Secure sharing of Higher Education Achievement Reports (HEARs) with User-Managed Access (UMA)

Maciej Machulak (Newcastle University, UK)
maciej.machulak@ncl.ac.uk
Outline

- User-Managed Access
  - Why needed
  - Architecture
  - Protocol
- SMART Project
  - Higher Education Use Case
  - Demo
- Summary
- Q&A
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
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 Players
(1) Trust a Token

(2) Get a Token

(3) Use a Token
UMA - Protocol

- Trust a Token

Authorization Manager (AM)  

Host  

Requester

- or -

Requesting Party

Authorizing User (user at browser or other user agent)
UMA - Protocol

- Trust a Token

Authorizing User (user at browser or other user agent)
Trust a Token

Step 1. User Introduces Host to AM

Authorizing User (user at browser or other user agent)
UMA - Protocol

- Get a Token

**Step 1. User Introduces Host to AM**

**Step 2. Requester Gets Access Token**

**Authorizing User** (user at browser or other user agent)
Uma - Protocol

- Use a Token

**Step 1. User Introduces Host to AM**

**Step 2. Requester Gets Access Token**

**Authorizing User** (user at browser or other user agent)
SMART Project
Newcastle University, UK
The SMARTAM.org project

See also the SMARTAM implementation FAQ at [http://tinyurl.com/umafaq](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](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://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario)
** [http://smartjisc.files.wordpress.com/2012/10/smart_hears_draft012.pdf](http://smartjisc.files.wordpress.com/2012/10/smart_hears_draft012.pdf)
HEAR Documents

- Electronic document that provides a single comprehensive record of a learner’s achievement at a HE institution.

- Contains information:
  - identifying the holder of the qualification;
  - on the HE institution and the national higher education system;
  - on the qualification, its level, and details of each of the modules or units studied
  - on the form of assessment (timed examination, essay, project, dissertation),
  - on marks awarded, and their relative weighting towards the final summary mark or grade, etc.
  - …
Problem scenario

- CareerMonster: job positions
- Newcastle University S3P: personal information (incl. name, academic records, etc.)

Bob
Problem scenario
Problem scenario
Problem scenario

Bob

CareerMonster
job positions

Newcastle University
personal information (incl. name, academic records, etc.)
Problem scenario

- CareerMonster: job positions
- Newcastle University: personal information (incl. name, academic records, etc.)
- Bob: printed Transcript of Records, eTranscript (HEAR)
Problem scenario
Problem scenario

Bob

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

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

CareerMonster
job positions

Provide Signature/Stamp
Problem scenario

no direct interaction between applications

CareerMonster
job positions

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

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

Bob

print transcript of records
eTranscript (HEAR)

Provide Signature/Stamp
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-education 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 S3P**: personal information (incl. name, academic records, etc.)
- **eTranscript (HEAR)**
- **smartam.**: your one place to share your data, securely
  - sharing settings (security policies)
  - access history (for accountability)

**Bob**: selecting information to be retrieved from S3P

- Back-channel communication
- Direct interaction between applications

Specify how data is shared
Benefits

- Apps access data directly from trustworthy sources:
  - Simplified trust path;
  - Possibly continuous access to “fresh” data;

- Access does not require manual processes (signining, uploading, etc.) to take place;

- Authorization to access distributed data using a central component:
  - Unified UI for setting access control permissions
  - Authorization stored centrally - can be easily managed and revoked by the end-user;

- Centrally-located dashboard provides insight into how information is shared and handled;
Demo
Demo
The SMART demo

- “Newcastle S3P” demo host app: https://pumahostone.appspot.com
- “CareerMonster” demo requester app: https://pumarequesterone.appspot.com
- SMARTAM.org authorization manager https://www.smartam.org
Questions and Discussion

Thanks!

Questions?
Acknowledgements

Eve L. Maler
UMA WG Chair
emaler@forrester.com

Thomas Hardjono
UMA WG Specification Editor
hardjono@mit.edu

Domenico Catalano
UX/Graphics Designer
domenico.catalano@oracle.com

Members of the UMA WG