OPTIONS FOR IDENTITY PROVIDERS

Mr. Terry Smith, Australian Access Federation
THERE ARE MANY OPTIONS AVAILABLE FOR ORGANISATIONS TO USE AND CONNECT AN IDENTITY PROVIDER TO A HIGHER EDUCATION IDENTITY FEDERATION. THESE INCLUDE OPEN SOURCE, VENDOR OPTIONS AND SOCIAL IDENTITIES. AS A FEDERATION OPERATOR YOU WILL BE EXPECTED TO SUPPORT THESE CONNECTIONS. TO SUSTAINABLY BE ABLE TO SUPPORT THESE CONNECTIONS IT MAKES SENSE TO LIMIT THESE OPTIONS TO A FEW AS POSSIBLE. IN THIS SESSION WE WILL DISCUSS STRATEGIES TO HELP ENSURE YOUR ORGANISATIONS DEPLOY SOFTWARE THAT YOU AS THE FEDERATION OPERATOR WILL BE ABLE TO SUCCESSFULLY SUPPORT.
Why SAML?

- It’s just a protocol!
- Been around for 10+ years
- Developed for the federated identity use case
- Developed for the Web
- Strong support in the Higher education and research sectors
- Global community
Alternative protocols...

- **LDAP**
  One of the oldest and most durable authentication protocols, LDAP has been an industry standard since the mid-1990s. Good for access to a local or enterprise Identity store.

- **Kerberos**
  Invented at MIT, Kerberos has been used extensively under the covers by Microsoft as the authentication protocol for Windows and Windows related systems.

- **RADIUS**
  Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol primarily used by network services such as wireless networks, VPNs, and network infrastructure equipment. Great for eduroam.

- **CAS**
  Central Authentication Service (CAS) is a legacy single sign-on (SSO) protocol for web applications. The name CAS also refers to a software package that implements the CAS protocol, which is now included in the Shibboleth IDP v3 package.
More alternatives

- OAuth 2.0
  OAuth 2.0 is an authorization framework, not an authentication protocol. OAuth 2.0 can be used for a lot of cool tasks, one of which is person authentication.

- OpenID Connect
  OpenID Connect is a “profile” of OAuth 2.0 specifically designed for attribute release and authentication.
  - Developers seem to prefer this protocol – simpler for Service providers
  - Uses JSON in place of XML
  - Works well with non-web applications – mobile devices
  - Includes Authorization
  - OpenID Connect federation standards under development

- WebAuthn
  The new W3C Specification Web Authentication. WebAuthn is supported in the Chrome, Firefox, and Edge browsers to different degrees, but support for credential creation and assertion using a U2F Token, like those provided by Yubico and Feitian, is supported by all of them.
Shibboleth IdP

- Reference implementation of SAML
- Federation IdP
  - Metadata consumption
  - Entity categories
  - Attributes (eduPerson)
- Highly configurable – mesh / hub & spoke / eduGAIN / MFA / SPNEGO
- Extensible

- Global community
- Support for CAS
  - Off loads auth to CAS
  - As a CAS v2 IdP
- OpenID Connect IdP (Planned)
- Java based
SimpleSAMLphp

- Simple to install and configure
- Used widely
  - particularly where there is strong community support for PHP
- Good support for the SAML standards
- Can offload authentication to CAS
- Multiple back end authenticators
Go with your strengths

- As a federation operator you will be supporting your subscribers
  - Most of the difficult support tickets will come from your IdPs
- An IdP that is down can
  - affect thousands of users
  - Become a reputational issue for the organisation
- Pick one IdP Software stack
  - Develop your skills in supporting it
  - Encourage / incentivise organisations to use the select stack
  - Be aware of alternatives and your reasons why the selected stack is the way to go
Commercial offerings

- Does the IdP meet the requirements of the SAML V2.0 Interoperability Deployment Profile?
  - https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

- Your members might have some commercial product that claims to “Supports SAML 2.0”
  - Why can’t the just use that?
Building bridges

- Between your Supported IdP and Commercial offerings
  - So the user perceives SSO (even though multiple systems are in play)

- Between SAML and other protocols
  - Allow Service providers to use their protocol of choice
  - Keeping things as simple as possible for your IdPs
    - Deploy SATOSA, Keycloak, or a similar proxy