Protecting “Personal Clouds” with UMA and OpenID Connect

@UMAWG
#UMApcloud for questions
19 June 2014
tinyurl.com/umawg for slides, recording, and more
The marvelous spiral of controlled personal data sharing

Further reading: tinyurl.com/umawg
Agenda

• The realities and challenges of personal data sharing
• “UMA for humans 101”
• A walk through personal cloud models
• Use cases
• How UMA leverages OpenID Connect – with demo
• Next steps
The realities and challenges of personal data sharing
What is personal data?

Personal Data is the *Life Blood* of the Information Age

Personal Data is the New “*Oil of the Internet*”

Personal Data is the new *currency*
Ways to measure the value of personal data

- Market capitalization
- Revenue per record/user
- Market Price
- Cost of data breach
- Pay to protect

“72% of European citizens are concerned that their personal data may be misused...”

Individuals have little visibility into the practices of the organizations they are putting their trust in – until their data is breached or misused.

Risks: Loss of Trust
The “personal data price” for online service is too high: typing…

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

• Meaningless consent to unfavorable terms
• Painful, inconsistent, and messy access management
• Oblivious oversharin
The “personal data price” for online service is too high: private URLs...

- Handy but insecure
- Unsuitable for really sensitive data
“UMA for humans 101”
UMA turns online sharing into a privacy-by-design solution

The “user” in User-Managed Access (UMA)

Further reading: tinyurl.com/umapbd
UMA turns online sharing into a privacy-by-design solution
UMA turns online sharing 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

I want to **control** access proactively, not just feel forced to consent over and over
UMA turns online sharing into a privacy-by-design solution

Outsources protection to a centralized “digital footprint control console”

Standardized APIs for privacy and “selective sharing”
A walk through personal cloud models
Personal data ecosystem emerging trends

Life Management Platforms

Informed Pull

Personal Clouds

App

Personal Data Store

App

Controlled Push

Native Data Store
Mapping UMA to personal clouds and life management platforms

Data Stores

Data Control

LMP

Informed Pull

Access

Requesting Party

Controlled Push

Bank
Healthcare
Home
Car

Access Requesting Party
LMP
Data
Data

Informed Pull
Controlled Push
Mapping UMA to personal clouds and life management platforms

- Data Stores
- LMP
- UMA AS
- Requesting Party
- Bank
- Healthcare
- Home
- Car
Mapping UMA to personal clouds and life management platforms

- **Data Stores**
- **Resource Owner**
- **Client**
- **Requesting Party**

Relationships:
- **manage**
- **consent**
- **protect**
- **authorize**
- **access**
- **negotiate**

Icons:
- Bank
- Healthcare
- Home
- Car
Use cases
Case studies for...

- Management and sharing of personal accessibility needs and preferences
- Secure sharing of university e-transcripts
- Healthcare relationship locator service and patient-centric consent directives
- Access management 2.0 for the enterprise (previous webinar)
- ...
- Protecting the personal data stores of everyone at MIT

Further reading: tinyurl.com/umacase
Protected personal data stores: MIT’s view

MIT Cloud Infra

MIT Personal Data Service

Privacy-Preserving Query Web-APIs

Data Sharing Web APIs

MIT Data Consumers

3. Privacy-Preserving Queries and BigData access (authorized by Alice)

Student Alice (owner of PDS)

Student Alice stores her personal data at her MIT PDS account

Bob (Alice’s friend)

Data-item Sharing with Authorization from Alice (e.g. calendar access)

User-generated data (mobile devices)

Other sources of data

MIT Administration

facebook

Google+ (G+)

fūnff (Open Sensing Framework)
How UMA leverages OpenID Connect
Use case: Transcript of Records sharing

• Student interacts with an online job application system
• Student fills in a job application form and provides:
  – Personal information
  – Transcript of Records document
• Data is transferred from the student’s personal data service
  – With explicit consent
• Employer requests access to additional data
  – …and this has to be confirmed by the student

“Sharing Trustworthy Personal Data with Future Employers”
http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario
UMA model

- Resource owner
- Authorization server
- Client
- Requesting party

Actions:
- Manage
- Consent
- Control
- Protect
- Negotiate
- Authorize
- Access
- Manage
Scenario (Peter sharing data)

- **Personal Information**
- **Transcript of Records**
- **PERSONAL DATA SERVICE**
  - Personal Information
  - Transcript of Records

- **nuve AM**
- **CAREERMONSTER**
  - Job Positions

- **Resource Owner**
  - Manage
  - Control
  - Consent

- **Requesting Party**
  - Negotiate
  - Manage

- **Peter (Student, Job Seeker)**
Scenario (Tom accessing data)
Live demo
NuveAM – Authorisation Manager

• UMA-compliant Authorisation Server (AS) from Cloud Identity Limited:
  – Access control to data in the Cloud
  – API security management
  – Real-time monitoring and audit

• Use cases: **Securing Cloud-based Personal Data Services (PDS)**; Managing access to Cloud-based APIs

• Uses open standards, including: UMA, OAuth 2.0, OpenID Connect, SAML 2.0

• Open source frameworks: Java and Python

http://www.cloudidentity.co.uk/products/nuveam
Nuve User-Managed Access
UMA claims-based authorisation

- UMA allows for the use of claims to support Claim-Based Access Control (CBAC):
  - Trusted claims from Trusted Third Parties
  - Self-asserted claims

- In CBAC, the decision to grant access to a protected resource is made based on Subject’s information/attributes, such as name, age, email address, role, location, credit score, etc.

- …or a Subject’s statement (e.g. promise to adhere to licensing terms)
OpenID Connect role in UMA

- OpenID Connect (OIDC) provides authentication, consented attribute sharing, and attribute transmission capability
- OIDC allows third-party asserted claims from distributed sources to be collected
- UMA leverages OIDC in claims-gathering flow in one of two ways:
  - AS interacts directly with requesting parties, or
  - indirectly via clients
UMA AS Collecting Claims from Requesting Party

Client redirects the Requesting Party to AS

Client acting as claims conveyor
Generic UMA Model

- Resource Owner
- UMA Domain
- Resource Server
- Policy Decision Point
- UMA AS
- Client
- Requesting Party
- OpenID Domain
- SSO
- Protect
- Manage
- Control
- Authorize
- Access
- Protected Resource
Client application conveying claims to UMA AS
UMA AS acting as Claims Client

1. Request
2. AuthN
3. Access_token
4. Request Userinfo
5. Userinfo
UMA AS acting as Claims Client

UMA AS can collect additional claims from internal user store

This can be a SAML-compliant IDP just as well
Next steps
Next steps for the WG…and you

• Get involved!
  – Become an “UMAnitarian” (it’s free)
  – Participate in the interop and our implementation discussions
  – Follow and engage with @UMAWG on Twitter

• Current work:
  – Technical: claim profiling and core spec variations
  – Business: access federation trust frameworks

• Stay tuned for a webinar on UMA and Healthcare in Q3

Join at:
tinyurl.com/umawg
Questions? Thank you!

@UMAWG
#UMApcloud for questions
19 June 2014
tinyurl.com/umawg for slides, recording, and more