2013-01-17

Shibboleth Developer's Meeting, January 17, 2013

Attendees: Scott, Ian, Rod, Tom, Brent, Daniel, David Bantz, Mike Grady, Brett Bieber, some lurkers?

Agenda

Project Tracking / Timekeeping (10 min.)

- Project Roadmap

Discussed the Board desire for improved timekeeping on the project and better alignment of reporting by Nicole to what we're spending time on. The two main issues seem to be concern over accounting for time worked by Scott and Brent because we're on university contracts, and the confusion over the differences between reported work areas and the project roadmap. The latter will require working on things with Nicole.

Ian has an issue with using Jira for minute by minute recording but is happy to input aggragated totals at the end of the month. Scott believes aggregation of the numbers is considered important but not day to day totals. The board just wants to see the big picture tracking against the roadmap and micro-management isn't likely, even down to monthly tracking. Quarterly is likely.

Summary: Scott is happy with way the Jira plugin is working. Others (worst case) dump in aggregated time worked. Need to keep Jira aligned to the technical reality of what we're working on.

IdP V2.4 (20 min.)

Scott recapped.

Project goal – need to be able to do an IdP release if we have to.

Scott personally wants to do some more work on the ECP code (in support of GSS work done by Jim Basney). Some new XMLObject providers and small changes to ECP profile code.

What's left:

- Update to xmlsec 1.5
    - DSIG 1.1 ECKeyValue syntax "has issues". Cannot easily roundtrip Java EC keys to XML (and back) Possible in C++ because the curve point syntax is direct fit for a OpenSSL API [which is unavailable in Java Crypto]. Curve names not documented. Brent: some issues with Java6? Scott: Not that I know of, you might be thinking of GCM. DEREncodedKeyValue syntax is available to support encoding EC keys in KeyInfo and can be roundtripped.
    - Scott working on completing KeyInfo processing code and XMLObject providers.
    - Upgraded POMs to xmlsec 1.5: All unit tests pass. Signature API change should not involve us (deprecated IdResolver API but "probably still the right thing to use" since it would be a possibly unsafe change if 1.4 were put back or left in place). Brent concurs.
    - Remove use of API in V3 and have hard requirement for using xmlsec 1.5
- Unicon changes – pending contributor paperwork, will supply patches for NotBefore option, login UI examples, and a proposal from Scott to accomodate injecting custom content into opensaml binding templates. Mike still needs to test whether Velocity #include will work for this.

Aiming for End Feb for external contributions, and March to ship.

IdP V3

New Developer Status (5 min.)

Welcome to Daniel Fisher.

Initial work on LDAP related resolver components, and LDAP testing needs: Unit testing or integration testing? Both, probably unit to start with. Some discussion of testing needs with AD. Virginia Tech might be able to host something, but we have a dedicated VM server at PSU that should be fine for this purpose.

Tom will speak with Daniel about work plans and testing requirements.

Latest on Phil is March availability to help out on WebFlow design and testing, Nicole is following up.

Face to Face Planning (10 min.)

2 half day blocks requested in Arlington in April, Sun/Mon. Shel indicated it would be approved, but no ETA on when will we find out right now. Travel budget right now not an issue for people making meetings, just best use of people's time. Arlington may be optional (e.g. Rod/Ian)

We discussed a more exhaustive meeting earlier – to keep momentum running. Late Feb? Allocate 3 days, use two, with a half if necessary.

After some to & froing we decided Feb 15/16/17 in Columbus. Agenda bashing will be done on the list, but focus will be on assigning design issues to people so they can bring proposals to the meeting for bashing. Scott will circulate details shortly.

OpenSAML V3 (15 min.)

Brent: Messaging related stuff just getting back up to speed. Remaining work is refactoring into new API. The main design work is around the notion of representing message state, fuzzy stuff we know was wrong in V2. Not much impl work, but getting the design right. Brent will pick it up and as he continues refactoring stuff may become more clear. Take to the table in Feb? Conrete details of context hierarchy and message state.

Metadata providers: Less work achieved there so far, Chad's design and that's about it.

Scott: What do we need rather than what do we want (what are the requirements)?
What I ran into trying to do a Dynamic provider was that each new entity cleared the general cache – it screwed the KeyInfo cache for everyone. Not a problem in SP by having the Observable layer signal which provider was changing and cache based on that.

The plan was to not have the cache at all. So we are not caching credentials, but we are caching the ingredients. Does this work? Where does this get done (in the ObjectProvider for the KeyInfo child or try to do it alongside the metadata layer somehow?) Why would the unmarshaller on an instance do the extra work for child entites, it feels icky combining across the hierarchy. Would we not lose some pluggability around KeyInfo processing? Is the compromise to put it into the "metadata" but at the EntityDescriptor level – still same problem but less granular? Loads of open questions. Can we bring this to the table for feb? Probably not enough time of the right sort of people, but maybe.

Scott trying to offload Brent of the grunt work so he can work on the harder parts, will look at porting up the V2 changes since they diverged.

Q1 Deliverables (15 min.)

- Project Planning

3 deliverables

- Attribute Resolver
- Attribute Filter
- OpenSAML design products (see above)

Tom to write up current thinking on the configuration layer. Scott and Rod noted the gap in their knowledge there. Producing an AACLI tool is the end goal. Some discussions on API consistencies and how much work we need to do. Focus would be to put in compatibility for request.principalName any anything else simple that's commonly used in scripts and see what blows up in people's configurations.

Other stuff to work on Pre Feb?

The IDP cannot consume SAML attributes effectively for comparison internally. Analogy to PrincipalConnector and NameID. Do we need a SAMLAttributeDataConnector?

- Hack things as we have done
- Do it properly and port SP AttributeDecoder work into Java (original config for that was partly Chad's to start with)

Open Technical Issues (15 min.)

Discussion on API dependencies. idp modules depending on opensaml-impl is a red flag (all agree). Within a project, api on impl is very bad, impl on impl is probably bad, but may be justifiable (code reuse).

Scott: but if you need to do it, why not make it a public API so others can benefit?

Brent: API vs IMPL is a bit misleading as compared to common Java assumptions about the terms, API is more about "this is what we stand by as non-changing" than "Interfaces only". All: But let's not rename the projects. And what is the contract about "not changing"? Is it a documentation issue?

Scott: Also how much does it matter. "We are building shibboleth, if you can use OpenSAML that's good, but if the documentation isn't enough, sorry".

Brent: issues with making things public for our ease might end up being used by accident. Be careful about making anything public on a base class.

More discussion needed. Do we need a third class of module, non sharable API? We know the IdP depends on the messaging components, so we'll have to tackle the issue soon.

Brent: Complication with factory is that the request state needs to be injected into the messaging objects, but Chad didn't want to use Spring to inject, I'm not so opposed. I think his concern was it would mean Spring using thread local variables. Need to look into this.

Session & storage design? Scott has floated a design and will bring it to the table for February and should have time to work on something else as well, since proposal is largely based on existing work.

Connection Information

Time: 16:30 UTC

Meeting ID: 534-352-638

Web URL: https://www3.gotomeeting.com/join/534352638

Dial-in Phone Numbers
Australia: +61 2 8355 1040
Austria: +43 (0) 7 2088 1400
Belgium: +32 (0) 92 98 0592
Canada: +1 (416) 900-1165
Denmark: +45 (0) 69 91 88 62
Finland: +358 (0) 942 41 5778
France: +33 (0) 182 880 456
Germany: +49 (0) 811 8899 6975
Ireland: +353 (0) 14 845 976
Italy: +39 0 247 92 12 39
Netherlands: +31 (0) 208 080 379
New Zealand: +64 (0) 4 974 7215
Norway: +47 21 03 58 96
Spain: +34 911 82 9782
Sweden: +46 (0) 313 613 558
Switzerland: +41 (0) 225 3314 51
United Kingdom: +44 (0) 203 535 0621
United States: +1 (786) 358-5410