THE LEGAL VALUE PERSPECTIVE FOR UMA USE CASES

Deriving user-centric access sharing use cases from consent requirements

Legal Model Paper 1

UMA | KANTARA INITIATIVE INC.

By Timothy S. Reiniger, Esq.
May 31, 2017

Overview

The efficient open market exchange of personal information in the global digital network-based information economy requires trusted access relationships for both disclosing and receiving parties. If a party is encouraged to rely on software code in the machine-mediated information economy, it is imperative that a trust framework or code of conduct, such as the Law Merchant or the emerging Lex Informatica,[1] for personal resource sharing provides adequately for user-centricity.

The general access consent-driven legal requirements for User-Managed Access (UMA)[2] use cases are: 1) user-centric autonomy for end-user access sharing, 2) reciprocity of rights and obligations with respect to the protection of personal resources for all participants in the UMA protocol, and 3) objectivity of access grants in the form of licensing permission tokens.

[1] The influence of software code, network architectures, technological capabilities, system design choices, and machine-mediated environments on creating information use rules and regulating behavior in cyberspace has been referenced as 'code is law' in LAWRENCE LESSIG, CODE VERSION 2.0 (2008) and as 'Lex Informatica' by Joel R. Reidenberg in Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEX. L. REV. 553 (1998).

[2] See the UMA 2.0 Draft Recommendations, available at: https://docs.kantarainitiative.org/uma/wg/oauth-uma-grant-2.0-05.html and https://docs.kantarainitiative.org/uma/wg/oauth-uma-federated-authz-2.0-05.html. Note, however, that UMA does not decide on the value propositions and standards for actual usage of the licenses by relying parties.

1. Autonomy: UMA User-Centric Protocol

To have the ability to control access sharing based on consent and authorization, end-users need autonomy as rights holders. UMA recognizes that autonomy is a fundamental enabler of consent in digital network markets.[3] The user-centric approach is a critically important component for achieving this autonomy.[4]

Value Perspectives for UMA (in Enabling the Right to Control Access Relationships) with Respect to Personal Resource Flows

UMA Value Perspectives	Law	Commerce	Communication
Autonomy	Consent	Sharing	Protocols
Reciprocity	Access Authorization	Transaction	Protection Policies
Objectivity	License	Economic	Permission Tokens

Access grants necessarily involve the communication of messages or information about someone or something, and reliance on that information by the recipient of the communication. As described on the Kantara Initiative, Inc. website, UMA is an "OAuth-based protocol designed to give an individual a unified control point for authorizing who and what can get access to their digital data, content, and services, no matter where all those things live."[5] In network-based systems, protocols serve as standards of communication that determine power relationships.[6] UMA, therefore, is a protocol for communicating consent in the context of granting access rights to protected resources, including personal data.

2. Reciprocity: UMA Protection Policies as Trust Framework Rules

[3] See the IDABC European eGovernment Services "Study on eID Interoperability for PEGS: Update of Country Profiles Analysis & Assessment Report" (October 2009) at 111 ("It is clear that the use of identity resources in a cross border context should as a general rule only be possible with the data subject's consent, i.e. it should be user centric.").

[4] For a discussion of the user-centric approach with respect to access sharing of personal resources, see TRUST::DATA A NEW FRAMEWORK FOR IDENTITY AND DATA SHARING, Edited by Thomas Hardjono, David Shrier, and Alex Pentland, Visionary Future (2016) at 110 and, at 199, citing the World Economic Forum, "Personal Data: The Emergence of a New Asset Class" (2014) (describing user-centricity as a "key enabler" of trust in the information economy).

[5] For an overview of UMA, see the Kantara Initiative, Inc. website at: https://kantarainitiative.org/confluence/display/uma/Home

[6] For a discussion of access relationships as power relationships, see Manual Castells, "A Network Theory of Power," INT'L JOURNAL OF COMM. 5 (2011), 773-787.

The order in all systems presupposes that their components stand in specific communicative relations to one another.[7] UMA currently is configured with five established roles that can serve as the functional components of an access-focused legal trust framework: Resource Owner (RO), Resource Server (RS), Authorization Server (AS), Requesting Party (RqP), and Client.[8]

Trust frameworks provide reciprocity and enforcement by means of the contracts that system participants enter into between and among themselves. Most notable examples are individual contract-based identity system trust frameworks (sometimes referred to as system rules or scheme rules) with which the identity system participants agree to comply.[9] These sets of rules, usually made legally binding by contract, often governing transaction liability as well. The rules agreed to by the trust framework participants, however, typically apply only to the participants and not third parties.[10]

A recent draft UMA technical specification has defined system rules or policy conditions as "Access grant rules configured at an authorization server that achieve resource protection."[11] These policy conditions reflect jurisdiction specific data protection requirements, such as the GDPR, and industry sector requirements imposed on medical, financial services, and telecommunications providers.

3. Objectivity: UMA Permission Tokens as Licenses of Access Rights

[7] See Pierre de Latil, THINKING BY MACHINE: A STUDY OF CYBERNETICS (1957), pp. 206-7. "The amount of information that can be transmitted depends on a measure of the degree of order….Any signal necessarily involves differentiation. A high degree of differentiation allows all sorts of codified variations and hence a large amount of information can be carried."

[8] For a discussion of a conceptually analogous emerging trust framework in Canada that recognizes the need for citizens to have tools for managing both digital identity and access sharing in regard to personal data, see "Pan-Canadian Trust Framework Overview, A Collaborative Approach to Developing a Pan-Canadian Trust Framework by the DIACC Trust Framework Expert Committee, Digital ID and Authentication Council of Canada (August 2016), *available at*: https://diacc.ca/wp-content/uploads/2016/08/PCTF-Overview-FINAL.pdf.

[9] For further information regarding the concept of a trust framework (a/k/a system rules) in the identity context, see "What Is a Trust Framework?" *available at* http://openidentityexchange.org/what-is-a-trust-framework, and TRUST::DATA A NEW FRAMEWORK FOR IDENTITY AND DATA SHARING, Edited by Thomas Hardjono, David Shrier, and Alex Pentland, Visionary Future (2016) at 210, citing the World Economic Forum report on personal data.

[10] For a discussion of the difficulty in applying contract requirements to third party beneficiaries, see Jeff Nigriny and Randy V. Sabett, 'The Third-Party Assurance Model: A Legal Framework for Federated Identity Management', Jurimetrics (Summer 2010) at 531. For a discussion of legal issues involving trust frameworks in the context of identity ecosystems, see Timothy Reiniger, Jeff Nigriny, and Kyle Matthew Oliver, "The Virginia Digital Identity Law: Legal and Policy Foundations for the Identity Trust Framework Model," ABA Information Security Law Journal Volume 6, Issue 4 (Autumn 2015) at 13-26, available at: http://www.americanbar.org/content/dam/aba/administrative/science_technology/2016/ilj_volume6_issue4.authcheckdam.pdf..

[11] For reference, see section 1.1 of User-Managed Access (UMA) 2.0 (3-12-2017), available at: https://docs.kantarainitiative.org/uma/wg/uma-core-2.0-20.html.

Three UMA Permission Tokens:

1. Protection API Access Token (PAT)
2. Requesting Party Token (RPT)
3. Persisted Claims Token (PCT)

For economic purposes, the UMA permission token mapped to a license is capable of serving as a means of communicating objective and assured value with respect to end-user consent to personal resource sharing.[12] In UMA, permission grants take the form of one of three tokens: a protection API access token (PAT), a requesting party token (RPT), or a persisted claims token (PCT).

The legal control of information assets in digital networks must be based on fundamental evidentiary requirements for proving consent or some other authority for data processing. However, there are current unresolved legal challenges facing service providers imposed by regulatory consent requirements, including scalability to maximize sharing of personal resources in a network environment, legal effectiveness over time, varying levels of consent by sector, varying jurisdictional requirements, and the persistent ability to revoke. Consent in the form of a license provides an objective means of achieving scalability, interoperability, duration, and revocation.

Legal consent issues are especially at issue with electronic medical records, cross-border data transfer requirements such as the GDPR,[13] and sharing of personal resources for identity authentication purposes.[14] End-user consent requirements, in general, fall within three categories: 1) affirmative consent,[15] 2) informed consent,[16] and authorization (or explicit consent for a specific purpose).[17]

Up to this time, a major challenge to implementing a user-centric personal resource sharing system has been the lack of a set of uniform default contractual rules. However, in the United States for example, UMA may leverage the

[12] For a discussion of the licensing of informational rights by individuals, see Mark A. Hall, Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records, 95 IOWA L. REV. 631, 660 (2010) ("People should be able themselves, or through their agents, to authorize access to and use of their medical information for financial rewards, and these licenses should be transferable."). See also, Pamela Samuelson, Privacy as Intellectual Property, 52 STAN. L. REV. 1125, 1134 (2000) (endorsing a licensing approach to the protection of information rights in personal data and citing UCITA as a source of default rules for the licensing of personal data in cyberspace).

[13] See Articles 41, 42, and 44 (1)(g) of the GDPR. See also Opinion 4/2017 of the European Data Protection Supervisor, sections 3.2 and 3.3, *available at:* https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.

[14] See Article 1(f)(i) of the eIDAS Regulation.

[15] As an example in the electronic document signing context, see The Federal Electronic Signatures in Global and National Commerce Act ("E-SIGN"), 15 U.S.C.A. §§ 7001 (c). On a global scale in the financial services sector, see the Know Your Customer rules.

[16] As an example in the healthcare context, see HIPAA, 42 U.S.C. 1320d – 3120d-8) and its implementing regulations at 45 C.F.R. 160 and 45 C.F.R. 164 (the "Privacy and Security Rule"), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act"). As a state law example in the context of the disclosure of genetic information see N.H. Rev. Stat. Ann. § 141-H:2.

[17] For a discussion of authorization and consent in the Health Information Exchange context, see the Report to the Legislature by the California Health & Human Services Agency, entitled "Demonstration Project Specific to Patient Consent for Health Information Exchange" (March 2014).

Uniform Computer Information Transaction Act ("UCITA")[18] as an available source of default contractual rules for licensing informational rights in the form of the right to control access to personal data.

4. Implications for Legal Mapping of UMA Roles

The predominant UMA communication relationships map to the following legal relations:

a. Resource Subject-to-RO – Resource Owner is delegated authority (either expressly or by operation of law, such as with a Resource Subject who is a minor) to provide consent to authorize access on behalf of the Resource Subject and, as such, becomes either a *legal representative* (when by law) or an *agent* of the Resource Subject.

b. RO-to-ASO – RO delegates authority to AS Operator ("ASO") to provide automated consent access on her behalf and, as such, becomes an *agent* of the RO.

c. AS-to-RS – AS has an *access contract* relationship with the RS Operator ("RSO") to enable personal resource protection and access grant rules.

d. ASO-to-RqP – ASO is *licensor* acting on behalf of the RO; RqP is a *licensee.*

e. ASO-to-Client Operator – ASO is *licensor* acting on behalf of the RO; Client Operator is *agent* for RqP who is *licensee*.

f. RqP legal person-to-RqP employee – RqP legal person, as the *licensee*, may share access with employees and independent contractors.

In several UMA communication flow contexts, much consideration has been given to applying the concept of *delegation* to downstream changes in users and uses. In fact, the consent to grant an access right is not legally equivalent to a delegation of duty or authorization (in this instance the authorization to give consent on behalf of another). Delegation of authority to act on behalf of and in the interest of another person constitutes an agency relationship. And an agent may not further delegate this authority to a subagent with the express prior consent of the principal (or the RO in the typical UMA context).[19] In the UMA context, this means, for example, that the ASO may not delegate her functions to another individual or legal entity without the consent of the RO.

With respect to grants of access rights, a licensee may not transfer the license right to another user downstream without the express prior consent of the licensor. In the use case of a connected car, the licensee of the car (RqP) may not transfer the licensed access to another user without either securing the prior consent of the RO (or possibly through the ASO agent) or having the ASO issue an access license to the new user. By comparison, in the

[18] VA CODE ANN § 59.1-501.1 et seq. UNIF.COMPUTER INFORMATION TRANSACTIONS ACT ('UCITA') § 102 Comment 34 (National Conference of Commissioners on Uniform State Laws 2002) (The term 'informational rights' in UCITA "includes 'intellectual property' rights. It also includes rights created under any law that gives a person a right to control use of information independent of contract, such as may be developing in privacy law."). Maryland also has enacted the UCITA.

[19] *Delegatus non potest delegare.* ("A delegate cannot delegate.") Black's Law Dictionary, Fifth Edition (1979).

circumstance of a medical doctor's practice group, an access license may be given to a medical practice as a legal person or entity so as to permit sharing amongst all of the members. However, sharing of personal resources outside of the medical practice may require an additional license from the RO. Finally, in the example of a nanny (RqP) who has been given an access license for use of a connected car for child care purposes only, the license would be violated if the nanny were to use the car for non-permitted purposes. These examples show how a legal framework built on a licensing model complements the technological capabilities of UMA to address unauthorized usage and attempted downstream changes to users and uses.

Conclusion

By allowing stakeholders comprehensive, real-time access to the business, legal, and technical building blocks of user-centric protocols, protection policies, and permission tokens as access grants, UMA will enable compliance with consent requirements of all levels and across all jurisdictions and industry sectors.

UMA is a protocol for communicating the legal requirement of consent as authorization to access personal resources. In turn, by treating consent as a *license* or grant of an access right, UMA provides legal solutions to the challenges of unauthorized downstream usage and users. Agents cannot legally delegate to subagents without prior consent from the RO. And Requesting Parties cannot legally transfer a license without prior RO consent. Licensing also provides end-users and service providers with a consent solution that is sensitive to dynamic use contexts, easily revocable, non-transferable, language agnostic, and self-enforcing.

The next Legal Model paper in this series will develop the UMA license model concept and, specifically, explore mapping of UMA permission tokens to the various levels of consent requirements.