Document	SWAMID Metadata Registration Practice Statement
Identifier	http://www.swamid.se/policy/mdrps
Version	3.0
Last modified	2021-12-10
Pages	5
Status	Final

SWAMID Metadata Registration Practice Statement

Federation Name: Swedish Academic Identity Federation – SWAMID
Federation Operator: Sunet, Sweden
Federation Web Page: http://www.swamid.se

Acknowledgements
This document is based on the REFEDS Metadata Registration Practice Statement template.

Table of Contents

1. Definitions and Terminology

The following definitions are used in this document:

Definition	Description
Federation	An association of organisations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions. Also known as Identity Federation.
Federation Member	An organisation that has joined the Federation by agreeing to be bound by the Federation Policy by the membership process.
Federation Operator	Organisation providing the infrastructure for Authentication and Authorisation to Federation Members.
Federation Participant	An organisation that has published one or more entities in the Federation Metadata Registry.
Federation Policy	A set of documents describing the obligations, rights and expectations of the Federation Participants and the Federation Operator.
Entity	A discrete component that a Federation Participant wishes to register and describe in the Metadata Registry. This is typically an Identity Provider or a Relying Provider.
Identity Provider	The system component that issues attribute assertions on behalf of Subjects who use them to access the services of the Relying Party. The Identity Provider is owned by a Federation Member
Metadata Registry	System used by the Federation Operator to register Entity metadata. This may be via a self-service tool or via other manual processes.
Relying Party	A Service that relies upon a Subject's credentials, typically to process a transaction or grant access to information or a system. The Relying Party is owned by a Federation Participant. Also known as Service Provider.

2. Introduction and Applicability

The SWAMID Identity Federation is governed by the SWAMID Policy Framework. The policy framework contains the SWAMID Policy, the SWAMID Identity Assurance Profiles and the SWAMID Technology Profiles. The full policy framework is published on the Federation website at https://www.swamid.se/policy.

This document describes the metadata registration practices of the Federation Operator with effect from the last modified date on top of the first page. All new Entity registrations and updates performed on or after this date has been processed as described in this document until this document is superseded.

This document is published on the Federation website at https://www.swamid.se/policy/mdrps.

All entities registered in the Metadata Registry are required to fulfil the current version of the SWAMID SAML WebSSO Technology Profile. When the Technology Profile is updated, all Federation Participants have a one-year transitional period from the earlier version. Entities that do not fulfil the updated Technology Profile after the transitional period are deregistered from the Federation Metadata Registry.

Identity Providers in the Federation are exported to eduGAIN unless otherwise requested by the Identity Provider (opt-out). Relying Parties in the federation are not exported to eduGAIN unless requested by the Relying Party (opt-in).

3. Member Eligibility

The SWAMID Federation Policy defines that all Federation Identity Provider Federation Participants are required to be a Federation Member of the Federation. To be able to be a member of the Identity Federation the participant must be connected to Sunet, the Swedish National Research and Education Network. SWAMID Board of Trustees accepts a new member after a formal application via the SWAMID Federation Membership Agreement. The participant is required to fulfil one or more of the SWAMID Identity Assurance Profiles.

The SWAMID Federation Policy defines that a Relying Federation Party Participant is not required to be a Federation Member. However, Relying Parties registered in the Federation Metadata Registry are required to fulfil the registration criteria in the SWAMID SAML WebSSO Technology Profile.

4. Metadata Format

Metadata for all entities registered by the Federation Operator uses the “SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0” metadata extension to indicate that the Federation Operator is the registrar for the Entity and to detail the MRPS statement that applies to the entity. The following is a non-normative example:

```
<mdrpi:RegistrationInfo
         registrationAuthority="http://www.swamid.se/"
         registrationInstant="2021-12-10T13:39:41Z">
  <mdrpi:RegistrationPolicy xml:lang="en">http://swamid.se/policy/mdrps
         </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Entity Eligibility and Validation

5.1. Entity Eligibility

The SWAMID SAML WebSSO Technology Profile published at http://www.swamid.se/policy/technology/saml-websso defines who is eligible to register an Entity in the Federation Metadata Registry:

All Federation Members can register an Identity Provider in the Federation if the Identity Provider has been accepted for at least one SWAMID Identity Assurance Profile.

The primary Relying Parties registration criteria is that the Entity must be:

- 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.

The secondary Relying Party registration criteria is that the Entity operator is required to accept the SWAMID Metadata Terms of Access and Use. The metadata terms of access and use is published at http://mds.swamid.se/md/swamid-tou-en.txt.

5.2. Entity Registration

The process by which a Federation member or a service owner can register an Entity is described at https://www.swamid.se/policy/getting-started.

In the registration process the Federation Operator validates the organisation behind the Entity registration and that the organisation owns or has been delegated the right to use the domain names related to the Entity attributes.

5.3. EntityID Format

The entityID is required to start with either urn:, https:// or http://. The urn: form is a legacy format and is not recommended to be used when registering a new Entity.

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

5.4. Entity Validation

On Entity registration and updates, the Federation Operator carries out Entity validations checks based on the SWAMID SAML WebSSO Technology Profile. These checks include that:

- required information is present in the metadata;
- metadata is correctly formatted;
- protocol endpoints are properly protected with TLS certificates; and
- protocol endpoints are properly protected with non-deprecated TLS versions.

6. Entity Management

Once an Entity has been registered in the Federation it can be modified or removed by the Federation Participant owning the entity.

6.1. Entity Change Requests

Any request for change or removal of a registered Entity from a Federation Participant needs to be communicated from or confirmed by their respective representatives.

The request for Entity metadata changes is initiated via the Federation Operator metadata Entity administration tool and then sent to the Federation Operator for validation and publication.

6.2. Unsolicited Entity Changes

The Federation Operator may amend or modify the Federation Metadata Registry at any time to:

- ensure the security and integrity of the metadata;
- comply with inter-Federation agreements; or
- improve interoperability.

Changes to the metadata of an Entity will be communicated to the representatives of the Federation Participant owning the Entity.

The Federation Operator is required to permanently or temporary remove the metadata of an Entity from the Metadata Registry if the Entity does not fulfil the SWAMID SAML WebSSO Technology Profile. Security incidents may lead to temporary removal of the metadata of an Entity from the Metadata Registry, as defined by the SWAMID Incident Management Procedures published at http://www.swamid.se/incident.