Federated Privilege and Access Management

Intended Audience: *here's what you want to get done, here are the issues*

What are the things that people need to get done to tackle these issues?

- Are we still at a point where we have lots of local solutions, but not enough experience to identify best practices?
- Support targeted-id from your IdP, using a database, rather than a dynamically generated hash.
- SPs should be ready to support targeted-id if eppn is not present.

What are the issues related AuthZ that are raised by federated authentication?

- Unlike traditional internal oriented applications, federated application may not be pre-provisioned with information about the users of the application. The first time a person uses the application is the first change that the application gets to learn anything about the user. The user is unlikely to appear in a local domain's LDAP directory. The privilege assignment must be done dynamically, based upon the attributes presented by the remote IdP or other third parties.
- In some cases we may not have a simple subject which can be added to groups. For example, the IdP might not be providing a unique persistent identifier to the application. It might only be providing general affiliation or entitlement information.
- How do we communicate to remote IdPs that a group of applications are cooperating applications, for which users should be presenting a single targeted-id, across each of the cooperating applications? What if the cooperating applications are hosted in different enterprises or by different universities?

Federated Use Cases should be collected **here**.

Interesting Projects Tackling this issue:

- OCLC's meta-IdP
- COmanage

Reading materials:

- Surfnet Report on Collaboration Infrastructure