Pilot on RAF and SFA

Goal

To get practical experience on REFEDS Assurance framework (RAF) and REFEDS Single-factor authentication (SFA) profile, including

- any remaining vagueness or obscurity in RAF and SFA specifications
- any issues with deploying the RAF and SFA specifications on existing SAML products

The pilot will

- deploy the RAF and SFA specifications to a handful of SAML IdPs and SPs exposed to eduGAIN from different federations. If an IdP can deliver REFEDS MFA, it should be deployed as well to support REFEDS Espresso.
- feed the pilot findings to the 1.0 release of the specifications.
- present the final report in the REFEDS meeting in June 2018.

The intention is to keep the pilot small and agile (to minimise the logistics) but have a good representation of SAML implementations.

Draft RAF specification and SFA specification suite is in the working group main page. REFEDS MFA v 1.0 is here.

Pilot steps

Steps for IdPs in the pilot

1. Read the RAF specification carefully and identify to which RAF assurance values the end users in the IdP would qualify
2. Read the SFA and MFA specifications and identify which profile the IdP can satisfy (at least for some users)
3. Decorate (at least some) end user accounts in the back-end IdM system with values found in (1). If all user accounts qualify to a particular value, the configuration can be done in the IdP server, too.
4. Configure the SAML IdP to process the incoming Authentication context class reference requests, carry out the authentication as requested (or provide a proper error message) and deliver the proper Authentication context class reference and eduPersonAssurance attribute values in the response

Steps for SPs in the pilot

1. Read RAF, SFA (and MFA) carefully and deciding which RAF assurance values are interesting for the SP
2. Configure the SP to request the SAML authentication context(s) from IdPs and observe/act on the values received.

For both IdPs and SPs it is also necessary to participate in the coordination and reporting of the pilot. In practice, it means

- biweekly coordination calls
- publish relevant IdP/SP server configurations
- contributing the findings to a final report

Pilot IdPs and SPs

Following IdPS have shown interest in the pilot

- The University of Chicago (urn:mace:incommon:uchicago.edu, InCommon federation), Shibboleth, supports R&S
- XSEDE IdP (https://idp.xsede.org/idp/shibboleth, InCommon federation), Shibboleth, supports R&S
- Aalto university (https://idp.aalto.fi/idp/shibboleth, Haka federation), Shibboleth, supports GEANT CoCo
- CSC - IT Center for Science (https://idp.csc.fi/idp/shibboleth, Haka federation), Shibboleth, supports GEANT CoCo

Following SPs have shown interest in the pilot

- ELIXIR (https://login.elixir-czech.org/proxy/, eduID.cz), SimpleSAMLphp based IdP/SP proxy, serving the ELIXIR research infrastructure AAI, claims REFEDS R&S and GEANT CoCo
- BBMRI (https://login.bbmri-eric.eu/proxy/, eduID.cz), SimpleSAMLphp based IdP/SP proxy, serving the BBMRI research infrastructure, claims REFEDS R&S and GEANT CoCo
- EGI Check-in (https://aai.egi.eu/proxy/module.php/saml/sp/metadata.php/sso, GRNET), SimpleSAMLphp based IdP/SP proxy, serving the EGI e-infrastructure, claims REFEDS R&S
- CILogon (https://cilogon.org/shibboleth, InCommon federation), Shibboleth based SP, serving the CILogon service, claims REFEDS R&S