A Proposed Licensing Model for User-Managed Access

How the UMA protocol enables a license-based model for controlling access rights to personal digital assets

Version 0.7e

UMA Work Group | Kantara Initiative Inc.

Editor: Timothy S. Reiniger, Esq.
Contributors: see end

January 22, 2018

Abstract: This Draft Report defines how the UMA protocol enables a license-based model for controlling access rights to personal digital assets.

Status of This Document: This is a Draft Report produced by the User-Managed Access Work Group. See the Kantara Initiative Operating Procedures for more information.

Executive Summary

The efficient open market exchange of personal data in the global digital network-based information economy requires trusted access relationships for both disclosing and receiving parties. This is especially true to monetize and fully enable personal data flow in markets that rely on machine-mediated communications and data collection. In particular, the User-Managed Access (UMA) access sharing protocol,[1] based on permission tokens that can be used as devices to license access rights with respect to personal digital assets collected and stored by devices, apps, and databases, provides an authoritative basis for communicating access consent as economic value.

Both public and private sector participants in the personal data economy recognize that trusted markets are essential to encouraging the sharing of access to personal data. Nevertheless, network-based information

[1] The UMA Version 2.0 protocol specifications can be viewed at: https://kantarainitiative.org/reports-recommendations/.

markets are dominated by systems in which individuals have little or no control over their personal digital assets and little to no visibility as to where the data flows and how it is used. In contrast, the sharing of personal digital assets as governed by the UMA access sharing protocol is *user-centric*. This method can be programmed into device software and APIs to enforce jurisdiction-specific consent and data protection requirements as well as to enable access rights licenses for governing personal data flows.

The information society requires trust in the capability to prove that individuals and entities seeking to access and use personal data in networks have the appropriate authorization to do so.[2] For cyber networks, this necessarily involves the structure of communications protocols amongst participants and their agents and the use of tokens, including those in the form of licenses, for a common meaning. Yet, in the machine-mediated communications environment, a user-centric access sharing license model has yet to be deployed.

UMA can provide the autonomy, reciprocity, and objectivity to grow market trust in widely sharing access to personal digital assets with devices, apps, and Internet databases. After integrating the UMA access sharing protocol, this market trust can be built on legitimate and internationally recognized licenses that signal both to sending and relying parties a common understanding of legal relationships with respect to personal data.

This paper seeks to explain the concept of the UMA access sharing method as an enabler of trusted granting and receipt of access rights in personal digital assets, and to develop a common understanding of what it means for participants in the information society to use UMA licenses to enable the exchange of personal information. Future business model papers will address specific market, legal, and technical applications of UMA licenses and the potential benefits of the UMA protocol in the global digital network-based information society.

Note: 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. Its purpose is to specify a mapping between legal devices and the technical constructs in the UMA protocol in a manner consistent both with protecting privacy rights and with UMA-compliant processing. The UMA protocol involves several roles interacting with an individual. One key role is that of a service called the authorization server; its corresponding representative party is in a position to act as an agent. This paper will provide some examples of UMA scenarios where these roles interact and later papers may provide additional

[2] For an example of a policy initiative built on creating trusted interoperable digital identities, *see* the European Union's Digital Single Market initiative, *available at:* https://ec.europa.eu/commission/priorities/digital-single-market_en.

Table of Contents

scenarios. (A separate paper may explore legal requirements for scenarios where a legal person, rather than an individual, seeks to manage access to its digital assets through UMA.)[3]

1. Policy Context: Creating a Market for the Control of Access Relationships to Personal Resources

The control of personal resources in networks must be based on legal devices that enable community recognition of the right to control access relationships with respect to the data. For personal data markets in the digital environment, this access control is enabled by community protocols, policies, and permissions making use of UMA.

The following is a description of some of the factors that constitute the current context for the creation of the UMA access sharing protocol and UMA licenses for granting and receiving access rights to personal digital assets.

The Challenge of Compliance with Regulatory Consent Requirements. The legal control of information assets in digital networks must be based on compliance with data protection and privacy requirements as well as the evidentiary capability for proving consent to data access and use. However, there are current unresolved legal challenges facing service providers imposed by regulatory consumer consent requirements: legal effectiveness, capability of automating processes, enforceability over time, and cross-sector interoperability. Outstanding current examples of these challenges with respect to personal data sharing exist in the areas of healthcare, financial services, and consumer transactions involving citizens in the European Union.

[3] For a paper that describes other use cases, *see:* http://kantarainitiative.org/confluence/download/attachments/78446705/UMALegalUseCasesforAnalyzingandDeterminingaLegalFramework%202017-03-26.pdf?api=v2.

GDPR

The EU General Data Protection Regulations (GDPR) come into effect in May 2018, and further limits the use of consumer data – new rules include consent for data usage, rights to portability, erasure and to be forgotten, and new accountabilities for third party data processors.[4] In particular, the data subject has increased rights where processing is based on consent.

HIPAA

Controllers or owners of medical records are required to obtain consent from patients before granting access to third parties in certain circumstances.[5] The challenge facing the global move toward electronic health records (EHR) is establishing a uniform and trustworthy approach for issuing and managing digital identity credentials and signatures. Key to achieving integrated and productive flow of EHRs will be enabling data holders to 1) classify the records, 2) allocate access rights, 3) determine the legal basis for and to whom access grants are being consented to. For these purposes, leveraging interoperable digital identities for authentication can provide significant advantages for EHRs. And EHR custodians need the means by which to leverage interoperable digital identities to ensure the ongoing integrity of digital records and to fulfill HIPAA informed consent and authorization requirements.[6]

PSD2

Under PSD2, payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.[7] Open Banking and PSD2 present the banking industry with a number of challenges that UMA may impact - on how to ensure data exposed to third parties is used properly and legally, on how third parties plan to use the data and in what volume, and on how consumers will consent to use of their data. To be compliant and relevant, Payment Service Providers (bank and non-bank) and FinTechs have to address these challenges. Specifically, UMA may be deployed to enable proof of the following requirements: a) the account holder has given explicit consent to that access if third party parties would like to use data for marketing purposes and b) it is required that consumers give their consent to merchants taking payments from bank accounts directly via APIs. Thus,

---

[4] See Articles 6, 7, 17, and 30 of the GDPR.

[5] 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").

[6] 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), *available at:* http://www.chhs.ca.gov/OHII/Documents/Demonstration%20Project%20Report%203.2014.pdf.

[7] EU's Payment Services Directive (PSD2), *available at:* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

UMA can solve party-to-party payment initiation and account information access-granting use cases that are not currently solvable/contemplated/viable through current technical solution paths (such as OAuth, OIDC, and "screen scraping+").

The Challenge of Ownership of Personal Data. Ownership of data, including personal information, is a matter that has yet to be resolved globally in a uniform manner.[8] With respect to reliable access control for online services and secure transactions, consumers need ways to be assured that the online service providers meet minimum standards that can be relied upon to protect their personal data without having to take the time to locate, read, and understand the many complex privacy policies and contracts.[9] In addition, protocols and software are needed to implement laws that deal with the granting of access rights to personal digital assets that might be stored by an array of record owners and custodians.[10]

Trust in Machine-Mediated Network Communications. Lack of trust is one of the most significant impediments to participation in the global digital network-based information society.[11] In many cases, online service end-users (consumers) often cannot easily understand the privacy or data protection policies used by holders of personal data that is shared whether for e-commerce, e-business, e-health, e-government, or social media processes and purposes.

User-Centric Personal Data Market. To enable the monetization of rights to control access to and use of personal data, end users need autonomy as rights holders. Of all available access management models, the user-centric model is the only one that can accomplish this. However, such a market system has yet to emerge.[12]

---

[8] Note the fundamental differences between the conception of privacy as a property right in the United States as compared with the European conception of privacy as a human right. And for a discussion of the inapplicability of both property law and intellectual property law concepts to determining legal rights in and control over personal information, *see* Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TEL. AND TECHNOLOGY LAW REV. 367-418 (2012), *available at*: http://repository.law.umich.edu/mttlr/vol18/iss2/1. "Whether we decide to give individuals "property" rights in their personal information or not, we will have to make hard choices about how power and authority – control – will be shared in a world of increasing interconnection." *Id.* 379-81.

[9] For a discussion of the context of consumer privacy concerns and medical devices. see Kathryn R. Coburn, *The Internet of Things: Scientific and Technical Innovations Predict, Preempt, and Treat Diseased*, THE SCITECH LAWYER, Volume 12, Issue 3, 18-20 (Spring 2016).

[10] *See*, for example, the need for Online Tools to implement the Revised Uniform Fiduciary Access to Digital Assets Act (2015). 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).

[11] For a discussion of the trust implications of machine-mediated communications, *see* Stephen Mason and Timothy Reiniger, *'Trust' Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?*, COMPUTER AND TEL. LAW REV., Volume 21, Issue 5, 135 – 148 (2015), *available at:* http://stephenmason.co.uk/wp-content/uploads/2017/03/2015_21_CTLR_issue_5_PrintFINALMASON.pdf.

[12] For a discussion of UMA, *see* THOMAS HARDJONO, DAVID SHRIER, AND ALEX PENTLAND EDS, TRUST::DATA A NEW FRAMEWORK FOR IDENTITY AND DATA SHARING, (Visionary Future 2016) at 110 ("end user centricity") and 199 (identified by the World Economic Forum as

2. UMA as a Method for Controlling Access and Processing Rights to Personal Digital Assets

UMA gives an individual a unified control point for authorizing who and what can get access to his or her personal digital assets no matter where he assets are held or stored. In addition, UMA allows the individual to make demands of other parties with which they must comply in order for their access request to be approved. These demands or policies can be tailored to many uses and contexts including recipient identity, scopes, and conditions.

The UMA protocol enables a new method for the granting and receipt of access rights by means of machine-readable licenses.[13] To enable automation and achieve greater efficiency, licenses in machine-readable form are already used for granting copyright permissions and information sharing permissions on the semantic web.[14] A possible challenge to implementing a user-centric access sharing protocol has been the lack of a set of uniform default contractual rules for the exchange of personal digital assets. Fortunately, UMA may leverage the Uniform Computer Information Transaction Act ("UCITA") as one source of default contractual rules upon which the licensing of access rights to personal digital assets may be based.[15]

UMA Protocol Access Sharing Strategy

- *Scalability: Asynchronous Consent Granting*
- *Revocability: Machine Readable Licenses that Enable Self-Enforcement*
- *Durability: Downstream Sharing Tailored to Context, Parties, and Time*

a "key enabler" in the report entitled "Persona Data: The Emergence of a New Asset Class") and 208-210 (describing the importance of personal data services and the emerging vendor relationship management model).

[13] For a discussion of the deployment of machine readable ontology licenses for setting and enforcing permissions for data sharing, *see* Andrew Clearwater, *The New Ontologies: The Effect of Copyright Protection on Public Scientific Data Sharing Using Semantic Web Ontologies*, 10 J. MARSHALL REV. INTEL. PROP. L. 182 (2010) (focusing on facilitating access to public scientific data through the semantic web).

[14] For an example of machine-readable copyright permission licenses, *see* Creative Commons, *available at*: https://creativecommons.org/licenses/.

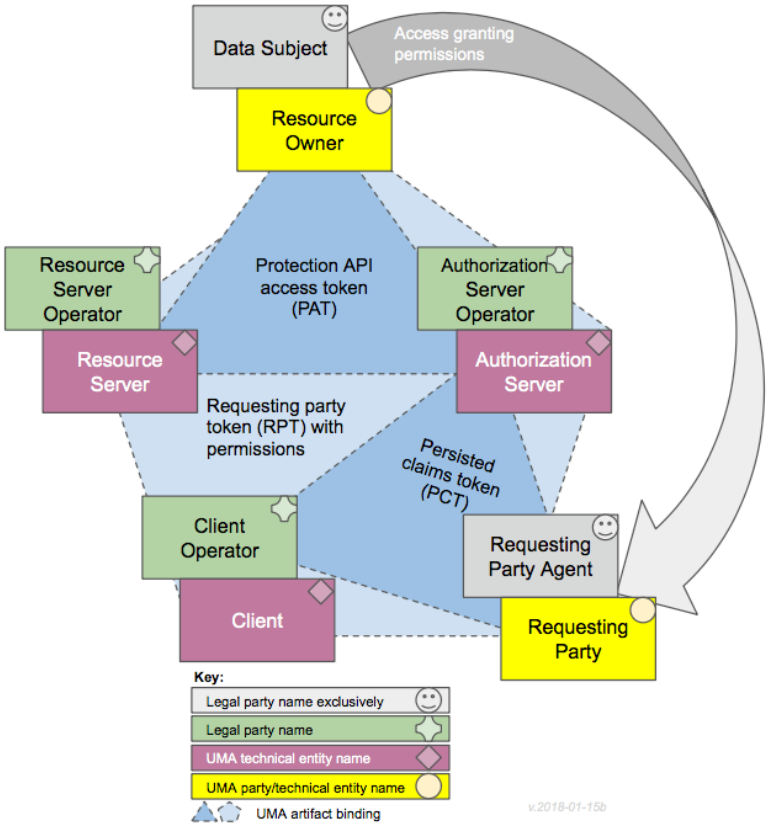
[15] For a discussion of the applicability of UCITA as a means of enabling individuals to control the transfer of personal data, *see* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy,* COLUMBIA LAW REV., Vol. 117, No. 6, 1369-1459 (2017) at 1457.

Value Propositions for UMA in Enabling the Right to Control Access and Processing Rights to Personal Digital Assets

UMA Value Perspectives	Law	Commerce	Communication
Autonomy	Access	Event	Protocols
Reciprocity	Consent	Effect	Policy Conditions
Objectivity	License	Economic	Permission Tokens

The UMA protocol enables the individual to centrally manage access and use rights (i.e. informational rights) with respect to personal digital assets by converting permission tokens into machine-readable licenses.[16] The Resource Owner needs to know that the license provider - the Authorization Server Operator - has the legal and technical capability to enforce a code of conduct and hold the licensees accountable to the license use terms. (For the reader's ease of reference, a complete set of UMA terms and definitions is provided in the Appendix to this paper.) UMA represents the first-time licensing has been applied to access rights or informational rights in general.

The following diagram provides an overview of the possible combination of participants in UMA and their interaction with the main available UMA artifacts.



[16] Machine-readable form is essential for UMA license to be easily integrated with various devices and interoperable with the wide array of UMA participants and rely parties while best respecting the Resource Owner's and Requesting Party's intentions.

3. The Legal Framework to Implement UMA

The basic legal framework to implement UMA consists of: 1) an Agency Contract, by which the Resource Owner delegates or appoints the Authorization Server Operator as licensing agent for access sharing, 2) creation of Access Contracts between the Authorization Server Operator and each Resource Server Operator, each Requesting Party, and each Client Operator, and 3) Authorization Server issuance of machine-readable licenses in the form of a) a protection API access token (PAT) to each Resource Server in a Resource Owner context and b) issuance of a requesting party token (RPT) and possibly a persisted claims token (PCT) to each Client on behalf of its Requesting Party. Note that conduct standards and controls regarding actual usage of the licenses by relying parties is out of scope for UMA.

Delegation to Authorization Server Operator as Agent

UMA recognizes the existence of a Data Subject, whether acting directly as the Resource Owner or acting through another legal person who is acting as Resource Owner on the Data Subject's behalf. Central to the UMA legal framework is the Resource Owner's appointment of the Authorization Server Operator as contractual and licensing agent for purposes of establishing and enforcing the Resource Owner's access and sharing policy conditions with respect to personal data and informational rights. By means of this agency relationship with the Authorization Server Operator, the Resource Owner's legal personality is multiplied in space *and time*.[17]

Access Contracts

Before any data sharing can take place within UMA, the Authorization Server Operator must enter into an Access Contract with each Resource Server Operator, Requesting Party, and Client Operator that establishes

[17] The key relationship, between principal and agent, "consists in the agent possessing the power to affect the principal's legal position and the principal being under a correlative liability to see his legal position altered by his agent." RODERICK MUNDAY, AGENCY LAW AND PRINCIPLES, 2nd ed (Oxford 2013) at 14.

UMA Token Types

Persisted Claims Token (PCT): A correlation handle issued by an Authorization Server that represents a set of claims collected during one authorization process to be used in a future authorization process.

Protection API Access Token (PAT): An OAuth access token used by the Resource Server at the Authorization Server's protection API.

Requesting Party Token (RPT): An OAuth access token associated with a set of permissions used by the Client to gain access to protected resources at the Resource Server.

agreement to: 1) the policy conditions in the form of protection policies, 2) the terms and conditions for the issuance and reliance upon licenses, and 3) enforcement. UMA defines policy conditions as "Access grant rules configured at an authorization server that achieve resource protection." These policy conditions reflect jurisdiction specific data protection requirements, such as the GDPR, and industry sector requirements imposed on medical, financial services, and telecommunications.[18]

Licensing of Access and Disclosure Rights: UMA Tokens as Machine Readable Licenses

Licenses are used to create a fixed reference for information integrity and shared meaning, upon which to determine legal relationships.[19] To be authoritative, the license designates the legal conditions under which the issuers and users agree with one another and create a trust relationship. In addition to ownership of the data or records, the source of the licensing authority could be a data protection law, consent requirement, or obligations with respect to personally identifying information.[20] UMA also may leverage laws such as the UCITA as a source of legal authority for licensing informational rights in the form of the user's right to control future access and use of his or her personal digital assets.

A license is a unilateral permission given to a licensee to use or take an

[18] 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.

[19] For consideration of the applicability to UMA of the conditional licensing model, see the discussion of this model in HEATHER MEEKER, OPEN SOURCE FOR BUSINESS: A PRACTICAL GUIDE TO OPEN SOURCE SOFTWARE LICENSING 2ed (2017) at 61-9.

[20] Note that informational rights in personal data do not currently derive from intellectual property laws. For a discussion of the inapplicability of copyright doctrines to the content created and captured by devices in the Internet of things, see Christina D. Frangiosa, *Copyright Ownership and IOT Devices*, THE SCITECH LAWYER, Volume 12, Issue 3, 21-5 (Spring 2016).

action with respect to the licensor's property, including property in the form of digital assets.[21] Without the license, the licensee would not be able lawfully to use or take such action with respect to another's property. A licensed may be conditional such that it is automatically revoked upon failure by the licensee to honor the conditions.[22]

The license has emerged around the world as an essential legal device for software copyright granting, information content sharing, and network communication usage.[23] Use of licenses, especially in machine-readable form, has several advantages. First, they are the only available legal means for a user unilaterally to control the granting of access rights. Second, license grants can be transferrable so as to enable individuals to facilitate the flow of personal digital assets. Third, licenses provide scalability and dynamism for (near-)future automation and removing friction from balanced empowerment.[24] Fourth, licenses build on the envisioned UMA "toolkit" of standard policies and permissions that are programmed into the access and agency contracts. Fifth, licenses for controlling the granting of access rights can be easily mapped to the UMA technical artefacts. Sixth, licenses can be easily self-enforced by the Resource Owner through ease of legal and technical revocation. In sum, the dynamic calibration of licensing relationships being enabled by UMA has potentially unlimited value. To this end, risk taken based on trust requires that there be a responsible enforcement agent, such as an Authorization Server Operator, in accordance with an applicable trust framework or code of conduct.

Mapping UMA Licensing Relationships

In the UMA protocol, access permissions invoke two categories of access rights: 1) permissions to grant access and 2) permission to receive access. And access permissions 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).

Authorization Server Operator Licensing to the Resource Server Operator

As an agent for the Resource Owner, the Authorization Server Operator has its service (the Authorization Server) issue a PAT to the Resource Server Operator as a means of licensing or permitting the Resource

---

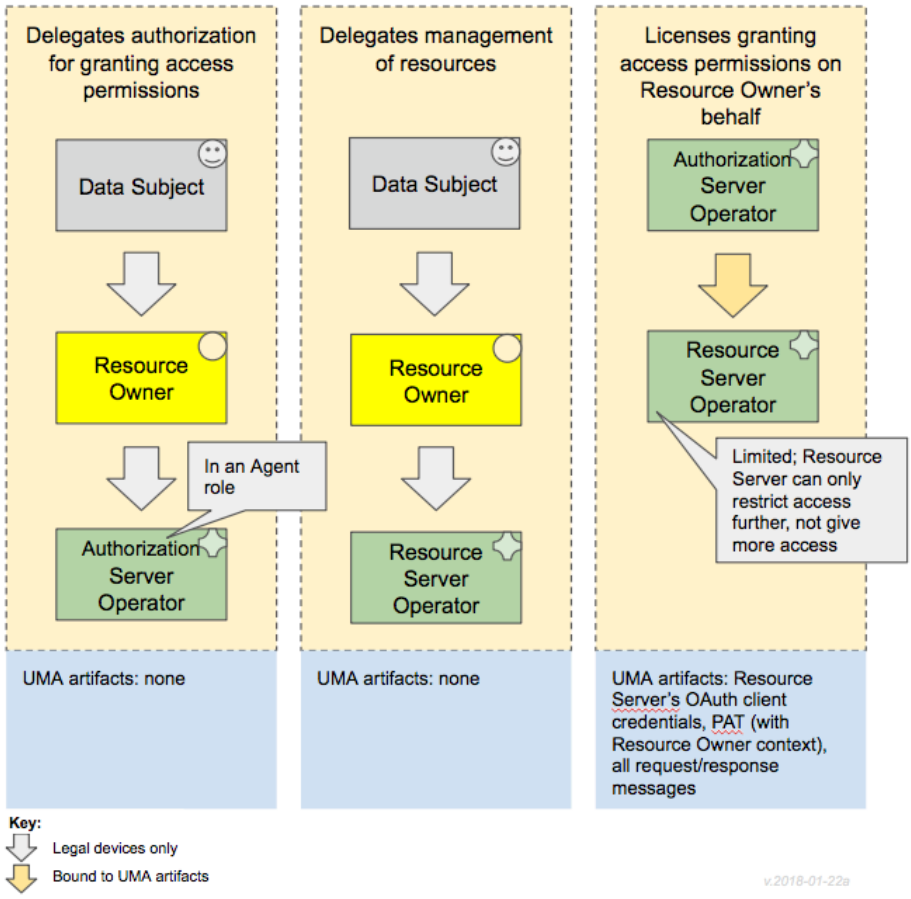
[21] "License" is defined as "[a] permission, usually revocable, to commit some act that would otherwise be unlawful." BLACK'S LAW DICTIONARY 9th ed (2009) at 1002.

[22] *Supra*, note 19. Conditional licenses and licenses as contracts differ in several ways, including form and enforcement mechanism.

[23] *Supra*, note 15 at 1407 and 1417. Licenses are emerging also as a legal device for the transfer of data in a Personal Data Economy model.

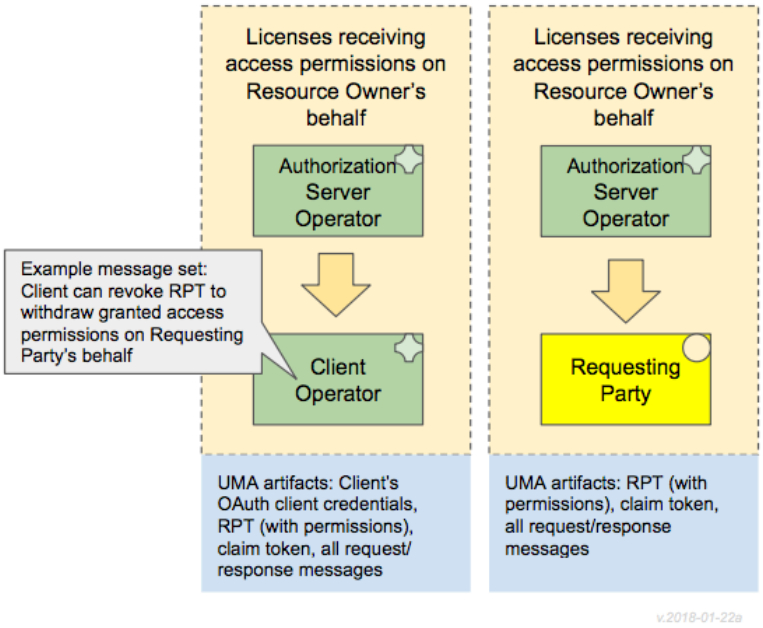
[24] *See* report of Blockchain and Smart Contracts Group to the Kantara Initiative, *available at:* www.tinyurl.com/bscdgreport. States in the United States are taking steps to give statutory recognition to the concept of smart contracts. For example, in Arizona, *see* ARS 44.7061 (E)(2) ("'Smart contract' means an event-driven program, that runs on a distributed, decentralized, shared, and replicated ledger and that can take custody over and instruct transfer of assets on that ledger"), *available at:* https://legiscan.com/AZ/text/HB2417/id/1588180/Arizona-2017-HB2417-Chaptered.html.

Server Operator to grant access to the Resource owner's Protected Resources. Such licensing permissions for access sharing are essential for custodians of financial information such as banks. These licensing permissions can also be deployed by owners of records, such as hospitals, in which the data subject has a measure of legal control over access rights. See the figure below.



Authorization Server Operator Licensing to Requesting Party and Client Operator

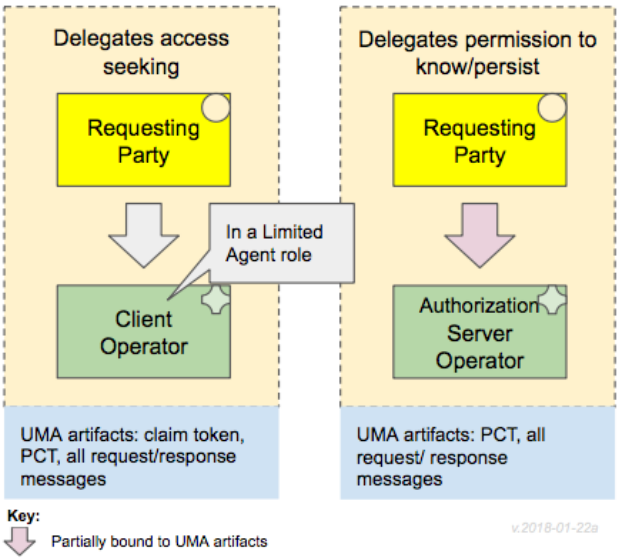
As an agent for the Resource Owner, the Authorization Server Operator has its service (the Authorization Server) issue a RPT to the Requesting Party as a means of licensing or permitting access to the Resource Owner's Protected Resources held by a Resource Server Owner. By performing the role of verifying both identity (or, alternatively, non-uniquely identifying claims) and authority of the Requesting Party, the Authorization Server Operator satisfies these challenging duties normally required of the Resource Server Operator whether as a record owner or custodian. See the figure below.



The Resource Owner has a choice of opting for issuing RPT licenses to the Requesting Party that are either transferable or non-transferable with respect to access rights.

Requesting Party and Client Operator Relationship

In some instances, the Requesting Party may desire to contract with Client Operator to serve as a limited purpose agent on the Requesting Party's behalf. The PCT is designed to enable a one-time authentication of the Requesting Party that can be leveraged by the Client Operator. See the figure below.



If the Requesting Party has contracted a Client Operator to serve as a limited purpose agent on the Requesting Party's behalf, the Authorization Server Operator has its service (the Authorization Server) issue a PCT to the Client Operator as a means of licensing or permitting access to the Resource Owner's Protected Resources held by a Resource Server Owner. As part of the Authorization Server Owner's function of verifying the Requesting Party, personally identifying information of the Requesting Party is necessarily processed by the Authorization Server Operator. As a means of limiting the access to and use of this personally identifying information and to best meet privacy obligations falling on the Authorization Server Operator, the PCT is an essential access licensing tool.

Consent Receipts for Protection of Requesting Party Privacy

A consent receipt is a record of a consent provided to an individual at the point in a person agrees to the sharing of personal information. Its purpose is to capture the privacy policy associated with the personal information so that the consent receipt can be easily used to communicate and manage consent and sharing of personal information once it is provided.[25] Some regulations, such as GDPR, will require the Authorization Server Operator to obtain a consent receipt from the Requesting Party to access personally identifying information for purposes of authenticating the Requesting. And, with respect to UMA, the Resource Server Operator may rely on a consent receipt from the Resource Owner as proof of the Resource Owner's appointment as a fiduciary, such as through a power of attorney document signed by the Data Subject.[26]

4. Advantages of the UMA Licensing Model for User-Centric Control of Access and Process Rights to Personal Digital Assets

The licensing model for UMA provides the necessary legal foundations for implementing and operating a regime for the creation and validation of authoritative access relationship both by public authorities and private entities. The open, dynamic structure of UMA will serve as essential infrastructure for unleashing the flow of trusted access sharing of personal data. The following is a brief description of several important implications.

[25] For a discussion of consent receipts, *see* the Kantara Initiative program, *available at*: https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification.

[26] In the United States, the term "fiduciaries" typically includes personal representatives of decedents' estates, conservators for protected persons, agents acting pursuant to a power of attorney, and trustees.

Enables Consent as Legal Basis for GDPR-Compliant Data Processing Rights

Legal consent issues are especially at issue with cross-border data transfers requirements such as the GDPR[27] and the associated sharing of personal data for identity authentication purposes.[28] Currently, Data Subject consent as a basis for Data Controllers and Data Processors to provide access to individual's data is unrealized for lack of available means that Data Controllers and Data Processors can integrate and make available to Data Subjects. The UMA licensing model provides a means of achieving GDPR-compliant user-specified access consent that is scalable for Data Controllers and Data Processors while, at the same time, giving the individual privacy enhancing tools that are proactive and preventative.[29]

- *Scalability.* A working hypothesis for UMA is that the capability for the asynchronous granting of access sharing consents is a fundamental enabler of privacy in digital network markets. By allowing data subjects and resource owners comprehensive and real-time ability to provide user-specified access sharing consent in the form of licenses, UMA will enable compliance with the GDPR as well any other requirement for proof of consent to share access to personal data.[30]
- *Withdrawal of Consent.* The UMA consent licensing model enables a data subject or resource owner to revoke previously granted consent to access and use rights.[31]
- *Durability.* When data processing is authorized by means of the consent of the Data Subject, Data Controllers may share the data with Data Processors who may, in turn, share the data with other downstream Data Processors.[32] Proof of consent to access sharing by means of a UMA license easily and effectively enables this. In addition, Data Controllers are required to notify downstream Data Processors about any withdrawal of consent. Revocation of the UMA license enables an effective means for companies to track the need for providing such notifications.

---

[27] *See* Articles 41, 42, and 44 (1)(g) of the GDPR and Opinion 4/2017 of the European Data Protection Supervisor, sections 3.2 and 3.3. *See also* the EC Article 29 Working Party on Data Protection entitled "Guidelines on Consent under Regulation 2016/679" adopted on November 28, 2017, *available at*: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

[28] *See* Article 1(f)(i) of the eIDAS Regulation, *available at:* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[29] *See* UMA Privacy Work Group study of privacy by design principles as applied to UMA, *available at:* https://kantarainitiative.org/confluence/display/uma/Privacy+by+Design+Implications+of+UMA. "While many systems focus solely on gathering user consent at the time of the access request, UMA enables users (human beings in the "resource owner" role of the UMA protocol) to choose access policies before a data requester attempts access. It also enables resource owners to consider data access requests and approve or deny them, either right away or at some time of their own choosing. This enables a different relationship between resource owners and requesters."

[30] Article 6(1)(a) of the GDPR authorizes the processing of personal data on the basis of the individual's granting of consent.

[31] Such capability is required, for example, in Article 7(3) (conditions of consent) as well as Article 17 (right to be forgotten) of the GDPR.

[32] Consent requirements for sharing by Data Controllers with Data Processors is found in Articles 24 and 28 of the GDPR.

- *Auditability and Record-keeping.* Data Controllers and Data Processors are required by Article 30 of the GDPR to maintain records of all data processing that they have performed.

Creation of a User-Centric Personal Data Market

UMA enables the emergence of a user-centric personal data market. For maximum user autonomy, an access sharing approach is needed by which users may grant access rights using a method of their own choosing and that meets a given relying party's required level of authorized access and use.

The UMA License as a Product

Disclosing parties need accessible means of assurance in advance of data transactions that receiving parties meet reliable minimum standards that protect their personal digital assets. For commercial purposes, the UMA license serves a legal device to monetize access and use rights in personal data that flows through communication networks.[33] A permission token in the form of a license is needed to provide objective authorization for access sharing to disclosing and receiving parties.[34]

Self-Enforceability of Informational Rights in Personal Data

Licensing of access rights brings the following important legal enforceability advantages to UMA:

- Complete set of default licensing rules
- Legal support for code-enable self-enforcing data protections based on licensing
- Language that defines sets forth Access Contracts
- Approval for the use of electronic agents
- Choice of law provisions that enable parties to choose an appropriate jurisdiction as the governing law

---

[33] 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).

[34] 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. For a discussion of the emerging Canadian trust framework that recognizes the need for citizens to have tools for managing both digital identity and the personal information, *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.

- Clearly defined attribution procedures for enabling relying parties to prove authentication events
- Implied warranties that better protect relying parties

As one example of an existing law, the UCITA may be leveraged as a source of default contractual rules for licensing the end users right to control access relationships to personal data.

Conclusion

Key to the exchange of personal digital assets in the global digital information society is knocking down trust barriers in machine-mediated network communications. Fear of abuse of unauthorized use of personal identifying information and violation of privacy policies is a significant barrier to access sharing for individuals. And receiving parties' inability to obtain automated consent to access sharing is a significant efficiency and liability risk barrier.

UMA provides a digital access management platform for digitizing and automating the individual's control of access rights to personal digital assets. The UMA access sharing method aligns with trust frameworks under development throughout the world to enable the provisioning of an enforceable personal data sharing market built on the dynamic granting of access rights by means of UMA licenses.

Personal data markets must be based on objective facts and not subjective or arbitrary interests. UMA is intended to help foster and normalize the interactions for sharing access to all personal digital assets. To best enhance the volume and velocity of information flow in networks, the access sharing permissions and receipts represented by each license must be clear, unambiguous, easily withdrawable, and self-enforcing.

This paper seeks to promote a common understanding for a user-centric model of licensing access rights as a means of controlling access relationships to personal digital assets and to make clear that:

- There is an opportunity for the UMA protocol to unleash a user-centric personal data sharing network-based market.
- The UMA-enabled platform can provide the capability of complying with an array of regulatory access consent requirements and on a global basis.
- There is a global need for UMA licenses that operate under clearly understood performance standards for granting and delegating access rights to personal data; and,

- Individuals need ways to be assured that the online service providers/relying parties operate with shared privacy commitments that can be relied upon to protect personal digital assets when granting access.

The next papers in this series will explore the application of UMA licensing model to specific use cases for various categories of owners and custodians of personal digital assets in the global digital information society.

Appendix: UMA Definitions From the Legal Perspective

Access Contract: A contract or agreement to obtain by electronic means access to, or Information from, an Information processing system of another Person, or the equivalent of such access.
Reference: Uniform Computer Information Transactions Act ("UCITA") (2002), sections 102(a)(1) and 611.

Agency Contract: A contract or agreement in which one Person (called the principal) delegates to another Person (called the agent) the transaction of some lawful business or the authority to do certain acts on the principal's behalf in relation to the principal's rights or property and subject to the principal's control.
Reference: American Law Institute's Restatement of the Law – Agency, section 1.01; Black's Law Dictionary (9th ed.).

Attribution Procedure: Procedure to verify that an electronic authentication, display, message, record, or performance is that of a particular Person or to detect changes or errors in Information. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment.
Reference: UCITA sections 102(a)(5), 107, 108, 211, and 212; Uniform Electronic Transactions Act (1999) ("UETA"), sections 2(14) ("Security Procedure") and 9.

Automated Transaction: A transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
Reference: UCITA section 102(a)(7); UETA sections 2(2) and 14.

Authorization Server Operator: A Person responsible for running and operating an Authorization Server that controls access and use policies pertaining to Protected Resources on behalf of a Resource Owner; acts as licensing agent for the Resource Owner and may perform these duties by means of an Electronic Agent.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization, section 1.2; RUFADA sections 2(9) ("Designated Recipient") and 2(16) ("Online Tool").

Client Operator: A Person responsible for running and operating a software application (the "Client") used by a Requesting Party or Requesting Party Agent to access and use a Protected Resource.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation.

Data Subject: The Person to whom a Protected Resource relates.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; RUFADA section 2(21)("Protected Person").

Digital Asset: An electronic Record in which a Person has an Informational Right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic Record.
Reference: Revised Uniform Fiduciary Access to Digital Assets Act (2015)("RUFADA"), section 2(10).

Electronic Agent: A computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.
Reference: UCITA sections 102(a)(27) and 112; UETA sections 2(6) and 14.

Individual: A natural Person**.**
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; UCITA section 102(a)(51); UETA section 2(12); RUFADA 2(17).

Information: Data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.
Reference: UCITA section 102(a)(35); UETA section 2(10); RUFADA section 2(15).

Informational Rights: All rights in Information created under any law that gives a Person, independently of contract, a right to control, preclude, or consent to another Person's access to or disclosure of the Information on the basis of the Person's or rights holder's interest in the Information.
Reference: UCITA section 102(a)(38).

Legal Person: A corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental subdivision, instrumentality, or agency, public corporation, or any other legal or commercial entity.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; UCITA section 102(a)(51); UETA section 2(12); RUFADA section 2(17).

License: A contract that authorizes access to or disclosure of a Protected Resource or Informational Rights in a Protected Resource, but expressly limits the access or disclosure authorized or expressly grants fewer than all such Informational Rights in the Protected Resource, whether or not the licensor has ownership of the data.
Reference: UCITA section 102(a)(41).

Licensee: A Person entitled by agreement to acquire or exercise rights in, or to give or receive access to, a Protected Resource under an agreement to which User Managed Access default or approve model contractual terms apply.
Reference: UCITA section 102(a)(42).

Licensor: A Person obligated by agreement to transfer or create access rights in computer Information or Informational Rights in it under an agreement to which User Managed Access default or approved model contractual terms apply.
Reference: UCITA section 102(a)(43).

Online Tool: An electronic service provided by a Resource Server Operator or Authorization Server Operator that allows the Resource Owner, in an agreement distinct from the terms-of-service agreement between the Resource Server Operator and the Resource Owner, to provide directions for disclosure or nondisclosure of digital assets to a Client Operator or Requesting Party.
Reference: RUFADA section 2(16)("Online Tool"). UMA is an example of an Online Tool.

Person: An Individual or Legal Person.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; UCITA section 102(a)(51); UETA section 2(12); RUFADA section 2(17).

Protected Resource: Information held by a Resource Server, including personal Digital Assets and Online Tools, in which a Resource Owner either has Informational Rights or over which and through which a Resource Owner has the authority to exercise Informational Rights.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; RUFADA section 2(10).

Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
Reference: UCITA section 102(a)(55); UETA section 2(7) and (13); RUFADA section 2(22).

Requesting Party: A Person with legal capacity and authority, either as an Individual or Legal Person, to request and secure access to a Protected Resource either directly with a Resource Server Operator or by means of a Client Operator.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization, section 1.2; RUFADA sections 2(5) ("Conservator"), 2(14)("Fiduciary"), 2(18)("Personal Representative", 2(19)("Power of Attorney"), and 2(25)("Trustee").

Requesting Party Agent: A Person seeking access to a Protected Resource on behalf of a Requesting Party and by means of a Client software application.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation.

Resource Server Operator: A Person responsible for running and operating a Resource Server that collects, stores, and disseminates Protected Resources: receives licenses from the Authorization Server Operator that provide the RO's permission to give RqP's and CO's access to Protected Resources.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization and supporting documentation; RUFADA section 2(8)("Custodian").

Resource Owner: A Person with legal capacity and authority to act as rights holder, either on behalf of a Data Subject or directly as an Individual or Legal Person, to license access to, sharing, and use of (permissions) relating to a Protected Resource or Informational Rights in a Protected Resource. The Resource Owner is authorized to delegate to an Authorization Server Operator access control, consent, and licensing functions relating to a Protected Resource.
Reference: User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization, section 1.2; RUFADA sections 2(5) ("Conservator"), 2(14)("Fiduciary"), 2(18)("Personal Representative", 2(19)("Power of Attorney"), 2(21)("Protected Person"), 2(25)("Trustee"), and 2(26)("User").

Contributors

The following people made significant contributions to this report:

- Domenico Catalano, Oracle Corporation
- Kathleen Connor
- Theresa Connor
- Devon Connor-Green
- Salvatore D'Agostino
- Scott L. David
- Adrian Gropper, HealthURL
- Thomas Hardjono, MIT
- Jim Hazard, CommonAccord
- Andrew Hindle, Hindle Consulting Limited
- Bjorn Hjelm, Verizon
- Mary Hodder, Customer Commons
- Andrew Hughes, ITIM Consulting
- Robert Lapes, Capgemini UK
- Mark Lizar, SmartSpecies
- Eve Maler, ForgeRock
- Ann Racuya-Robbins, World Knowledge Bank
- Jeff Stollman
- John Wunderlich, John Wunderlich & Associates, Inc.

Additional contributors to this specification include the Kantara UMA Work Group participants, a list of whom can be found here.