LOA for Research and Education Federations

One of the questions that has arisen from discussions on Level of Assurance for Identity Federations in the R&E sector has been the need to establish what the 'baseline' common practises are for federations in this space today. At the moment, there is no standard for what this assurance might mean when dealing with cross-federation use cases. This work attempts not to define the equivalent of an LOA1 in any standard space, but an unspecified REFEDS Assurance Profile that can be met by all existing federations.

This work draws heavily on work already undertaken by SWAMID and on the Kantara Identity Assurance Framework Service Assessment Criteria.

Contents

Why do this?

It could be argued that REFEDS is duplicating the work already being pursued by many other organisations with an interest in identity assurance, and that federations could simply sign up to and use these schemes. What we have found is that there are several barriers to such adoption:

1. There is no commonly accepted definition or understanding of the current base level of assurance within R&E identity federations, and this is impacting on progress in areas such as interfederation with our own sector.
2. The overhead for each federation to do the work to meet an existing assurance scheme is prohibitive.
3. The costs of engaging with established schemes for many federation is prohibitive.
4. The strict 1 - 4 'levels' approach does not necessarily match the needs and requirements of existing identity federations well.
5. The overheads and costs are unnecessary to meet and assert the general equivalent of a 'level 1' assertion.

The REFEDS work proposes that R&E federations undertake some joint work to get our own houses in order first, meaning we will be able to move forward and engage with stronger assurance profiles more effectively as a group. The work on a REFEDS assurance profile is intended to be:

- Reasonably lightweight.
- Rely on self assertion by federation operators and identity providers.
- Have no charges associated with it.
- Focused on establishing the current norms of assurance behaviour in identity federations.

What does this assurance profile mean?

As stated above, this work explicitly ignores any mapping to assurance 'levels' used in a variety of standards work. It sets out to find a common baseline assurance profile for identity federations. SWAMID have suggested that such a profile could be interpreted as follows:

- The subject is probably affiliated with a federation member.
- The subject is very likely a human and not a robot or piece of software.
- The subject is most likely identified by a (unique permanent) user identifier.

It is clear that for all federations chosing to assert that IdPs comply with this assurance profile, there would need to be an assessment of the operational practices and standing of the Federation Operator. This will be addressed in the Federation Operator Best Practice Work that will be carried out in conjunction with this work. Federations should also be able to draw heavily on the Federation Policy Best Practise Approach work that has established wording used by federations in policy documents around many of these requirements.

It is suggested that this exploratory work will be further developed and published as formal documents under the REFEDS RFC.

Compliance and Audit

In current operations, most federations assert two things:

- Identity Providers must have an Identity Management Practice Statement (IMPS).
- That the Federation Operator reserves the right to carry out audits.

There is a varying degree of practice as to whether the Operator actively checks the existence of the Practice Statement and when, what the Practice Statement contains and looks like, and what audit requirements are. It is suggested that by claiming an IdP meets the requirements of the REFEDS Assurance Profile, the Federation Operator will be required to:

- Ensure the IMPS is in place before accepting a member.
- Carry out annual checks against the IMPS by asking IdPs to self declare they are compliant.
- Use a standardised IMPS document that will be defined as part of this process.

Comparing with Kantara

Where possible, it is proposed the work use the headings defined in the Kantara Identity Assurance Framework to make future mapping an easier exercise. * See the simplified spreadsheet of the LOA requirements for the Kantara Assurance Framework.

Kantara uses the following criteria headings within its service assessment criteria:

Organisational Service Criteria

The purpose of this section is to define conditions and guidance regarding participating organisations responsibilities.

1. Enterprise and Service Maturity;
2. Notices and User Information;
3. Information Security Management;
4. Security-relevant Event Records;
5. Operational Infrastructure;
6. External Services and Components;
7. Secure Communications.

For the Kantara equivalent of an LOA 1, Kantara expresses requirements only in sections 1,2 and 7 above however most identity federations already support requirements in other sections. It is clear that the current 'level' of R&E federations is somewhere between a Kantara defined LOA1, and LOA2.

Operational Service Criteria

The purpose of this section is to ensure safe and secure operations of the service.

1. Credential Operating Environment;
2. Credential Issuing;
3. Credential Renewal and Reissuing;
4. Credential Revocation;
5. Credential Status Management;
6. Credential Validation/Authentication.