Configuring a Shibboleth SP for SURFsecureID

⚠ This documentation describes how to connect a SP to the SURFsecureID gateway directly. New SP's must connect to the SURFconext gateway.

Request authentication at a specific LoA

An example Apache configuration snippet where a request for a specific URL triggers a SAML request with LoA 2.
The LoA identifier (`http://surfconext.nl/assurance/loa2`) in the example below is specific for the Production environment and the Test environments use different identifiers.

```
<Location /secure>
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    ShibRequestSetting authnContextClassRef http://surfconext.nl/assurance/loa2
    require valid-user
</Location>
```

Below is an example of the resulting subset of environment variables that are set by the Shibboleth SP. You can use these for authorisation purposes in your application.

```
[Shib-Application-ID] => default
[Shib-Session-ID] => _77421bdf5f17e10c70efb9a89aa3737e
[Shib-Identity-Provider] => https://sa-gw.surfconext.nl/authentication/metadata
[Shib-Authentication-Instant] => 2013-10-29T22:08:46Z
[Shib-Authentication-Method] => http://surfconext.nl/assurance/loa3
[Shib-AuthnContext-Class] => http://surfconext.nl/assurance/loa3
[Shib-Session-Index] => c8a493e33432686feb5cc683a9fd0c7c
[persistent-id] => https://sa-gw.surfconext.nl/authentication/metadata!https://my-sp.example.com
/shibboleth!urn:collab:person:surfnet.nl:john
```

Note that a LoA2 authentication was requested, yet the user was authenticated at LoA3.

Security

You can only rely on the value of `Shib-Authentication-Method` or `Shib-AuthnContext-Class` when `Shib-Identity-Provider` is indeed the `EntityID` of the SURFsecureID IdP. For Production that is `https://sa-gw.surfconext.nl/authentication/metadata`, the other SURFsecureID environments use different `EntityIDs`.

Note that when your Shibboleth SP trusts other IdPs in addition to the SURFsecureID IdP (e.g. the normal SURFconext IdP, `https://engine.surfconext.nl/authentication/idp/metadata`). Shibboleth will by default accept unsolicited assertions as used in the IdP-initiaded SSO flow. This means that an IdP can login without the SP having first created an authentication request. We recommend that you **always verify** that the `EnityID` of the IdP is the one you expect for each authentication, e.g. by verifying the value of `Shib-Identity-Provider`.

More info

- Configuring a Shibboleth SP for step-up authentication
- Connecting a Shibboleth SP to SURFconext