UMA Legal

UMA Legal

The overall goal of this subgroup is to accelerate adoption and reduce inhibitors in a business context.

This subgroup has produced its first draft report: **A Proposed Licensing Model for User-Managed Access** (or, "How the UMA protocol enables a license-based model for controlling access rights to personal digital assets"). This paper is intended for professionals in the areas of **law, privacy, risk, compliance, security policy, and business policy**, particularly those responsible for building and running UMA-enabled services.

What is the purpose of this model? The UMA technical protocol enables individuals to apply protection policies to their digital assets by using services to issue "permission tokens". The UMA business model maps those permission tokens and related 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.

Mission

- Produce a set of toolkits and associated educational materials whose purpose is to accelerate the ability of those in the following roles to adopt, deploy, and use UMA-enabled services in a manner consistent with protecting privacy rights:
    - Individuals ("natural persons")
    - Organizations ("legal persons" such as businesses and governments)
    - Legal representatives of the above
- Focus on GDPR-related toolkits first. A toolkit could be anything that helps use or leverage an existing piece of legislation or framework, such as an SDK, a checklist, consent receipt templates or profiles, or a set of CommonAccord text, and could be related to the GDPR itself, the EU-U.S. Privacy Shield, BCRs, and so on.
- To inform the roadmap work, develop:
    - Comparative analysis of UMA and GDPR concepts such as data subject, processor, and controller
    - Roundup of contractual and regulatory use cases
- Leverage specialist legal expertise wherever possible to complete and review the deliverables.

Background

The subgroup found funding to work with legal expert Tim Reiniger starting in 2017, with a schedule to produce three staged deliverables. The first, Use Cases for Analyzing and Determining a Legal Framework, was delivered in draft on 28 Feb 2017, with the group providing commentary and revisions as input to later stages, resulting in a revised final version delivered 26 Mar 2017. The second, The Legal Value Perspective for UMA Use Cases, was delivered on 31 May 2017, again after extensive group review and commentary. The third, UMA Definitions Annotated, was delivered 25 Aug 2017. A broader "legal framework" (now called business model), incorporating a revised version of the definitions, was published in early 2018.

Subgroup meetings

The subgroup's meeting times and notes are here. Legal topics are currently being covered in the main Work Group call series. See the UMA home page, UMA calendar, and main Meetings and Minutes page for details.

If you are just visiting and are interested to join the UMA Work Group, we invite you to join! Visit our home page and see the Join link there.

Sources of liability tension

These are some key trust relationships we are exploring for the "liability tensions" within them, that is, the misalignment of incentives that leads to a reluctance to deal with each other, mistrust, or added friction in decisions to use or deploy UMA. Here are some of our use cases?

- When Alice sets up criteria for access to a digital data resource of hers, such as "Only Bob can access this", can she ensure that the other actors in the authorization chain are doing their best to make sure Bob "is who he says he is" by the time he (someone) actually gets access?
- If Alice wants to impose limitations on how Bob uses her stuff using business-legal methods vs. some kind of (say) encryption or DRM methods, such as "Bob must promise not to share this data with third parties", how can she ensure these limitations stand up?
- Can the host of some sensitive information of Alice's, such as personal data, trust an authorization service that promises to do the job of protecting that information in an outsourced fashion? This is roughly akin to the challenges of federated authentication, only for authorization.
- Can Alice trust an authorization service to do as she bids when it comes to protecting her stuff, if she didn't personally hand-code it?
- Can an authorization service rely on the hosts of Alice's data and the client applications that Bob uses to operate correctly in their UMA roles?
- Can the host of Alice's data ensure that it can keep out of legal trouble even if Alice's authorization service appears to want it to share data with a recipient who is in a jurisdiction to which personal data is not allowed to be sent?

Work to date on model text

The model text work is being encoded in the CommonAccord.org system. CommonAccord is:

"...an initiative to create global codes of legal transacting by codifying and automating legal documents, including contracts, permits, organizational documents, and consents. We anticipate that there will be codes for each jurisdiction, in each language. For international dealings and coordination, there will be at least one "global" code."

Here is one version of the draft model text. The definitions are more mature than the clauses, but all of this text predates the analysis being performed and may be radically changed.

Additional artifacts

This slide deck, presented at **Digital Contracts, Identities, and Blockchain** at MIT in May 2016, shares some key use cases. A few additional artifacts are available on the WG's GitHub wiki. All of this work predates the analysis being performed. Ask the chair to get access to the "UMA Legal Definitions" slide deck.