Senast uppdaterad: 2022-11-30

UPPSALA UNIVERSITET

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:

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

Requirement / Rule / Recommendation	Clarification	Examples
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 OASISSecurity Assertion Markup Language(SAML) V2.0 (section 8.3.6 Entity Identifier).	• `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` If using the SP software Shibboleth SP, this is usually its base URL. • `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` This indicates that the URL has something to do with SAML. • `https://myservice.uu.se/` This is a URL that is unique to the service.

Requirement / Rule / Recommendation	Clarification	Examples
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.	See Entity Categories for Service Providers for details for the respective entity category.
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

Step	Instruction	Recommendation
1	**Identify the appropriate entity category** The entity category should contain the information (attributes) needed.	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 & Scholarship will usually suffice. For services that need a personal identity number, GÉANT Data Protection Code of Conduct is required.
2	**Check that the purpose of the service matches the purpose of the entity category** 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	Instruction	Recommendation
	REFEDS Research & Scholarship cannot be used.	• GÉANT Data Protection Code of Conduct (good, accurate, controlled, secure and minimised handling of personal data)
3	**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.	

4 Setup and Configuration

Step	Instruction	Guidance and Examples
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.

Step	Instruction	Guidance and Examples
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:
	
	`MIIDJDCCAgygAwIBAgIVAMAqC57ZiqOY9LvU7W7YjaZ2U8GtMA0GCSqGSIb3DQEB`
	`CwUAMBkxFzAVBgNVBAMMDndlYmxvZ2luLnV1LnNlMB4XDTE2MDcxMDIwNDgxNloX`
		SSO = Single Sign On
		
		SLO = Single Log Out

Step	Instruction	Guidance and Examples
	DTI2MDcxMDIwNDgxNlowGTEXMBUGA1UEAwwOd2VibG9naW4udXUuc2UwggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXwo9+t6G/fp7dFcap5s8vygdIGWEx h7zDfKW43aSXBlT3hQXmyUNR8E1wynpswZz9OG57vklte6BwCpj6/+o/T4S6DDrz E80YKwF08Y9JMoyXB6YWk5awu4BBU1k1QDyz6wy+o27NK+dS07ZaEhbiFxZjgjkM UQSE1qBeOTX91uyp/Oud3VpyV31AbAN9Wcw33HvoRSeIy3njq3XBmW5Xbuae8SSY BDqR+M6Fu+YSk04EblIcl0zFtBDh6N9U+OCR+G8YsZvyUfs8WSx1Y4uOxygxOGgZ /f2Raiq8WuE8uy4o2UQL7NqJ9PyhTTk+94HsxT0haLOrS/MNI1l5Zw9XAgMBAAGj YzBhMB0GA1UdDgQWBBROpn9mvA5O1XugKjgnthIFsRwCBzBABgNVHREEOTA3gg53 ZWJsb2dpbi51dS5zZYYlaHR0cHM6Ly93ZWJsb2dpbi51dS5zZS9pZHAvc2hpYmJv bGV0aDANBgkqhkiG9w0BAQsFAAOCAQEAXR4BLVIAwqZTzz3iwjGskMw2WzfBQ/nG l3rjpj5tpayQ1NrEbidLiyUQD4m9PBS/zTsxIB9TJ5r/Ye3jf39+9plG51tQALUq Psz27W4CGdEe0CBeiGTJ0gnlSVNqezXsRzk+EXTkzQbQ4sov9eWeWe9c/5Cbyf6l wRUoSoZ5j0Lo9+03ZiNBBD2PRpfyrXjXuIEw5xDeE2YR/2W++3J79hWjydJPlzl/ K0lTdUS/JfVbNpxufJxPp/R1iLjU4hypLi+N3fh4xh0HOdLskIV+xCPzwn6uLsPG AbrZzItGWOuUunKpQBejEO5F+q+z1dU41x2m4oONHzdQ+3IX75GUEg== Encryption certificate for SAML messages: MIIDIzCCAgugAwIBAgIUU/H0eVODSSmZoDRn6Lz3GR/1kzMwDQYJKoZIhvcNAQEL BQAwGTEXMBUGA1UEAwwOd2VibG9naW4udXUuc2UwHhcNMTYwNzEwMjEwNDMzWhcN MjYwNzEwMjEwNDMzWjAZMRcwFQYDVQQDDA53ZWJsb2dpbi51dS5zZTCCASIwDQYJ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKvjMIOzZJS4B6CpNZ2aAcMlHDPloeGm cmiAIoC5odr2b1qutyj2X1k0TnlEGLVnQMbgsIZR0qz0/0Dd0RL15+SnNswBB5wa ShHiTkkZATaFaed2kmO9DDXV7m3dxgF8a3DWaSWF12jNiGwxmvCIeEmQUsSVY52r uoKbv04q+vQB2aJPTdKGzrSqGxZw6pWPjZotiuT/Hn6aWVfSeya6OTgtOgybsWsn a4A/ncMhj8tl5lnpQGxWwJWFBQm9T3mEDrzgJND4E+ZxdFmrUZGFSRmkWe+ma9Ii Y1z1IXNedOZMshrMelD9UMEnc3ZCZJCeWfsdpe6ecZU+T4l5kWuALqkCAwEAAaNj MGEwHQYDVR0OBBYEFM3QZFFxSaebrz860E57FdtWScA7MEAGA1UdEQQ5MDeCDndl YmxvZ2luLnV1LnNlhiVodHRwczovL3dlYmxvZ2luLnV1LnNlL2lkcC9zaGliYm9s ZXRoMA0GCSqGSIb3DQEBCwUAA4IBAQCXHAy+YMui0rPK83sEU2MEYvrD7ehI0Wff EcrQCroT1i2x2ajBkQ/4TVge2F9KHgiiKfgEG8saqdgTgwq3wP6UPGTMwgdMIlAX AN16kAibmTOZ4Kx+yqy+roFj919i9uPI998TlXJG85LpjqsX+gDoVzKw68F2fw8W Vgl9zHmoBnf765evetN8aJkQ/t2nNkqHiV83LXQ80fdtu52T2lkb6GM9nXN81jNt	

Step	Instruction	Guidance and Examples
	`OiJ3wNKvx2hkOJqEs+p9ESI8IiNxjPyjdk5V9VlIl65W0WO1WfrT0qur5NhdZsl+nQPiHsyW3apD4+IJzI2nGQfeL4XO6MPUPVvn+7TiduFaCe+TXJQW` 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.	
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. It is normally the SP of the service who should indicate that multifactor authentication is required and with which technology.	See e.g. How do I actually use the REFEDS MFA Profile to request MFA?, Requiring Multi-Factor Authentication, Configure a Service Provider for Two-Factor Authentication and Multi-Factor Access for further information and SP configuration examples. For FIDO U2F, the authentication class (AuthnContextClassRef) is called: `https://refeds.org/profile/mfa` For TOTP, the authentication class (AuthnContextClassRef) is called:

Step	Instruction	Guidance and Examples
	Important: • that the SP of the service only indicates **one** preferred technology for multifactor authentication in login requests! The Joint Web Login service currently has no way of knowing which technology/technologies are supported for a given user. • that the SP of the service **verifies** that multifactor authentication was performed and with the correct technology! See `require authnContextClassRef` in the examples. • that the SP of the service **prevents manipulation** of login requests so that the multifactor authentication requirement cannot be circumvented! Turn on signing of login requests in the SP of the service and add `<SPSSODescriptor AuthnRequestsSigned="true" ...>` to the service metadata. The Joint Web Login service will then require all login requests to be signed by the SP of the service.	`urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken`

5 Metadata

Step	Instruction	Guidance and Examples
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.	Examples of metadata for *other* services can be found at 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.

Step	Instruction	Guidance and Examples
	See the SP software documentation for details.	
2	**Supplement with user information** 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.	See SWAMID SAML WebSSO Technology Profile (section 6.1.12–6.1.13 Metadata Extensions for Login and Discovery User Interface (MDUI)) for formal requirements. See Service Provider Metadata Extensions for Login and Discovery User Interface (MDUI) for examples See Service Provider Privacy Policy Template for the appropriate template to use for the service usage and personal data handling page.
3	**Supplement with contact information** Contact information is needed so that responsible persons can be reached.	See SWAMID SAML WebSSO Technology Profile (section 6.1.21 Organization samt 6.1.22–6.1.27 ContactPerson*)* for formal requirements. See Contact and Organization information for Service providers for examples.
4 If DS	**Supplement with special tag for DS** When selecting the higher education institution (DS), you must supplement the service metadata with a tag `<DiscoveryResponse>` inside the tag `<SPSSODescriptor> and <Extensions>.` This is a security feature to prevent arbitrary web pages from misusing institution selection and tricking the user after login. 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.	See Identity Provider Discovery Service Protocol and Profile (section Use of Metadata*)*, for information on this security feature. See Enabling OpenAthens Wayfinder: Shibboleth for illustrative examples of how this configuration can be done. See Redirect to SSO Service at the IdP for general information on how the web flow works when selecting the institution (DS).

Step	Instruction	Guidance and Examples
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.	

6 Publication of Metadata

Step	Instruction	Further Information
1	**Verify metadata before publishing**	

Step	Instruction	Further Information
	Check that your SP and service metadata meet all the requirements in SWAMID SAML WebSSO Technology Profile (section 6 Operational Requirements for Relying Parties*)*.	
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) via the SWAMID metadata tool. Metadata tool login is done 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 in order for the publication to be performed.	For further information on the metadata tool and its use, please contact 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 and ask to be put in touch with the operators of the Joint Web Login service.