SWAMID

Document	SWAMID Federation Policy
Identifier	http://www.swamid.se/policy
Version	V3.0
Last modified	2020-06-15
Pages	6
Status	FINAL
License	Creative Commons BY-SA 3.0

SWAMID Federation Policy

1. Terminology

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.

1.1. Definition of terminology

Subject: Any natural person affiliated with a SWAMID Member, 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 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 a Service Provider (SP).

2. Introduction

The *Swedish Academic Identity Federation* (SWAMID) facilitates and simplifies shared services across the Identity Federation. This is accomplished by using Federation Technologies to extend the scope of a Digital Identity issued by one Member of the Federation to be trusted across the whole Federation.

This Policy defines the Federation by defining the procedures and practices which allows participating organisations to use available Federation Technologies for digital identification. This Policy does not directly describe practices or procedures specific to any particular choice of Federation Technology.

Identity Management are the processes by which *Identity Providers* issue and manage digital identities throughout their lifecycles and by which they also make *Claims of identity*. A Claim of identity is a digital representation, using a specific identity management technology, of a set of attributes identifying a Subject.

The SWAMID Policy has three main parts:

- this document which describes governance, membership and scope;
- a set of Identity Assurance Profiles; and
- a set of Federation Technology Profiles.

The Identity Assurance Profiles and the Federation Technology Profiles are based on current and evolving standards and are described in separate documents.

An Identity Assurance Profile describes levels of trust in claims and organisations. An Identity Assurance Profile allows a *Relying Party* to determine the degree of certainty of the identity of a Subject and its personal data. Identity assurance is to a large extent independent of the technology used to convey Claims of identity.

The Federation Technology Profiles describe concrete realisations of the Policy and Assurance Profiles in terms of specific technologies (e.g. SAML2, OpenID Connect or eduroam).

3. Purpose and Scope

The purpose of SWAMID is to make it possible for Relying Parties to provide services to Subjects in the Federation. This is accomplished by making infrastructure for federated identification and authentication available to the higher education and research community in Sweden, including but not limited to universities, university colleges, research hospitals, government agencies and private sector organisations involved in higher education and research.

The scope of the SWAMID Policy is limited to those technologies which are capable of supporting federated secure authentication and authorisation of Subjects as described by the Federation Technology Profiles. The set of procedures and practices described in this document applies equally to all Federation Technology Profiles of SWAMID.

In order to facilitate collaboration across national and organisational borders SWAMID SHOULD actively participate in interfederation agreements (e.g. eduGAIN or cross sector interfederations).

4. Governance and Roles

4.1. SWAMID Board of Trustees

SWAMID is operated by the Swedish University Network (SUNET). The governance of SWAMID is delegated from SUNET to the SWAMID Board of Trustees. The SWAMID Board of Trustees is appointed by SUNET. A majority of the members of the SWAMID Board of Trustees SHALL be affiliated with SWAMID Members. SUNET appoints the chair of the SWAMID Board of Trustees. Each member of the SWAMID Board of Trustees is appointed for a period of up to 2 years. Information about the board members is published on the SWAMID web site (https://www.swamid.se).

Any changes to the SWAMID Policy MUST be approved by the SWAMID Board of Trustees, published on the SWAMID web site and communicated to the SWAMID Members.

All decisions made by the SWAMID Board of Trustees are public due to Swedish legislation.

SUNET is responsible for maintaining formal ties with relevant national and international organisations.

4.2. SWAMID Operations Team

The SWAMID Operations Team is appointed by SUNET. A majority of the members of the SWAMID Operations Team SHALL be affiliated with SWAMID Members. The chair of the SWAMID Operations Team is the SWAMID federation operation manager and is appointed by SUNET.

Information about the team members and other contact information is published on the SWAMID web site.

The SWAMID Operations Team is responsible for:

- the daily operations of the SWAMID federation;
- the development of the SWAMID federation including the SWAMID Policy Framework and operational tools; and
- maintaining and publishing a list of SWAMID Members including approved Identity Assurance Profiles and implemented Federation Technology Profiles of each Member.

The SWAMID Operations Team acts as a third line support for support requests from the second line support of SWAMID Members. Members MUST NOT redirect Subjects to the SWAMID Operations Team.

4.3. SWAMID Member

In order to be an Identity Provider in SWAMID an organisation MUST be a Member of SWAMID. Federation Technology Profiles MAY impose additional requirements on SWAMID Members.

A Relying Party is not required to become a Member of SWAMID in order to consume identity information from SWAMID Identity Providers. Federation Technology Profiles MAY impose additional requirements on Relying Parties.

All organisations connected to SUNET are allowed to become a SWAMID Member. An organisation not connected to SUNET MAY under special circumstances become a SWAMID Member by decision of SUNET. An organisation becomes a Member of SWAMID by applying for membership according to the process of Membership Application described in this document.

Members operating Identity Providers will in most cases have Subjects associated with them: these are individuals with an employment, student, business or other form of association with the Member. Each Member is responsible for its own Subjects. In particular each Member is responsible for fulfilling the requirements of the Swedish personal data protection legislation with respect to its own Subjects.

Members are responsible for first line (e.g. call centre or equivalent) and second line (technical support and problem classification) support for its Subjects. Membership in SWAMID does not mandate any specific service level for this support.

All SWAMID Members and their Subjects MUST fulfil one or more of the SWAMID Identity Assurance Profiles.

5. Identity Management Practice Statement

Each SWAMID Member with an Identity Provider MUST create and maintain an Identity Management Practice Statement.

The Identity Management Practice Statement is a description of the Identity Management lifecycle including how Subjects are enrolled, maintained and removed from the identity management system based on the Identity Assurance Profiles.

The Identity Management Practice Statement is audited against claims of compliance with Identity Assurance Profiles.

6. Procedures

6.1. Membership application

In order to become a Member of SWAMID an organisation MUST formally apply for membership. Detailed information and application forms are published on the SWAMID website.

For organisations with an Identity Provider the Membership Application MUST include an Identity Management Practice Statement.

Each Membership Application is evaluated by the SWAMID Operations Team against the SWAMID Policy Framework. The SWAMID Operations Team presents a recommendation for membership with an evaluation report to the SWAMID Board of Trustees. The SWAMID Board of Trustees decides on whether to approve or deny the membership.

The SWAMID Operations Team communicates the decision of the SWAMID Board of Trustees to the applying organisation.

6.2. Membership cancellation

A SWAMID membership MAY be cancelled by the SWAMID Member at any time by sending a request to the SWAMID Operations Team. A cancellation of the SWAMID membership implies the automatic and immediate cancellation of the use of all Federation Technology Profiles for the organisation.

6.3. Membership revocation

A SWAMID Member who fails to comply with the SWAMID Policy Framework SHOULD have its membership in SWAMID revoked by the SWAMID Board of Trustees.

If the SWAMID Operations Team is made aware of a breach of SWAMID Policy Framework by a SWAMID Member, the SWAMID Operations Team SHALL issue a formal *notification of concern*. If the cause for the *notification of concern* is not rectified within the time specified by the SWAMID Operations Team, the SWAMID Board of Trustees SHALL issue a formal *notification of impending revocation* after which the SWAMID Board of Trustees SHOULD revoke the membership. If the SWAMID Policy breach is severe, SWAMID Operations Team MAY temporarily revoke the membership under the revocation dispute process.

A SWAMID Member not connected to SUNET MAY have its SWAMID membership revoked by decision of SUNET.

A revocation of the SWAMID membership implies the automatic and immediate revocation of the use of all Federation Technology Profiles for the organisation.

7. Audit

Identity Assurance Profiles and Federation Technology Profiles MAY impose audit of compliance on SWAMID Members.

8. Fees

SUNET will decide on yearly fees for SWAMID Members which will cover the operational costs of SWAMID. This decision MUST be made no later than July 1 each year or the fees will default to the fees from the previous year.

9. Liability

Neither the SWAMID Operations Team nor the SWAMID Board of Trustees SHALL be liable for damage caused to the SWAMID Member or its Subjects. SWAMID Members SHALL NOT be liable for damage caused to the SWAMID Operations Team or the SWAMID Board of Trustees due to the use of the SWAMID federation services, service downtime or other issues relating to the use of the SWAMID federation services.

SWAMID Members are REQUIRED to ensure compliance with the Swedish Personal Data Protection Regulation. The SWAMID Operations Team or the SWAMID Board of Trustees SHALL NOT be liable for damages caused by failure to comply with this law on behalf of the SWAMID Member or its Subjects relating to the use of the federation services.

For any other damage, the liability for damages in case of a breach is limited to one thousand (1000) euros. The SWAMID Operations Team and SWAMID Members SHALL refrain from claiming damages from each other for damages caused by the use of the SWAMID federation services, downtime or other issues relating to the use of the SWAMID federation services.

Neither party SHALL be liable for any consequential or indirect damage.