Extending the Power of Consent with User-Managed Access
A Standard Architecture for Asynchronous, Centralizable, Internet-Scalable Consent

Eve Maler, ForgeRock
eve.maler@forgerock.com
@xmlgrrl
May 21, 2015
“Privacy” goals vs. reality

• **Aspirations:** FIPPs and Privacy by Design speak of transparency, control, participation, consent...

• **Risk mitigation:** The top driver for corporate privacy funding is meeting compliance obligations
  – >50% of corporate and government privacy groups report into Legal or Compliance

• **Ready for a change?** 91% of Americans agree or strongly agree consumers have lost control over PII collection and use
  – 80% who use social networking sites are concerned about third-party access
In ordinary online contexts, the consent experience is dire.
In the Internet of Things, it’s not going to get easier

The Next Step in Wearable Electronics

By Julia Goldstein on May 4 2015 // No Comments
A funny thing happened in the API economy: beyond-compliance consent paradigms

OAuth opt-in consent for scoped API access

Authorize Meshfire to use your account?

This application will be able to:
• Read Tweets from your timeline.
• See who you follow, and follow new people.
• Update your profile.
• Post Tweets for you.
• Access your direct messages.

Authorize app Cancel

Directed scoped sharing with other people
Consent requirements that freshen up our aspirations

- **Choice**
- **Relevance**
- **Granularity**
- **Scalability**
- **Automation**
- **Reciprocity**

**Authorization**
- Time
- Manner
- Consciousness

**Agreement**
- Sources
- Data items
- Parties
- Modification

**Acquiescence**
- Sources
- Data items
- Consent interactions

**Consent of resource owner to share**

**Consent of requesting party to be recognized**
How do classic and new consent mechanisms do against the requirements?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>ToS opt-in</th>
<th>Cookie opt-in/out</th>
<th>OAuth</th>
<th>“Share”</th>
<th>Consent directive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>+1</td>
</tr>
<tr>
<td>Relevance</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>+1</td>
<td>0</td>
</tr>
<tr>
<td>Granularity</td>
<td>-1</td>
<td>0</td>
<td>0/+1</td>
<td>+1</td>
<td>0</td>
</tr>
<tr>
<td>Scalability</td>
<td>-1</td>
<td>+1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>Automation</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>+1</td>
<td>-1</td>
</tr>
<tr>
<td>Reciprocity</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>
The User-Managed Access (UMA) V1.0 standard builds on OAuth, and adds “Share” features.

- Loosely coupled to enable centralized authorization-as-a-service for any number of an individual’s resource servers.
- A new concept, to enable party-to-party sharing driven by policy (or access approval) rather than requiring the individual to be present at access time.

Diagram:
- RO (resource owner)
- RS (resource server)
- AS (authorization server)
- RqP (requesting party)
- C (client)
- PAT (protection API token)
- RPT (requesting party token)
- AAT (authorization API token)

Expiration of PAT is driven by the RqP through asynchronous consent by RO.

Authorization data is added to this token if trust in the requesting party is successfully elevated, typically through authentication and/or claims-gathering.
## Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Host</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allergies</td>
<td>BlueHealth</td>
<td><a href="https://bluehealth.openrock.org:443/types/medical">https://bluehealth.openrock.org:443/types/medical</a></td>
</tr>
<tr>
<td>Allergies</td>
<td>BlueHealth</td>
<td><a href="https://bluehealth.openrock.org:443/types/medical">https://bluehealth.openrock.org:443/types/medical</a></td>
</tr>
<tr>
<td>Heartrate</td>
<td>HappyHeart</td>
<td><a href="https://happyheart.openrock.org:443/types/medical">https://happyheart.openrock.org:443/types/medical</a></td>
</tr>
</tbody>
</table>
How does UMA do against the requirements?

<table>
<thead>
<tr>
<th></th>
<th>UMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice</td>
<td>0/+1</td>
</tr>
<tr>
<td>Relevance</td>
<td>+1</td>
</tr>
<tr>
<td>Granularity</td>
<td>+1</td>
</tr>
<tr>
<td>Scalability</td>
<td>0/+1</td>
</tr>
<tr>
<td>Automation</td>
<td>0/+1</td>
</tr>
<tr>
<td>Reciprocity</td>
<td>+1</td>
</tr>
</tbody>
</table>
Thank you

Eve Maler, ForgeRock
eve.maler@forgerock.com
@xmlgrrl
May 21, 2015