Document SWAMID SAML WebSSO Technology Profile
Identifier http://www.swamid.se/policy/technology/saml-websso
Version V2.0
Last modified 2021-12-10
Pages 24
Status FINAL

SWAMID SAML WebSSO Technology Profile

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.

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

All normative parts of the profile are governed by the SWAMID Board of Trustees.

The non-normative (guidance) is maintained by the SWAMID Operations team.

1.1. Definition of terminology

Member Organisation: The SWAMID Member with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

Service Owner: An organisation that is responsible and liable for operating a service registered in SWAMID. The Service Owner may delegate the technical operation of the Relying Party to another organisation.

Subject: Any natural person affiliated with a Member Organisation, e.g. as a teacher, researcher, staff or student.

Identity Provider (IdP): The system component that issues Attribute assertions on behalf of Subjects who use them to access the services of the Relying Party.

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

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

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 Organisation's Identity Provider. This can be for example the combination of a username and password or a username and cryptographic device.

2. Purpose, Scope and Summary

This document defines the SWAMID Identity Federation Policy Technology Profile which specifies how the SWAMID Identity Federation is realised using SAML WebSSO.

SWAMID implements SAML2 WebSSO as a multilateral and full-mesh identity federation. All Relying Parties and Identity Providers should support automatic import and update of metadata files with multiple entities.

SWAMID has multiple interfederation agreements. SWAMID provides signed metadata repositories containing both entities from SWAMID and entities from other federations where SWAMID entities take precedence.

The SAML WebSSO Technology Profile is based on the Kantara Initiative “SAML V2.0 Deployment Profile for Federation Interoperability” and the “eduGAIN SAML Profile” but does not contain all elements from those profiles.

3. Compliance and Audit

The purpose of this section is to define how to ensure compliance with this technology profile.

3.1 Member Organisations and Service Owners MUST ensure compliance with this Technology Profile via an internal self-audit.

3.2 For Identity Providers, Member Organisations MUST annually confirm that the Identity Provider is operational and fulfils this Technology Profile.

3.3 For Relying Parties, Service Owners MUST annually confirm that the Relying Party is operational and fulfils this Technology Profile.

3.4 SWAMID Board of Trustees MAY impose an additional audit of the Member Organisation or Service Owner performed by SWAMID Operations, or another party approved by SWAMID Board of Trustees.

4. Organisational Requirements

The purpose of this section is to define conditions and guidance regarding participating organisations and their registered entities.

4.1 Identity Providers

Registration criteria

4.1.1 For an organisation to be eligible to register an Identity Provider in SWAMID metadata the organisation MUST be a member of the SWAMID Identity Federation.

4.1.2 All Member Organisations MUST fulfil one or more of the SWAMID Identity Assurance Profiles to be eligible to have an Identity Provider registered in SWAMID metadata.

Deregistration

4.1.3 An Identity Provider no longer fulfilling the registration criteria in 4.1.1 and 4.1.2, MUST be deregistered from SWAMID.

Incident Management

4.1.4 All Member Organisations MUST follow the SWAMID Incident Management Procedure in case of a suspected security incident if

- the Identity Provider is at risk; or
- at least one user with federated logins is at risk or involved.

4.2 Relying Parties (Service Providers)

Registration criteria

4.2.1 A Relying Party is eligible for registration in SWAMID if they are:

- a service owned by a Member Organisation;
- a service under contract with at least one Member Organisation;
- a government agency service used by at least one Member Organisation;
- a service that is operated at least in part for the purpose of supporting research and scholarship interaction, collaboration or management; or
- a service granted special approval by SWAMID Board of Trustees after recommendation by SWAMID Operations.

4.2.2 For a Relying Party to be registered in SWAMID the Service Owner MUST accept the SWAMID Metadata Terms of Access and Use.

Deregistration

4.2.3 If a Relying Party no longer fulfils the registration criteria in 4.2.1 and 4.2.2, it MUST be deregistered from SWAMID.

Incident Management

4.2.4 All Service Owners MUST follow the SWAMID Incident Management Procedure in case of a suspected federated security incident if

- the Relying Party is at risk; or
- at least one user with federated login is at risk or involved.

4.3 Federation Operator

Registration criteria of an Identity Provider

4.3.1 The Federation Operator MUST NOT register an Identity Provider not fulfilling the registration criteria in 4.1.1 and 4.1.2.

4.3.2 The Federation Operator MUST ensure that metadata of an Identity Provider fulfils this Technology Profile before registering the metadata.

4.3.3 The Federation Operator MUST ensure that the domain used in 5.1.6 is registered by the organisation of the Identity Provider or which the organisation has delegated usage of.

4.3.4 The Federation Operator MUST ensure that domains used in 5.1.15 are registered by the organisation of the Identity Provider or which the organisation has delegated usage of.

4.3.5 The Federation Operator MUST ensure that requirements of entity attributes in 5.1.9 – 5.1.12 are fulfilled before registering entity attributes of an Identity Provider.

Deregistration of an Identity Provider

4.3.6 The Federation Operator MUST deregister an Identity Provider no longer fulfilling the registration criteria in 4.1.1 and 4.1.2.

4.3.7 The Federation Operator MUST deregister an Identity Provider that has not fulfilled the audit criteria in 3.2.

4.3.8 The Federation Operator MUST deregister an Identity Provider no longer fulfilling this Technology Profile.

4.3.9 The Federation Operator MUST remove parts of metadata of an Identity Provider no longer fulfilling 4.3.4 and 4.3.5.

Registration criteria of a Relying Party

4.3.10 The Federation Operator MUST NOT register a Relying Party not fulfilling the registration criteria in 4.2.1 and 4.2.2.

4.3.11 The Federation Operator MUST ensure that metadata of a Relying Party fulfils this Technology Profile before registering the metadata.

4.3.12 The Federation Operator MUST ensure that the domain used in 6.1.6 is registered by the organisation of the Relying Party or which the organisation has delegated usage of.

4.3.13 The Federation Operator MUST ensure that requirements of entity attributes in 6.1.9 and 6.1.10 are fulfilled before registering entity attributes of a Relying Party.

Deregistration of a Relying Party

4.3.14 The Federation Operator MUST deregister a Relying Party no longer fulfilling the registration criteria in 4.2.1 and 4.2.2.

4.3.15 The Federation Operator MUST deregister a Relying Party that has not fulfilled the audit criteria in 3.3.

4.3.16 The Federation Operator MUST deregister metadata of a Relying Party no longer fulfilling this Technology Profile.

4.3.17 The Federation Operator MUST remove parts of metadata of a Relying Party no longer fulfilling 4.3.13.

Incident Management

4.3.18 The Federation Operator MUST follow the SWAMID Incident Management Procedure in case of a suspected security incident.

5. Operational Requirements for Identity Providers

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

5.1 Metadata registration

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

Language attributes (lang)

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

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

5.1.2 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.

5.1.3 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.

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

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

entityID

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

5.1.6 The entityID MUST be globally unique and based on a domain name registered by the organisation or which the organisation has delegated usage of.

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

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

5.1.8 The entityID attribute MUST NOT exceed 256 characters in length.

Entity Attributes

5.1.9 SWAMID Identity Assurance Profile compliance MUST be registered in the **assurance-certification** entity attribute as defined by each SWAMID Identity Assurance Profile.

5.1.10 Compliance of assurance profiles not governed by SWAMID SHOULD be registered in the **assurance-certification** entity attribute as defined by each assurance profile.

5.1.11 Support for Entity Categories SHOULD be registered in the **entity-category-support** entity attribute as defined by each Entity Category.

5.1.12 Entity Categories applicable to the Identity Provider SHOULD be registered in the **entity-category** entity attribute as defined by each Entity Category.

errorURL

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

5.1.13 An Identity Provider MUST have a registered errorURL.

5.1.14 An Identity Provider SHOULD implement the “SAML V2.0 Metadata Deployment Profile for errorURL”.

Scope

Scopes are used to provide authoritative information to Scoped Attributes.

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

5.1.16 Scopes MUST NOT include regular expressions.

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.

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

- **DisplayName**
  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.
- **InformationURL**
  URL to the Service Definition of the Identity Provider.
- **PrivacyStatementURL**
  URL to the privacy statement of the Identity Provider.

- **Logo**
  URL to the organisation 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 organisation or which the organisation has delegated usage of
    - The logotype SHOULD be in PNG file format
    - The logotype SHOULD be transparent and work on white or light grey 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

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

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

5.1.19 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**
  Domain of DNS-names of IP-addresses of expected users of 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.

SAML certificates

5.1.20 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**).

SAML endpoints

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

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

Organization

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

5.1.22 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 organisation, i.e. the legal name of the organisation.
- **OrganizationDisplayName**
  The well-known name of the organisation, e.g. if the organisation is more known by their abbreviation instead of its full name.
- **OrganizationURL**
  The official web address of the organisation.

ContactPerson

Contact information for the Identity Provider. Due to current personal data protection legislation all contact person information should be non-personal.

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

Guidance: *The e-mail address should be a non-person functional address.*

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

5.1.25 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.*

5.1.26 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.*

5.1.27 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.*

5.1.28 An Identity Provider SHOULD have one **ContactPerson** element of contactType **other** with remd:contactType **http://refeds.org/metadata/contactType/security** registered in metadata. If the element is present, a **GivenName** element MUST be present and the person(s) behind the **EmailAddress** MUST respect the Traffic Light Protocol (TLP) during all incident response correspondence.

Guidance: *The security ContactPerson is the contact point for all suspected security incidents and issues regarding the use of the Identity Provider. If the organisation security contact is not able to use the Traffic Light Protocol (https://www.first.org/tlp/) the organisation must omit the security contact from the metadata of the Identity Provider.*

Non-secure cryptographic algorithms

5.1.29 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.*

Unnecessary, large metadata

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

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

5.1.31 The Identity Provider **IDPSSODescriptor** element in metadata MUST NOT include any **Attribute** elements.

Guidance: *Attribute elements of the IDPSSODescriptors element are large and are unnecessary in the federation.*

5.2 SAML Keys and Certificates

The purpose of this subsection is to define 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.

5.2.1 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.

5.2.2 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.*

5.2.3 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.*

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

5.2.5 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.*

5.2.6 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.*

5.3 Endpoint security

5.3.1 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.*

5.3.2 All Member Organisations operating an Identity Provider MUST take into account 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.*

5.4 Identity Provider software requirements

Metadata consumption and validation

5.4.1 An Identity Provider MUST refresh the metadata from SWAMID at least every 24 hours or use the SWAMID Metadata Query service to load metadata on-demand.

Guidance: *SWAMID recommends all Identity Providers to refresh the metadata from SWAMID every 4 hours if not using the SWAMID Metadata Query service.*

5.4.2 An Identity Provider MUST validate the signature of the metadata from SWAMID using the signing certificate of SWAMID.

Guidance: *If the metadata is compromised, the bundled certificate in the metadata may also be compromised. Make sure to use the certificate of SWAMID during validation.*

5.4.3 An Identity Provider MUST NOT accept SWAMID metadata without a **validUntil** attribute in its root element or SWAMID metadata with passed **validUntil**.

Authentication request

5.4.4 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.*

5.4.5 If a multi-factor authentication is requested and performed it MUST use one of the methods described in 5.1.1 in the SWAMID Identity Assurance Profiles.

5.4.6 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.*

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

5.4.8 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.

5.4.9 If an authentication request contains 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.*

Clock skew

5.4.10 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.

Operational Security

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

5.5 Attribute Release

5.5.1 Each value of released attributes MUST NOT exceed 256 characters.

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

Subject identifiers

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

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

Guidance: *The NameID element is primary used for Single Logout purposes.*

5.5.3 An Identity Provider MUST support release of the attribute **eduPersonPrincipalName**. The value of the attribute for a Subject MUST NOT be reassigned to another Subject.

Guidance: *The e-mail address of a Subject is not suitable as value for the attribute eduPersonPrincipalName due to name changes and later reassignments to other Subjects.*

5.5.4 An Identity Provider MUST support the release of the attribute **subject-id**. The value of the attribute for a Subject MUST NOT be reassigned to another Subject.

Guidance: *The subject-id is a globally unique identifier identical for all Relying Parties for a given Subject. SWAMID recommends that the value of eduPersonPrincipalName is used for subject-id since it is already defined for all Subjects, widely used as identifier in Relying Parties in SWAMID, unique and non-reassigned for all Identity Providers in SWAMID. The subject-id should not be changed as a result of a change to any other data associated with the Subject (e.g., name, email address, organisational role).*

5.5.5 An Identity Provider MUST support the release of the attribute **pairwise-id**. The value of the attribute for a Subject and a Relying Party MUST be unique and MUST NOT be reassigned to another Subject for the Relying Party.

Guidance: *The pairwise-id is a unique persistent identifier based on the combination of a Subject and a specific Relying Party. For a given Subject, the pairwise-id is not*

the same for different Relying Parties. The value may be computed using a unique identifier of the Subject and a unique identifier of the Relying Party, in combination with a secret for privacy reasons.

Support for Entity Categories

Entity Categories are used for data release minimisation and scalable attribute release from an Identity Provider within SWAMID to a Relying Party in SWAMID and/or interfederations.

Entity Categories are tools for Identity Providers to make informed decisions of automatic or manual attribute release configuration to Relying Parties. Identity Providers are strongly recommended to implement automatic attribute release via Entity Categories.

If Entity Categories support is not implemented, bi-lateral agreements between each Identity Provider and each Relying Party are required for users to access services.

5.5.6 An Identity Provider SHOULD support and release attributes according to "SWAMID Best Current Practices for Entity Categories for Service Providers".

Guidance: *SWAMID Best Current Practices for Entity Categories for Service Providers are available at the SWAMID Wiki.*

5.5.7 An Identity Provider that releases attributes based on an Entity Category SHOULD register support for the Entity Category in its metadata as defined by the Entity Category.

Guidance: *If Entity Category Support is not correctly registered in the metadata of an Identity Provider, their users may not be able to access services due to filtering at Relying Parties.*

Scoped attributes

Attributes with scope must match the scope in the metadata of the Identity Provider, otherwise they normally get filtered out by Relying Parties. Scoped attributes include subject-id, pairwise-id, eduPersonPrincipalName and eduPersonScopedAffiliation.

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

Attribute freshness

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

5.5.10 Changes on information regarding a Subject or the organisation MUST be reflected in released attributes within one work week.

Assurance

5.5.11 An Identity Provider SHOULD support release of Identity Assurance of Subjects as defined in Section 6 of the SWAMID Identity Assurance Level Profiles, using the Identifiers of the respective Identity Assurance Profiles.

Guidance: *The Identifiers of SWAMID AL1, SWAMID AL2 and SWAMID AL3 are http://www.swamid.se/policy/assurance/al1, http://www.swamid.se/policy/assurance/al2 and http://www.swamid.se/policy/assurance/al3 respectively.*

5.5.12 An Identity Provider SHOULD support the REFEDS Assurance Framework (RAF) according to "SWAMID Best Practices".

5.5.13 To release Identity Assurance of Subjects, the multi-valued **eduPersonAssurance** attribute MUST be used.

Guidance: *eduPersonAssurance is defined by eduPerson Object Class Specification (2020-01), https://wiki.refeds.org/display/STAN/eduPerson+2020-01.*

6. Operational Requirements for Relying Parties

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

6.1 Metadata registration

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

Language attributes (lang)

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

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

6.1.2 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.

6.1.3 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.

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

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

entityID

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

6.1.6 The entityID MUST be globally unique and based on a domain name registered by the organisation or which the organisation has delegated usage of.

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

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

6.1.8 The entityID attribute MUST NOT exceed 256 characters in length.

Entity Attributes

6.1.9 Compliance of assurance profiles SHOULD be registered in the **assurance-certification** entity attribute as defined by the respective profile.

6.1.10 Entity Categories applicable to the Relying Party SHOULD be registered in the **entity-category** entity attribute as defined by each Entity Category.

6.1.11 If applicable, the Subject Identifier Attribute required by the Relying Party MAY be register in the **subject-id:req** entity attribute as defined by the “SAML V2.0 Subject Identifier Attributes Profile Version 1.0”.

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.

6.1.12 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 interfederation.
- **Description**
  Short description of the Relying Party.
- **InformationURL**
  URL to information about the Relying Party.
- **PrivacyStatementURL**
  URL to the privacy statement of the Relying Party.

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

- **Logo**
  URL to the organisation 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 organisation or which the organisation has delegated usage of
- The logotype SHOULD be in PNG file format
- The logotype SHOULD be transparent and work on white or light grey 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

SAML certificates

6.1.14 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**).

SAML endpoints

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

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

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

Requested Attributes

Adding requested attributes to the metadata of a Relying Party does not imply that any Identity Provider releases the requested attributes. Referrer to SWAMID Best Current Practices for Entity Categories for Service Providers for recommendations regarding attribute release.

6.1.17 The **AttributeConsumingService** element(s) of a Relying Party, if present, MUST have a **ServiceName** with **lang** attributes.

Guidance: *The ServiceName is recommended to be identical to or contain the value of MDUI DisplayName of the Relying Party.*

6.1.18 Any **AttributeConsumingService** present MAY have a **ServiceDescription** with **lang** attributes.

6.1.19 Any **AttributeConsumingService** present MUST have at least one **RequestedAttribute** element.

6.1.20 If a **RequestedAttribute** element has a **FriendlyName** attribute, its value SHOULD match the FriendlyName value from the schema definition of the **Name** attribute value.

Guidance: *SWAMID Best Current Practices for Entity Categories lists common Name attribute values and their respective FriendlyName based on their respective schema definitions.*

Organization

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

6.1.21 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 organisation, i.e. the legal name of the organisation.
- **OrganizationDisplayName**
  The well-known name of the organisation responsible of the service, e.g. if the organisation is more known by their abbreviation instead of its full name.
- **OrganizationURL**
  The official web address of the organisation.

ContactPerson

Contact information for operation of the Relying Party. Due to current personal data protection legislation all contact person information should be non-personal.

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

Guidance: *The e-mail address should be a non-person functional address.*

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

6.1.24 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.*

6.1.25 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.*

6.1.26 A Relying Party SHOULD 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.*

6.1.27 A Relying Party SHOULD have one **ContactPerson** element of contactType **other** with remd:contactType **http://refeds.org/metadata/contactType/security** registered in metadata. If the element is present, a **GivenName** element MUST be present and the person(s) behind the **EmailAddress** MUST respect the Traffic Light Protocol (TLP) during all incident response correspondence.

Guidance: *The security ContactPerson is the contact point for all suspected security incidents and issues regarding the use of the Relying Party. If the organisation security contact is not able to use the Traffic Light Protocol (https://www.first.org/tlp/) the organisation must omit the security contact from the metadata of the Relying Party.*

Non-secure cryptographic algorithms

6.1.28 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.*

Unnecessary, large metadata

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

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

6.2 SAML Keys and Certificates

The purpose of this subsection is to define 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.

6.2.1 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.*

6.2.2 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.*

6.2.3 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.*

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

6.2.5 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.*

6.2.6 A Relying Party SHOULD 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.*

6.3 Endpoint security

6.3.1 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.*

6.3.2 The Service Owner operating a Relying Party MUST take into account 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.*

6.4 Relying Party software requirements

Metadata consumption and validation

6.4.1 A Relying Party MUST refresh the metadata from SWAMID at least every 24 hours or use the SWAMID Metadata Query service to load metadata on-demand.

Guidance: *SWAMID recommends all Relying Parties to refresh the metadata from SWAMID every 4 hours if not using the SWAMID Metadata Query service.*

6.4.2 A Relying Party MUST validate the signature of the metadata from SWAMID using the signing certificate of SWAMID.

Guidance: *If the metadata is compromised, the bundled certificate in the metadata may also be compromised. Make sure to use the certificate of SWAMID during validation.*

6.4.3 A Relying Party MUST NOT accept SWAMID metadata without a **validUntil** attribute in its root element or SWAMID metadata with passed **validUntil**.

Authentication request

6.4.4 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.*

6.4.5 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.

6.4.6 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.*

6.4.7 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.*

Clock skew

6.4.8 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.

Operational Security

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

Error handling

6.4.10 The Service Owner operating a Relying Party is RECOMMENDED to implement usage of the “SAML V2.0 Metadata Deployment Profile for errorURL” in order to support users to solve issues regarding login requirements using customised information from their home organisation.

6.5 Attribute Release

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

Guidance: *For multivalued attributes, such as eduPersonAffiliation, eduPersonEntitlement and eduPersonAssurance, 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.*

Subject identifiers

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

6.5.2 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.*

6.5.3 If a Relying Party requires identifiers of Subjects, the Relying Party SHOULD use one of **subject-id, pairwise-id** or **eduPersonPrincipalName** as the identifying attribute.

Guidance: *Referrer to SWAMID Best Current Practices for Entity Categories for Service Providers for recommendations regarding subject identifiers.*

Entity Categories

Entity Categories are used for data release minimisation and scalable attribute release from an Identity Provider within SWAMID to a Relying Party in SWAMID and/or interfederations.

Entity Categories are tools for Identity Providers to make informed decisions of configuration of automatic or manual attribute release to Relying Parties. Note that Identity Providers are not required to implement Entity Categories.

If a Relying Party does not implement Entity Categories, bi-lateral agreements between the Relying Party and Identity Providers are required for the Relying Party to receive any attributes from Identity Providers.

6.5.4 A Relying Party SHOULD implement Entity Categories based on attribute requirements and policies.

Guidance: *SWAMID Best Current Practices for Entity Categories for Service Providers are available at the SWAMID Wiki.*

Scoped attributes

Attributes with scope must match the scope in the metadata of the Identity Provider, otherwise they should be filtered out by Relying Parties. Scoped attributes include subject-id, pairwise-id, eduPersonPrincipalName and eduPersonScopedAffiliation.

6.5.5 A Relying Party MUST NOT trust scoped attributes not matching scopes registered in the metadata of the Identity Provider.

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

Assurance

6.5.6 If the value for one or more SWAMID Identity Assurance Profiles is received in the **eduPersonAssurance** attribute and used by a Relying Party, the Relying Party MUST validate that the SWAMID Identity Assurance Profile exists in the **assurance-certification** entity attribute of the Identity Provider.

Guidance: *An Identity Provider may release multiple assurance values. Assurance certification validation is important due to identity impersonation risk management. All SWAMID identity assurance profiles start with http://www.swamid.se/policy/assurance/.*

7. Operational Requirements for Federation Operator

7.1 Metadata management

Metadata registration practice

7.1.1 Access to administration of metadata to be published MUST be limited to SWAMID Operations, or another party approved by SWAMID Board of Trustees.

Language attributes (lang)

7.1.2 Metadata elements that support the **lang** attribute MUST have a **lang** attribute with a value from “ISO 639-1”.

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

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

Metadata registration information

7.1.5 The Federation Operator MUST publish a Metadata Terms of Use in English and Swedish.

7.1.6 Each metadata publication MUST include a **PublicationInfo** element in its **Extensions** element of its root element with the attributes **creationInstant** and **publisher**. The **PublicationInfo** element MUST include references to the published Metadata Terms of Use in **UsagePolicy** elements.

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

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

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

7.1.8 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.

7.2 SAML Federation Metadata signing

7.2.1 Metadata MUST NOT be signed unless approved by SWAMID Operations.

7.2.2 Signed metadata or signed aggregates of metadata MUST have a **validUntil** attribute in its root element set to 15 days after the signing instant.

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

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

7.2.3 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.

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

7.2.5 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.

7.2.6 Signing certificates MUST be self-signed with a lifespan of at least 10 years.

7.2.7 Signing certificates MUST NOT be expired.

7.2.8 Signing keys MUST be protected from unauthorized usage.

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

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

7.3 Metadata publishing

7.3.1 Metadata MUST NOT be published unless signed.

7.3.2 Metadata MUST be published as metadata aggregates and through the Metadata Query Protocol.

7.3.3 Metadata MUST be published in a way that mitigates single point of failure.