



| | |
|----------------------|---|
| Document | SWAMID Metadata Registration Practice Statement |
| Editor | Pål Axelsson & Paul Scott |
| Identifier | http://www.swamid.se/policy/mdrps |
| Version | 2.0 |
| Last modified | 2016-08-19 16:00 |
| Pages | 2 |
| Status | Published |

SWAMID Metadata Registration Practice Statement

Federation Name: Swedish Academic Identity Federation – SWAMID

Federation Operator: SUNET, Sweden

Federation Web Page: <http://www.swamid.se>

Common Practices

All Identity Providers and Service Providers communicate with SWAMID Operations Teamⁱ via mail and the issue-tracking system of operations@swamid.se.

Service providers are only published to interfederations (currently eduGAIN) if they request to opt-in. They must fulfill the requirements for publishing that the interfederation imposes (if any). Identity Providers are published by default to eduGAIN. If they wish to opt-out, this must be requested.

Only organisations with Identity Providers are REQUIRED to be members of SWAMID, Service Providers MAY be members but can participate in SWAMID without being members.

Practices on Identity Provider Registration

SWAMID Federation Policy section 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 Trusteesⁱⁱ 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.

Identity Providers Domain Name Scopes

For all Identity Providers the shibmd:Scope extension elements in metadata (or equal) represents user security domain(s) of the organisation. The scope in scoped attribute values can only be these user security domain(s). The domain(s) must be owned by the organisation in the Domain Name System (DNS), or the organisation must be authorised to use the domain as scope by the owner of the domain in the DNS (if applicable).

Practices on Service Provider Registration

Each Service Provider must be manually approved by SWAMID Operations Team in order to be registered with the federation. The Service Provider must also accept SWAMID Metadata Terms of Access and Use (<http://md.swamid.se/md/swamid-tou-en.txt>) before using SWAMID metadata.

It is the duty of the SWAMID Operations Team to review and approve all the details provided by the Service Provider administrator. In addition, SWAMID Operations Team can reject changes or further modify details of a Service Provider before approving it.

Only users with rights for a specific approved Service Provider are able to modify its elements and attributes in SWAMID. Such changes require re-approval by SWAMID Operations Team.

ⁱ SWAMID Operations Team is the group of individuals responsible for the day to day task of running SWAMID. Roles and responsibilities are defined in SWAMID Federation Policy section 4.2, available at <http://www.swamid.se/policy/>.

ⁱⁱ SWAMID Board of Trustees is the group of individuals responsible for the management of SWAMID. Roles and responsibilities are defined in SWAMID Federation Policy section 4.1, available at <http://www.swamid.se/policy/>.