scope of this profile, unless explicitly specified by this profile.

## Requirements Notation

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](http://www.ietf.org/rfc/rfc2119.txt)].

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.

## References to SAML 2.0 Standards and Profiles

When referring to elements from the SAML 2.0 core specification [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], 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](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)].
* <mdui:Element> – for elements defined in [[SAML2MetaUI](https://www.oasis-open.org/committees/download.php/39441/draft-sstc-saml-metadata-ui-03.pdf)].
* <mdattr:Element> – for elements defined in [[SAML2MetaAttr](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html)].

When referring to elements from the Identity Provider Discovery Service Protocol and Profile [[IdPDisco](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)], the following syntax is used:

* <idpdisc:DiscoveryResponse>

When referring to elements from the W3C XML Signature namespace (http://www.w3.org/2000/09/xmldsig#) the following syntax is used:

* <ds:Signature>

# Metadata and Trust Management

Identity Providers and Service Providers that are part of the federation for Swedish eID MUST provide a SAML 2.0 Metadata document representing its entity. Provided metadata MUST conform to [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] as well as the SAML V2.0 Metadata Interoperability Profile Version 1.0 [[MetaIOP](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)].

## Requirements for Metadata Content

### Generic

All services that are represented in the Metadata SHALL include a <md:Organization> element with mandatory child elements, which includes at least one of each of the elements <md:OrganizationName>, <md:OrganizationDisplayName> and <md:OrganizationURL>.

The <md:OrganizationName> element SHALL hold a registered name of the organization, which matches the agreement with the federation operator.

The <md:OrganizationDisplayName> element SHALL contain a display name of the organization and SHALL NOT contain a service name that is unrelated to the name of the organization.

All services represented in the metadata SHALL include RSA public keys in the form of a certificate, which supports both signature validation and encryption. The same public key MAY support both signature validation and encryption, indicated by an absent "use" attribute.

### Service Providers

Metadata for a Service Provider SHOULD contain at least one service entity category attribute [[EntCat](http://macedir.org/entity-category/)] that has been defined in [Eid2EntCat] identifying a service entity category of the provided service, identifying its needs in relation to identity services.

The example below illustrates how an entity declares the entity category **http://id.elegnamnden.se/ec/1.0/loa3-pnr** in its metadata.

...

<md:Extensions>

<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

<saml:Attribute Name="http://macedir.org/entity-category"

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

<saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

http://id.elegnamnden.se/ec/1.0/loa3-pnr

</saml:AttributeValue>

</saml:Attribute>

</mdattr:EntityAttributes>

</md:Extensions>

...

Any needs for particular attributes from identify providers, when present, MUST be expressed through present service entity category in combination with <md:RequestedAttribute> elements in the service provider metadata. The present <md:RequestedAttribute> elements in the service provider metadata, when present, holds a list of requested and/or required attributes. This list of attributes MUST be interpreted in the context of present service entity categories defined in [[EntCat](http://macedir.org/entity-category/)]. Attribute requirements defined by a present service entity category takes precedence over present <md:RequestedAttribute> elements. For example, if the service entity category identifies an attribute profile with a set of prohibited attributes, then those attributes MUST not be returned in an assertion to this service provider even if listed in the a present <md:RequestedAttribute> element. When the service provider requires one out of a particular set of attributes then such conditions and preferences MUST be defined through a present service entity category.

Metadata for a Service Provider SHALL contain an <mdui:UIInfo> extension, extending the <md:SPSSODescriptor> element. This <mdui:UIInfo> element SHALL at least contain a <mdui:DisplayName> element with the language attribute "sv" (Swedish), representing the Service Provider name that has been approved by the federation operator. The <mdui:UIInfo> element SHALL also contain a reference to a logotype image (<mdui:Logo>) and SHOULD contain a <mdui:Description> element with the language attribute "sv" (Swedish).

It is RECOMMENDED that the above elements represented in Swedish also be represented with the language attribute "en" (English).

### Identity Providers

The entity descriptor for an Identity Provider SHOULD contain at least one service entity category attribute [[EntCat](http://macedir.org/entity-category/)] identifying a defined service entity category of the identity service that has been defined in [Eid2EntCat].

Metadata for an Identity Provider SHALL contain an <mdui:UIInfo> extension, extending the <md:IDPSSODescriptor> element. This <mdui:UIInfo> element SHALL at least contain a <mdui:DisplayName> element with the language attribute "sv" (Swedish), representing the Identity Provider service name that has been approved by the federation operator. The <mdui:UIInfo> element SHALL also contain a reference to a logotype image (<mdui:Logo>) and SHOULD contain a <mdui:Description> element with the language attribute "sv" (Swedish).

It is RECOMMENDED that the above elements represented in Swedish also be represented with the language attribute "en" (English).

The entity descriptor for an Identity Provider SHALL contain an entity attribute according to [[SAML2IAP](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html)] with Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" holding at least one attribute value identifying a Level of Assurance (LoA) level for which the Identity Provider has been approved and where the value is one of the LoA identifiers provided in [Eid2LoA] and whose meaning are defined in [Eid2Tillit].

### Signature Service

The Signature Service within the framework for Swedish eID is a Service Provider with specific requirements concerning its representation in metadata. Its entry in metadata SHALL contain an <mdui:UIInfo> element, extending the <md:SPSSODescriptor> element. This <mdui:UIInfo> element SHALL at least contain a <mdui:DisplayName> element with the language attribute "sv" (Swedish), representing the signature service that has been approved by the federation operator.

The <mdui:UIInfo> element SHALL also contain a reference to a logotype image (<mdui:Logo>) and at least contain one <mdui:Description> element with the language attribute "sv" (Swedish), providing a description of the service according to requirements provided by the federation operator.

It is RECOMMENDED that the above elements represented in Swedish also be represented with the language attribute "en" (English).

The entity descriptor for a Signature Service SP entity SHALL contain an entity category attribute [[EntCat](http://macedir.org/entity-category/)] specifying the value **http://id.elegnamnden.se/st/1.0/sigservice**.

# Name Identifiers

Identity Providers and Service Providers MUST support both the urn:oasis:names:tc:SAML:2.0:nameid-format:persistent and the urn:oasis:names:tc:SAML:2.0:nameid-format:transient name identifier formats as specified in [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)].

# Attributes

Attribute specifications for the Swedish eID Framework is defined in [Eid2Attributes].

The content of <saml2:AttributeValue> elements exchanged via any SAML 2.0 messages or assertions SHOULD be limited to a single child text node.

# Authentication Requests

## Discovery

The federation for Swedish eID uses a central discovery service as specified in Identity Provider Discovery Service Protocol Profile [[IdPDisco](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)]. A Service Provider is not obliged to use the central discovery service and MAY instead implement discovery using an integrated technique as described in [Eid2Disco].

A Service Provider SHOULD use either the central discovery service or the integrated discovery techniques as described in [Eid2Disco].

Service Providers making use of the central discovery service MUST be able to handle empty responses for the cases where no Identity Provider was chosen. In these cases an error message should be displayed for the end user.

## Security Requirements

The endpoints at which an Identity Provider receives a <saml2p:AuthnRequest> message, and all subsequent exchanges with the user agent, MUST be protected by TLS/SSL ([SAML2Int] specifies SHOULD).

## Message Content

A Service Provider may choose to override its default LoA-requirement by specifying a LoA identifier URL as a value to the <saml2:AuthnContextClassRef> element that is part of the <saml2p:RequestedAuthnContext> element. Identity Providers conformant with this profile MUST support explicitly requested Level of Assurance processing.

The <saml2p:AuthnRequest> message SHOULD contain a <saml2p:NameIDPolicy> element with an element with an AllowCreate attribute with the value "true". Its Format attribute, if present, SHOULD be set to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

Identity Providers conformant with this profile MUST support the <saml2p:ForceAuthn> attribute received in a <saml2p:AuthnRequest> message.

## Processing Requirements

### Identity Provider User Interface

Where the requirements for user interfaces defined for the federation requires presentation of information elements related to the service provider, these information elements MUST be obtained from the <mdui:UIInfo> element in the service provider’s metadata entry. Implementers of this profile MUST be capable of handling display information stored in the <mdui:DisplayName>, <mdui:Logo> and the <mdui:Description> elements.

### Overriding Level of Assurance

If an <saml2p:AuthnRequest> contains an <saml2p:RequestedAuthnContext> element with a Level of Assurance URL specified in the <saml2p:RequestedAuthnContext> element [Eid2LoA], the Identity Provider is obliged to follow this requirement. This means that the LoA given as a requirement as an Entity Category [Eid2EntCat] in the Service Provider’s metadata entry is overridden, and that the Identity Provider should process the request as the LoA specified in the request message specifies.

**Note**: In the situation where a Service Provider overrides its default required Level of Assurance by assigning it in the authentication request, the Service Provider should ensure that the Identity Provider to which the request is sent will be able to process the request regarding the required Level of Assurance. This is specifically important when the Discovery Service has been used to select which Identity Provider the end user wishes to use to authenticate – the Discovery Service will only perform its matching based on the entity categories specified in the metadata (see [Eid2EntCat]).

# Responses

## Security Requirements

The endpoint(s) at which a Service Provider receives a <saml2p:Response> message MUST be protected by TLS/SSL ([[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] states SHOULD).

The <saml2:Assertion> element issued by the Identity Provider MUST be signed using a <ds:Signature> element within the <saml2:Assertion>.

Identity Providers SHALL utilize XML Encryption and return a <saml2:EnctyptedAssertion> element in the <saml2p:Response> message. The elements <saml2:EncryptedID> and <saml2:EncryptedAttribute> MUST NOT be used; instead the entire assertion should be encrypted.

Service Providers MUST support unsolicited <samlp2:Response> messages (i.e., responses that are not the result of an earlier <saml2p:AuthnRequest> message). The reason for this is that seamless login should be possible between Service Providers within the federation for Swedish eID. A Service Provider may direct the user agent to another Service Provider via the Identity Provider where the user was authenticated.

## Message Content

The <saml2:Subject> element of the assertions issued by an Identity Provider SHOULD contain a <saml2:NameID> element. The <saml2:Subject> element MUST NOT include a <saml2:BaseID> nor a <saml2:EncryptedID>. In the absence of a <saml2p:NameIDPolicy> Format attribute in the Service Provider's <saml2p:AuthnRequest> message, or a <md:NameIDFormat> element in the Service Provider's metadata, the Format of the <saml2:NameID> SHOULD be set to urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

An Identity Provider conformant to this profile MUST, in its issued assertions, include an identifier indicating under which Level of Assurance [Eid2LoA] the assertion was issued. This LoA identifier MUST be placed under the <saml:AuthnStatement> element as the value of an <saml:AuthnContextClassRef> element that is part of the <saml:AuthnContext> element.

...

<saml:AuthnStatement AuthnInstant="2013-03-15T09:22:00" SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">

<saml:AuthnContext>

<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa3</saml:AuthnContextClassRef>

...

</saml:AuthnContext>

</saml:AuthnStatement>

...

The Identity Provider may include an authentication context class declaration according to the XML Schema identified by the LoA identifier, specified in [Eid2LoA]. When present, this declaration is placed in a <saml2:AuthnContextDecl> element after the <saml2:AuthnContextClassRef> element.

Example of how the LoA identifier is included as an authentication statement.

...

<saml2:AuthnStatement AuthnInstant="2014-04-28T14:50:24.125Z" SessionIndex="\_8f480832d962de6138a4d78c1a199fbd">  
 <saml2:AuthnContext>  
 <saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa3</saml2:AuthnContextClassRef>  
 <saml2:AuthnContextDecl>  
 <loa3:AuthenticationContextDeclaration xmlns:loa3="http://id.elegnamnden.se/loa/1.0/loa3">  
 <loa3:GoverningAgreements>  
 <loa3:GoverningAgreementRef

governingAgreementRef="http://elegnamnden.se/doc/tillitsramverk.pdf#loa3"/>  
 </loa3:GoverningAgreements>  
 <loa3:Extension>  
 <loacp:AuthContextParams xmlns:loacp="http://id.elegnamnden.se/ns/1.0/loa-context-params">  
 <loacp:AuthContextParam Name="securitycontext"

ContentType="base64">EfcC5i…loa:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loa:AuthContextParam>  
 </loacp:AuthContextParams>  
 </loa3:Extension>  
 </loa3:AuthenticationContextDeclaration>  
 </saml2:AuthnContextDecl>  
 </saml2:AuthnContext>  
</saml2:AuthnStatement>

...

Example of how an authentication context class declaration is amended to the authentication statement.

Identity Providers MUST support processing of a Service Provider’s requirements according to its specified Entity Categories as specified in in its metadata entry and defined by [Eid2EntCat]. If an Identity Provider cannot issue an assertion containing all attributes specified in present <md:RequestedAttribute> metadata elements with isRequired set to **true**, or any other requirements defined in [Eid2EntCat], it MUST respond with an error response where the top-level <saml2p:StatusCode> SHOULD have the value urn:oasis:names:tc:SAML:2.0:status:Responder, and where the subordinate status code, if present, has the value urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)].

An Identity Provider MUST NOT include any other attributes in issued assertions than those requested by the Service Provider. The set of allowed attributes are limited to the union of all attributes explicitly requested through any present Service Entity Category identifiers [Eid2EntCat] and all attributes specified in present <md:RequestedAttribute> elements in the Service Provider’s metadata entry.

## Error Responses

If the Identity Provider returns an error, it MUST NOT include any assertions in the <saml2p:Response> message.

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](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], and 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 Service Provider.
* 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 confirms taking part of the information (i.e., clicks on the OK-button), the <saml2p:Response> message is posted back to the Service Provider according to the HTTP POST binding [[SAML2Bind](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)].

# Normative References

[RFC2119]

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

[SAML2Int]

[SAML 2.0 INT SSO Deployment Profile.](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)

[SAML2Core]

[OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

[SAML2Bind]

[OASIS Standard, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)

[SAML2Prof]

[OASIS Standard, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

[SAML2Meta]

[OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

[SAML2IAP]

[SAML V2.0 Identity Assurance Profiles Version 1.0, 05 November 2010](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html).

[MetaIOP]

[OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0,](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)

[August 2009.](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)

[SAML2MetaUI]

[OASIS Draft, SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, September 2010.](https://www.oasis-open.org/committees/download.php/39441/draft-sstc-saml-metadata-ui-03.pdf)

[SAML2MetaAttr]

[OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009.](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html)

[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.](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)

[Eid2LoA]

[Authentication Context Classes for Levels of Assurance for the Swedish eID Framework.](ELN-0605+-+Bilaga+Tekniskt+ramverk+-+Authentication+Context+Classes+for+Levels+of+Assurance+for+the+Swedish+eID+Framework.pdf)

[Eid2Attributes]

[Attribute Specification for the Swedish eID Framework.](ELN-0604+-+Bilaga+Tekniskt+ramverk+-+Attribute+Specification+for+the+Swedish+eID+Framework.pdf)

[Eid2Tillit]

[Tillitsramverk för Svensk E-legitimation.](ELN-0700+-+Tillitsramverk+f%C3%B6r+Svensk+e-legitimation.pdf)

[Eid2EntCat]

[Entity Categories for the Swedish eID Framework.](ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)

[Eid2Disco]

[Discovery within the Swedish eID Framework.](ELN-XXYY+-+Bilaga+Tekniskt+ramverk+-+Discovery+within+the+Swedish+eID+Framework.pdf)

# Changes between versions

**Changes between version 1.0 and version 1.1:**

* In chapter 5.1, “Discovery”, a reference to the specification “Discovery within the Swedish eID Framework” [Eid2Disco] was added.
* In chapter 5.4.2, “Overriding Level of Assurance”, a note was added that informs about the need to ensure IdP-capabilities regarding level of assurance before issuing a request.
* In chapter 6.2, “Message Content”, an example of how an Identity Provider may include an authentication context class declaration was provided.
* Some faulty references were corrected.