UMA and Higher Education
A presentation by the Kantara User-Managed Access Work Group

17 Oct 2012
Your hosts today

- Eve Maler (@xmlgrrl), WG chair
- Maciej Machulak (@mmachulak), WG vice-chair
- Thomas Hardjono (@findthomas), WG spec editor

Big thanks to our webinar sponsors: CloudIdentity.co.uk and IEEE-ISTO.org
Agenda

What is UMA?
The higher education data-sharing challenge
Demo of the SMART system solution
Additional use cases and implementations
Next steps
The “data price” for online service is too high: typing...

• Provisioning by hand
• Provisioning by value
• Oversharing
• Lying!
The “data price” for online service is too high: connecting...

- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oversharing of lots of real information
The “data price” for online service is too high: private URLs...

- Handy but insecure
- Unsuitable for really sensitive data
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, Ontario Information and Privacy Commissioner, Privacy in the Clouds paper

It’s about context, control, choice, and respect
UMA gives users a true digital footprint control console

- Web 2.0 access control is inconsistent and unsophisticated
- To share with others, you have to list them literally
- You have to keep rebuilding your “circles” in new apps
- You can’t advertise content without giving it away
- You can’t get a global view of who accessed what

- You can unify access control under one app
- Sharing policies can test for claims like “over 18”
- You can reuse the same policies with multiple sites
- You can control access to stuff with public URLs
- You can manage and revoke access from one place
UMA turns online sharing with anyone into a “privacy by design” solution.

I want to **share** this stuff selectively!
- Among my own apps
- With family and friends
- With organizations

I want to **protect** this stuff from being seen by everyone in the world!

---

- Historical
- Biographical
- Reputation
- Vocational
- Artistic/user-generated
- Social
- Location/geolocation
- Computational
- Genealogical
- Biological/health
- Legal
- ...
UMA leverages OAuth 2.0 and OpenID Connect

- **OAuth 2.0**
  - You control access to web APIs
  - Apps can use a variety of access token types
  - You control access to claims about you
  - You grant access by consenting to terms at run time
  - The authorization function is local to protected resources

- **OpenID Connect**
  - You achieve federated single sign-on and login-time attribute exchange
  - You control access to claims about you
  - You grant access by consenting to terms at run time
  - You can grant access to apps operated by you
  - The authorization function is local to protected resources

- **UMA**
  - You can grant access to apps operated by anyone
  - You control access to a variety of protected resources
  - You can grant access by setting policies and terms ahead of time
  - The authorization function is standard and centralizable
  - Requesting party is authorized based on claims

**Claims** can come from distributed sources
Apps get access using bearer-style tokens
You delegate scope-constrained access to other apps
Calling app is recognized based on authenticated identity
Apps can get access after you go offline
Agenda

What is UMA?

The higher education data-sharing challenge

Demo of the SMART system solution

Additional use cases and implementations

Next steps
The SMARTAM.org project

See also the SMARTAM implementation FAQ at http://tinyurl.com/umafaq
The SMART project is…

• About “Student-Managed Access to Online Resources” with UMA
• At the School of Computing Science, Newcastle University, UK
• Affiliated with the Centre for Cybercrime and Computer Security
• The team Prof. Aad Van Moorsel, Maciej Machulak, Łukasz Moreń
  – Alumni: Maciej Wolniak, Chris Franks, Jacek Szpot, and Domenico Catalano (Oracle)
• A product of HEFCE/JISC funding (Jan ’10–Aug ‘12)
• Developing SMARTAM, UMA/j, Puma, and Apache Amber
• Blogging at http://smartjisc.wordpress.com and tweeting @smartproject
One of the SMART use cases: Transcript of Records sharing

• Based on “Sharing Trustworthy Personal Data with Future Employers” scenario* submitted to UMA WG
  – Students interact with online job application systems
  – Share their exam marks, certificates, references, etc.
  – Data is stored at their various home Higher Education institutions

• See “Secure sharing of Higher Education Achievement Reports (HEARs) at Newcastle University using SMART” case study**

* http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario
** http://smartjisc.files.wordpress.com/2012/10/smart_hears_draft012.pdf
Problem scenario

CareerMonster

Bob

no direct interaction between applications

Newcastle University

personal information (incl. name, academic records, etc.)

Signed, Stamped & Scanned Transcript of Records / eTranscript (HEAR)

printed Transcript of Records

eTranscript (HEAR)
Problems

– Getting the “Transcript of Records” document:
  • Engaging University staff to obtain a signed/stamped version of the document, or…
  • Printing out the document from an online system provided by a higher-ed institution, such as the S3P Portal* at Newcastle University, or…
  • Obtaining an eTranscript document, digitally signed by a higher-ed institution, e.g. in HEAR form

– Going through this process every time the document changes

* [https://s3p.ncl.ac.uk](https://s3p.ncl.ac.uk)
Improvements

• Allow students and graduates to easily establish access to their educational data:
  – Without having to engage University staff

• Give third-party web apps, such as career services and other universities, access to current student data:
  – Continuous access to academic records during (often long) job application processes

• Give students full control over sharing of their personal information stored at Higher Education institutions
  – Access authorization
  – Insight into access requests
Improved scenario

**CareerMonster**
- job positions

**Newcastle University**
- personal information (incl. name, academic records, etc.)

**eTranscript (HEAR)**

**Back-channel communication**
- selecting information to be retrieved from S3P
- specify how data is shared

**smartam**
- your one place to share your data securely
  - sharing settings (security policies)
  - access history (for accountability)

**Bob**

Direct interaction between applications
Agenda

What is UMA?

The higher education data-sharing challenge

Demo of the SMART system solution

Additional use cases and implementations

Next steps
The SMART demo

• “Newcastle S3P” demo host app: https://pumahostone.appspot.com

• “CareerMonster” demo requester app: https://pumarequesterone.appspot.com

• SMARTAM.org authorization manager
  – It’s public; try it yourself at https://www.smartam.org!
  – See the blog for instructions: http://smartjisc.wordpress.com/2011/05/27/smartam-v2-0-public-beta/
Agenda

What is UMA?
The higher education data-sharing challenge
Demo of the SMART system solution
Additional use cases and implementations
Next steps
The Fraunhofer AISEC UMA project

• It participates in an Information and Communication Technology alliance
• Its Secure Services and Quality Testing development group has an Identity Management project
• Goals: secure, unified management of virtual identities
  – Ambient lifestyle, identity ecosystems, mobile authentication and authorization
• Challenges:
  – User empowerment in managing the identity lifecycle, harmonization of approaches, seamless interoperability

• Reach out to Head of Dept Mario Hoffmann for full details:
  mario.hoffmann@aisec.fraunhofer.de
Key use case: a Life Management Platform for use in eGov
Mobile integration is key
The OX Project hosted by Gluu

• Use case: organizational API authorization
  – The authorizing party is the enterprise
  – Its agent is a policy administrator
  – It controls what parties access what scopes at what endpoints
  – Akin to traditional enterprise access management, for the “API economy”

• oxAuth already implements OAuth 2.0 and OpenID Connect
  – Including session management
  – The team is finding it relatively easy to add UMA support
oXAuth sequence diagram

oxAuth Use Case is here
Policies are outside of the UMA core spec but are required for the UMA flow (see 3.5 of spec). In general it is expected to have automatic authorization without human interaction (from oXAuth side). Once policies are satisfied client is authorized. oXAuth allows the oXAuth admin manually authorize client.
Use case: filling out online personal loan applications with PDS content

- Requires both UMA and AXN capabilities
- See the case study*

* [http://kantarainitiative.org/confluence/display/uma/Case+Studies](http://kantarainitiative.org/confluence/display/uma/Case+Studies)
Additional use cases under discussion

• Patient-centric healthcare data sharing
  – Among care providers, the patient, his or her family, “quantified self” apps…

• Citizen-centric secure government services
Agenda

What is UMA?
The higher education data-sharing challenge
Demo of the SMART system solution
Additional use cases and implementations

Next steps
Next steps for UMA

• Continue to revise the spec (now at rev 05*) in response to experience and comments
  – Ultimately moving to a formal standards org
• Conduct interop testing through the OSIS wiki**
• Support implementers and deployers
• Facilitate open source
• Liaise with AXN and other actors in the broader “trusted identities in cyberspace” ecosystem
• More webinars and tweet chats…

* [http://kantarainitiative.org/confluence/display/uma/UMA+1.0+Core+Protocol](http://kantarainitiative.org/confluence/display/uma/UMA+1.0+Core+Protocol)
** [http://osis.idcommons.net/wiki/UMA1:UMA_Interop_1](http://osis.idcommons.net/wiki/UMA1:UMA_Interop_1)
Next steps for you

• Check out our case studies* to see which might match your own use cases
• Experiment with open-source UMA implementations** and with deployments
• Join*** the group – become an UMAnitarian
• Follow the WG on Twitter @UMAWG
• Reach out!

* [http://kantarainitiative.org/confluence/display/uma/Case+Studies](http://kantarainitiative.org/confluence/display/uma/Case+Studies)
** [http://kantarainitiative.org/confluence/display/uma/UMA+Implementations](http://kantarainitiative.org/confluence/display/uma/UMA+Implementations)
*** [http://signup.kantarainitiative.org/?selectedGroup=11](http://signup.kantarainitiative.org/?selectedGroup=11)
Questions?

Thank you

tinyurl.com/umawg | tinyurl.com/umafaq | tinyurl.com/umav1
tinyurl.com/umatrust | tinyurl.com/umaiop | tinyurl.com/umawgfb