

UMA F2F 2010-10-20

UMA F2F 2010-10-20

- [Date and Time](#)
- [Agenda](#)
- [Attendees](#)
- [Minutes](#)
 - [Updates](#)
 - [Resource registration](#)
- [Next Meetings](#)

Date and Time

- WG F2F at [Kantara conference](#) on Wednesday, 20 Oct 2010, at 9am-noon CET ([time chart](#))
 - No dial-in
 - No telecon this week
 - Room #3 F017

Agenda

- Administrative
 - Identify someone to take minutes
 - [Roll call](#)
 - Approve minutes of [2010-10-14](#) meeting
 - [Action item](#) review
 - Updates from the wider UMA world
- Conclude resource/scope registration decision-making
 - Maciej plans to present on this topic
- Drill down into the [location scenario](#) and its constituent use cases
- (optional) Push forward trusted claims if possible
- AOB

Attendees

Attendees:

1. Trent Adams
2. Maciej Machulak

Non-voting participants:

- Gael Gourmelen
- Fulup Ar Foll
- Jonas Hogberg
- Tim Cole
- Rainer Horbe
- Mark Lizar
- Hervé Ganem
- Ingo Friese
- Hiroki Itoh
- Alam Mohammed
- Philippe Clement
- Sebastien Brault
- Bill Braithwaite
- John Bradley
- Mikael Ates
- Serge Ravet
- Benoit Ballieux
- Dervla O'Reilly (staff)
- Anna Ticktin (staff)

Minutes

Updates

- Domenico passed new [Trusted Claims diagram + UX](#) to list

Main simplification assumptions are:

- Subject Authentication: support for SSO affiliated authentication (OpenID, Fed/SAML) in the step 1 and step 4 to reduce authentication processes.
- AM2 Subject session management in the step 5 (allow cache subject consent).

- "Silent Consent" (no online consent, only subject notification) based on claims release policy at AM (i.e. Subject specifies silent consent for specific identity attributes which have low privacy impact) -> not included in the UX.

Resource registration

Maciej explains what scope registration means - Host communicates to the AM all the resources that they are managing that need protection. Scope defines the resource, describes the things you can do to a bunch of stuff e.g. from OAuth. (JB says it's claims based access, others says it's groups) Scope also refers to AM resources access as opposed to Host-based access. This prompts Maciej to provide an overview.

John Bradley digs into understanding the scope and registration issues - asks if it makes sense to exchange the keys and the (? - missing) in the initial OAuth flow.

Maciej describes the UMA flows and presents an introduction to UMA. JB asks about dynamic PEP/PDP and remote validation. JB asks about opaque tokens so the host knows which AM to talk to. Maciej says that this can be a problem. JB says that making the assumption that the host knows is a bad design choice.

JB brings up a great point: if the requester is talking to a non-human requester vs. a human requester.

Rainer brings up an enterprise use case - where the administrator sets the policy, and the user executes the policy. Herve explains that there is a use case for this and that this is baked into UMA. JB reiterates this in an enterprise context and discuss that this can be done through claims. Herve explains that you look at claims as if they are protected resources. JB another way to look at this can be like a Secure Token Service (STS).

JB points out that UMA is just one way to transform one type of token into another.

Next Meetings

- WG telecon on Thursday, 28 Oct 2010, at 9-10:30am PT ([time chart](#)) on line C ([agenda page](#))
- WG F2F on Monday, 1 Nov 2010, at 11am-5pm PT ([time chart](#)) - no dial-in, and no telecon this week ([agenda page](#))
- WG telecon on Thursday, 11 Nov 2010, at 9-10:30am PT ([time chart](#)) - Maciej to chair?