SWAMID Federation Policy v2.0

Document	SWAMID Federation Policy v2.0
Editor	Leif Johansson Torbjörn Wiberg Valter Nordh Pål Axelsson Mikael Berglund
Identifier	urn:mace:swami.se:swamid:2.0:policy
Version	2.0
Last Modified	2010-09-17
Status	FINAL
License	Creative Commons BY-SA 3.0

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, see http://www.ietf.org/rfc/rfc2119.txt.

2 Introduction

The *Swedish Academic Identity Federation* is introduced to facilitate and simplify the introduction of shared services across the (Identity) Federation. This is accomplished by using Federation Technologies to extend the scope of an (Electronic) Identity issued by one Member of the Federation to be valid across the whole Federation.

This (Federation) Policy defines the Federation by defining the procedures and practices which allows participating organisations to use available Federation Technologies for electronic identification and for access to authorisation information about individuals, resources and other objects in the Federation. In what follows the Swedish Academic Identity Federation is abbreviated **SWAMID**. 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* first issue and then manage identities throughout their life-cycles and by which they also make *Claims* of identity for *Subjects* (e.g. individuals, resources and other objects). A Claim of identity is an electronic 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. Further, a set of (*Identity*) *Assurance Profiles* and a set of (*Federation*) *Technology Profiles*. The Assurance Profiles and the Technology Profiles are based on current and evolving standards and are described in separate documents.

An Assurance Profile describes levels of trust in claims and organisations. An Assurance Profile allows a *Relying Party* (also known as a *Service Provider*) to determine the degree of certainty that the identity of a Subject presenting a Claim of identity is truly represented by the presented claim. This degree of certainty is represented by a commonly agreed-upon "Level of Assurance". Identity assurance is to a large extent independent of the technology used to convey Claims of identity.

The Technology Profiles describe concrete realisations of the Policy and Assurance Profiles in terms of specific technologies (eg SAML, eduroam etc). By employing specific choices of technologies for identification and authorisation this Policy MAY be used to support federated identity for a wide range of applications. The use of federation technology (e.g. SAML, 802.1x, WS-Federation, OpenID) is governed by a Federation Technology Profile.

3 Purpose and Scope

The purpose of SWAMID is to make it possible for Service Providers to provide services to End Users 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 users as described by the SWAMID Technology Profiles. The set of procedures and practices described in this document applies equally to all Technology Profiles of SWAMID.

In order to facilitate collaboration across national and organisational borders SWAMID MAY participate in interfederation agreements.

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 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.

Any changes to this policy MUST be approved by the SWAMID Board of Trustees. All decisions made by the SWAMID Board of Trustees are public and MUST be published on the SWAMID website.

The SWAMID Board of Trustees is responsible for maintaining formal ties with relevant national and international organisations.

4.2 SWAMID Operations Team

The operational management of SWAMID following the procedures described in this document, is assigned to the *SWAMID Operations Team* which is appointed by the SWAMID Board of Trustees. The chair of the SWAMID Operations Team is the SWAMID federation manager ("systemförvaltare"), appointed by the SWAMID Board of Trustees. Information about the team members and other contact information is published on the SWAMID web site: http://www.swamid.se.

SWAMID Operations Team is responsible for maintaining and publishing a list of SWAMID Members along with information about which Assurance Profiles each Member fulfills and which Technology Profiles each Member implements.

The SWAMID Operations Team acts as a third line support for support requests from the second line support of Members. Members MUST NOT redirect End User queries directly to the SWAMID Operations Team but MUST make every effort to ensure that only relevant problems and queries are sent to the SWAMID Operations Team.

4.3 SWAMID Member

In order to become an Identity Provider in SWAMID an organisation MUST be eligible for SUNET membership and MUST become a Member of SWAMID. A Relying Party is in general NOT REQUIRED to become a Member of SWAMID in order to consume identity information from SWAMID identity providers. Technology Profiles MAY impose additional requirements on Relying Parties.

An organisation becomes a Member of SWAMID by applying for membership according to the process described in this document. If the application is accepted by the Board of Trustees, the organisation becomes a Member by signing the SWAMID membership agreement.

Members operating identity providers will in most cases have End Users 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 End Users. In particular each Member is responsible for fulfilling the requirements of the Swedish Personal Data Act (see the section on Liabilities) with respect to its own End Users.

Members are responsible for first line (e.g. call center or equivalent) and second line (technical support and problem classification) support for its End Users. Membership in SWAMID does not mandate any specific service level for this service but Members are encouraged to maintain a help desk for normal office-hours in the local time zone of the Member for user queries. Each End User SHALL BE identified by at least one SWAMID Member.

Each Member MUST publish a local acceptable use policy for any services covered by the SWAMID Policy. The local acceptable use policy MUST contain information about any activities and/or behavior which is deemed unacceptable when using the service. Members are encouraged to make user acknowledgement of the the acceptable use policy a part of the service access process.

5 Identity Management Practice Statement

Each Identity Provider that wishes to become a Member of SWAMID MUST create, publish and maintain an Identity Management Practice Statement. The Identity Management Practice Statement is a description of the Identity Management life-cycle including a description of how identity Subjects are enrolled, maintained and removed from the identity management system. The statement MUST contain descriptions of administrative processes, practices and significant technologies used in the identity management life-cycle. The processes, practices and technologies described MUST be able to support a secure and consistent identity management life-cycle. Specific requirements are imposed by Assurance Profiles.

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

6 Procedures

6.1 Membership application

In order to become a Member of SWAMID an organisation formally applies for membership. Detailed information and application forms are published on the SWAMID website: http://www.swamid.se. For Identity Providers the membership application MUST include an Identity Management Practice Statement.

Each membership application including (if applicable) the Identity Management Practice Statement is evaluated by the SWAMID Operations Team. The evaluation process involves checking if the applying organisation fulfills the requirements of the SWAMID Policy. The SWAMID Operations Team presents a recommendation for membership with an evaluation report to the SWAMID Board of Trustees who in turn decides on whether to grant or deny the application.

If the application is granted, the SWAMID Operations Team presents a membership agreement to the applying organisation for signing by an official representative of the organisation. If the application is denied, this decision and the reason for denying the application is communicated to the applying organisation by the SWAMID Operations Team.

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 SWAMID Technology Profiles for the organisation.

6.3 Membership revocation

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

If the SWAMID Operations Team is aware of a breach of Policy by a Member, the SWAMID Operations Team MAY 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 MAY issue a formal *notification of impending revocation* after which the SWAMID Board of Trustees MAY choose to revoke the membership.

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

7 Audit

The SWAMID Policy does NOT REQUIRE any audit. Assurance Profiles MAY impose audit requirements on Members.

8 Fees

The SWAMID Board of Trustees will decide on yearly fees for SWAMID Members which will cover the operational costs of SWAMID. This decision MUST be made no later than on 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 Federation Member or its End User. 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.

The SWAMID member is REQUIRED to ensure compliance with the Swedish personal data act (SFS 1998:204 Personuppgiftslag). 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 End Users relating to the use of the federation services.

The SWAMID member is REQUIRED to inform End Users about the existence of local acceptable use policy which MAY be applicable when End Users use services published and/or belonging to other SWAMID members. 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 the SWAMID member SHALL refrain from claiming damages from other SWAMID members 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.