PROTOCOL OFFERINGS FOR SERVICES

Mr. Terry Smith, Australian Access Federation
OVER THE PAST 10 YEARS HIGHER EDUCATION IDENTITY FEDERATIONS SUPPORTED SAML AND ONLY SAML. IN MORE RECENT YEARS THE GROWTH OF OPENID CONNECT HAS RESULTED IN MANY SOFTWARE DEVELOPERS MOVING THEIR PRODUCTS TO THIS NEWER AND GENERALLY SIMPLER PROTOCOL. FEDERATION MUST MOVE TO PROVIDE OPTIONS THAT CAN SUPPORT MORE THAN JUST SAML TO CONTINUE TO BE RELEVANT TO THEIR SUBSCRIBERS. WE WILL DISCUSS INITIATIVES THAT WILL ALLOW YOUR FEDERATION TO PROVIDE MULTIPLE PROTOCOL OPTIONS TO SERVICE PROVIDES WHILE MINIMIZING THE EFFORT AT ORGANISATIONS PARTICIPATING AS IDENTITY PROVIDERS.
Local Accounts

- High overheads
- Credential per service
LDAP

- Many applications used in past, before federation
- Enterprise solution
Kerberos

- On Campus SSO
- SPENGO for Web Applications
- Can be used by Shibboleth IdP (needs to though through)
SAML

- XML based
- Predominantly web based
- Developers find hard to use
- Many applications are already SAML ready
- Not many new applications are choosing SAML

- Many SAS Services offer this in their premium offerings
OpenID Connect

- Preferred by developers
- Authentication and Authorization
- Goes beyond the web
  - Mobile devices
- Many SAS Services offer this in their premium offerings
- Shibboleth Integrations:
Shibboleth OIDC extensions

Two OIDC implementations for the Shibboleth IDP...

- https://github.com/uchicago/shibboleth-oidc
- https://github.com/CSCfi/shibboleth-idp-oidc-extension

The UChicago implementation was done by Unicon on behalf of the University of Chicago (and later the University of Michigan) and it basically embeds MitreID Connect OIDC server (https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server) into the Shibboleth IDP. It's not a tight integration. MitreID maintains its own session store completely independently of the IDP, and we found it didn't work well with our clustering configuration. The attributes available via OIDC are also limited to the standard claims defined in OpenID Connect Core 1.0, and the mappings between the SAML attributes that are used to populate those claims are "hard" - they are located in java source code, so to change them, you'd need to recompile the extension. If you have a single IDP, and don't need anything beyond the standard claims, it works ok.

The CSCfi implementation was sponsored by GEANT. It is a "from the ground up" implementation. While it depends on the "Nimbus OAuth 2.0 SDK with OpenID Connect Extensions", this was written as an extension to the Shibboleth IDP from the very beginning. It is much more tightly integrated - they use common session storage, new claims and scopes are easily defined in using the native attribute resolver and filter mechanisms, and there is an excellent chance that this code will eventually be adopted as into the Shibboleth IDPv4 distribution. We've been very happy using this extension.

Reference: Email on Shib Users users@shibboleth.net from Liam Hoekenga liamr@umich.edu
WebAuthn

- New browser authentication
- MFA built in
Multi-Factor

- REFEDS Work Package

- Is becoming a requirement for service
  - Attempt to reduce the amount of account theft