2019-03-15

Shibboleth Developer's Meeting, 2019-03-15

Call Administrivia

09:00 Central US / 10:00 Eastern US / 14:00 UK / 16:00 FI

Calls are normally the 1st and 3rd Fridays of each month. Next call would be Friday 2019-04-05. Any reason to deviate from this?

60 to 90 minute call window.

Call Details

This week's call will use the Zoom system at GU, see ZoomGU for access info.

AGENDA

1. Duration (or Instant/DateTime) parsing - JAXP vs. java.time

Attendees:

Brent

- **OSJ-265** - TLS socket factory clears client TLS credential too early `CLOSED`
    - Unless we (really) bind our rules, tentative plan would be to do a new **minor** release of java-support 7.5.0, and a patch release of java-opensaml (and possibly java-identity-provider). Concerns?

Daniel

- **OSJ-269** - JPA StorageService fails badly with case-insensitive tables `CLOSED`
    - Fighting with standing up MySQL for testing
- **IDP-1357** - java11 NPE with ldap configuration (Thread local SslConfig has not been set), works fine in 1.8.0_191-b12 `OPEN`
    - Testing system properties
    - Guiding some development for ldaptive 2.0

Henri

- Finishing OIDC flow-tests, polishing, ...
- Aiming at releasing the first official OIDC plugin version before end of March

Ian

- Maven version now enforced: **JPAR-118** - use Maven enforcer instead of prerequisites element in parent POM `RESOLVED`
    - Replaces older `prerequisites` element, so enforcing version 3.3.1
    - 3.3.1 was 2015-03-18, so five years ago.
    - I'd like to enforce something newer in the interests of consistent builds.
    - Maven versions: https://maven.apache.org/docs/history.html

Marvin

Phil

- Work on IDP-1191.
    - Since servlet spec 3.0 (session tracking config is a bit more standardised since 3.0), setting session tracking mode to COOKIE (and only that) in web.xml, should not expose jsessionid unless bug. This is already being set by the IdP.
    - Not sure the impact of stolen JSESSIONID, ship_idp_session is more a form of ambient authority. Although is used by webflow for conversation state and shib session manager internals (needs more looking into)

- Looked at the potential to steal cookies with injected JavaScript - unlikely - although httpOnly bypasses have existed in the past. Also injected script could steal any anti-csrf token if used - but can not see how JavaScript could be injected into the views (dynamic stuff is being escaped).
- Will look at anti-csrf token - and or the impact of session surfing, as not sure how useful that is.
- Will write something small up unless somebody tells me I am wasting time.

Rod

- Out for much of last week.
- Working through deprecations in custom schemas

Scott

- LDAP test behavior works under Maven now, still get failures during "whole package" testing under Eclipse
- **JSPT-79** - Review date and time handling for Java 8 IN PROGRESS
    - Most uses of @Duration now gone, some long APIs left to clean up
    - Possible future work item: a standardized Spring context for tests to match runtime environment
- Next up is ProfileConfig API consistency/cleanup

Tom

- Wrangling Jenkins, Java. Still having trouble with Java 11 and Windows

Other