Federating Software Considerations

Scott Cantor
Shibboleth Consortium

Requirements / Use Cases

- Technical Platform / Skill Set (*)
  - Customizability / Integration
- Technical Support Requirements
- Federation Use Cases
  - Single/limited purpose
  - B2B
  - Research Collaboration
  - At scale

Shibboleth

- Java Server technologies / XML-based config
- Extensibility, integration, features, standards compliance emphasized over ease of use
- Open source with the most responsive free support anywhere, few relevant commercial support options
- Focused on federation at scale while maintaining rigorous trust model

SimpleSAML.php

- LAMP technologies
- Decent feature coverage, less advanced configuration than Shibboleth
- Support for non-SAML protocols like OpenID Connect, well-suited to gateways
- Open source, some commercial support of unknown value
- Supports scalable federation but hitting scaling issues on large federation metadata files

ADFS

- Microsoft gateway add-on to Active Directory, black-box from a technology point of view
- Good integration with AD, less flexibility in other respects, customizing requires Powershell
- Ok SAML coverage, many proprietary WS-Trust/WS-Federation features that are mostly dead-ending
- “Free” with Server licenses
- Support not well-regarded
- Suited to B2B or single-purpose deployments, requires extensive customization to handle metadata-based federations

Ping / OIF / Novell AM / Others

- Commercial federation gateway products, usually Java-based but GUI-drivem
- Good AD and LDAP integration, generally not as well-suited to other requirements
- Good SAML coverage, usually support other technologies like WS-* or OpenID Connect
- Generally five-figure price tag, OpenAM excepted
- Suited to B2B or single-purpose deployments, very limited support if at all for metadata-based federation at scale (though Ping is talking about it of late)

ForgeRock

- Open Source forks of Sun's IDM products (pre-buyout), Java-based
- OpenAM has good SAML coverage, overall product suite very broad
- Commercial support and security releases available from ForgeRock via subscription, price unknown
- Suited to B2B or single-purpose deployments, very limited support if at all for metadata-based federation at scale

Why Metadata Matters

- Third-party certification of information
- Change management
- Algorithm agility
  - Prediction: SHA-1 falls within the decade
  - Less likely prediction: RSA falls within two
- Revocation