UMA telecon 2014-07-17

UMA telecon 2014-07-17

Date and Time

- **Focus** meeting Thu Jul 17 9-10am PT (time chart)
- Voice: Skype: +99051000000481 or US +1-805-309-2350 (international dial-in lines), room code 178-2540#
- Screen sharing: [http://join.me/findthomas](http://join.me/findthomas)

Agenda

- APAC-friendly meeting schedule status
- Public review status
- Audit ID idea
- Interop prep
  - Feature test status: do they need revisions? which are in scope for "UMA1iop" (V0.9 specs)?
  - Other interop prep
- Review and rationalize GitHub issues
- AOB

Minutes

APAC-friendly meeting schedule status

What do people think of the proposal? General agreement.

**AI:** Eve: Make the new meeting schedule happen and message appropriately.

Public review status

We agreed that the spiral form of the diagram isn't as helpful as the "Gluu paradigm" diagram (second one [here](#)).

**AI:** Domenico: Create SVG version of Gluu diagram for hopeful inclusion in HTML versions of the spec.

In terms of the "draft-hardjono-xxx" naming convention, it's expected to be one or two words plus a version number. So let's do this: Rev the nn version numbers in preparation for submitting the V0.9 versions to IETF once again, but only mention "V0.9" in the abstract and similar text of each doc. The pattern should be "draft-name-oauth-uma-something-nn".

**AI:** Eve: Final V0.9 edits. Mention V0.9 in abstract of claim-profiles. Keep all the IETF keyphrases to two words and change the versioning.

**AI:** Domenico: Create SVG version of delivery vs. redirect flow model for claim profiling spec.

Permissions associated with RPT

Mike proposes that permissions should have a timestamp for the time of creation. Let's focus on this and other substantive questions in the 0.9-to-1.0 timeframe.

**AI:** Mike: Write up the request for permission timestamps.

Audit ID idea

Zhanna would like to have a token that's easily processed for audit purposes, so that all participants in the end-to-end conversation would have the same token. This is her proposed "audit ID". Also, she would like to define what count as auditable events, with reference to Common Criteria. Eve asks: Does the ID need to be made tamper-proof? It could be a string or a JSON structure. Encryption would involve overhead. Eve proposes a signed-by-AS value, which all parties would have to produce and could be verified as coming from the AS.

Jin notes that in healthcare, auditability is standardized for that sector. Something like this functionality would be really welcome. Zhanna points out that Kerberos has a similar idea itself. Many large players, such as Oracle, have welcomed the idea. There are not only medical but also defense etc. requirements. Adrian points to the Accounting for Disclosures standard required by HIPAA in addition; for the ONC pilot, the goal is to provide patients this capability. It would be very helpful to have an audit ID to support AID functionality. The FHIR SecurityEvents spec is relevant here. (We have captured this in issue #63.)

Eve hopes we can capture the "horizontally applicable" parts of auditability in the core spec, and make the mechanism extensible to serve lots of vertical needs. Salt proposes a design distinction: Auditable inside UMA, or auditable outside UMA (instead or in addition)? So this is a question of interoperability with externally used audit systems. Zhanna notes that UMA would still have to generate the relevant events. Does "log" = "audit"? Sal and Jin like the concept of signing. Where might OAuth play a role in this, so that UMA and OIDC could both take advantage?

**AI:** Ema: Capture the latest audit discussion in issue 63.
Interop prep

- Feature test status: do they need revisions? which are in scope for "UMA1iop" (V0.9 specs)?
- Other interop prep

We discussed challenges with testing Gluu's enterprise-use-case UMA implementation. In Mike's case, there's typically no human resource owner. Should we require (or optionally include) dynamic client registration? Mike notes that his implementation supports it.

AI: Eve: Capture issue around how an RS can refer to the policies of multiple authorization servers in getting token status.

AI: Mike: Review the current FTs to see if any of them are problematic for the "UMA for the enterprise" use case.

AI: Eve: Add a mention on the Participants page of the RS's requirement to point to any libraries or SDKs that would assist client components in interacting with the RS.

AI: Mike/Gluu: Fill in their fields in the Participants page for interop.

AI: Eve: Capture issue around including an optional FT for the trust elevation profile, for resolution ASAP.

AI: Eve: Capture issue around expectations for federated SSO, e.g. with OIDC, and with which scopes and claims (identity claims = user claims = RqP or RO claims), into all the various services for interop purposes.

Review and rationalize GitHub issues

Deferred.

Attendees

- Eve
- Casey
- SteveO
- Adrian
- Zhanna
- Mike
- Domenico
- Jin
- Sal

Regrets:

- Mark D

Next Meetings

- **Focus** meeting Thu Jul 17 9-10am PT (time chart)
- **All-hands** meeting Thu Jul 24 9-10am PT (time chart)
- **Focus** meeting Wed/Thu Aug 6/7 at APAC-friendly time? (time chart)
- **Focus** meeting Thu Aug 14 9-10am PT (time chart)
- **Focus** meeting Thu Aug 21 9-10am PT (time chart)
- **All-hands** meeting Thu Aug 28 9-10am PT (time chart)