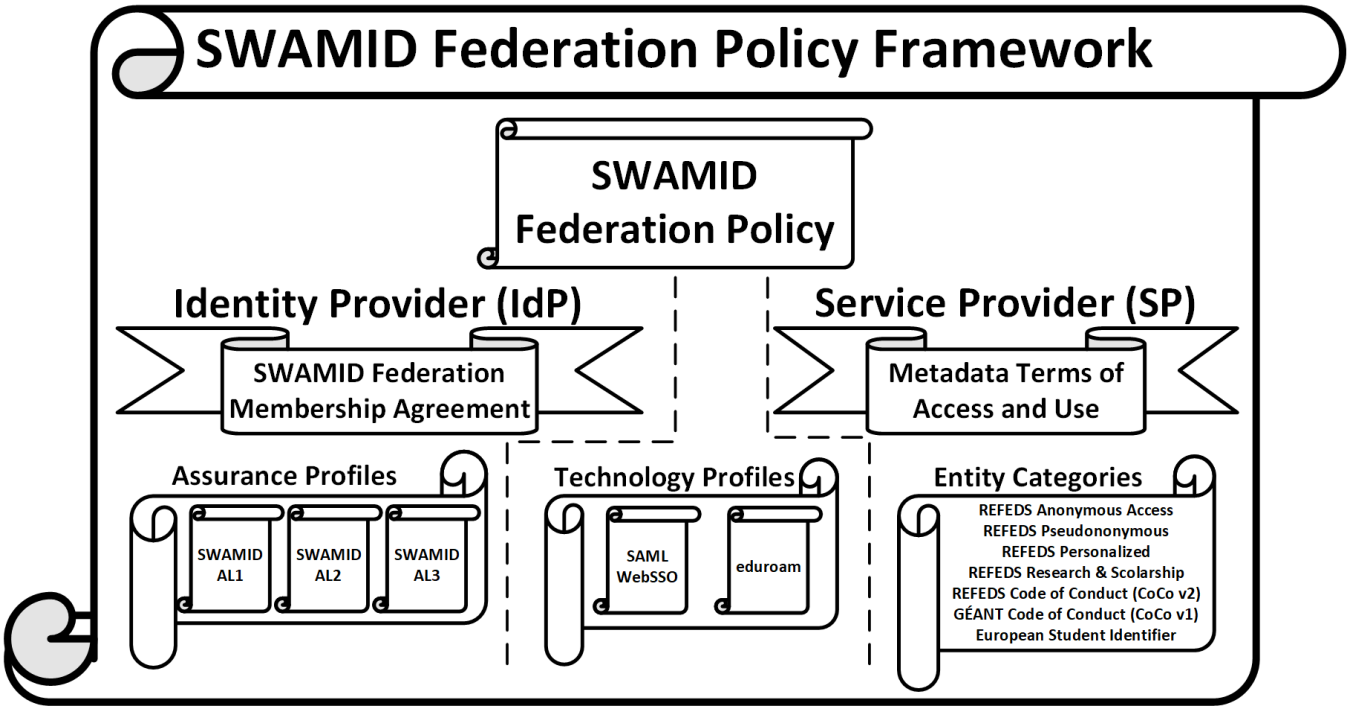
SWAMID Policy

For an Identity Federation trust is everything. To enable trust there is a federation policy that regulates the federation operator's organisation and working methods as well as the regulatory framework for Identity Providers and Service Providers.

SWAMID Federation Policy Framework

The policy framework for SWAMID consists of three parts: SWAMID Federation Policy describes the management and organization, assurance profiles describing what a relying party can expect from a login via SWAMID and technology profiles describing the technical interfaces WebSSO SAML and eduroam. Alongside the assurance and technology profiles are also Entity Categories to facilitate attribute release between Identity Providers and Service Providers.



SWAMID Federation Policy

The Federation Policy defines the rule set for SWAMID including the use of assurance and technology profiles. It describes the formal management of SWAMID and the membership processes.

- SWAMID Federation Policy

SWAMID Identity Assurance Profiles

SWAMID is built on trust and the Identity Providers expressed user trust based on the SWAMID Identity Assurance Profiles. THe Identity Providers are only allowed to assert assurance levels that they have been audited by.

- SWAMID Identity Assurance Level 1 Profile (SWAMID AL1)
- SWAMID Identity Assurance Level 2 Profile (SWAMID AL2)
- SWAMID Identity Assurance Level 3 Profile (SWAMID AL3)

SWAMID Technology Profiles

SWAMID uses a set of federation technologies to enable federated login and each of them is described in a SWAMID Technology Profile.

- Technology profile SAML WebSSO
- Technology profile eduroam

Entity Categries within SWAMID

Entity categories are not a separate policy document in the SWAMID's policy framework but are highly recommended for attribute release according to the SAML WebSSO Technology Profile. Entity Support Categories are used to signal that an Identity Provider supports a specific Entity Category.

The following Entity Categories are supported within SWAMID:

- GÉANT Data Protection Code of Conduct
- REFEDS Research and Scholarship Entity Category
- REFEDS Hide From Discovery Entity Category
- European Student Identifier Entity Category

The following Entity Support Categories are supported within SWAMID:

- GÉANT Data Protection Code of Conduct
- REFEDS Research and Scholarship Entity Category

Identity Provider (IdP)

For an organisation to be able to use services linked to SWAMID the organisation needs to become a member of the Federation. Only organisations connected to the Swedish NREN Sunet can be members of SWAMID if no special circumstances occur. This is done by the Membership Agreement signed and submitted to SWAMID by mail and e-mail. Together with the Membership Agreement an Assurance Declaration for SWAMID Identity Assurance Profiles in form of an Identity Management Practice Statement must be submitted. The Assurance Declaration may be sent by e-mail.

Service Provider (SP)

SWAMID has a set of formal registartion requirements for services that a service must fulfil. The SWAMID Metadata Terms of Access and Use outline the purpose, access to and how you can use SWAMID Metadata. The SWAMID Metadata Terms of Access and Use is used instead of a contract between SWAMID and external service providers. To further enable the service providers to get the right information about users who log in using SWAMID there are Entity Categories.

- Formal registration requirements for services
- SWAMID Metadata Terms of Access and Use
- Service Provider Entity Categories used within SWAMID

Interfederation

SWAMID is member of two interfederations. An interfederation is a federation of federations. This means that the federations exchanges metadata with each other so that users in one federation can log into services in another federation.

- The eduGAIN Interfederation connects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN comprises over 80 participant federations connecting more than 8,000 Identity and Service Providers.
    - SWAMID eduGAIN Metadata Registration Practice Statement - In the same way that every member of SWAMID must write a Trust Declaration in the Identity Management Practice Statement, any member of the interfederation write and publish a Federation Metadata Registration Practice Statement.
    - SWAMID export all Identity Providers to eduGAIN by default. A member organisation can decide to opt-out this export.
    - SWAMID only export services to eduGAIN that opt-in and uses current international entity categories.
- FIDUS is an interfederation for government services aimed at primary and secondary schools and adult education. SWAMID participates in the interfederation because universities and university colleges have systems to support teacher training that are used by the schools and the Swedish Council for Higher Education has systems that schools report in. Furthermore, users from universities and university colleges log into systems at Swedish National Agency for Education to construct the Swedish national tests for primary and secondary schools.