GDPR, PSD2, CIAM, and the Role of User-Managed Access (2.0)

Eve Maler, UMA Work Group Chair
@xmlgrrl | tinyurl.com/umawg | @UMAWG
Kantara CIWUSA17 pre-conference workshop 11 Sep 2017
We're all individuals!

I'm not
What makes data privacy regulations different this time around?

• Virality
• Aspirations
Take steps

Identify intersections between digital transformation opportunities and user trust risks

Conceive of personal data as a joint asset

Lean in to consent

Take advantage of identity and access management for building trust
How can UMA be relevant to these imperatives?

The UMA extension grant enhances OAuth in the following ways:

- The resource owner authorizes protected resource access to clients used by entities that are in a requesting party role. This enables party-to-party authorization, rather than authorization of application access alone.

- The authorization server and resource server interact with the client and requesting party in a way that is asynchronous with respect to resource owner interactions. This lets a resource owner configure an authorization server with policy conditions at will, rather than authorizing access token issuance synchronously just after authenticating.

UMA’s federated authorization enhances the UMA grant as follows:

- Multiple resource servers operating in different domains can communicate with a single authorization server operating in yet another domain that acts on behalf of a resource owner.

- A service ecosystem can thus automate resource protection, and the resource owner can monitor and control authorization grant rules through the authorization server over time.

- Authorization grants can increase and decrease at the level of individual resources and scopes.
What does it enable?
Pinpoint sharing without caring what others want first
What does it enable?
“Single pane of glass” control
What’s UMA 2.0 all about?

• UMA1 built all this capability using OAuth and OpenID Connect piece-parts
  • Some of its design preceded (and influenced) modern OAuth, OIDC, JWT, etc. practice

• We collected implementation experience
  • In the meantime, the Internet of Things happened, a natural fit for UMA, as did HEART

• So we embarked on an upgrade roadmap
UMA2 goals

• Wide ecosystem = when Alice knows who she wants to share with (or a class of “who’s”), but the service managing her access has never met them before they attempt access

• We believe we have met all these goals and increased security
Timeline

Mar ‘15: UMA V1.0 ratified as Recommendations
Dec ‘15: UMA V1.0.1 ratified as Recommendations
May ‘16 to Sep ‘17: specs refactored, over 100 issues closed, lots of implementation input received, Disposition of Comments doc written...
17-19 Oct ’17: IIW interop? ForgeRock, Gluu, Keycloak, ...?
10 Sep ‘17: UMA WG approves Draft Recommendations for finalization

2015
2016
2017
Want to get a little geeky? Here’s the whole UMA grant in a nutshell

• All major options, with success paths
• Find links to detailed swimlanes at tinyurl.com/umawg
UMA2 is not the end of our work

**UMA Legal**

- Exciting work on a **legal framework**, a major underlying portion of which is just being completed
- We have been working with legal expert **Tim Reiniger**, who wrote the Virginia digital identity law

**Extensions and futures**

- The Work Group has saved off a variety of exploratory ideas for future work in GitHub issues with the label **extension**
- Examples:
  - Integration points for consent receipts
  - Optimized flows that remove the need for the permission ticket
Thank you! Questions?

Eve Maler, UMA Work Group Chair
@xmlgrrl | tinyurl.com/umawg | @UMAWG