UMA telecon 2011-01-20

Date and Time

- Agenda
- Attendees
- Minutes
  - Roll call
  - Approve minutes of 2011-01-06 meeting
  - Action item review
  - Discussion
- Next Meetings

Date and Time

- WG telecon on Thursday, 20 Jan 2011, at 9-10:30am PT (time chart) – regrets from Eve; Maciej M. will chair
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Assign note-taker for the day
- Roll call
- Approve minutes of 2011-01-13 meeting
- Action item review
- Scope issues (report from last week)
  - Discuss further issues related to invisibility of resource set info to requester
  - Have requester get new token for every resource at same host/user? Have requester upgrade the same token over and over? Other?
  - Assign AIs for core/scoped-access/reg spec edits
- Further discussion of tclaims and OpenID Connect influence on them?
- AOB

Attendees

As of 6 Jan 2011 (pre-meeting), quorum is 8 of 15

1. Mohammed Alam
2. Trent Adams
3. Paul Battersby
4. Paul Bryan
5. Domenico Catalano
6. Sal D'Agostino
7. George Fletcher
8. Thomas Hardjono
9. Maciej Machulak
10. Maciej Wolniak

Non-Voting:

1. Kevin Cox

Guest:

1. Greg Turner

Apologies:

1. Eve Maler
2. Lukasz Moren
3. Susan Morrow

Minutes

Roll call

Quorum was reached.

Approve minutes of 2011-01-06 meeting

Minutes have not yet been approved. Approval postponed to next conference call.

Action item review
Discussion

Discussion regarding scope-related issues - in particular, with reference to the:

1. ad hoc scope call 12 Jan 2011
2. last week’s conference call

There are 3 things that need to be discussed further, which are related to invisibility of resource set info to requester. Earlier calls proposed three solutions:

Solution 1: “Requester as smart mule”
Host gives information to requester in the clear, to convey to the AM.
- Pro: Little crypto, no extra web service calls.
- Con: Exposes data the requester has no right to.

Solution 2: “Requester as dumb mule”
Host gives encrypted information to requester, to convey to the AM.
- Pro: No extra web service calls.
- Con: Requires host/AM "prearranged key infrastructure" to manage this trust

Solution 3: "Referral resource and artifact"
Host creates a referral resource at the AM on a back channel, and gives the requester only a pointer to it.
- Pro: Secure, allows referral to have lots of useful info in it.
- Con: Requires extra web service calls, requires more endpoints and sub-protocols.

The back channel between the Host and the AM has performance issues. This should be included in the specification - i.e, that there are “known performance issues”. If the AM gets hundreds of thousands of requests from the requester then it may need to go to the AM with every such request - then the AM may stop responding to the Host if it decides to.

DDoS-type attacks can be stopped without a problem (not accepting requests from Hosts) but the problem is more severe for legitimate requests that come from Hosts.

We discuss how the requester knows which token to use if it wants to access a resource? Requester has to know what the resource is and what the group is for every single resource the requester has to get a token. PAP/PDP/PEP model - the token is only used to authenticate the requester.

We should decide whether the token should be used for authorization or for authentication only.

In the classic model, the host and the AM need to be more tightly integrated, sharing occurs between the two. Host has to have a back channel to the AM - for registering resource groups, etc. Uses this channel for requesting authorization from the AM as well.

The requester may act as an intermediary for transmitting the authorization.

The specification might be pushed towards the PDP model - the token is mostly for authenticaing and not authorizing requests. UMA use cases are different than OAuth use cases - you cannot take a token from AOL and go with this token to Yahoo. Scopes are not bound to resources.

We should look at JSON tokens and JWT.

What should be the granularity of tokens and resources. Are we OK with one token per resource? It’s better to have different one. One token per resource group.

We’ve decided to possibly schedule an ad hoc call regarding the protocol next week to discuss resource registration and scoped access.

Domenico discusses the newly sent Trusted Claims document and mockups.

Next Meetings

- WG telecon on Thursday, 27 Jan 2011, at 9-10:30am PT (time chart)