Shibboleth Consortium Update

Ian Young, channelling Scott Cantor

Legacy Product Note: OpenSAML

- Noted during comment injection investigations many products still refusing to get off OpenSAML 2

- Recent issues did not directly implicate the Java library but if they had all those stacks would have been forced to fork or find some workaround.

- ¯_(ツ)_/¯

- We have taken additional steps to warn people off using OpenSAML alone and have removed it from the Products list on the web site.

Project Accomplishments

- Second half of 2017 devoted to IdP V3.4

- First half of 2018 devoted to SP V3 and preparing for changes to the Java platform release process and pace
  - https://wiki.shibboleth.net/confluence/display/DEV/Product+Platforms

- Completed setup and rollout of new support tools for paying members
  - Community has stepped up handling of casual questions on list, good to see

- Proper SP package mirroring provided, seeking mirrors with only 1-2 takers so far

IdP Update

- Couple of security patches delivered over previous 12 months
- Work on 3.4 interrupted by SP (yes, we still need more diversified resources) but is probably 75% done
  - Deprecation warnings in place in preparation for V4 changes, publicly enumerated in wiki
  - https://marc.info/?l=shibboleth-users&m=152692023016531&w=2
- See JIRA for summary of features and outstanding work
  - https://issues.shibboleth.net/jira/issues/?filter=12173
- Delivery no later than end of 2018, aiming for Q3

What's in IdP v3.4?

Around 140 issues so far:

- HSTS (HTTP Strict Transport Security) support

- Metadata-driven configuration (ref. TIER/Unicon GUI)

- Probably, MFA improvements

- Probably, OpenID Connect assists

- Deprecations. Did I mention the deprecations?

SP Update

- V3 is now in public beta:
  - https://wiki.shibboleth.net/confluence/display/SP3/ReleaseNotes
- Documentation moved to dedicated SP3 wiki space and some cleanup is done, likely will have to extend into 2019 as time permits
- Compatibility is near 100%, upgrading should be no different than previous V2 patches
- Notable impacts:
  - Dropping Solaris, nominally dropping Windows desktop OS support
  - Officially dropping support for pre-2.2 Apache, code still maintained
  - Windows package omits FastCGI binaries (no thanks to owning the fcgi library there)

What's in SP v3?

- Defaults to SHA-256 for DSIG; other crypto tightening.
- SAML 1.1 support and support for attribute queries not enabled by default for new installs.
- Better IIS7 support
- Stateless Clustering
- Simplified Virtual Hosting Support
- Dynamic Metadata support enhanced
- Administrative Logout

Project Roadmap

- Looking at some additional developers with financials stabilizing

- Focus will shift to IdP V4 in 2019, delivery likely in 2020, probably based on Java 11, Spring 5

- Outreach topics:
  - OpenID Connect work by ~~GEANT project~~ Team Finland, certainly a candidate for V4 inclusion
  - GUI for TIER by Unicon
  - Coordinating with outside packaging teams to extend SP support to e.g., Debian

Questions?