Shibboleth SP security checklist

--- This page is a work in progress! ---

A basic tutorial for setting up a Service Provider (SP) with Shibboleth is already provided in this wiki. When enabling such an SP in a production environment, security of the Shibboleth setup becomes important. Below you can find a checklist that enables an SP to review it's security setup with Shibboleth.

> Note that Shibboleth and it's security depends on other components like a HTTP server, the Operating System, Firewalls, Network Infrastructure, etc. Specific security measures for these components is outside of the scope of this checklist.

1. Use the latest Shibboleth software. What the latest version is can be found here on the Shibboleth wiki
2. Follow the Shibboleth security advisories and/or subscribe yourself to (at least) the Announcements mailing list. This will ensure you are kept up-to-date on the latest security issues in Shibboleth.
3. SAML communication with SURFconext does not support XML encryption but instead HTTPS is used. Use only HTTPS for the Shibboleth URLs and for your application URLs. In Shibboleth, you can force the use of HTTPS by setting the `handlerSSL` to `true` in the Sessions element of `/etc/shibboleth/shibboleth2.xml`. You can use SURFnet's certificate service for requesting the necessary certificates or any other Certificate Authority's services.
4. There is no back-end communication between Shibboleth and SURFconext. This means that only port 443 needs to be accessible on the server where Shibboleth runs.
5. The public certificate and private key necessary for signing the SAML messages can be self-generated. Use a key length of at least 2048 bits. The certificate and key need to be configured in the `/etc/shibboleth/shibboleth2.xml` configuration file, in the `CredentialResolver` element as mentioned here. Never allow anybody to be able to read or otherwise have access to the private key. Make sure to protect your private key on the server's filesystem by only allowing the "root" or "Administrator" user to access it.
6. The communication with SURFconext is based on trust and is implemented out-of-band by exchanging SAML metadata. The SP needs to know for sure that the metadata it receives is from SURFconext and SURFconext must know that the SP's metadata represents the said service. The SURFconext metadata is located on a verified HTTPS location in https://metadata.surfconext.nl/idp-metadata.xml. The SP should also provide its metadata on a verified HTTPS link. This is a standard URL inside the Shibboleth setup.
7. Evaluate the options for limiting a users session time in Shibboleth. These options are set with the `lifetime`, `timeout` and `maxTimeSinceAuthn` attributes of the Sessions element in `/etc/shibboleth/shibboleth2.xml` file. See an explanation of these attributes here.
8. Set the `redirectLimit` option to "exact" or "host" to prevent an open redirect vulnerability in the logout handler with the default configuration.
9. Shibboleth does not support Single Logout. This is also the case with SURFconext. When performing a local logout, please advise your user to close their browser to complete the Single Logout process.