UMA telecon 2012-01-26

UMA telecon 2012-01-26

Date and Time
- WG telecon on Thursday, 26 Jan 2012, at 9am PT (time chart)
  - Skype: +9905100000481

Agenda
- Roll call
- Approve minutes of 2012-01-12 and 2012-01-19 meetings
- Event planning
  - IIW Satellite event report
  - RSA plans
  - Tweet chat planning
- Interop activity planning
  - Planned F2F interop on April 17 in Munich
  - Cordny progress report
  - Need an interop- or dev-focused mailing list?
  - "UMA in a nutshell" blog post?
- Brief review of non-spec action items
- Work through issues
  - Work on 24/14, 12, 31, 25...
- AOB

Attendees
As of 17 Jan 2012, quorum is 8 of 14.
1. Catalano, Domenico
2. D'Agostino, Salvatore
3. Fletcher, George
4. Hardjono, Thomas
5. Machulak, Maciej
6. Maler, Eve
7. Miles, Arnie
8. Moren, Lukasz
9. Szpot, Jacek
10. Wray, Frank

Non-voting participants:
- Bradley, John
- Cox, Kevin
- Gropper, Adrian
- Nederkoorn, Cordny

Minutes

Roll call
Quorum was reached.

Approve minutes of 2012-01-12 and 2012-01-19 meetings
Deferred due to getting distracted. 😐

Event planning
IIW Satellite event report: Sal, Eve, and George attended. It was NSTIC-flavored. An UMA session was requested, so we covered scope interoperability, and it also came up in the sessions related to profiling of OpenID Connect/OAuth. Eve worked up a nascent Venn diagram comparing features of OAuth, OIDC, and UMA. George's take: The government is keen to somehow enable Facebook as an IdP, even though Facebook has no current plans to be compliant with any of the current or planned SSO profiles.

Facebook announced yesterday that they're changing their offline access policy, so that user authorization is not required to switch from immediate access to offline access (with the token likely good for 60 days). This is being interpreted as negative for privacy, and FB is getting pushback. As part of achieving this, they are extending OAuth to become more proprietary.

RSA plans: There's an OpenID Connect interop on the Friday, when there will be OIX and OpenID board meetings.
**IETF plans:** There’s a room booked for the prior Saturday to do an OIDC BOF. The agenda isn't quite set yet.

**Tweet chat planning:** We should tweet this daily and also blog it. Eve will keep trying to get into the "official" tweet chat Google doc.

**Interop activity planning**

- Planned F2F interop on April 17 in Munich
- Cordny progress report
- Need an interop- or dev-focused mailing list?
- "UMA in a nutshell" blog post?

Let's use the OpenID Connect interop list for coordinating UMA interop activities for now, since we want to focus on OpenID Connect integration heavily, and it will be valuable to get interaction going with the approximately five OpenID Connect endpoint owners. The benefit of a separate dev/interop list is that it doesn't require IPR licensing agreements. We still have uma-dev in reserve if we want to use it later.

Cordny has been working through his test cases from last year and updating them. In many cases, the latest version of the spec has fixed instances of wording that was too vague to test against.

What version to target in interop testing? We should be working off the very latest candidate rev 03 (published last week), and plan to flag any breaking changes that we make in future.

**Work through issues**

Domenico sent a resource aggregation proposal to the list, related to issue #31. There is some discussion on the list. Further discussion today:

JohnB asks Domenico why Scopes are needed for his Financials use-case (in PDF slides) – the point being that you don't necessarily need to ask for the entire (set of) claims again. It's often sufficient just to ask for the scopes. The better approach would be for the authorizing user to predefine a set of required claims at the AM. Then, for repeated requests the client (requester) just needs to provide the scopes for the pre-defined claims.

JohnB estimates that the OpenID scopes satisfy almost 80% of the cases. If more sophisticated claims are needed (for specific requesters), then yes, require the complete aggregation to be supplied. This also means that the request object is relatively small and minimal.

We need to have a claims definition page (end point) where requesters can discover/learn the claims needed to access resources. This is also where you would define if signatures are required. There is the issue of where the signature originates (is it the third party issuing the claims, or is it the requester that is asked to sign?).

The request object being sent to the authorization server could also be required to be signed. The user should define this when creating his/her account at the AM. Basically this says that AM should only accept requests (from me) if they are signed (by me). This could be the place to put a URL to your X.509 certificate, so that the server can fetch and verify the signature.

In OpenID connect, the OpenID token is signed using a symmetric key.

**Next Meetings**

- WG telecon on Thursday, 2 Feb 2012, at 9am PT (time chart)
- WG telecon on Thursday, 9 Feb 2012, at 9am PT (time chart)
- WG telecon on Thursday, 16 Feb 2012, at 9am PT (time chart)
- WG telecon on Thursday, 23 Feb 2012, at 9am PT (time chart)