

# Status Report: UMA WG, UMA Legal, Blockchain and Smart Contracts DG

Eve Maler | @xmlgrri | [eve.maler@forgerock.com](mailto:eve.maler@forgerock.com)  
19 June 2017



# Update on the UMA WG

From the UMA Work Group chair  
[tinyurl.com/umawg](https://tinyurl.com/umawg) @UMAWG

# Must-see this week at CIS

Thursday 2:15pm: **Introducing UMA 2.0** in Chicago Ballroom IX



# What does UMA do? It's based on OAuth...



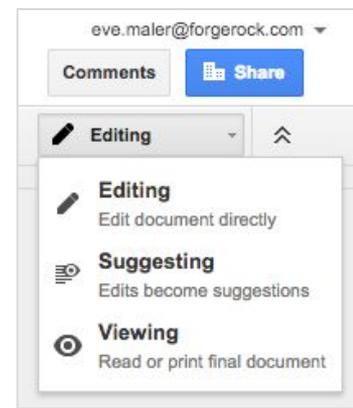
The resource owner authorizes protected-resource access to clients used by entities that are in a **requesting party** role. This enables **party-to-party authorization**, rather than authorization of application access alone.

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 **authorization grant rules** (policies) at will, rather than authorizing access token issuance synchronously just after authenticating.

...Loosely couples, or federates, the authorization process. This enables multiple resource servers operating in **different domains** to 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 policies** at a central service location over time. Further, with the use of token introspection, authorization grants can **increase and decrease at a relatively fine grain**.

# Typical use cases: think **share**, **delegate**, **grant access**, **consent** (!), ...

- **Patient** chooses to share (or shares on request) PHR/EHR/smart device data with a doctor, caregiver, or family member
  - OAuth, OpenID Connect, and UMA have been profiled in the OpenID Foundation HEART group
- **Citizen** shares access to online government forms, data, or other digital resources with assistants or family members
- **Bank customer** grants account access with a wealth manager, or in order to pay someone



# UMA 2.0 timeline

- Dec 2015: UMA V1.0.1 Recommendations published
- Mar 2016: 2.0 roadmap themes decided
- Apr 2016: Major design decision-making begun
- May 2016: 2.0 spec editing begun
- Jan 2017: Completed editing of key “jricher” design issues
- Mar 2017: Completed editing of follow-on issues
- Apr 2017: Completed spec refactoring
- May 2017: 45-day Public Comment and IPR Review period begun
  - Ends 12 Jul 2017, with Recommendation balloting to follow

# What are those 2.0 themes?

- Align more closely to OAuth
- Improve suitability for IoT scenarios
- Improve suitability for “wide” ecosystems
  - 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 achieved these goals with greater **simplicity**, **security**, and even **feature parity**

# Status of implementations

- Several industry and open-source implementations of UMA2 have been started
- A couple of requests for conformance testing in order to be able to list conformant implementations
- V1.2 of MITREid Connect (one rev back) has a partial (95%?) implementation of UMA2 in a branch, called MPD (“multi-party delegation”)
  
- Interest in directed funding or other resources to build out a test harness?

# Update on the UMA Legal Subgroup

From the UMA Work Group chair  
[@UMAWG](https://tinyurl.com/umalegal)

# We are well along developing a **legal framework** to support **legal toolkits** -- why?

- UMA applies protection policies to permission tokens and other artifacts on the wire
- The legal framework maps those artifacts to licenses as legal devices
- This licensing mechanism is valuable to individuals, organizations, legal professionals, and privacy professionals because it allows Alice to license Bob to use her digital resources on her terms

Our first toolkit will be a set of model (sample) contract clauses that will be easy to pull into real UMA-enabled service agreements and policies, to accelerate adoption and deployment -- consistent with the protection of privacy rights in any jurisdiction

# Update on the Blockchain and Smart Contracts DG

From one of the BSC DG co-chairs

<http://kantarainitiative.org/confluence/display/BSC/Home>

# BSC DG timeline

- 5 Jul 2016: DG launched with a six-month completion timeframe
- Jul 2016: DG crisped up its area of inquiry:
  - *“analyzing novel attempts to use blockchain and distributed ledger technologies to achieve an **equitable distribution of accountability and risk**: what could be described as “personal data and transaction ecosystems in which individuals and organizations can interact more equitably and efficiently”*
- 5 Jan 2017: DG agreed to keep working on its draft Report
- 5 May 2017 (*“January 125th”*): DG achieved consensus to wrap up its Report (except for copy-editing) and deliver to Kantara Initiative
- 5 Jun 2017: Editing completed and Report delivered

# Technologies and techniques included in the [report](#)

- Blockchains and Distributed Ledger Technologies (DLTs)
- Legal Contracts and Smart Contracts
- InterPlanetary File System (IPFS) & Content Based Networks
- Certificate Transparency
- Verifiable Claims
- OPAL/Enigma
- Protocol-Specific Contract Provisions
- CommonAccord
- User-Managed Access (UMA)
- Consent Receipts
- User Submitted Terms
- Identity and Access Management

# Use cases included in the [report](#)

- Personal Health Information for Research Purposes
- Sovrin-Based Self-Sovereign Identity
- Alice Participates in Bob's Research Study
- Research Evidence Notebook
- Smart Medical Telematics
- Prescription Writing Into a Patient's Health Record

# Recommendations provided in the [Report](#)

- Launch a Blockchain and Smart Contracts WG
  - Suggested deliverable: “Recommendations for good practice on use and handling of data related to individuals, so as to facilitate individual autonomy and enable equitable and efficient participation in transaction ecosystems”
  - Discussion continues regarding specifics of charter formation
- Consider a Kantara-Wide Legal WG
  - The topic is seeing broader discussion
- Research Inside and Outside Kantara

*Many thanks to the tireless DG participants, and special thanks to Thorsten Niebuhr and his contributors from the IRM and IDPro groups who helped us with content!*

# Thank you

Eve Maler | @xmlgrrl | eve.maler@forgerock.com  
19 June 2017