3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTFI

Check for SWAMID Assurance Profiles (Swedish users)

SWAMID has three defined levels of assurance, SWAMID AL1 (http://www.swamid.se/policy/assurance/al1), SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) and SWAMID AL3 (http://www.swamid.se/policy/assurance/al3).

All by SWAMID approved assurance levels for an Identity Provider are defined in the SAML metadata as a SAML extended attribute *urn:oasis:names:tc:SAML:attribute:assurance-certification*. The assurance certification attribute in metadata defines what assurance profiles the Identity Provider and its home organisation has been approved for or has declared that they fulfill.

The Identity Provider uses the attribute *eduPersonAssurance* (urn:oid:1.3.6.1.4.1.5923.1.1.1.11) to assert the logged in user's assurance profile. Please observe that the Identity Provider must not indicate any other assurance profile than it's approved for. Signaling the user's assurance profile via the attribute eduPersonAssurance means that the user validation fulfills all parts of the asserted assurance profile. Attribute mapping for eduPersonAssurance is defined as *assurance* in 3.2 Configure Shibboleth SP - attribute-map.xml.

- An Identity Provider that *has* an assurance certification in metadata for SWAMID AL3 (http://www.swamid.se/policy/assurance/al3) *is* allowed to assert that a user is approved for SWAMID AL3.
- An Identity Provider that *has* an assurance certification in metadata for SWAMID AL2 (http://www.swamid.se/policy/assurance/al2) *is* allowed to assert that a user is approved for SWAMID AL2.
- An Identity Provider that *has* an assurance certification in metadata for SWAMID AL1 (http://www.swamid.se/policy/assurance/al1) *is* allowed to assert that a user is approved for SWAMID AL1.

To check a user's assurance profile, you need to check that the Identity Provider is approved for the same assurance profile as it has asserted for the user. To do this you need to activate extended functionality in the Shibboleth Service Provider. This extension is available since version 2.2.

Expected Web Application behavior for SWAMID Assurance Profiles

If the web application needs to check if a user is approved for an SWAMID Assurance Profile the application needs to check approved assurance profiles for both the user and the used Identity Provider as described in the bullet list in this document.

Please note that this approach only checks that the Identity Provider and the user fulfills the checked assurance profile. To check that the credentials used to log in fulfills the assurance profile is more advanced and needs more configuration of both Service Provider and Identity Provider.

Check for REFEDS Assurance Framework (international users)

Internationally within eduGAIN REFEDS Assurance Framework (RAF) is used send information about the user assurance levels. RAF is different from SWAMID Assurance Profiles, but they are more or less mappable. For Identity proofing SWAMID A1 maps to RAF low (https://refeds.org/assurance/IAP/low), SWAMID A2 maps to RAF medium (https://refeds.org/assurance/IAP/medium) and SWAMID A3 maps to RAF high (https://refeds.org/assurance/IAP/high). REFEDS Assurance Framework is only signaled for users in the attribute eduPersonAssurance (urn:oid:1.3.6.1.4.1.5923.1.1.1.11).

Indication of uniqueness of identifiers is released as separate RAF values. If the identifier attribute eduPersonPrincipalName is used to identify the user and the identifier is unique for a specific person and will never be used for another person, eduPersonAssurance includes the value https://refeds.org/assurance/ID/eppn-unique-no-reassign. If the newer SAML V2.0 Subject Identifier Attributes Profile Version 1.0 attributes subject-id or pairwise-id is used to identify the user and the identifier is unique for a specific person and will never be used for another person, eduPersonAssurance includes the value https://refeds.org/assurance/ID/unique.

Expected Web Application behavior for SWAMID Assurance Profiles

If the web application needs to check if a user is approved for a REFEDS Assurance Framework claim the application needs to check approved assurance values for the user.

Please note that this approach only checks that the Identity Provider and the user fulfills the checked assurance claims. To check that the credentials used to log in fulfills the assurance profile is more advanced and needs more configuration of both Service Provider and Identity Provider.

Check for REFEDS SIRTFI

"*The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant.*" The purpose with REFEDS SIRTFI (https://refeds.org/sirtfi) framework is to add trust based on a defined Best Current Practice on incident response and operational security.

All Identity Providers that has declared that they follow the REFEDS SIRTFI framework are defined in the SAML metadata as a SAML extended attribute *urn:oasis:names:tc:SAML:attribute:assurance-certification*. The assurance certification attribute in metadata defines what assurance profiles the Identity Provider and it's home organisation has declared that they fulfill or has been approved for.

Service Providers can also via metadata declare that they fulfill the REFEDS SIRTFI framework and that gives the Identity Providers added trust in that the Service Providers fulfills the same Best Current Practice.

Expected Web Application behavior for REFEDS SIRTFI framework

If the web application need to check if an Identity Provider has declared that they fulfill the security framework REFEDS SIRTFI the application needs to check approved assurance profiles the Identity Provider metadata. The web application may also use a filter in the Discovery Service that narrow down the shown Identity Providers to only those who fulfills the framework.

Get assurance profiles from metadata in the Shibboleth Service Provider

Activate Metadata Attribute Extraction for Identity Provider metadata

To get the approved assurance profiles from metadata you need to activate the Metadata Attribute Extraction extension in Shibboleth SP. This is done by extending the ApplicationDefaults tag in shibboleth2.xml by adding *metadataAttributePrefix="Meta-"* after REMOTE_USER="...", see example. This is a standard example in the file example-shibboleth2.xml in later versions of Shibboleth SP. It is also included in the SWAMID Configure Shibboleth SP - SWAMID-shibboleth2.xml

Example ApplicationDefaults in shibboleth2.xml

```
<ApplicationDefaults
    entityID="https://example.com/shibboleth"
    REMOTE_USER="eppn persistent-id targeted-id"
    metadataAttributePrefix="Meta-">
```

Important information

Please note that you may get to many headers after activating this extension. If you do, please remove all unused attributes from attribute-map.xml or modify backend header limits (LimitRequestFields/LimitRequestFieldSize in Apache HTTPD Server, maxHeaderCount/maxHttpHeaderSize in Apache Tomcat Connectors).

Define metadata assurance certification attribute

Next step is to make approved assurance levels available in the application. This is done attribute-map.xml the same way as normal Identity Provider asserted attributes. It is also included in 3.2 Configure Shibboleth SP - attribute-map.xml

Definition of metadata assurance certification attribute in attribute-map.xml

```
<Attribute name="urn:oasis:names:tc:SAML:attribute:assurance-certification" id="Assurance-Certification"/>
```

After the activation of Metadata Attribute Extension and the attribute definition all Identity Provider approved assurance profiles are available in the multi-valued attribute *Meta-Assurance-Certification*.