Title:
Subtitle:
Version:
Date:
Editor:

Abstract:

Status of This Document:

UMA Business-Legal Framework Use Cases

tbs

Draft (not yet WG-approved)

Last edited August 25, 2019

Timother S. Reiniger, Esq., UMA WG Legal Editor

This Draft Report provides use cases and a complete set of terms and definitions for the UMA business-legal framework to help explicate how the UMA protocol enables a license-based model for controlling access rights to personal digital assets.

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

Legal Role	Abbrev	Definition	Source
Authorization Server Operator	ASO	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.	Proposed Licensing Model for UMA
Client Operator	CO	A Person responsible for running and operating a software application (the “Client”) used by a Requesting Party or Requesting Agent to access and use a Protected Resource.	Proposed Licensing Model for UMA
Data Subject	DS	The Person to whom a Protected Resource relates.	Proposed Licensing Model for UMA
Individual	I	A natural Person.	Proposed Licensing Model for UMA
Legal Person	LP	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.	Proposed Licensing Model for UMA
Licensee	n/a	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.	Proposed Licensing Model for UMA
Licensor	n/a	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.	Proposed Licensing Model for UMA

Org equivalent of a Data Subject

Person	n/a	An Individual or Legal Person.	Proposed Licensing Model for UMA
Representative	Rep	A Person empowered to act for another, including an agent, a legal guardian, conservator, an officer of or proxy for a corporation or association, and a trustee, executor, or administrator of an estate. (Reference: UCC 1-201(33).)	Tim Reiniger, UMA WG Legal Editor
Requesting Agent	RqA	A Person seeking access to a Protected Resource on behalf of a Requesting Party and by means of a Client software application.	Proposed Licensing Model for UMA
Requesting Party	RqP	A Person with legal capacity and authority to request and secure access to a Protected Resource either directly with a Resource Server Operator or by means of a Client Operator.	Proposed Licensing Model for UMA
Resource Rights Administrator	RRA	A Person with legal capacity and authority to act as rights holder on behalf of a Data Subject 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.	Proposed Licensing Model for UMA
Resource Server Operator	RSO	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.	Proposed Licensing Model for UMA

Link	Mapping to Technical Role
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	as
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	c
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a

	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	rqp
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	n/a
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	ro
https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/	rs

Comments

Corrected the definition to say Requesting Agent, matching our current term.

This would be useful for discussing use cases in which an Individual is an RRA acting on behalf of such an organization. Such use cases are not precisely in our scope for now. "Principal"? Note that "Principal" is used as part of the definition of Agency Contract. (Or can we simply stick to Legal Person?) We decided we don't need this term yet.

Was "Requesting Party Agent" and we renamed it after publishing the Proposed Licensing Model for UMA.

Tweaked the definition to remove the phrase mentioning "as an Individual or Legal Person" after publishing the Proposed Licensing Model for UMA.

Was "Resource Owner" and we renamed it after publishing the Proposed Licensing Model for UMA. Tweaked the definition to remove the phrase mentioning "as an Individual or Legal Person" after publishing the Proposed Licensing Model for UMA.

Technical Entity	Abbrev	Definition
authorization server	as	A server that protects, on a resource owner's behalf, resources hosted at a resource server.
client	c	An application that is capable of making requests for protected resources with the resource owner's authorization and on the requesting party's behalf.
requesting party	rqp	A natural or legal person that uses a client to seek access to a protected resource. The requesting party may or may not be the same party as the resource owner.
resource owner	ro	An entity capable of granting access to a protected resource, the "user" in User-Managed Access. The resource owner MAY be an end-user (natural person) or MAY be a non-human entity treated as a person for limited legal purposes (legal person), such as a corporation.
resource server	rs	A server that hosts resources on a resource owner's behalf and is capable of accepting and responding to requests for protected resources.

Source	Link
UMA Grant Sec 1.2	https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.2
UMA Grant Sec 1.2	https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.2
UMA Grant Sec 1.2	https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.2
UMA Grant Sec 1.2	https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.2
UMA Grant Sec 1.2	https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.2

tbs - add all static 1:1 is-a, acts-as, and other relationships

Legal Device, Artifact, or Concept	Abbrev	Definition	Source	Link	Comments			
(business relationship) Access Contract (alternatively: Delegates resource management to)	Delegates-mgmt-to	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.			Also see the UMA Legal role definitions slide deck.			
(business relationship) Agency Contract (alternatively: Delegates authority for granting and managing access permissions to)	Delegates-perm-authority-to	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.			Also see the UMA Legal role definitions slide deck.			
(business relationship) Delegates access seeking authority to	Delegates-seek-authority-to							
(business relationship) Delegates permission to know/persist to	Permits-knowing-claims							
(business relationship) Licenses granting access permissions to	Licenses-perm-granting-to							
(business relationship) Licenses receiving access permissions to	Licenses-perm-getting-to							
(business relationship) Party in role A also acts in role B	Acts-as-a							
Attribution Procedure	n/a	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.						
Automated Transaction	n/a	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.						
Digital Asset	n/a	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.						
Electronic Agent	n/a	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.	Proposed Licensing Model for UMA	https://kantarainitiative.org/file-downloads/uma-business-model-0-7e-2018-02-01-pdf/				
Information		Data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.						
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.						
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.						
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.						
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.						
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.						

Technical Artifact or Concepts	Technical Artifact Abbrev
claim	n/a
claim token	n/a
permission	n/a
permission ticket	n/a
persisted claims token	PCT
protection API access token	PAT
requesting party token	RPT

Definition	Definition Source
A statement of the value or values of one or more attributes of an entity. The authorization server typically needs to collect and assess one or more claims of the requesting party or client against policy conditions as part of protecting a resource. The two methods available for UMA claims collection are claims pushing and interactive claims gathering. Note: Claims collection might involve authentication for unique user identification, but depending on policy conditions might additionally or instead involve the collection of non-uniquely identifying attributes, authorization for some action (for example, see Section 3.3.3), or other statements of agreement.	UMA Grant Sec 1.3
A package of claims provided directly by the client to the authorization server through claims pushing.	UMA Grant Sec 1.3
Authorized access to a particular resource with some number of scopes bound to that resource. A permission ticket represents some number of requested permissions. An RPT represents some number of granted permissions. Permissions are part of the authorization server's process and are opaque to the client.	UMA Grant Sec 1.3
A correlation handle representing requested permissions that is created and maintained by the authorization server, initially passed to the client by the resource server, and presented by the client at the token endpoint and during requesting party redirects.	UMA Grant Sec 1.3
A correlation handle issued by an authorization server that represents a set of claims collected during one authorization process, available for a client to use in attempting to optimize a future authorization process.	UMA Grant Sec 1.3
An [RFC6749] access token with the scope uma_protection, used by the resource server as a client of the authorization server's protection API. The resource owner involved in the UMA grant is the same entity taking on the role of the resource owner authorizing issuance of the PAT.	UMA Federated Authorization Sec 1.2
An OAuth access token associated with the UMA grant. An RPT is unique to a requesting party, client, authorization server, resource server, and resource owner.	UMA Grant Sec 1.3

Definition Source Link
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html#rfc.section.1.2
https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html#rfc.section.1.3

Pattern Name	Pattern Type	Pattern
Self-Managed Resources	Steady state	DS=I **DS=RRA** **∴ DS=ro**
Representative-Managed Resources	Steady state	DS=I Representative=I DS≠RRA **Representative=RRA** **∴ Proxy=ro**
		DS=I Representative=I **DS=RRA** **Representative=RRA** **∴ multiple RRA's = multiple ro's**
		"DS=I Representative=I **DS≠RRA** **Representatives=RRA's** **∴ multiple RRA's = multiple ro's**
		"Org equivalent of a Data Subject"=LP Representative=I **Representative=RRA** **∴ Representative=ro**

Use Cases

• DS Alice is a competent adult who manages sharing her own resources: health data, financial data, and/or smart device data/control.

• DS Johnny is an underage child. Rep Alice is his mother and legal guardian. She manages the sharing of his resources on his behalf.

• DS Karl is elderly and incompetent to consent. Rep Alice holds his power of attorney and acts as his legal guardian. She manages the sharing of his resources on his behalf.

• DS Alice manages sharing her own bank account information and payments. She has arranged for Proxy Bob to be a joint account holder.

• DS Alice manages sharing her own legal document resources. She has delegated Proxy Bob to hold her power of attorney and manage sharing equally with her.

• DS Johnny is an underage child. Proxies Bob and Carol are his parents and are both required to manage consent over release of his health information to provide medical care.

• Proxy Penny is an employee of organization AlphaCo managing resource sharing on its behalf.

• Employee Penny is is an employee of organization AlphaCo creating and managing resources on her own recognizance as an employee, for as long as she is an employee, for example, documents and spreadsheets.

Comments

Technically this hasn't been in the scope of the business-legal work. Defer for now?