RAF pilot final report

Background

The goal of the pilot was to get practical experience on REFEDS Assurance Framework (RAF) and Single-Factor Authentication (SFA) profile, including the content of the specifications and how they can be deployed using existing SAML products. See pilot charter for details on the pilot goal.

The pilot took place between February and May 2018 and reflected the RAF and SFA specifications that REFEDS exposed to the public consultation in May 2018.

IdPs and SPs in the pilot

In the pilot, a small number of SAML SPs/IdPs were configured to issue/receive authentication requests/responses and eduPersonAssurance attributes according to the REFEDS MFA profile and the latest drafts of the REFEDS SFA profile and REFEDS Assurance Framework.

Following SAML Identity Providers participated in the pilot:

- The University of Chicago (Shibboleth IdP)
- XSEDE (Shibboleth IdP)
- Aalto university (Shibboleth IdP)
- CSC - IT Center for Science (Shibboleth IdP)

Following SAML Service Providers participated in the pilot:

- ELIXIR (SimpleSAMLphp)
- EGI Check-in (SimpleSAMLphp)
- CILogon (Shibboleth SP)
    - in the pilot, CILogon didn't request an authentication context but observed what the IdP delivered.
- SWITCHaai attribute test (Shibboleth SP)

IdP/SP test matrix

ePA = eduPersonAssurance tested and works
SFA = SFA tested and works
MFA = MFA tested and works

IdP SP	Chicago	XSEDE	Aalto	CSC
ELIXIR	ePA/SFA/MFA	ePA/MFA	n/a	ePA/SFA/MFA
EGI Check-in	n/a	n/a	n/a	n/a
CILogon	ePA/SFA/MFA	ePA/MFA	n/a	ePA
SWITCHaai	ePA/SFA/MFA	ePA/MFA	n/a	ePA/SFA/MFA

For the pilot, Aalto and EGI used test providers which were not exposed to eduGAIN and couldn't be tested with the others.

Findings on IdP products

The participating Shibboleth IdPs were successfully configured to handle the authentication context requests/responses and release eduPersonAssurance attribute to the SP. See configuration examples for details.

No SimpleSAMLphp installations participated directly as an IdP in the pilot but the ELIXIR SP was a SimpleSAMLphp based IdP/SP proxy deployment that successfully acted also as an IdP for its downstream SPs.

No ADFS IdP installations participated in the pilot. Some parallel studying on ADFS as SAML IdP revealed that RAF support is straightforward (because it requires just supporting the custom eduPersonAffiliation attribute and values) but supporting REFEDS SFA, MFA or any other custom AuthenticationContextClassReference is cumbersome because by default ADFS supports only a pre-defined set of authentication contexts.

IdPs releasing the eduPersonAssurance attribute

For the roll-out of the RAF, attention needs to be paid for making sure the IdPs actually release the eduPersonAssurance attribute to the SPs. The REFEDS community should consider adding the eduPersonAssurance to the R&S attribute bundle.

The same applies to OpenID Connect protocol. In the current draft eduPersonAssurance belongs to the same scope with the other eduPerson Attributes.

Conclusions

The main challenge of REFEDS Assurance Framework and SFA/MFA configuration is in the Identity Provider side which needs to be configured properly to populate the eduPersonAssurance attribute and SFA/MFA authentication context handling.

Shibboleth IdP (and SimpleSAMLphp in a limited proxy setup) was found capable of supporting RAF, SFA and MFA.