1 Technical Configuration for SAML 2.0

This document describes how to configure your service/product to use Joint Web Login, a service within Uppsala University that enables simple login for staff and students.

Note: Before performing configuration, preparatory steps must be taken to start the work. See the checklist for more information.

Contents:

- Technical Configuration for SAML 2.0
- Formal Requirements, Rules and Recommendations
- Prerequisites
- Setup and Configuration
- Metadata
- Publication of Metadata

Expectations:
As a provider, you are expected to

- be oriented in the field of SAML 2.0. Read more about SAML 2.0 here.
- be familiar with how your service/product connects to an IdP with SAML 2.0.

NOTE: All authorization (authorization management) and role management must be done in your service/product. The Joint Web Login service does not perform any authorization management or role management for your service/product.

Read more under Authentication and authorisation principles (Authorisation section).
# 2 Formal Requirements, Rules and Recommendations

<table>
<thead>
<tr>
<th>Requirement / Rule / Recommendation</th>
<th>Clarification</th>
<th>Examples</th>
</tr>
</thead>
</table>
| All SAML keys/certificates you create when setting up your SP should have  
  - a **key length** of at least 4096 bits (RSA)  
  - a **validity period** that is very long (e.g. 100 years) | To comply with current recommendations and requirements and to avoid having to regenerate SAML certificates on an ongoing basis. | |
| The **entityID** of the service should be in **URL format**. | **The entityID of the service must be unique** and is usually set to be a base URL to the part of the service that handles SAML 2.0.  
Having a metadata URL as the entityID is recommended by Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (section 8.3.6 Entity Identifier). | |

- [https://myservice.uu.se/Shibboleth.sso/Metadata](https://myservice.uu.se/Shibboleth.sso/Metadata)  
  If using the SP software Shibboleth SP, this is the URL to its metadata generator.  
- [https://myservice.uu.se/Shibboleth.sso](https://myservice.uu.se/Shibboleth.sso)  
  If using the SP software Shibboleth SP, this is usually its base URL.  
- [https://myservice.uu.se/shibboleth](https://myservice.uu.se/shibboleth)  
  This indicates that the URL has something to do with Shibboleth and the Shibboleth SP software.  
- [https://myservice.uu.se/saml](https://myservice.uu.se/saml)  
  This indicates that the URL has something to do with SAML.  
- [https://myservice.uu.se/](https://myservice.uu.se/)  
  This is a URL that is unique to the service.
There are application processes to the entity categories that must be followed in order for the service to be tied to ("tagged with") them. It is those formally responsible for the service who should be able to produce the required information, ensure that the necessary information pages and the like are available, and ensure that all the requirements for an application are met.

Your SP and service metadata should meet all the requirements in SWAMID SAML WebSSO Technology Profile section 6 Operational Requirements for Relying Parties.

### 3 Prerequisites

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Identify the appropriate entity category</strong>&lt;br&gt; The entity category should contain the information (attributes) needed.</td>
<td>See Entity Categories for Service Providers or the comparative overview Entity Category attribute release in SWAMID and select one of these. For services that do not need a personal identity number, REFEDS Research &amp; Scholarship will usually suffice. For services that need a personal identity number, GÉANT Data Protection Code of Conduct is required.</td>
</tr>
</tbody>
</table>
| 2    | **Check that the purpose of the service matches the purpose of the entity category**<br> If e.g. the service is not used in whole or in part to carry out studies or research, then | More information on the purpose of some of the available entity categories can be found on the following pages:  
- REFEDS Research & Scholarship (collaborative tools for conducting studies and research; see Definition) |
### Step 3

**Instruction**

Find out if the service needs to have the user ID sent to it via so-called SAML2 Persistent NameID instead of via "normal" attributes

Many services use this technique because it is a more standardised way of transmitting user IDs.

**Recommendation**

- GÉANT Data Protection Code of Conduct (good, accurate, controlled, secure and minimised handling of personal data)

### 4 Setup and Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Guidance and Examples</th>
</tr>
</thead>
</table>
| 1    | Create a Service Provider (SP) for the service  
Install and configure software capable of handling SAML 2.0 for the service. If the service has built-in support for SAML 2.0, configuration in the service administration interface is what needs to be performed instead. | See SAML SP Best Current Practice for guidance. |
| 2    | Use a specific login server (IdP) or choice of higher education institution (DS) in the SP of the service  
IdP:  
**entityID**: https://weblogin.uu.se/idp/shibboleth  
DS:  
**discoveryURL**: https://service.seamlessaccess.org/ds/ | See Discovery Service Integration for more information. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Guidance and Examples</th>
</tr>
</thead>
</table>
| Option 3 a URL | **Load metadata for IdP via URL**  
In order for your SP to know how to communicate with (or interpret data from) the IdP – either the IdP you have chosen or the one chosen by the user in the choice of higher education institution (DS) – it needs to have access to the metadata of the IdP. Signing certificates are used to validate IdP metadata.  
**Standard:**  
IdP-metadata: http://mds.swamid.se/md/swamid-idp.xml  
Signing certificate: http://mds.swamid.se/md/md-signer2.crt  
Here we assume that the IdP belongs to an organisation that is a member of the SWAMID identity federation, which is the case with the Joint Web Login service at Uppsala University.  
**Exeption:**  
IdP-metadata: https://weblogin.uu.se/idp/shibboleth  
Signing certificate: https://weblogin.uu.se/md/uu-signer.crt  
This option should only be used in case memory limitations or metadata parsing restrictions prevent the default option from being used. | |
| Option 3 b Static data | **Load IdP metadata via static data**  
If your SP does not support loading IdP metadata from a URL (see option 3 a), e.g. if you can only enter "static" data in an administration interface or similar. Note that the following static strings are specific to the Joint Web Login service.  
Signing certificate for SAML messages:  
MIIDJDCCAgygAwIBAgIVAMAqC57ZiqOY9LvU7w7YjaZ2U8GtMA0GCSqGSIb3DQEBAU wombkkxFzAVBgNVAMMDnd1YmxvZ21uLnV1LnN1MB4XDTExMDcxMDIwNDgxNi0X | SSO = Single Sign On  
SLO = Single Log Out |
<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Guidance and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTI2MDCxMDIwNDgxNlowGTEXMBUGA1UEAwOD2VibG9naW4udXUuc2UwggEiMA0GCSqGSIb3QEBQQUAA4IBAwggEKAoIBAQDXw09+6G/fp7dFcaps5s8vygdIGEXh7zDfkw43aSXB1T3hXmyUNR81wynpswZ99G57vk1te6BuCp6+/+T4S6DrzE80YkwF08Y9JMoXYB6YWk5aw4BBU1k1Qdyz6wy+o27N+KdS07zAebh1fxZjgjkM UQSE1qBeOTX91uyjU0d3VpyV31AbAN9wcm33HvoRSeI3n3jq3XmBwM5Xbuae8SSYBDqRxM6Fu+YSkO4Ebi1c1o2zFtBDh6N9U+OCR+G8ysZvyUfs8Ws51Y4U0xygxOGGZ/f2Raiq8wUe8uy4o2UQL7n9QpyhTEE/94HsxT0halOrS/MI115zw9XAgMBAAgjYzBhMB0GA1UdDgQWBBQxRpo9n9mvAS051XugKjgntHFsRwCBwzBABgNVHREEOTAG555ZWjs3dpb151d5szZY1aRH0cM6Ly93ZwJSb2dpb151d5szSZ9pHZAhv2hpYmV bGV0aDANBgkghkiG9w0BAQfasFA0ACQQAEXR48LBVIAwqZ7z31wrgsMwKwWafq0/NG13rpj5tpayQ1NebIdlyUQPM4m9PBS/zTsxIBT975rj/Ye3jxf39+9p1G51tQALUq Psz27tWCGdEe0CB6i1GT30gn15VNqezXZrz+EXtxkzBq4fso9v9eWe9ec5Cbyf6l wRUosZ5jL0903INDB2DRPffyrXjXuEmxwDeEYR/2w++379hwYjdJplZ1/ K01TUsJ/FvBnpxuJ3FxPp/R11j4uhpLi+N3fh4x50H0DlsKIV+xCPzw6uLSpH ABrzItGWOuUunkP0Bj8205qF+q+zidU41x2m4oONHzdQ+3IX75GUEg==</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encryption certificate for SAML messages:

```
MIIDzCCAgAwIBAgIUAHUETQJYKoIzIhvcNzAQLBQAwGTEXMBUGA1UEAwOD2VibG9naW4udXUuc2UwggEiMA0GCSqGSIb3QEBQQUAA4IBAwggEKAoIBAQDXw09+6G/fp7dFcaps5s8vygdIGEXh7zDfkw43aSXB1T3hXmyUNR81wynpswZ99G57vk1te6BuCp6+/+T4S6DrzE80YkwF08Y9JMoXYB6YWk5aw4BBU1k1Qdyz6wy+o27N+KdS07zAebh1fxZjgjkM UQSE1qBeOTX91uyjU0d3VpyV31AbAN9wcm33HvoRSeI3n3jq3XmBwM5Xbuae8SSYBDqRxM6Fu+YSkO4Ebi1c1o2zFtBDh6N9U+OCR+G8ysZvyUfs8Ws51Y4U0xygxOGGZ/f2Raiq8wUe8uy4o2UQL7n9QpyhTEE/94HsxT0halOrS/MI115zw9XAgMBAAgjYzBhMB0GA1UdDgQWBBQxRpo9n9mvAS051XugKjgntHFsRwCBwzBABgNVHREEOTAG555ZWjs3dpb151d5szZY1aRH0cM6Ly93ZwJSb2dpb151d5szSZ9pHZAhv2hpYmV bGV0aDANBgkghkiG9w0BAQfasFA0ACQQAEXR48LBVIAwqZ7z31wrgsMwKwWafq0/NG13rpj5tpayQ1NebIdlyUQPM4m9PBS/zTsxIBT975rj/Ye3jxf39+9p1G51tQALUq Psz27tWCGdEe0CB6i1GT30gn15VNqezXZrz+EXtxkzBq4fso9v9eWe9ec5Cbyf6l wRUosZ5jL0903INDB2DRPffyrXjXuEmxwDeEYR/2w++379hwYjdJplZ1/ K01TUsJ/FvBnpxuJ3FxPp/R11j4uhpLi+N3fh4x50H0DlsKIV+xCPzw6uLSpH ABrzItGWOuUunkP0Bj8205qF+q+zidU41x2m4oONHzdQ+3IX75GUEg==
```
4. If MFA is required

**Add multifactor authentication (MFA)**

The Joint Web Login service currently supports multifactor authentication according to two different standards:

- **FIDO U2F**, with Yubico YubiKey USB keys issued and managed by Uppsala University. These are linked to the user in Uppsala University's AKKA authorisation system according to specific procedures.

- **TOTP**, using an app in their smart phone or tablet to obtain time-based one-time codes. Users activate the possibility of using TOTP themselves on the [account website](https://weblogin.uu.se/idp/profile/SAML2/POST/SLO).

It is normally the SP of the service who should indicate that multifactor authentication is required and with which technology.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Guidance and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Add multifactor authentication (MFA)</td>
<td>See e.g. <a href="https://refeds.org/profile/mfa">How do I actually use the REFEDS MFA Profile to request MFA?</a>, <a href="https://refeds.org/profile/mfa">Requiring Multi-Factor Authentication</a>, <a href="https://refeds.org/profile/mfa">Configure a Service Provider for Two-Factor Authentication</a> and <a href="https://refeds.org/profile/mfa">Multi-Factor Access</a> for further information and SP configuration examples. For FIDO U2F, the authentication class (AuthnContextClassRef) is called: <code>https://refeds.org/profile/mfa</code> For TOTP, the authentication class (AuthnContextClassRef) is called:</td>
</tr>
</tbody>
</table>

**Guidance and Examples**

URLs for SAML messages:

**SSO:**
- HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SSO`
- HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SSO`

**SLO:**
- HTTP POST: `https://weblogin.uu.se/idp/profile/SAML2/POST/SLO`
- HTTP Redirect: `https://weblogin.uu.se/idp/profile/SAML2/Redirect/SLO`

Which variant of URL should be used depends on what your SP supports, but HTTP POST is most common.
### Step 1: Create metadata in XML format

The most fundamental part of this is purely technical details such as the unique ID of the service (entityID), keys (for signing and possibly encrypting SAML messages) and URLs (SAML endpoints).

In most cases, SP software can be used to generate this metadata.

**Guidance and Examples**

Examples of metadata for other services can be found at [https://metadata.swamid.se/](https://metadata.swamid.se/).

Select any service and then Show XML or Download XML and look at the file with any suitable text viewer.

This may also be helpful to see if you seem to have "missed" anything in the metadata for your service compared to others.
<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Guidance and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><strong>Supplement with user information</strong>&lt;br&gt;Supplement with information displayed to the user at login, known as MDUI information. This may include formal requirements, use of the service and handling of personal data.</td>
<td>See <a href="#">SWAMID SAML WebSSO Technology Profile</a> (section 6.1.12–6.1.13 Metadata Extensions for Login and Discovery User Interface (MDUI)) for formal requirements.&lt;br&gt;See <a href="#">Service Provider Metadata Extensions for Login and Discovery User Interface (MDUI)</a> for examples&lt;br&gt;See <a href="#">Service Provider Privacy Policy Template</a> for the appropriate template to use for the service usage and personal data handling page.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Supplement with contact information</strong>&lt;br&gt;Contact information is needed so that responsible persons can be reached.</td>
<td>See <a href="#">SWAMID SAML WebSSO Technology Profile</a> (section 6.1.21 Organization samt 6.1.22–6.1.27 ContactPerson) for formal requirements.&lt;br&gt;See <a href="#">Contact and Organization information for Service providers</a> for examples.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Supplement with special tag for DS</strong>&lt;br&gt;When selecting the higher education institution (DS), you must supplement the service metadata with a tag <code>&lt;DiscoveryResponse&gt;</code> inside the tag <code>&lt;SPSSODescriptor&gt;</code> and <code>&lt;Extensions&gt;</code>.&lt;br&gt;This is a security feature to prevent arbitrary web pages from misusing institution selection and tricking the user after login.&lt;br&gt;In principle, this controls which URL the user is allowed to be redirected to after login, and thus where the login information is allowed to be sent.</td>
<td>See <a href="#">Identity Provider Discovery Service Protocol and Profile</a> (section Use of Metadata), for information on this security feature.&lt;br&gt;See <a href="#">Enabling OpenAthens Wayfinder: Shibboleth</a> for illustrative examples of how this configuration can be done.&lt;br&gt;See <a href="#">Redirect to SSO Service at the IdP</a> for general information on how the web flow works when selecting the institution (DS).</td>
</tr>
</tbody>
</table>
### Step 5

**If SAML2 Persistent NameID is used**

Specify NameID format

If the service uses **SAML2 Persistent NameID** for user ID transmission, the NameID format `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` must be specified in the service metadata or in the login request.

**NOTE!** It is very important that the NameID format `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` is not listed as an available option in the service metadata. Otherwise, all NameID formats in the metadata will be ignored and the NameID may not be sent at all.

You need to let us know if the service needs the user's actual user ID (e.g. `abcd1234@user.uu.se`) or the value of any other SAML attribute sent as **SAML2 Persistent NameID**. Otherwise, an anonymised version of the user ID will be sent by default.

### Step 6

**Publication of Metadata**

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Further Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify metadata before publishing</td>
<td></td>
</tr>
</tbody>
</table>
Instructions & Technical Configuration to New SSO Users

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
<th>Further Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check that your SP and service metadata meet all the requirements in [SWAMID SAML WebSSO Technology Profile](section 6 Operational Requirements for Relying Parties).</td>
<td></td>
</tr>
</tbody>
</table>
| 2    | **Submit the service metadata to SWAMID for publication**  
Metadata should be published either in the SWAMID (IdP) metadata stream or in SWAMID and eduGAIN (DS). 
From January 2022 onwards, this is something you normally do yourself (see [blog post](blog post)) via the SWAMID metadata tool. 
Metadata tool login is done [here](here) with an account from any organisation connected to SeamlessAccess via eduGAIN.  
**NOTE!** When requesting publication of metadata from within the metadata tool, an email will be sent which must be manually forwarded to [SWAMID Operations](SWAMID) in order for the publication to be performed. | For further information on the metadata tool and its use, please contact [SWAMID](SWAMID). |
| 3    | **Done! Your service is now ready to use the Joint Web Login service**  
**NOTE!** It is not until the metadata is published (plus a certain time delay, up to 8 hours) that Joint Web Login is aware of your service and can be used to log in to it. | |

If you have any questions, please [contact IT Support](contact IT Support) and ask to be put in touch with the operators of the Joint Web Login service.