SAML SP Best Current Practice

To register a Service Provider you need to fulfill the SWAMID Service Provider criteria in the SAML WebSSO Technology Profile. For more information on how to register a service in SWAMID please go to Getting Started with SWAMID.

SWAMID WebSSO Service Provider

How to provide services to users associated with SWAMID members

Is your service provider already published to the interfederation eduGAIN by another federation?

We have an opt-out policy regarding eduGAIN for SWAMID Identity Providers, so you should already been able to communicate with most SWAMID member institutions. You may need to talk to the federation that publishes your metadata to eduGAIN about which eduGAIN enabled entity categories to use to get the appropriate attributes released by our IdPs.

If you still want to register your service with SWAMID:

1. Review the registration criteria at Getting Started with SWAMID.
2. We tag Service Providers with entity categories and encourage our IdPs to use them for attribute release. Please read 4.1 Entity Categories for Service Providers and decide which apply best for you. Please provide a motivation for your choice as described in the defined request processes for each entity category!
3. Integrate SWAMID Metadata into the service provider and optionally configure use of the SWAMID Discovery Service.
4. Register the metadata for the service provider. This step *implies* acceptance of the SWAMID Service Provider registration criteria, as described in Getting Started with SWAMID, and constitutes a legally binding agreement to abide by the ToU. Please look into step 4 in the Shibboleth Service Provider installation instructions below to make your service provider work better with users within the federation and inter-federations.

How to install a Shibboleth Service Provider

Step 1 - Installing a Web Server

- 1.1 Installing Apache Web Server 2.0 or higher for Shibboleth Service Provider
- 1.2 Configuring Apache Web Server to use Shibboleth
- 1.3 Configuring IIS for MS windows

Step 2 - Installing Shibboleth Service Provider

- 2.1 Installing Shibboleth SP 3.x on Linux with yum
- 2.2 Installing Shibboleth SP on Windows with IIS Web Server
- 2.3 Docker Image with apache and shibboleth
- 2.4 Shibboleth for Java Applications

Step 3 - Configuring Shibboleth Service Provider for use in the SWAMID federation

- 3.1 Configure Shibboleth SP - shibboleth2.xml
- 3.2 Configure Shibboleth SP - attribute-map.xml
- 3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTFI
- 3.4 Configure Shibboleth SP - Automatically validate metadata with ws-* extensions for ADFS IdPs
- 3.5 Contact and Organization information for Service providers

Step 4 - Get the correct attributes from Identity Providers

To make the login work smoother for your users you need to get the right attributes from the Identity Providers. To make it more easy to get the right attributes you need to follow the instructions below.

- 4.1 Entity Categories for Service Providers is used to enable support for automatic attribute release from Identity Providers.
- 4.2 How to inform user of missing required attributes when accessing a service.
- 4.3 Service Provider Metadata Extensions for Login and Discovery User Interface (MDUI) enhance user experience in Identity Providers and Discovery Services.
- 4.4 Implementera krav på tillitsnivå samt ev. multifaktor vid inloggning
- 4.5 If your service shall be available within the international academic identity federations inform SWAMID Operations that your Service Provider shall be exported to eduGAIN.

- 4.6 If nothing else helps or you need special attributes that is not part of entity categories contact the Identity Providers that you've users from and that doesn't release needed attributes.

Step 5 - Register your Service Provider metadata in SWAMID

- When you your Service Provider is ready for production you must register your metadata with SWAMID. To register the metadata you log into the SWAMID metadata tool and upload your metadata file. In the metadata tool you refine the metadata with the extra metadata information from step 4. If you don't have an account in any Identity Provider within SWAMID you can use the Identity Provider eduID.se. When you create an account in eduID please take the identity proofing steps and if that is not possible register your name after you've activated your account.
- When you request to publish the registered metadata you will get a mail that you must forward to the SWAMID Operations team. When you forward the mail, you must add which registration criteria in Getting Started with SWAMID you fulfill and give proof of that.