UMA telecon 2010-08-19

UMA telecon 2010-08-19

- Date and Time
- Agenda
- Attendees
- Minutes
  - AI summary
  - Roll call
  - Discussion on Resource/scope registration
- Next Meetings

Date and Time

- WG telecon on Thursday, 19 Aug 2010, at 9-10:30am PT (time chart)
  - Skype line "C": +9900827042954214
  - US: +1-201-793-9022 | Room Code: 295-4214

Agenda

- Administrative
  - Roll call
  - Approve minutes of 2010-08-05 meeting
  - Action item review
  - Status reports from the wider UMA world
- Resource/scope registration discussion
  - Hopefully lots of new fodder coming out in email by Thursday...
  - Discuss any impacts on Steps 1-3 if possible
- AOB

Attendees

As of 11 Aug 2010, quorum is 6 of 11.

1. Fletcher, George
2. Hardjono, Thomas
3. Holodnik, Tom
4. Machulak, Maciej
5. Moren, Lukasz

Non-voting participants:

- Kevin Cox
- Herve Ganem
- Gerry Gebel
- Mark Lizar
- Anna Ticktin (staff)

Regrets:

- Domenico Catalano

Minutes

AI summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Open</th>
<th>Action Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-12-03</td>
<td>Eve</td>
<td>Open</td>
<td>Add terms-negotiation scenarios to Scenarios document.</td>
</tr>
<tr>
<td>2010-08-12</td>
<td>Eve, Mario</td>
<td>Open</td>
<td>Meet to discuss how to move forward on the Scenarios and Use Cases document.</td>
</tr>
<tr>
<td>2010-08-12</td>
<td>Mario</td>
<td>Open</td>
<td>Revise the Scenarios and Use Cases document by end of August.</td>
</tr>
<tr>
<td>2010-08-12</td>
<td>Maciej, Christian, Eve</td>
<td>Open</td>
<td>Write up answers to the philosophical questions posed on 2010-08-12 related to resource/scope registration, for the SMART implementation, resource registration spec, and scope registration spec proposal respectively.</td>
</tr>
</tbody>
</table>

Roll call

Quorum was not reached.

Discussion on Resource/scope registration
The group discusses resource registration and where state about protected resources needs to be maintained. George provides an example: widget code on the website can talk to the instant messaging app. No need for maintaining state of the Host anywhere.

The problem is as following: User at the host deleted some resources. Some client asks for a resource at the AM - should the AM be aware that this resource does not exist? Another angle of the problem: the user disassociated a resource from a policy at the AM (resource no longer protected). If a requester asks for the resource at the host - what should the host do? Should the host say that it is UMA protected?

User interacting both with the host and the central server - AM. The host is saying to the AM - “Has this user given consent to access this resource.” Yes / No answer.

Thomas - how do you sync up this stuff.

George - a user would manage who got access to resources using the AM. Resources are protected or are default public/private.

Thomas - the resource server - the user would connect to it to delete the resource.

George - I want to be able to manage what I’ve shared in one place. Therefore, the AM should be aware what resource are there in the cloud. George - this is similar to the token revocation problem. George - AM should simply delete the policy (set it to null) and reply with “no token” to the requester.

Introducing a host to the AM - establishment of trust-relationship.

A user interacts with the host and discusses what to share with AM.

Is that feasible to allow the host to control all of the scopes and resource references.

There are three problems with resource registration/management:

1 - synchronization between the host and the AM
2 - communication of resources from the host to the AM
3 - condition of access/policies (how are these policies expressed for various hosts at a single location)

Is that back channel useful to the host? Depends on the application - some may actually want this.

George - users should use the Host to manage resources. It’s ambiguous if this is managed on the AM side. Maybe it might be good to redirect the user to the host if the management process starts from the AM side. Maybe it might be good to simply switch the policy. AM may have really good sharing options comparing to the host.

The problem might be similar to authentication - OpenID or username/password. Invalidating credentials of the OpenID provider side (users cannot log in with their OpenID anymore).

Going to the AM interface and saying “I no longer want you to manage this resource.”

George - the user should be logged at the host to define relationship with the AM.

Synchronization of data - generic problem.

What’s the policy for this resource. AM is authoritative for the policy. Host is authoritative for the resource and to enforce the policy. User - change the policy for a resource - do this at the AM
User - change the resource - do this at the host.

Host now has more work - take messages from the AM and do something with these messages in case we want to introduce management. Host is responsible for physical access control and AM is responsible for policies.

Host can push data to the AM but AM should not be able to push data to the Host (e.g. updates that resources are no longer protected).

If you restrict yourself to the use cases where you accept that nothing bad can happen due to lack of synchronisation. Policies as defined by AM are opaque to the host. Host can register anything it wants.

Scope - different on different hosts may have different meanings.

UX studies should add much to our discussions and show what users actually want.

Scopes are only meaningful for the host - AM is used only for managing multiple resources in a single place.

Problem - synchronization, semantic description of resources and actions, description of all the policies that the AM

How much can we minimize the need for bidirectional synchronization/communication. Doesn’t always work well. How do you resolve conflicts, etc.

Host Introduction + Resource Registration - good from the UI perspective.

**Next Meetings**

- Legal subteam telecon on Wednesday, 25 Aug 2010, at 8-9am PT (time chart) on line C
- WG telecon on Thursday, 26 Aug 2010, at 9-10:30am PT (time chart) on line C