Enforcement mechanisms for distributed authorization across domains in UMA – aka “UMA trust”

Eve Maler | eve@xmlgrrl.com
22 Aug 2012 draft
Distributing resource protection to third parties is hard

- Identity federation solutions outsource only authentication, and that’s already hard
  - And a few attributes, which the “relying party” gets to use in making its own authorization decisions (thank you very much)

- XACML offers a strict separation of policy decision points and enforcement points
  - But it’s mostly used within a single enterprise or circle of trust – because the alternative is hard
User-Managed Access (UMA) goes there

• Why? Primarily to empower individual resource owners to:
  – Consolidate management of sharing into one place
  – Set claims-based policies at config time, and then be absent at run time if they like
  – Share with other people and orgs, not just other apps they themselves use
  – Solve managed access Internet-style, with radical loose coupling and light weight
What else will need UMA’s abilities?

• In small part:
  – OAuth, as it seeks to make resource server/authorization server communication interoperable

• In large part:
  – OpenID Connect, as it seeks models for IdPs to broker user-authorized access by other people and orgs, not just other apps, to third-party-asserted attributes
In the “BLT sandwich of trust”, UMA specs provide the B and the T

- Contractual framework
  - Deals in Subjects that operate or use endpoints
  - Subjects declaring conformance take on obligations

- Web protocol specification
  - Deals in endpoints
  - Operators of software endpoints can declare conformance

Binding Obligations on UMA Participants

Mutual document cross-references

UMA Core Protocol
The contractual framework is **not** a full trust framework

- It dictates only the lowest-common-denominator responsibilities that anyone “doing UMA” would take on
  - These are precisely what “doing UMA” entails!
  - E.g., “If you register a resource to be protected by somebody else, you commit to letting them do it”

- It is designed to be pulled into higher-order contracts
  - Both pairwise agreements and trust frameworks
  - Both sector-specific and “horizontal” use cases
UMA endpoints

Host Operator

Host Protected Resource

Authorize

Authorize User

Authorizing Party

Control

Manage

AM Operator

Delegate

Requester Operator

Requester

Requesting Party

Requesting Party
The UMA technical-business relationship is subtle

• FICAM thinking: For **flexibility**, operational and legal profiles try to **remain apart** from technical profiles

• UMA thinking: For **enforceability**, behavioral obligations are tied to specific **protocol interactions**
  
  – This way, audit trails can support findings of fault that are as **unambiguous** as possible
Example

When the AM issues a “protection API token” to the host...

...the Host Operator, AM Operator, and Authorizing Party gain a number of obligations to others

Each obligation has a clause ID in the contractual framework

(full diagrams for Phase 1 and Phases 2/3)
Example clauses: they have three parts

• **H1.** When the AM issues a PAT to a Host, the Host Operator gains an obligation to the Authorizing Party to delegate protection services to the AM Operator for the set of protectable resources for which it represents this capability to the Authorizing Party, and to respect the access constraints represented by RPTs generated by the AM.

• **AP2.** When the AM issues a PAT to a Host, the Authorizing Party gains an obligation to the AM Operator to introduce the desired Host to this AM in outsourcing protection of this host's resources.
What is needed to make this a “minimum viable approach”?

• Vetting of the contractual framework clauses
• Vetting of the security and auditing provisions in the UMA core spec
• Vetting of the spec/contractual connection
• UMA conformance must have concrete meaning
  – Interop feature test development is under way
• A way for operators of UMA endpoints to declare (first-party) or be certified (third-party) as “UMA-conformant”
  – UMA already has a logo; does it need a Kantara-administered “UMA-conformant” logo?
Thank you

@UMAWG

tinyurl.com/umawg | tinyurl.com/umafaq
tinyurl.com/umav1 | tinyurl.com/umatrust
tinyurl.com/umaiop