
Thomas Hardjono (hardjono@mit.edu)
Maciej Machulak (maciej.machulak@gmail.com)
Eve Maler (eve@xmlgrrl.com)
@UMAWG
Agenda

What is UMA?
Demos
Why UMA-enable?
Q&A
Let’s start with “What is Street Identity?”
If an app you want to use needs to know your verified street address, a trusted authority can share it with your consent.

Learn more at streetidentity.com or email mmachulak@google.com
Privacy is not about secrecy

“\nThe goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be”

– Ann Cavoukian, Information and Privacy Commissioner of Ontario, Privacy in the Clouds paper

It’s about context, control, choice, and respect
The price for sharing access to data and services is too high

Either we have to do all the work ourselves

Or we have to agree to install large data pipelines

...resulting in oversharing of high-quality data and a “too many subscriptions” problem

Or we share with friends through “secret links”

...rebuilding friend lists over and over – and hoping they won’t give away the store

...often in the role of the “product,” not the “customer”
UMA is...

• A web protocol that lets you control access by anyone to all your online stuff from one place

• A set of draft specifications, free for anyone to implement

• Undergoing multiple implementation efforts

• A Work Group of the Kantara Initiative, free for anyone to join and contribute to

• Simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly

• Contributed to the IETF for consideration: draft-hardjono-oauth-umacore

• Currently undergoing interop testing and increased OpenID Connect integration
What could you do with Street Identity if it were UMA-enabled?

• **Centralize** how you manage sharing your street address *and* other data and content hosted elsewhere

• Share your address with **others** in an automatic, policy-driven way ("only bob@gmail can see this")

• Let others qualify to get access **without** your having to be around at access-time

• Impose enforceable **terms and conditions** on address recipients ("you may not sell this data"), privacy-enabling your data sharing more actively
Protecting Project hData electronic health records

• EHRs need high security and third-party access and dynamic introduction of parties
The UMA architecture echoes OAuth, by design.
OAuth leaves unspecified how the two servers interact

**Phase 1: protect resource**

...so UMA makes their interactions interoperable
UMA must extend OAuth to make claims-based authorization work

Phases 2 & 3: get authz and access resource

...so an access token becomes a bucket for permissions
Agenda

What is UMA?

Demos

Why UMA-enable?

Q&A
The SMARTAM.org project

See also the SMARTAM implementation FAQ
SMART demo scenario

Host
(Puma Host One)
Personal Information

Requester
(Puma Requester One)

Bob

socialconnect.pl

smartam.

Resource Metadata
Access Control Policies

facebook
Google
Yahoo!
twitter
LinkedIn
OpenID
Setting the scene

1. **Mario** takes a photo of Eve at a conference.
2. Eve agrees on **uploading the photo** to AISEC’s photo gallery service.
3. Before uploading Eve chooses the sticky policy determining who might get access to the photo. Here, default policies are:
   - (a) Only the user her-/himself
   - (b) Participants of the conference
   - (c) Internet – free download
4. According to the policy (a) the photo will be **uploaded restricted** to Eve’s eyes only.
5. Mario’s boss checks the gallery for available photos but **he cannot see** Eve’s photo.
Synergetics project:
TAS³ is getting an UMA connector

*Trusted Architecture for Securely Shared Services*

The TAS³ project is working to produce an architecture in which data can be shared and reused securely and safely within a trusted environment. Most importantly, it puts users in control of what happens to their data and allows them to see when and by whom it has been accessed. For more information visit [www.tas3.eu](http://www.tas3.eu) or [www.zxid.org](http://www.zxid.org).

Synergetics is now developing the UMA connector to its end-to-end trust assurance framework, which otherwise focuses primarily on machine-to-machine and deep web service calls.
Agenda

What is UMA?

Demos

Why UMA-enable?

Q&A
Web apps that become UMA hosts can easily offer “context, control, choice, and respect”

• You can provide sophisticated protection and sharing of any user content or data that isn’t meant to be fully public

• You can outsource the entire job to third parties (AMs)

• You can ensure that the protection of sensitive resources is stronger than the “private URL trick”

• You can build trust more readily with users who are “privacy fundamentalists”

• You can integrate these features using lightweight OAuth, JSON, HTTP, and REST paradigms and a freely implementable protocol
Identity providers that become UMA AMs can centrally coordinate sharing of anything to anyone

• The separation between IdPs and other attribute providers has long been acknowledged – you can never be the sole trusted source of all interesting user data

• OpenID Connect is solving how you as an IdP can act as a discovery hub for OAuth-mediated access to attributes

• UMA complements it by solving how you as an IdP can now act as an authorization hub for access by “others besides Alice” to:
  • Trusted attributes
  • User-generated content
  • APIs
Agenda

What is UMA?

Demos

Why UMA-enable?

Q&A
Thank you

Thomas Hardjono (hardjono@mit.edu)
Maciej Machulak (maciej.machulak@gmail.com)
Eve Maler (eve@xmlgrrl.com)
@UMAWG