Deployment Profile for the Swedish eID Framework

ELN-0602-v1.2

Version 1.2

2015-04-29

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 6

3 Name Identifiers 7

4 Attributes 7

5 Authentication Requests 7

5.1 Discovery 7

5.2 Binding and Security Requirements 7

5.3 Message Content 8

5.4 Processing Requirements 8

5.4.1 Validation of Destination 8

5.4.2 Validation of Assertion Consumer Addresses 8

5.4.3 Identity Provider User Interface 9

5.4.4 Overriding Level of Assurance 9

5.4.5 Single Sign On Processing 9

6 Responses 10

6.1 Security Requirements 10

6.2 Message Content 10

6.3 Processing Requirements 12

6.3.1 Signature Validation 12

6.3.2 Subject Confirmation 12

6.3.3 Conditions 12

6.3.4 The Authentication Statement 13

6.3.5 General Security Validation 13

6.4 Error Responses 13

7 Normative References 14

8 Changes between versions 16

# 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.

This profile does not handle requirements regarding algorithms and different versions of underlying security mechanisms. This information is distributed by the federation operator in other channels.

## 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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)] 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">

<saml2:Attribute Name="http://macedir.org/entity-category"

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

xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

<saml2: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

</saml2:AttributeValue>

</saml2: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 <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).

A Service Provider MAY sign authentication request messages sent to Identity Providers. A Service Provider that signs authentication requests messages MAY also ensure that a receiving Identity Provider will only accept valid signed requests from this Service Provider by assigning the AuthnRequestsSigned attribute of the <md:SPSSODescriptor> to a value of "true".

Section E7, “Metadata for Agreeing to Sign Authentication Requests”, of [SAML v2.0 Errata 05] specifies the following concerning the AuthnRequestsSigned attribute:

Optional attribute that indicates whether the <saml2p:AuthnRequest> messages sent by this service provider will be signed. If omitted, the value is assumed to be false. A value of false (or omission of this attribute) does not imply that the service provider will never sign its requests or that a signed request should be considered an error. However, an identity provider that receives an unsigned <saml2p:AuthnRequest> message from a service provider whose metadata contains this attribute with a value of true MUST return a SAML error response and MUST NOT fulfill the request.

### 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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)].

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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f2/1404733204565/ELN-0605+-+Bilaga+Tekniskt+ramverk+-+Authentication+Context+Classes+for+Levels+of+Assurance+for+the+Swedish+eID+Framework.pdf)] and whose meaning are defined in [[Eid2Tillit](http://www.elegnamnden.se/download/18.77dbcb041438070e039d237/1404726253939/ELN-0700+-+Tillitsramverk+f%C3%B6r+Svensk+e-legitimation.pdf)].

An Identity Provider MAY require authentication request messages to be signed. This is indicated by assigning the WantAuthnRequestsSigned attribute of the <md:IDPSSPDescriptor> element to a value of "true". See further section E7, “Metadata for Agreeing to Sign Authentication Requests”, of [SAML v2.0 Errata 05].

### 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**](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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f1/1404733027997/ELN-0604+-+Bilaga+Tekniskt+ramverk+-+Attribute+Specification+for+the+Swedish+eID+Framework.pdf)].

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](http://www.elegnamnden.se/download/18.3aa8c78a1466c584587733f/1404891886694/ELN-0610+-+Bilaga+Tekniskt+ramverk+-+Discovery+within+the+Swedish+eID+Framework.pdf)].

A Service Provider SHOULD use either the central discovery service or the integrated discovery techniques as described in [[Eid2Disco](http://www.elegnamnden.se/download/18.3aa8c78a1466c584587733f/1404891886694/ELN-0610+-+Bilaga+Tekniskt+ramverk+-+Discovery+within+the+Swedish+eID+Framework.pdf)].

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.

## 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 be protected by TLS/SSL ([SAML2Int] specifies SHOULD).

[SAML2Int] specifies that a <saml2p:AuthnRequest> message MUST be communicated to the Identity Provider using the HTTP-REDIRECT binding. This profile will also allow the usage of the HTTP-POST binding for sending <saml2p:AuthnRequest> messages (see section 3.5 of [[SAML2Bind](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)]).

An Identity Provider that requires <saml2p:AuthnRequest> messages to be signed 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.

An Identity Provider that itself does not require authentication messages to be signed MUST still accept and verify signed request messages from Service Providers that indicate, in their metadata, that they sign request messages (see 2.1.2 above). If this signature verification fails, the Identity Provider MUST return a SAML error response and MUST NOT fulfill the request.

An Identity Provider that receives a request message that is not signed from a Service Provider that has indicated, in its metadata, that it will only send signed request messages (see 2.1.2 above) MUST respond with an error.

The signature for authentication request messages is applied differently depending on the binding. The 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](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)]). For the HTTP-POST binding the <saml2p:AuthnRequest> element MUST be signed using a <ds:Signature> element within the <saml2:AuthnRequest>.

## Message Content

[[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] specifies that a <saml2p:AuthnRequest> message MUST contain an AssertionConsumerServiceURL attribute identifying the desired response location. The Service Provider 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](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)]).

The Destination attribute of the <saml2p:AuthnRequest> message MUST contain the URL to which the Service Provider has instructed the user agent to deliver the request. This is useful to prevent malicious forwarding of signed requests from being accepted by unintended Identity Providers.

A Service Provider may choose to override its default Level of Assurance requirement by specifying a Level of Assurance 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 (see section 5.4.4).

Identity Providers conformant with this profile MUST support the ForceAuthn and IsPassive attributes received in <saml2p:AuthnRequest> messages.

Service Providers SHOULD include the ForceAuthn attribute in all <saml2p:AuthnRequest> messages and explicitly set its value to true or false, and not rely on its default value. The reason for this is to avoid accidental SSO.

## Processing Requirements

### Validation of Destination

An Identity Provider receiving a <saml2p:AuthnRequest> message MUST verify that the Destination attribute is present, and that it is consistent with URLs configured in the Identity Provider’s metadata.

### Validation of Assertion Consumer Addresses

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 Service Provider’s metadata entry. If this is not the case, the request must be rejected.

Section 6.2 of [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] specifies how comparisons between the AssertionConsumerServiceURL value and the values found in the Service Provider’s metadata should be performed.

### 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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f2/1404733204565/ELN-0605+-+Bilaga+Tekniskt+ramverk+-+Authentication+Context+Classes+for+Levels+of+Assurance+for+the+Swedish+eID+Framework.pdf)], the Identity Provider is obliged to follow this requirement. This means that the Level of Assurance given as a requirement as an Entity Category [[Eid2EntCat](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)] in the Service Provider’s metadata entry is overridden, and that the Identity Provider should process the request as the Level of Assurance specified in the request message specifies. However, the Identity Provider MUST NOT issue an assertion if the Identity Provider does not support, or is not approved to deliver, the requested Level of Assurance. In these cases the Identity Provider MUST respond with an error response where the top-level <saml2p:StatusCode> SHALL 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:RequestDenied [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)].

**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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)]).

### Single Sign On Processing

An Identity Provider conformant to this profile MAY issue an assertion relying on a previously established security context (active session) instead of authenticating the user. However, the Identity Provider MUST NOT re-use an already existing security context in the following cases:

* When the security context has expired, i.e., the time elapsed since the security context was established is too long given the SSO-policy stipulated by the federation.
* When the <saml2p:AuthnRequest> contains a ForceAuthn attribute with the value of "true".
* If the original authentication process, which led to the establishment of the security context, was performed using a weaker Level of Assurance that what is requested in the current <saml2p:AuthnRequest> message.

If the Identity Provider user interface contains some sort of user consent, or information, concerning which attributes, or any other information, that is included in an assertion being issued, the Identity Provider SHOULD preserve this functionality if a <saml2p:AuthnRequest> message requesting a different set of attributes (or any other information) compared to what was delivered in the assertion at the time of establishing the security context. The Identity Provider may require re-authentication or display a user interface for consent/information in these cases.

# 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 SHOULD NOT accept unsolicited <saml2p:Response> messages (i.e., responses that are not the result of an earlier <saml2p:AuthnRequest> message). Service Providers that do accept unsolicited response messages MUST ensure, by other means, that the security and processing requirements of this profile (section 6.3) can be fully satisfied. [[SAML2Int](http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG_SAML2.0_INT_SSO+Deployment+Profile_v0.1.pdf)] allows the use of unsolicited responses, but this profile has more strict security and processing requirements that make the use of unsolicited responses violate these requirements.

## Message Content

The <saml2:Response> message MUST contain an <saml2:Issuer> element containing the unique identifier (entityID) of the issuing identity provider.

The AuthnInstant attribute of the <saml2:AuthnStatement> element MUST be assigned the time when the actual authentication took place. This time may differ from the IssueInstant attribute of the assertion itself, which holds the time when the assertion was issued. This is especially important in cases of re-use of already established security contexts at the Identity Provider side.

The <saml2:Subject> element MUST contain one <saml2:SubjectConfirmation> element containing a Method of urn:oasis:names:tc:SAML:2.0:cm:bearer. This element MUST contain a <saml2:SubjectConfirmationData> element that contains at least the following:

* An InResponseTo attribute matching the request’s ID.
* A Recipient attribute containing the Service Provider’s assertion consumer service URL (see sections 5.3 and 5.4.1).
* A NotOnOrAfter attribute containing a time instant at which the subject no longer can be confirmed.

The <saml2:SubjectConfirmationData> SHOULD also contain an Address attribute containing the network address from which an attesting entity (user) can present the assertion.

The assertion MUST contain a <saml2:Conditions> element containing the following attributes and elements:

* A <saml2:AudienceRestriction> element including the requesting Service Provider’s unique identifier (entityID) as an <saml2:Audience> value.
* A NotBefore attribute specifying the earliest time instant at which the assertion is valid.
* A NotOnOrAfter attribute specifying the time instant when the assertion expires.

An Identity Provider conformant to this profile MUST, in its issued assertions, include an identifier indicating under which Level of Assurance [[Eid2LoA](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f2/1404733204565/ELN-0605+-+Bilaga+Tekniskt+ramverk+-+Authentication+Context+Classes+for+Levels+of+Assurance+for+the+Swedish+eID+Framework.pdf)] the assertion was issued. This Level of Assurance identifier MUST be placed under the <saml2:AuthnStatement> element as the value of an <saml2:AuthnContextClassRef> element that is part of the <saml2:AuthnContext> element.

...

<saml2:AuthnStatement AuthnInstant="2013-03-15T09:22:00" SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">

<saml2:AuthnContext>

<saml2:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa3</saml2:AuthnContextClassRef>

...

</saml2:AuthnContext>

</saml2:AuthnStatement>

...

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

The Identity Provider may include an authentication context class declaration according to the XML Schema identified by the Level of Assurance identifier, specified in [[Eid2LoA](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f2/1404733204565/ELN-0605+-+Bilaga+Tekniskt+ramverk+-+Authentication+Context+Classes+for+Levels+of+Assurance+for+the+Swedish+eID+Framework.pdf)]. When present, this declaration is placed in a <saml2:AuthnContextDecl> element after the <saml2:AuthnContextClassRef> element.

...

<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…<loacp:AuthContextParam>  
 <loacp:AuthContextParam Name="othercontext">OtherStuff</loacp: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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)]. 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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)], 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](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)] and all attributes specified in present <md:RequestedAttribute> elements in the Service Provider’s metadata entry.

## Processing Requirements

This profile mandates a correct processing of a <saml2p:Response> message in order to ensure proper protection from the security threats described in [[SAML2Sec](http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf)]. Processing requirements are listed in [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], [[SAML2Prof](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)] and [[SAML2Sec](http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf)]. This document will list the necessary requirements that apply to this profile.

After the Service Provider has encrypted the assertion from the received response message the following requirements apply. Any verification that fails MUST lead to that the Service Provider rejects the response message and does not use the assertion.

Some of the processing requirements below are defined in order to protect from MITM- or MITB-attacks[[1]](#footnote-1) were unsigned authentication requests may be changed before being sent to the Identity Provider. However, a Service Provider MUST implement all of the specified processing requirements even if it sends signed authentication request messages.

### Signature Validation

The signature present on the assertion MUST be successfully verified.

The public key being used to verify the signature MUST appear in the issuing Identity Provider’s metadata record (as a <ds:X509Certificate> or <ds:KeyValue> element under the <ds:KeyInfo> element).

### Subject Confirmation

Based on the InResponseTo attribute of the <saml2:SubjectConfirmationData> the Subject Provider MUST be able to obtain the corresponding <saml2p:AuthnRequest> message, or a secure context containing corresponding information from the request (for future processing of the assertion).

The Recipient attribute from the bearer <saml2:SubjectConfirmationData> element MUST match the location to which the <saml2p:Response> message was delivered **and** match value the AssertionConsumerServiceURL attribute included in the request message.

The time from the NotOnOrAfter attribute from the bearer <saml2:SubjectConfirmationData> MUST NOT have passed compared with the time instant at which the subject is confirmed (i.e., when the assertion is validated). A reasonable allowable clock skew between the providers should be taken in account.

If the Address attribute is assigned to the bearer <saml2:SubjectConfirmationData> element, the Service Provider MAY choose to check the user agent’s client address against it. Practical issues regarding the Service Provider’s network setup and the risk of introducing false negatives makes this an optional step in the validation phase.

### Conditions

The Service Provider MUST assert that the value of the <saml2:Audience> element under the <saml2:AudienceRestriction> element matches the unique entityID of the Service Provider.

The Service Provider MUST verify that the time instant at which the assertion is validated is within the range given by the NotBefore and NotOnOrAfter attributes of the <saml2:Conditions> element (allowing for a reasonable clock skew). See also the processing of the NotOnOrAfter attribute in section 6.3.2.

### The Authentication Statement

The Service Provider MUST assert that the <saml2:AuthnStatement> contains a <saml2:AuthnContext> element that holds a <saml2:AuthnContextClassRef> element having as its value the Level of Assurance identifier under which the authentication was made. This value MUST be equal to, or stronger[[2]](#footnote-2) than, the Level of Assurance required by the Service Provider.

### General Security Validation

In order to protect itself from replay attacks, the Service Provider MUST ensure that the same Assertion is not processed more than once within the time it is valid (with respect to the NotOnOrAfter attribute of the <saml2:Conditions> element).

In order to prevent stolen assertions and user impersonation, the Service Provider SHOULD implement a validation that rejects an assertion if the time given it its IssueInstant attribute compared to the time when the response message is received is too great. This time is typically on the order of seconds, and limits the time window when a stolen assertion could be used.

If the Service Provider included the attribute ForceAuthn with a value of "true" in the authentication request, the Service Provider SHOULD ensure that the AuthnInstant attribute of the <saml2:AuthnStatement> element is greater than the time when the request was sent (allowing for a reasonable clock skew).

## 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)

[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/errata05/os/saml-v2.0-errata05-os.html).

[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)

[SAML2Sec]

[Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-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.](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f2/1404733204565/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.](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f1/1404733027997/ELN-0604+-+Bilaga+Tekniskt+ramverk+-+Attribute+Specification+for+the+Swedish+eID+Framework.pdf)

[Eid2Tillit]

[Tillitsramverk för Svensk E-legitimation.](http://www.elegnamnden.se/download/18.77dbcb041438070e039d237/1404726253939/ELN-0700+-+Tillitsramverk+f%C3%B6r+Svensk+e-legitimation.pdf)

[Eid2EntCat]

[Entity Categories for the Swedish eID Framework.](http://www.elegnamnden.se/download/18.77dbcb041438070e039d6f3/1404733218067/ELN-0606+-+Bilaga+Tekniskt+ramverk+-+Entity+Categories+for+the+Swedish+eID+Framework.pdf)

[Eid2Disco]

[Discovery within the Swedish eID Framework.](http://www.elegnamnden.se/download/18.3aa8c78a1466c584587733f/1404891886694/ELN-0610+-+Bilaga+Tekniskt+ramverk+-+Discovery+within+the+Swedish+eID+Framework.pdf)

# Changes between versions

**Changes between version 1.1 and version 1.2:**

* This profile now explicitly defines requirements for the use of signed authentication request messages, see sections 2.1 and 5.2.
* This profile now allows the HTTP-POST binding to be used for sending authentication request messages (see chapter 5.2, “Binding and Security Requirements”). The main reason for this is to facilitate the use of signed authentication request messages.
* In chapter 5.4, additional processing requirements for received authentication requests were added or changed. These include:
* Validation of assertion consumer addresses (5.4.1).
* Clarifications to chapter 5.4.4, “Overriding Level of Assurance”.
* Single Sign On processing (5.4.5).
* This profile now states that “Unsolicited response” messages are not accepted by Service Providers due to security reasons, see chapter 6.1, “Security Requirements”.
* Changes and additions in chapter 6.2, “Message Content”, for responses including:
* Clarifications about the usage of the AuthnInstant attribute of the <saml2:AuthnStatement> element.
* Specifications of the use of <saml2:SubjectConfirmation> in assertions.
* Clarifications on the use of audience restrictions and assertion validity.
* Chapter 6.3, “Processing Requirements”, was added. This chapter contains specifications and requirements of how a response message should be processed in order to maintain security.

**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 5.4.4, “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.

1. MITM stands for ”man in the middle” and MITB stands for ”man in the browser”. [↑](#footnote-ref-1)
2. A stronger Level of Assurance identifier is simply a LoA having a higher value than what it is compared with, i.e., http://id.elegnamnden.se/loa/1.0/loa4 is stronger than http://id.elegnamnden.se/loa/1.0/loa3. [↑](#footnote-ref-2)