INTERNET
STIFTELSEN

| | |
|---|---|
| **Document** | SAML WebSSO Technology Profile |
| **Identifier** | https://skolfederation.se/policy/draft/swtp |
| **Version** | V1.0.1 |
| **Last modified** | 2023-01-20 |
| **Pages** | 16 |
| **Status** | Draft |
| **License** | Creative Commons BY-SA 3.0 |

# SAML WebSSO Technology Profile

Stefan Halén

**Abstract**

This document defines the SAML WebSSO technology profile for the federations of The Swedish Internet Foundation.

# Contents

# 1 Terminology and Typographical Conventions

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 [1]

Text in Italics is non-normative. All other text is normative unless otherwise stated.

## 1.1 Definition of terminology

**Credential:** A combination of information, cryptographic software and/or cryptographic hardware which a Subject proves possession of in order to authenticate itself in the Member Organization’s Identity Provider. This can be for example the combination of a username and password or a username and cryptographic device.

**Identity Provider:** The system component that issues attribute assertions on behalf of Subjects who use them to access the services of the Relying Party.

**Member Organization:** An organization that either is the owner of an Identity Provider or a Relying Party registered in one of the federations of The Swedish Internet Foundation.

**Relying Party:** A Service that relies upon a Subject’s credentials, typically to process a transaction or grant access to information on a system. Also known as Service Provider (SP). The Relying Party is owned by a Service Owner.

**Service Provider:** See Relying Party.

**Service Owner:** A Member Organization that is responsible and liable for operating a service registered in the federation. The Service Owner may delegate the technical operation of the Relying Party to another organization.

**Shared secret:** A piece of information that is shared exclusively between the parties involved in a secure communication.

**Subject:** Any natural person affiliated with a User Organization.

**User Organization:** A Member Organization with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

# 2 Operational Requirements for Identity Providers

The purpose of this section is to define requirements of Identity Providers in the federation.

## 2.1 Metadata registration

The purpose of this subsection is to define requirements regarding metadata registration of Identity Providers in the federation.

### 2.1.1 Language attributes (lang)

All metadata elements where language is relevant, i.e., MDUI/UIInfo and organizational elements, should include languages useful for the Identity Provider's users.

Metadata elements supporting the **lang** attribute MUST have a **lang** attribute with a value from "ISO 639-1".

For each metadata element supporting the **lang** attribute, there MUST NOT be more than one instance of each **lang** value for the element in question, except for the Logo MDUI element.

A **lang** attribute value used in one metadata element MUST be represented for all metadata elements supporting the **lang** attribute, except for the RegistrationPolicy element.

Metadata elements supporting the **lang** attribute MUST have a definition in English (en).

Metadata elements supporting the **lang** attribute MUST have a definition in Swedish (sv).

### 2.1.2 entityID

The entityID of an Identity Provider is its unique identifier in the federation.

The entityID MUST be globally unique.

The entityID attribute is a URI that MUST start with either **https://**, **http://** or **urn:**. The **urn:** form is a legacy format and SHOULD NOT be used when registering a new entity.

*Guidance: The https:// format is preferred.*

The entityID attribute MUST NOT exceed 256 characters in length.

### 2.1.3 errorURL

A Relying Party may use the errorURL of an Identity Provider to assist users in resolving login issues.

An Identity Provider MUST have a registered errorURL.

An Identity Provider SHOULD implement the "SAML V2.0 Metadata Deployment Profile for errorURL" [2].

### 2.1.4 Scope

Scopes are used to provide authoritative information to Scoped Attributes.

The <shibmd:Scope> element MUST appear within the <md:Extensions> element of an <md:EntityDescriptor> element or the <md:Extensions> element of a producer role descriptor element (such as <md:IDPSSODescriptor> or <md:AttributeAuthorityDescriptor>) [3].

An Identity Provider MUST have at least one Scope registered, representing a domain name owned by the Member Organization or which the Member Organization has delegated usage of.

Scope elements MUST contain a regexp attribute of false.

Scopes MUST NOT include regular expressions.

At request by the Federation Operator, the member MUST prove control of the domain by adding a DNS TXT resource record to the domain. The value for the record is provided by the Federation Operator.

The record is created by adding the label "_scope-challenge" to the domain being validated. TTL SHOULD be set to no more than 300.

*Guidance: This is an example record for the domain example.com.*
*_scope-challenge.example.com. 300 IN TXT "value"*

The Federation Operator validates the record by querying for the TXT record. The validation is successful if the response contains a resource record that matches the value provided by the Federation Operator.

If the validation is unsuccessful the Federation Operator will remove the metadata containing the scope from the federation.

### 2.1.5 Metadata Extensions for Login and Discovery User Interface (MDUI)

MDUI for an Identity Provider is information expected to be presented to end users and used by discovery services to help users select their Identity Provider for access to services.

An Identity Provider MUST have the following elements with **lang** attributes:

- **DisplayName**
  The name of the Identity Provider MUST be unique within the federation. The English name MUST be unique within the federation and all interacting interfederations.
- **Description**
  Short description of the Identity Provider.
- **Logo**
  URL to the organization logotype or the logotype of the Identity Provider itself. Multiple Logo elements with different height and/or width MAY be specified for the same language.
  - The value MUST be a URL that starts with https://
  - The logotype MUST NOT be embedded in the metadata
  - The logotype MUST be publicly accessible
  - The domain part of the URL MUST be a domain owned by the organization or which the organization has delegated usage of
  - The logotype SHOULD be in PNG file format
  - The logotype SHOULD be transparent and work on a white or light gray background
  - The logotype SHOULD be square (i.e., aspect ratio of 1:1) or, if not appropriate, SHOULD have landscape orientation (i.e., width > height)
  - The width of the logotype SHOULD be between 64 and 350 pixels
  - The height of the logotype SHOULD be between 64 and 146 pixels

An Identity Provider MAY have the following elements with lang attributes:

- **Keywords**
  Comma-separated list of search keywords of the Identity Provider.

An Identity Provider MAY have the following DiscoHints elements:

- **IPHint**
  CIDR block of expected users of the Identity Provider. Multiple IPHint elements MAY be specified.
- **DomainHint**
  DNS domain names of expected users serviced by the Identity Provider. Multiple DomainHint elements MAY be specified.
- **GeolocationHint**
  Geographic coordinates of expected users of the Identity Provider. Multiple GeolocationHint elements MAY be specified.

### 2.1.6 SAML certificates

For an Identity Provider there MUST be at least one signing certificate present in the metadata (i.e., a **KeyDescriptor** element with no **use** attribute or one set to **signing**).

### 2.1.7 SAML endpoints

SAML endpoints are the receivers of SAML requests and similar SAML messages.

All SAML endpoint URLs of an Identity Provider MUST start with **https://**.

### 2.1.8 Supported attributes

An Identity Provider MUST define supported attributes in metadata. An Identity Provider MUST have at least one **Attribute** element.

**Attribute** element(s) of an Identity Provider MUST have the following attributes:

- **Name**
  The value MUST be an attribute name from the Attribute Profile of the federation.
- **FriendlyName**
  The value MUST match the FriendlyName value from the Attribute Profile of the federation of the Name attribute value.
- **NameFormat**
  The value MUST be "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"

An **Attribute** element MAY have one or more **AttributeValue** elements.

### 2.1.9 Organization

The organization elements relate to the official name of the organization that the Identity Provider is operated for.

An Identity Provider MUST have the following **Organization** elements with **lang** attributes:

- **OrganizationName**
  The OrganizationName MUST be the same for all Identity Providers and Relying Parties owned by the organization, i.e., the legal name of the organization.
- **OrganizationDisplayName**
  The well-known name of the organization, e.g., if the organization is more known by its abbreviation than its full name.
- **OrganizationURL**
  The official web address of the organization.

### 2.1.10 ContactPerson

Contact information for the Identity Provider. Due to personal data protection legislation, contact information MUST NOT refer to a natural person.

**ContactPerson** elements MUST have an **EmailAddress** element starting with mailto:.

*Guidance: The e-mail address MUST be a functional mailbox where the address does not refer to a natural person.*

There MUST NOT be more than one **ContactPerson** element of each type.

An Identity Provider MUST have one **ContactPerson** element of type **administrative** registered in metadata.

*Guidance: The administrative ContactPerson is the contact point for governance of the Identity Provider.*

An Identity Provider MUST have one **ContactPerson** element of type **technical** registered in metadata.

*Guidance: The technical ContactPerson is the contact point for technical questions and issues regarding the use of the Identity Provider.*

An Identity Provider MUST have one **ContactPerson** element of type **support** registered in metadata.

*Guidance: The support ContactPerson is the contact point for end users and non-technical questions and issues regarding the use of the Identity Provider.*

### 2.1.11 Non-secure cryptographic algorithms

The metadata of an Identity Provider MUST only include **DigestMethod**, **SigningMethod** and **EncryptionMethod** elements containing algorithms defined in the latest published version of W3C Recommendations xmldsig-core and xmlenc-core respectively. Algorithms discouraged in the latest published version of xmldsig-core and xmlenc-core respectively SHOULD NOT be included.

*Guidance: At the time of writing, MD5 is obsolete and RSA v1.5 is not recommended in the latest published version.*

### 2.1.12 Unnecessary, large metadata

The metadata of an Identity Provider MUST NOT include **RoleDescriptor** elements.

*Guidance: RoleDescriptor elements are large and are unnecessary in the federation.*

## 2.2 SAML Keys and Certificates

The purpose of this subsection is to define the requirements of the SAML keys and certificates of Identity Providers. To minimize interoperability issues, certificates should be long-lived and self-signed. Note that the security of the federation is based on the signing of the metadata and not on the certificate verification chain or the lifespan of the entity certificates.

Identity Provider credentials (i.e., entity keys) MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than 2048-bit RSA/DSA keys or 256-bit ECC keys. 4096-bit RSA/DSA keys or 384-bit ECC keys are RECOMMENDED.

*Guidance: To minimize the administrative burden, keys should not be replaced unless they are at risk. Keys should be replaced when doing a major software upgrade or a hardware replacement. New keys should not use shorter comparable key strength than 4096-bit RSA/DSA keys or 384-bit ECC keys.*

Signing and encryption certificates MUST NOT be expired.

*Guidance: To minimize the administrative burden, certificates should not be replaced unless they are at risk. Certificates should have a lifespan of 10 years.*

Signing and encryption certificates SHOULD be self-signed.

*Guidance: To be able to use long-lived certificates, certificates should not be signed by well-known Certificate Authorities. Note that the signature of SAML certificates is not verified by Relying Parties.*

Keys known to be compromised or weak MUST be replaced in a timely manner.

An Identity Provider MUST support multiple signing certificates in the metadata of a Relying Party and MUST support validation of signatures using any of them.

*Guidance: This is used during key roll-over of a Relying Party.*

An Identity Provider SHOULD support multiple encryption certificates in the metadata of a Relying Party and SHOULD support encryption using one of them.

*Guidance: This is used during key roll-over of a Relying Party.*

## 2.3 Endpoint security

An Identity Provider MUST NOT support deprecated SSL/TLS protocols.

*Guidance: At the time of writing, SSLv2 was deprecated by RFC6176 in 2011, SSLv3 was deprecated by RFC7568 in 2015, TLS1.0 and TLS1.1 was deprecated by RFC8996 in March 2021.*

All Member Organizations operating an Identity Provider MUST consider applicable web protocol threats and apply appropriate controls to all relevant endpoints.

*Guidance: sslabs.com and similar services provide tools to detect known web protocol security issues. It is recommended to be continuously graded level A or higher at SSL Labs.*

## 2.4 Identity Provider software requirements

### 2.4.1 Metadata consumption and validation

An Identity Provider MUST refresh the metadata at least once every one (1) hour.

To ensure the validity of the federation metadata, the refresh process MUST verify the signature on every federation metadata fetch. The federation's signing certificate authenticity must be assured and verified in a secure way.

*Guidance: If the metadata is compromised, the bundled certificate in the metadata may also be compromised. Make sure to use the signing certificate of the federation that are distributed out of band.*

Federation metadata without a validUntil attribute or with a passed validUntil MUST not be trusted and MUST be discarded.

### 2.4.2 Authentication request

If a **RequestedAuthnContext** attribute is present in an authentication request, an Identity Provider MUST authenticate Subjects using one of the authentication methods requested.

*Guidance: If an authentication request has no RequestedAuthnContext attribute, the Identity Provider may choose any authentication method during authentication.*

If a multi-factor authentication is requested and performed it MUST use one of the methods described in the federation's identity assurance profile.

If an Identity Provider cannot authenticate the Subject using any authentication methods requested in a **RequestedAuthnContext** attribute in an authentication request, it MUST fail the authentication request and SHOULD respond to the Relying Party with a SAML error status.

*Guidance: If a RequestedAuthnContext SAML error response is sent to the Relying Party, it should contain the top-level StatusCode "urn:oasis:names:tc:SAML:2.0:status:Responder" and the second - level StatusCode "urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext".*

*Guidance: If no RequestedAuthnContext SAML error response is sent from the Identity Provider to the Relying Party, the user should be informed by the Identity Provider regarding the failure to authenticate using the requested method.*

An Identity Provider MUST include the authentication method used in the **AuthnContext** attribute of the response.

An Identity Provider MUST set the value of the **AuthnInstant** attribute in an authentication response to a current timestamp when and only when the Subject has performed a new authentication.

If an authentication request has the attribute **ForceAuthn** set to "true" or "1", an Identity Provider MUST perform a new authentication of the Subject.

*Guidance: Any present web single sign-on session of the Subject at the Identity Provider must not be used. Note that ForceAuthn is normally combined with specific RequestedAuthnContextClassRefs to force, for example, MFA to verify that Subject is present.*

### 2.4.3 Clock skew

An Identity Provider MUST allow between three (3) and five (5) minutes of clock skew, in either direction, when verifying the validity of an authentication request.

### 2.4.4 Operational security

An Identity Provider and their supporting infrastructure MUST NOT use software that is no longer maintained or software configurations with known security issues.

## 2.5 Attribute Release

Each value of released attributes MUST NOT exceed 256 characters.

*Guidance: For multivalued attributes, the separate values of each attribute must not exceed 256 characters. The complete value set of a specific attribute may be longer.*

### 2.5.1 Subject identifiers

The purpose of this subsection is to define requirements regarding identifiers of Subjects.

An Identity Provider MUST support release of a **NameID** with **nameid-format:transient** format.

*Guidance: The NameID element is primarily used for single logout purposes.*

Attributes used to identify a subject are defined in the Attribute Profile of the federation.

### 2.5.2 Scoped attributes

Attributes with scope must match the scope in the metadata of the Identity Provider, otherwise, they usually get filtered out by Relying Parties. Scoped attributes are defined in the attribute profile of the federation.

Scoped attributes MUST use one of the scopes defined in the metadata of the Identity Provider.

### 2.5.3 Attribute freshness

Attributes released from an Identity Provider MUST be kept up to date in accordance with administrative processes.

If a Subject or organization's information changes, it MUST be reflected in released attributes within one workweek.

### 2.5.4 Assurance

An Identity Provider SHOULD support the release of identity assurance of Subjects as defined in the identity assurance level profiles of the federation, using the identifiers of the respective identity assurance profiles.

The attribute used to release identity assurance of Subjects is defined in the attribute profile of the federation.

# 3 Operational Requirements for Relying Parties

The purpose of this section is to define requirements of Relying Parties in the federation.

## 3.1 Metadata registration

The purpose of this subsection is to define requirements regarding metadata registration of Relying Parties in the federation.

### 3.1.1 Language attributes (lang)

All metadata elements where language is relevant, i.e., MDUI/UIInfo and organizational elements, should include languages useful for the Relying Party's users.

Metadata elements supporting the **lang** attribute MUST have a **lang** attribute with a value from "ISO 639-1".

For each metadata element supporting the **lang** attribute, there MUST NOT be more than one instance of each **lang** value for the element in question, except for the Logo MDUI element.

A **lang** attribute value used in one metadata element MUST be represented for all metadata elements supporting the **lang** attribute, except for the RegistrationPolicy element.

Metadata elements supporting the **lang** attribute MUST have a definition in English (en).

Metadata elements supporting the **lang** attribute MUST have a definition in Swedish (sv).

### 3.1.2 entityID

The entityID of a Relying Party is its unique identifier in the federation.

The entityID MUST be globally unique.

The entityID attribute is a URI that MUST start with either **https://**, **http://** or **urn:**. The **urn:** form is a legacy format and SHOULD NOT be used when registering a new entity.

*Guidance: The https:// format is preferred.*

The entityID attribute MUST NOT exceed 256 characters in length.

### 3.1.3 Metadata Extensions for Login and Discovery User Interface (MDUI)

MDUI for a Relying Party is information expected to be presented to end users and used by discovery services and login services to inform users what Relying Party they are authenticating for.

A Relying Party MUST have the following elements with **lang** attributes:

- **DisplayName**
  Name of the Relying Party. MUST be unique within the federation. The English name MUST be unique within the federation and all interacting interfederations.
- **Description**
  Short description of the Relying Party.
- **Logo**
  URL to the organization logotype or the logotype of the Relying Party itself. Multiple Logo elements with different height and/or width MAY be specified for the same language.
  - The value MUST be a URL that starts with https://
  - The logotype MUST NOT be embedded in the metadata
  - The logotype MUST be publicly accessible
  - The domain part of the URL MUST be a domain owned by the organization or which the organization has delegated usage of
  - The logotype SHOULD be in PNG file format
  - The logotype SHOULD be transparent and work on a white or light gray background
  - The logotype SHOULD be square (i.e., aspect ratio of 1:1) or, if not appropriate, SHOULD have landscape orientation (i.e., width > height)
  - The width of the logotype SHOULD be between 64 and 350 pixels
  - The height of the logotype SHOULD be between 64 and 146 pixels

### 3.1.4 SAML certificates

For a Relying Party there MUST be at least one encryption certificate registered in the metadata (i.e., a **KeyDescriptor** element with no **use** attribute or one set to **encryption**).

### 3.1.5 SAML endpoints

SAML endpoints are the receivers of SAML responses and similar SAML messages.

All SAML endpoints of a Relying Party MUST start with https://.

A Relying Party MUST NOT have AssertionConsumerService elements where the attribute Binding value is urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.

### 3.1.6 Requested attributes

A Relaying Party MUST define requested attributes in metadata. A Relaying Party MUST have at least one **AttributeConsumingService** element.

The **AttributeConsumingService** element defines a particular service offered by the Service Provider. Adding requested attributes to the metadata of a Relying Party does not imply that any Identity Provider releases the requested attributes.

**AttributeConsumingService** element(s) of a Relying Party MUST have the following elements:

- **ServiceName**
  The lang attribute MUST be present (see Section 3.1.1).
- **ServiceDescription**
  The lang attribute MUST be present (see Section 3.1.1).
- **RequestedAttribute**
  At least one.

A **RequestedAttribute** element of a Relying Party MUST have the following attributes:

- **Name**
  The value MUST be an attribute name from the attribute profile of the federation.
- **FriendlyName**
  The value MUST match the FriendlyName value from the attribute profile of the federation of the Name attribute value.
- **NameFormat**
  The value MUST be “urn:oasis:names:tc:SAML:2.0:attrname-format:uri”

A **RequestedAttribute** element MAY have one or more **AttributeValue** elements.

### 3.1.7 Organization

The organization elements relate to the official name of the organization that the Relying Party is operated for.

A Relying Party MUST have the following **Organization** elements with **lang** attributes:

- **OrganizationName** The OrganizationName MUST be the same for all Identity Providers and Relying Parties owned by the organization, i.e., the legal name of the organization.
- **OrganizationDisplayName** The well-known name of the organization responsible for the service, e.g., if the organization is more known by its abbreviation than its full name.
- **OrganizationURL** The official web address of the organization.

### 3.1.8 ContactPerson

Contact information for the Relying Party. Due to personal data protection legislation, contact information MUST NOT refer to a natural person.

**ContactPerson** elements MUST have an **EmailAddress** element starting with mailto:.

*Guidance: The e-mail address MUST be a functional mailbox where the address does not refer to a natural person.*

There MUST NOT be more than one **ContactPerson** element of each type.

A Relying Party MUST have one **ContactPerson** element of type **administrative** registered in metadata.

*Guidance: The administrative ContactPerson is the contact point for governance of the Relying Party.*

A Relying Party MUST have one **ContactPerson** element of type **technical** registered in metadata.

*Guidance: The technical ContactPerson is the contact point for technical questions and issues regarding the use of the Relying Party.*

A Relying Party MUST have one **ContactPerson** element of type **support** registered in metadata.

*Guidance: The support ContactPerson is the contact point for end users and non- technical questions and issues regarding the use of the Relying Party.*

### 3.1.9 Non-secure cryptographic algorithms

The metadata of a Relying Party MUST only include **DigestMethod**, **SigningMethod** and **EncryptionMethod** elements containing algorithms defined in the latest published version of W3C Recommendations xmldsig-core and xmlenc-core respectively. Algorithms discouraged in the latest published version of xmldsig-core and xmlenc-core respectively SHOULD NOT be included.

*Guidance: At the time of writing MD5 is obsolete and RSA v1.5 is not recommended in the latest published version.*

### 3.1.10 Unnecessary, large metadata

The metadata for a Relying Party MUST NOT include RoleDescriptor elements.

*Guidance: RoleDescriptor elements are large and are unnecessary in the federation*

## 3.2 SAML Keys and Certificates

The purpose of this subsection is to define the requirements of the SAML keys and certificates of Relying Parties. To minimize interoperability issues certificates should be long-lived and self-signed. Note that the security of the federation is based on the signing of the metadata and not on the certificate verification chain or the lifespan of the entity certificates.

Relying Party credentials (i.e., entity keys) MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than 2048-bit RSA/DSA keys or 256-bit ECC keys. 4096-bit RSA/DSA keys or 384-bit ECC keys are RECOMMENDED.

*Guidance: To minimize the administrative burden, keys should not be replaced unless they are at risk. Keys should be replaced when doing a major software upgrade or a hardware replacement. New keys should not use shorter comparable key strength than 4096-bit RSA/DSA keys or 384-bit ECC keys.*

Signing and encryption certificates MUST NOT be expired.

*Guidance: To minimize the administrative burden, certificates should not be replaced unless they are at risk. Certificates should have a lifespan of 10 years.*

Signing and encryption certificates SHOULD be self-signed.

*Guidance: To be able to use long-lived certificates, certificates should not be signed by well-known certificate authorities. Note that the signature of SAML certificates is not verified by Identity Providers.*

Keys known to be compromised or weak MUST be replaced in a timely manner.

A Relying Party MUST support multiple signing certificates registered in the metadata of an Identity Provider and MUST support validation of signatures using any of them.

*Guidance: This is used during key roll-over of an Identity Provider.*

A Relying Party MUST support multiple encryption certificates registered in the metadata of an Identity Provider and SHOULD support encryption using one of them.

*Guidance: This is used during key roll-over of an Identity Provider.*

## 3.3 Endpoint security

A Relying Party MUST NOT support deprecated SSL/TLS protocols.

*Guidance: At the time of writing, SSLv2 was deprecated by RFC6176 in 2011, SSLv3 was deprecated by RFC7568 in 2015, TLS1.0 and TLS1.1 was deprecated by RFC8996 in March 2021.*

The Service Owner operating a Relying Party MUST consider applicable web protocol threats and apply appropriate controls to all relevant endpoints.

*Guidance: sslabs.com and similar services provide tools to detect known web protocol security issues. It is recommended to be continuously graded level A or higher at sslabs.com.*

## 3.4 Relying Party software requirements

### 3.4.1 Metadata consumption and validation

A Relying Party MUST refresh the metadata at least once every one (1) hour.

To ensure the validity of the federation metadata the refresh process MUST verify the signature on every federation metadata fetch. The federation's signing certificate authenticity must be assured and verified in a secure way.

Federation metadata without a validUntil attribute or with a passed validUntil MUST not be trusted and MUST be discarded.

### 3.4.2 Authentication request

A Relying Party MAY specify one or more requested authentication methods in the **RequestedAuthnContext** attribute in an authentication request.

*Guidance: If an authentication request has the RequestedAuthnContext attribute set, the Identity Provider must authenticate the Subject using one of the methods provided. Note that the list is not ordered. If an Identity Provider cannot authenticate the Subject using any authentication methods requested in a RequestedAuthnContext attribute in an authentication request, it must fail the request and should respond to the Relying Party with a SAML error status. If an authentication request has no RequestedAuthnContext attribute, the Identity Provider may choose any authentication method during authentication.*

If a **RequestedAuthnContext** was included in an authentication request, the Relying Party SHOULD verify that the value of the AuthnContext attribute of the response is one of the specified authentication methods in the authentication request.

A Relying Party MAY request a new authentication by including the attribute **ForceAuthn** with the value "true" or "1" in the authentication request.

*Guidance: If an authentication request has the ForceAuthn attribute set to "true" or "1", the Identity Provider must perform a new authentication of the Subject.*

If a **ForceAuthn** attribute was included in the authentication request with the value "true" or "1", the Relying Party SHOULD verify that the **AuthnInstant** attribute is set to a fresh value in the authentication response.

*Guidance: The value of the AuthnInstant attribute should be newer than the time of the authentication request, including defined clock skew.*

### 3.4.3 Clock skew

A Relying Party MUST allow between three (3) and five (5) minutes of clock skew, in either direction, when verifying the validity of an authentication response.

### 3.4.4 Operational security

A Relying Party and their supporting infrastructure MUST NOT use software that is no longer maintained or software configurations with known security issues.

### 3.4.5 Error handling

The Service Owner operating a Relying Party is RECOMMENDED to implement usage of the "SAML V2.0 Metadata Deployment Profile for errorURL" [2] in order to support users to solve issues regarding login requirements using customized information from their home organization.

## 3.5 Attribute Release

A Relying Party MUST support attribute values up to 256 characters long.

*Guidance: For multivalued attributes the separate values of each attribute may each be up to 256 characters long. The complete value set of a specific attribute may be longer.*

### 3.5.1 Subject identifiers

The purpose of this subsection is to define requirements regarding identifiers of Subjects.

A Relying Party MUST NOT require the presence of a NameID element.

*Guidance: The NameID element should not be used for anything else than single logout purposes. Note that SAML Single Logout terminates the single sign-on session at the Identity Provider, it does not guarantee that the user is logged out from other Relying Parties with active sessions.*

If a Relying Party requires identifiers of Subjects, the Relying Party MUST require one of the identity attributes from the attribute profile of the Federation.

### 3.5.2 Scoped attributes

Scoped attribute values are compared against the asserting Identity Providers' scope value(s) in metadata. Relying Parties MUST discard attributes if the scope component of the attribute value does not exactly match.

Scoped attributes are defined in the attribute profile of the federation.

*Guidance: An Identity Provider may have multiple scopes registered in metadata. Scope validation is important due to identity impersonation risk management.*

### 3.5.3 Assurance

If a Relying Party receives and uses the value(s) in an assurance attribute, the relying party MUST validate that the identity assurance profile is present in the assurance-certification entity attribute of the Identity Provider.

The attribute used to release identity assurance of Subjects is defined in the attribute profile of the federation.

*Guidance: An Identity Provider may release multiple assurance values. Assurance certification validation is important due to identity impersonation risk management.*

# 4 Operational Requirements for Federation Operator

## 4.1 Metadata management

### 4.1.1 Metadata registration practice

Language attributes (lang)

Metadata elements that support the lang attribute MUST have a lang attribute with a value from "ISO 639-1".

Metadata elements that support the lang attribute MUST have a definition with language English (en).

Metadata elements that support the lang attribute MUST have a definition with language Swedish (sv).

### 4.1.2 Metadata registration information

*Guidance: The root of a metadata aggregate is the EntitiesDescriptor element.*

The root element of individual metadata entity publications is the EntityDescriptor element.

The Federation Operator MUST publish a SAML Metadata Registration Practice Statement in English.

Every **EntityDescriptor** published in federation metadata MUST include a **RegistrationInfo** element in its **Extensions** element of its root element with the attributes **registrationAuthority** and **registrationInstant**. The **RegistrationInfo** element MUST include references to published SAML Metadata Registration Practice Statements in **RegistrationPolicy** elements.

### 4.2 SAML Federation Metadata signing

Metadata MUST NOT be signed unless approved by Federation Operator.

Signed metadata or signed aggregates of metadata MUST have a validUntil attribute in its root element.

*Guidance: The root element of metadata aggregates is the EntitiesDescriptor element.*

The root element of individual metadata entity publications is the EntityDescriptor element.

Signing keys MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 4096-bit RSA/DSA key or a 384 - bit ECC key.

The signature’s digest algorithm MUST be at least as strong as SHA- 256 and MUST NOT use MD5 or SHA-1.

The signature’s signature method MUST be RSA with an associated digest at least as strong as SHA-256 and MUST NOT use MD5 or SHA-1.

Signing certificates MUST be self-signed.

Signing certificates MUST NOT be expired.

Signing keys MUST be protected from unauthorized usage.

Signing keys known to be compromised or weak MUST be replaced in a timely manner.

The Federation Operator MUST have documented procedures for key rollover of signing keys.

### 4.3 Metadata publishing

Metadata MUST NOT be published unless signed.

## 5 Acknowledgements

A greater part of the content in this document has been retrieved from SWAMID SAML WebSSO Technology Profile (c) by Sunet licensed under CC BY-SA 3.0

## 6 References

[1] S. Bradner, Key words for use in RFCs to indicate requirement levels, RFC Editor; Internet Requests for Comments; RFC Editor, 1997. http://www.rfc-editor.org/rfc/rfc2119.txt.

[2] REFEDS, SAML V2.0 metadata deployment profile for errorURL version 1.0, REFEDS, 2020. https://refeds.org/specifications/errorurl-v1.

[3] I. Young, SAML 2.0 metadata extensions for shibboleth, Shibboleth, n.d. https://shibboleth.atlassian.net/wiki/spaces/SC/pages/1843887946/ShibMetaExt+V1.0.