2013-04-05

Shibboleth Developer's Meeting, April 5, 2013

Attendees: Bill Thompson, Brent, Daniel, Ian, Marvin Addison, Rod, Scott, Tom

Call Administrivia

Next call is next Friday.

60 to 90 minute call window.

Brent

- Researched current JSR-223 support in various scripting languages supported today by the IdP
- Self-education about the Java release process and Maven config, setting up my build environment and server access
- Today/Next week:
    - Close out a couple of remaining Jira issues
    - Draft of security advisory for HttpClient socket factory issue.
    - OpenSAML v2 release - target next Wednesday 4/10

Probably build on Linux VM.

Next release will ship without JSR-223 scripting engines due to lack of activity in those projects, we will now rely on built-in Java 6 support (Rhino).

Will finish v2 work, then circle back to v3 refactoring.

Daniel

Taking longer than expected to port spring wiring for the LDAP DataConnector.

Yes, Velocity support is needed in the LDAP DC. Revisit Velocity instantiation later.

Will provide a second impl for template tests.

Ian

Release of xmlsectool is downstream of IdP 2.4.0.

Build VM.

Rod

- Finished legacy support for Scripting (enough for the AACLI release anyway)
- Started on configuration for Attribute resolvers:
    - Building 'test framework' as well
    - Making changes to the AttributeResolvers as implicated by the realities of parsing (e.g. <Dependency />)
    - Realized that we will need to do work to build syntax,parsers and implementations of the Criteria. But not for AACLI release.
    - No looking at the DataConnectors
- Plan for next week: More of same, there is probably 2 calendar weeks work in doing the wiring.

AI : Look at JOST-191

Scott

IdP 2.4.0 release next Wednesday, coordinating with Brent.

Looking for feedback and decision regarding Spring neutral Web Flow adaptor.

Looking for feedback regarding recently checked-in storage service alternate coding style.

Some issues with v3 Attribute Resolver Action dependencies on relying party configurations, since Context hierarchy is not complete.

Continued work on v3 AACLI.

Tom

Spent time working on IdPv3 configuration, installation, jetty, etc.

Had trouble with setting initialization parameter via context deployment descriptor and jetty 8 and 9.

[1] http://www.eclipse.org/jetty/documentation/current/configuring-specific-webapp-deployment.html

AI : commit maven-plugin version updates to parent poms after 2.4.0 release.

Topics

Marvin : shibboleth-idp-ext-cas

CAS work consists of two parts : (1) get a ticket and (2) validate a ticket. Initial work done on the first part, what next ? (Authn)

Authentication will be handled by a yet-to-be-determined subflow.

Integration looking good, persistence manager API satisfactory for ticket store.

How long lived are flows? Short (their output is long lived).

Question about Prinicipal Disambiguation. Scott explained the canonical problem (“one true principal”) and persistence (reversible identifiers in SAML, plus clustering).

What is the cardinality between a session and a principal ? One and only one canonical principal per session. When we see two prinicpals we are forced into doing something (kill the old session, fail the authn). This is a critical thing that V2 got wrong and there are a series of issues in there.

Should we talk about how we capture request state. Protocol neutral? Protocol dependant? Base hierarchy with Protocol specific concrete classes. Maybe Marvin start by defining the contexts he needs and see how that works. OK, but what does SAML need? SAML sample flows capture it, in an oblique way. Can we define base context classes with protocol neutral info (motivated by SAML/CAS)?

Understanding the context tree is the critical, and a lot of it ties back to OpenSAML (because of the profiles), not IdP. Equally Security.

Next step is to for Scott and Marvin to coordinate work on authentication.

AI for Marvin: document Context objects needed for authentication.

AI for Scott : Authentication Actions, Contexts, and flows.

AI for Tom : document current state of Action API, inputs and outputs.

Decisions

Coding convention : getLdapUrl or getLDAPURL

Tabled for further discussion.