User-Managed Access (UMA) Update

29 January 2010
Eve Maler, UMA WG Chair
Paul Bryan, UMA WG Vice-Chair and Spec Editor

The UMA WG site will have links to these slides and the webinar recording
Topics we’ll cover today

• The problem space
• Introducing UMA
• Next steps
• Technical deep-dive
The “data price” for online service is too high

- Why must we laboriously type the **same data** over and over?
- Why must we **manually update** it in a hundred places when something changes?
- Why must we surrender **all the data** requested, under terms favorable only to the recipient?
- Can we get a **global view** of our sharing preferences, patterns, and recipients?
- Can websites give us better service if we **trust them** enough to give each one more data, selectively?
The classic web-form model

disclose

site that consumes data

http://tinyurl.com/uma-wg
Apps think they “own” something special...but do they?
Apps think they “own” something special...but do they?

- We lie (and resent being asked)
Apps think they “own” something special...but do they?

• We lie (and resent being asked)

• The data goes stale
There’s proof
a better way is possible
There’s proof
a better way is possible

- Calendar and photo sharing
- With “friends and family” or with specific email addresses
There’s proof  
a better way is possible

- Calendar and photo sharing
  - With “friends and family” or with specific email addresses

- OAuth-style connections
  - To share tweets, geolocations, social graphs, professional associations, health data
The OAuth model
Forging and managing OAuth connections

Fire Eagle executes my sharing policy

Dopplr talks directly to Fire Eagle to get this

http://tinyurl.com/uma-wg
Privacy is not about secrecy

“The 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
What if...

• You can give prospective employers a set of links to your CV and transcripts, so they see your accomplishments – and you can revoke their access when you land a job?

• You have a “protected inbox” that rejects too-frequent marketing communications from retailers?

• You can offer custom “feeds” of personal data to get personalized user experiences – only to sites that have privacy policies you like?
How can users manage and control lots of connections like these?

**User-managed access**

Dedicated interface and service for:

- Authorizing data sharing and service access
- Imposing sharing terms on any app wanting access
- Monitoring, changing, and stopping access relationships
- Letting services make requests of all of your authoritative sources directly
The UMA model for relationship management
UMA is...

- A web protocol that lets you control authorization of data sharing and service access made between online services on your behalf
- A Work Group of the Kantara Initiative that is free for anyone to join and contribute to
- A set of draft specifications that is free for anyone to implement
- Heading towards multiple implementation efforts
- Going to be contributed to the IETF
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly
Working through one scenario*

*See the UMA Scenario document for many more

Selectively share an ever-changing CV with prospective employers
The simple CV scenario

Alice Adams chooses to store and maintain her CV at her university.

Unseen University

Host

BigCo.Com

Requester

Authorizing User

CopMonkey

Authorization Manager

http://tinyurl.com/uma-wg
The simple CV scenario

She introduces the university to her chosen AM for CV protection (just once)
The simple CV scenario

She sets up policies and terms for that CV at the AM

Unseen University

BigCo.Com

Requester

Authorizing User

CopMonkey

Authorization Manager

http://tinyurl.com/uma-wg
The simple CV scenario

She tells a prospective employer where to find her CV (just once)
The simple CV scenario

The prospective employer tries to retrieve the CV and gets introduced to the AM as a result (a one-time event)
The simple CV scenario

The prospective employer and the AM negotiate terms for access (which can be cached if nothing else changes)
The simple CV scenario

The prospective employer retrieves the CV, once the AM tells the university it’s okay to release it (as often as Alice’s policy allows; the policy can be cached by the university as long as the AM allows)
The simple CV scenario

One day, Alice revokes access, blocking that employer’s CV access going forward

...sorry, Charlie
Let’s look at a potential user experience...
Next steps for the UMA work

• Rapidly incubate the specs *(with your help)*
  • And facilitate their testing with multiple independent implementations

• Continue to seek out *(your)* contributed scenarios and use cases
  • And facilitate prototype deployments

• **Join us!**
Questions before the deep-dive?...

eve@xmlgrrl.com / emaler@paypal.com
email@pbryan.net

Thanks to the Kantara staff and the UMA WG participants, especially the rest of our WG leadership team: Hasan Akram, Use Cases Editor; Domenico Catalano, Graphics/UX Editor; and Maciej Machulak, Implementation Coordinator

The UMA site will have links to these slides and the webinar recording
Thanks!

eve@xmlgrrl.com / emaler@paypal.com
email@pbryan.net

Thanks to the Kantara staff and the UMA WG participants, especially the rest of our WG leadership team: Hasan Akram, Use Cases Editor; Domenico Catalano, Graphics/UX Editor; and Maciej Machulak, Implementation Coordinator

The UMA site will have links to these slides and the webinar recording
The CV scenario in more detail
The CV scenario in more detail

Unseen University

BigCo.Com

Requester

Authorizing User

CopMonkey

Authorization Manager

User Stores CV
The CV scenario in more detail

Unseen University

User Stores CV
User manages CV on Host site

BigCo.Com

Requester

Authorizing User

Host

Store CV

CopMonkey

Authorization Manager
The CV scenario in more detail
The CV scenario in more detail

User Registers Host at AM
a. User introduces Host to AM
The CV scenario in more detail

User Registers Host at AM
a. User introduces Host to AM
b. Host requests creation of a new host resource on AM
The CV scenario in more detail

User Registers Host at AM
a. User introduces Host to AM
b. Host requests creation of a new host resource on AM
c. User authorizes the connection

Unseen University

BigCo.Com

Requester

Authorize

Unseen University

Host

New Host Resource

CopMonkey

Authorize

Authorizing User

Authorization Manager

29

http://tinyurl.com/uma-wg
The CV scenario in more detail

User Registers Host at AM
a. User introduces Host to AM
b. Host requests creation of a new host resource on AM
c. User authorizes the connection
d. Host requests and gets an H➔A access token

29
http://tinyurl.com/uma-wg
The CV scenario in more detail

User Sets Up CV Protection

BigCo.Com
Requester

Unseen University
Host

Authorizing User

CopMonkey
Authorization Manager

Your Policy Folder
The CV scenario in more detail

User Sets Up CV Protection
User manages policies and terms at AM
The CV scenario in more detail

Unseen University

Host

Unseen University

BigCo.Com

Requester

Authorizing User

CopMonkey

Authorization Manager

User Tells Requester About CV

http://tinyurl.com/uma-wg
The CV scenario in more detail

User Tells Requester About CV
User provides protected resource URL to requester
The CV scenario in more detail

Requester Attempts CV Access

BigCo.Com Requester

Unseen University Host

Authorizing User

CopMonkey Authorization Manager

http://tinyurl.com/uma-wg
The CV scenario in more detail

Requester Attempts CV Access
a. Requester attempts to access the resource

BigCo.Com

Requester

Unseen University

Host

Authorizing User

CopMonkey

Authorization Manager

Attempt Access
The CV scenario in more detail

Requester Attempts CV Access

a. Requester attempts to access the resource

b. Requester requests and gets an R♂H access token
The CV scenario in more detail

Requester Attempts CV Access

a. Requester attempts to access the resource
b. Requester requests and gets an RPKH access token
The CV scenario in more detail

Requester Attempts CV Access
a. Requester attempts to access the resource
b. Requester requests and gets an \( R \to H \) access token
c. Host requests a “referral resource” from AM to return to Requester
The CV scenario in more detail

Requester Attempts CV Access

a. Requester attempts to access the resource
b. Requester requests and gets an R%H access token
c. Host requests a “referral resource” from AM to return to Requester
d. Requester requests and gets an R%A access token
The CV scenario in more detail

Requester Attempts CV Access
a. Requester attempts to access the resource
b. Requester requests and gets an R›H access token
c. Host requests a “referral resource” from AM to return to Requester
d. Requester requests and gets an R›A access token
The CV scenario in more detail

Negotiate Terms of CV Access
The CV scenario in more detail

Negotiate Terms of CV Access
a. Requester asks AM for the authorization state
The CV scenario in more detail

Negotiate Terms of CV Access

a. Requester asks AM for the authorization state

b. AM responds with “claims-required” authorization state
The CV scenario in more detail

Negotiate Terms of CV Access

a. Requester asks AM for the authorization state
b. AM responds with “claims-required” authorization state
c. Requester sends required claims
The CV scenario in more detail

Requester Successfully Accesses CV

Unseen University

BigCo.Com

Authorizing User

CopMonkey

Authorization Manager
The CV scenario in more detail

Requester Successfully Accesses CV
a. Requester attempts access to protected resource on Host

http://tinyurl.com/uma-wg
The CV scenario in more detail

Requester Successfully Accesses CV
a. Requester attempts access to protected resource on Host
b. Host requests a policy decision from AM
The CV scenario in more detail

Requester Successfully Accesses CV
a. Requester attempts access to protected resource on Host
b. Host requests a policy decision from AM
c. AM provides “Allow” response
The CV scenario in more detail

Requester Successfully Accesses CV

a. Requester attempts access to protected resource on Host
b. Host requests a policy decision from AM
c. AM provides “Allow” response
d. Host returns the CV resource
The CV scenario in more detail
The CV scenario in more detail

User Revokes Access

a. User changes policy to revoke this Requester’s access to this resource
The CV scenario in more detail

User Revokes Access
a. User changes policy to revoke this Requester’s access to this resource
b. Requester attempts access as usual
The CV scenario in more detail

User Revokes Access
a. User changes policy to revoke this Requester’s access to this resource
b. Requester attempts access as usual
c. Host requests a policy decision from AM
The CV scenario in more detail

User Revokes Access
a. User changes policy to revoke this Requester’s access to this resource
b. Requester attempts access as usual
c. Host requests a policy decision from AM
d. AM denies the request
The CV scenario in more detail

User Revokes Access
a. User changes policy to revoke this Requester’s access to this resource
b. Requester attempts access as usual
c. Host requests a policy decision from AM
d. AM denies the request
e. Host blocks Requester access