



User-Managed Access (UMA) 101

Steve Venema, Kantara Initiative UMA Work Group Vice-chair

IIWXXXVI | 18Apr2023





UMA Topics

- Why?
- Actors/Roles
- Use Cases
- Specs
- Privacy and “BOLTS” implications

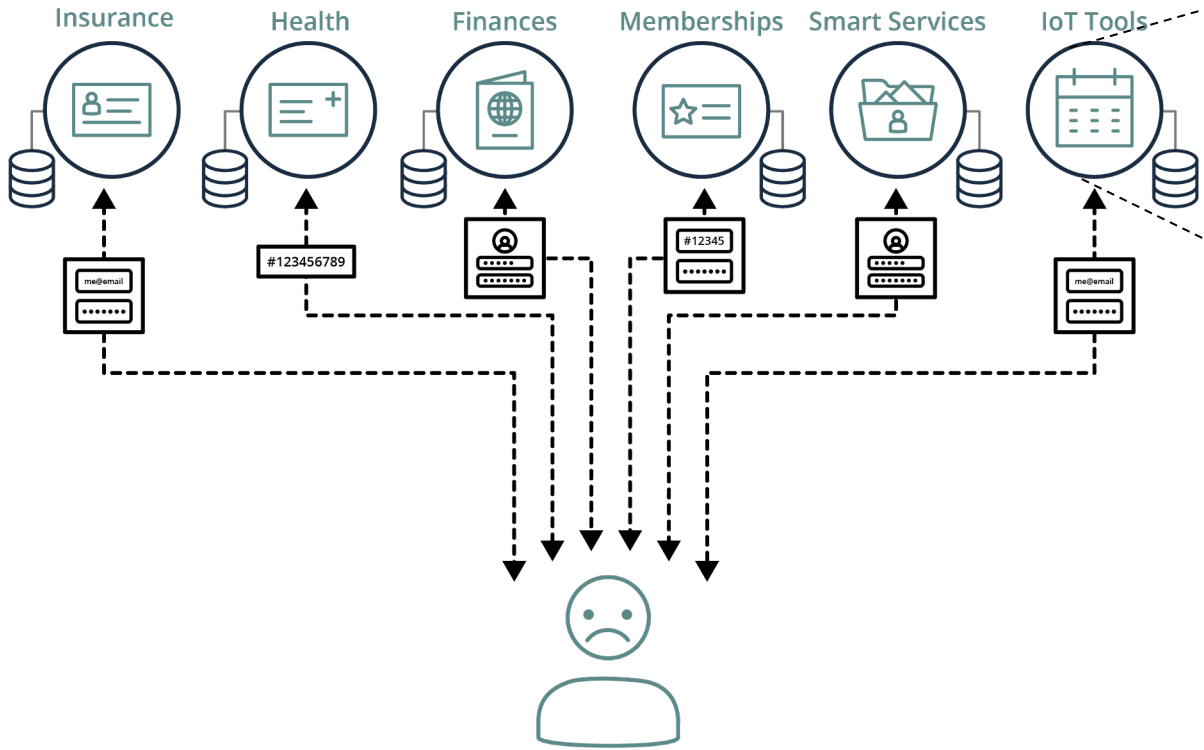


Why UMA?

The Usual Walled Gardens

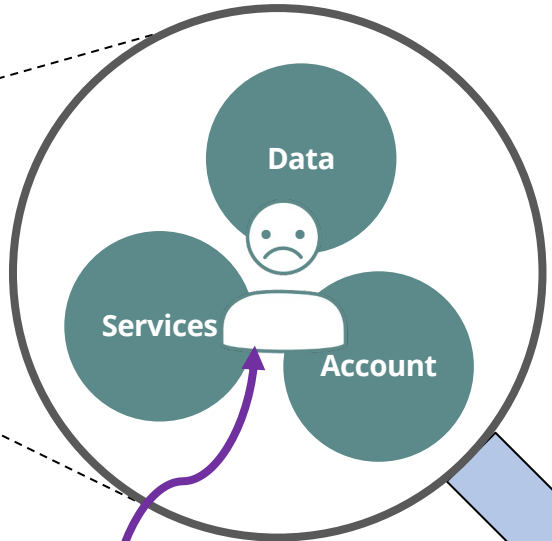
Difficult to share your data with others

120 Walled Gardens – 1 identity at a time

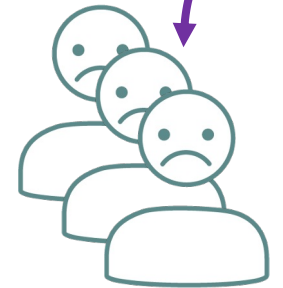


Me online x 120!

Resource Owner (RO)

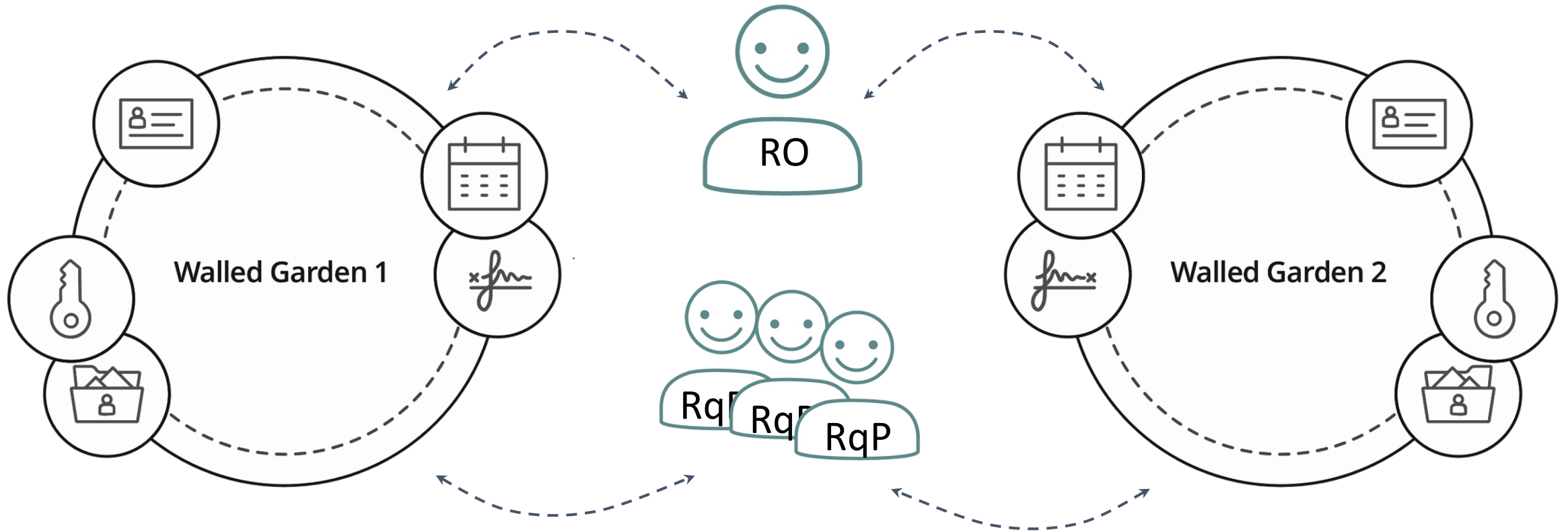


Requesting Parties (RqP)



How can I selectively share access to my data and services with others?

We Can Do Better



What if... we could create a user centered ecosystem that makes it simple to share your data with others?
Without sharing your credentials!

UMA in a nutshell

- Developed in the Kantara Initiative
 - V2.0 complete in Jan 2018
 - <https://kantara.atlassian.net/wiki/spaces/uma/overview>
- Leverages existing open standards:
 - OAuth2
 - OpenID Connect
- Profiled by multiple industry sectors
 - Financial, healthcare
- UMA business model effort (“BLT”) supports **legal licensing** for personal digital assets
 - Example: Mother (legal guardian) manages sharing for child (data subject); child becomes old enough and starts to manage sharing herself



UMA Roles:

RO - Resource Owner
- Client (App)

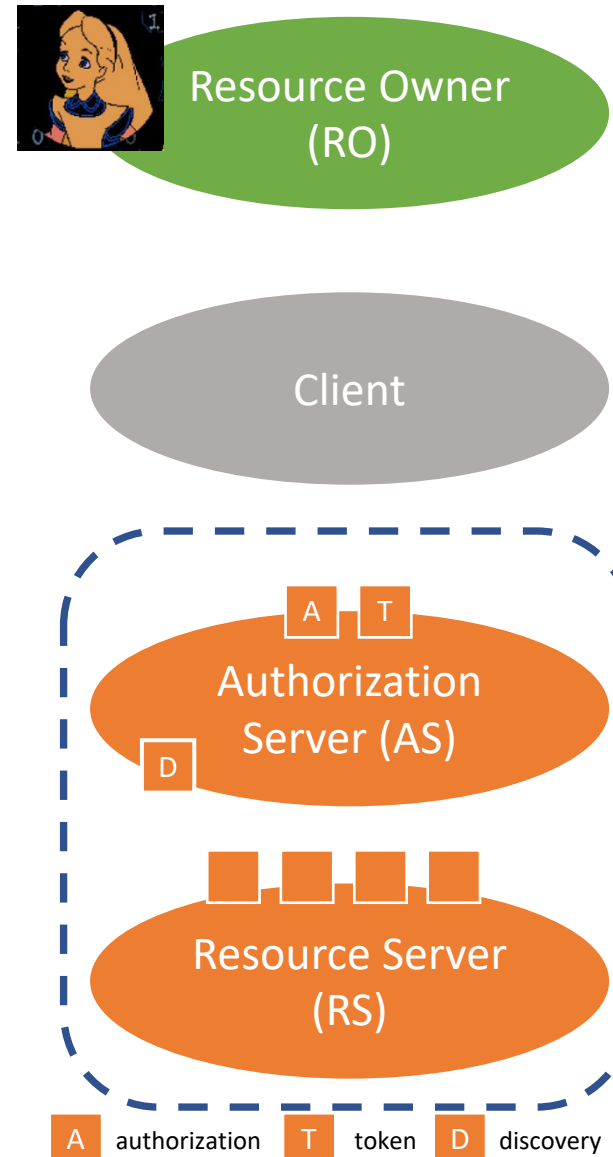
RS - Resource Server

AS - Authorization Server

RqP - Requesting Party

OAuth enables constrained delegation of access to apps

- Benefits**
- Flexible, clever API security **framework**
 - Alice can **agree** to app connections and also **revoke** them



UMA adds cross-party sharing...



Resource Owner
(RO)

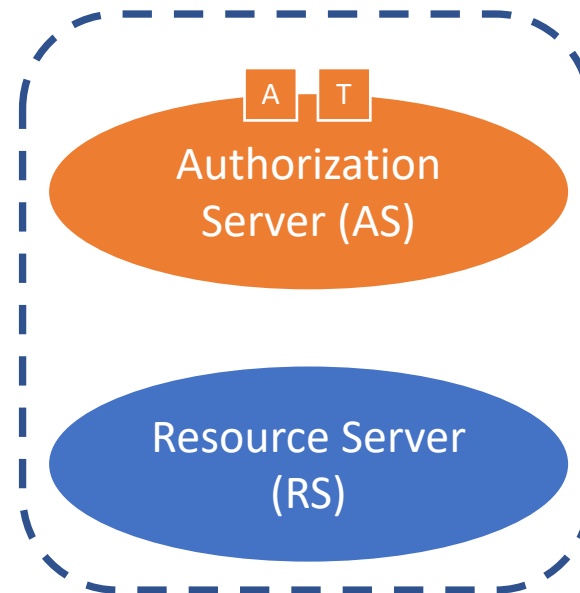
Benefits

- **Secure** delegation
- Alice **can be absent** when Bob attempts access
- Helpful **error handling** for client applications



Requesting
Party (RqP)

Client



...in a wide ecosystem...



Resource Owner
(RO)

Benefits

- Alice **controls trust** between a service that hosts her resources and a service that authorizes access to them



Requesting
Party (RqP)

Client

A T

Authorization
Server (AS)



Resource Server
(RS)



...of resource servers



Resource Owner (RO)



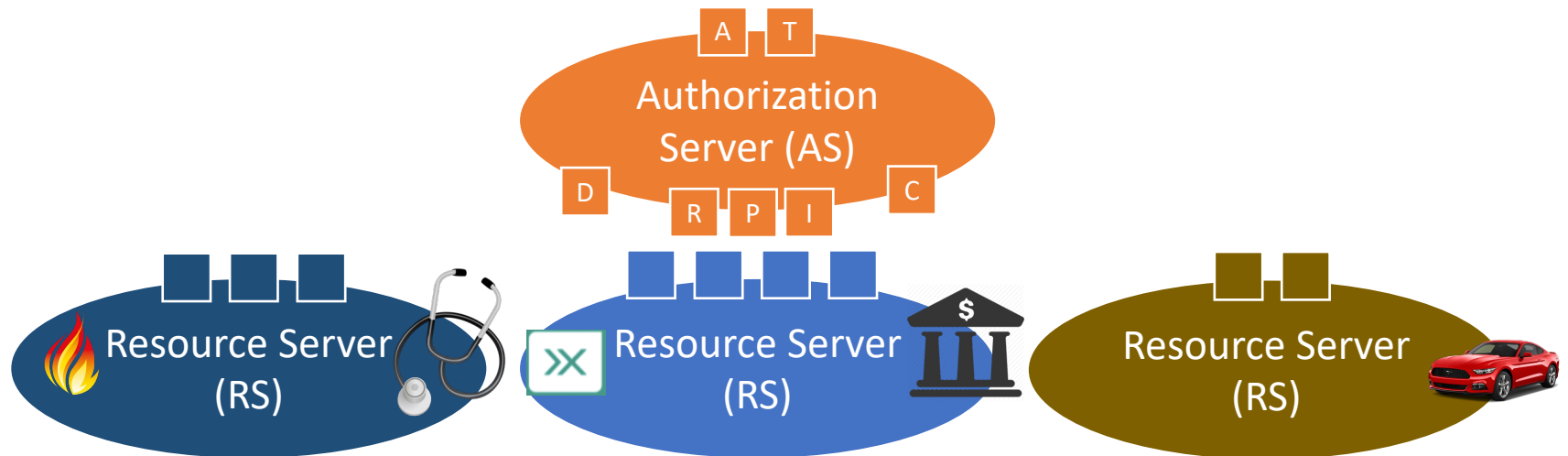
Requesting Party (RqP)



Client

Benefits

- Resource servers can **outsource authorization** management – and liability – to a specialist service
- Alice can **manage sharing** at a centralizable service
- Bob can **revoke his access** to *Alice's* resources



A authorization T token D discovery R resource registration P permission I token introspection C claims interaction¹¹

UMA in Action: Use Cases

Typical use cases

- Alice to Bob (person to person):
 - Patient-directed health data/device sharing
 - Discovering/aggregating pension accounts and sharing access to financial advisors
 - Connected car data and car sharing
- Enterprise to Alice (initial RO is an organization):
 - Enterprise API access management
 - Access delegation between employees
- Alice to Alice (person to self/app):
 - Proactive policy-based control of app connections

- Profiled or referenced by:
 - OpenID Foundation HEART Working Group
 - UK Department for Work and Pensions

Example: PatientShare

Alice Patient, authorize

To disclose my information to
HealthyMePHR Dr. Erica , Lush Medical

Medical Information

Select how you would like to share your medical information

SHARE ALL information in my medical Record

SHARE SPECIFIC medical data sets

Consent Term

Enter a start and end date during which your medical data will be shared

Consent Start	Consent End
31 May 2017	31 December 2019

- Patient Alice creates a policy to share with Dr. Erica, she selects her sharing preferences, and presses SHARE

SHARE

- Patient sharing is easy!

Example: ForgeRock IAM Platform




ROCK 'N' ROLL SUPERMARKET Shop Coupons Recipes

MY ACCOUNT

- Personal Info
- Sign-in & Security
- Preferences
- Trusted Devices
- Authorized Apps
- Privacy & Consent
- Sharing**
- Activity
- Account Controls

Sharing

Manage your shared resources.

	Party Food Shopping List	Shared with 2 people
	Shopping List	Not shared
	Oliver's Bday Wish List	Shared with 2 people





ROCK 'N' ROLL SUPERMARKET Shop Coupons Recipes

MY ACCOUNT

- Personal Info
- Sign-in & Security
- Preferences
- Trusted Devices
- Authorized Apps
- Privacy & Consent
- Sharing
- Activity**
- Account Controls

Activity

Account actions you've taken in the last 28 days.

	Party Food Shopping List You updated sharing	9 hours ago
	Party Food Shopping List ed.enduser@example.com viewed	1 day ago
	Oliver's Bday Wishlist You allowed access to ed.enduser@example.com	1 day ago
	Oliver's Bday Wishlist edna.enduser@example.com shared	July 2, 2017

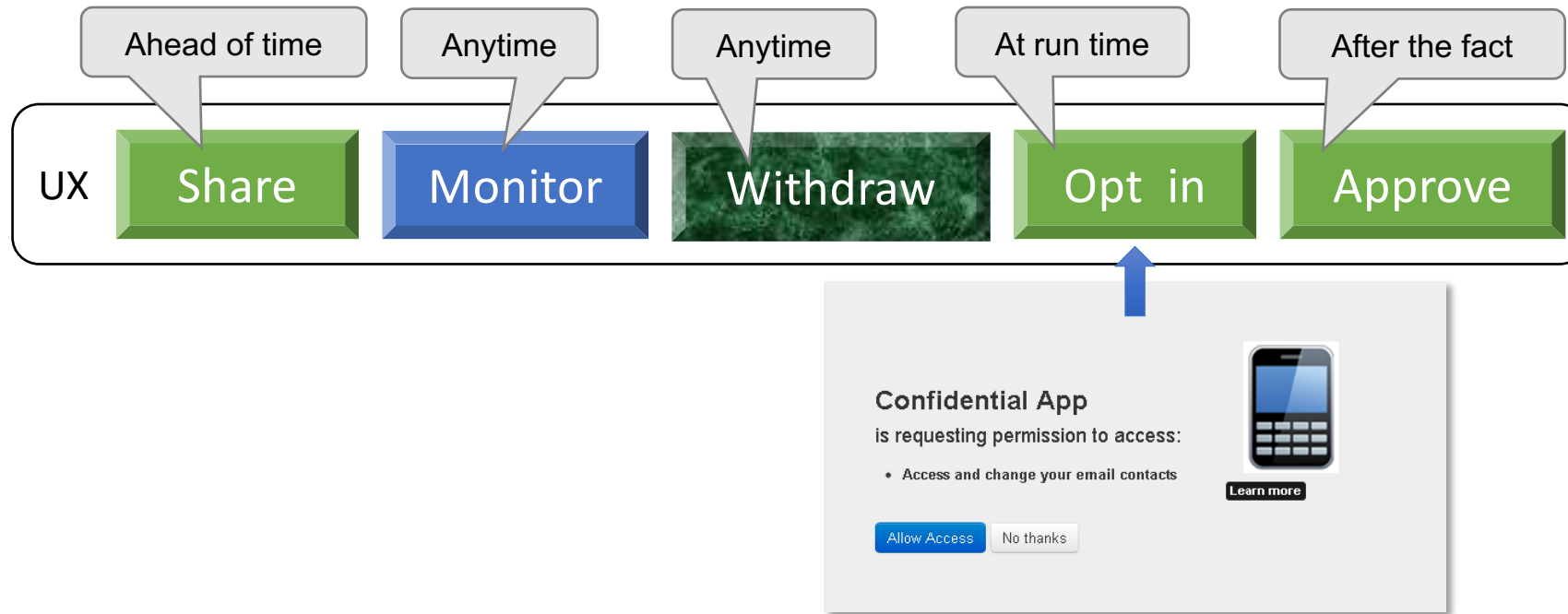
A teal rectangular box is centered on the left side of the slide, containing the text 'UMA Benefits'. In the bottom right corner of the slide, there is a yellow triangle pointing towards the center. The entire slide is framed by a light gray border.

UMA Benefits

UMA user experience opportunities



Resource Owner
(RO)

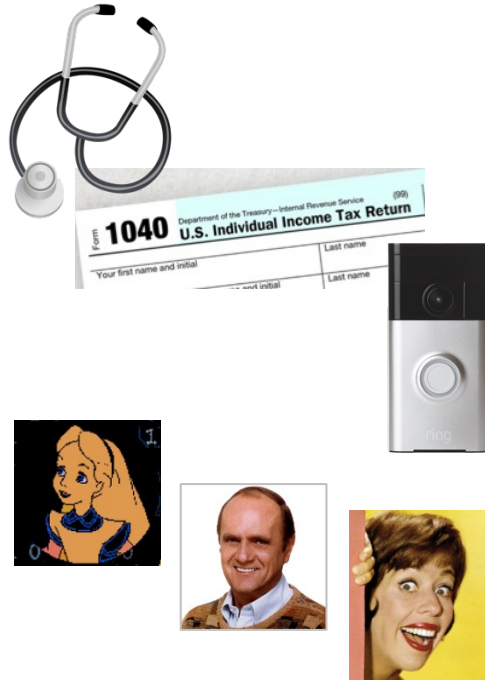


Benefits for service providers

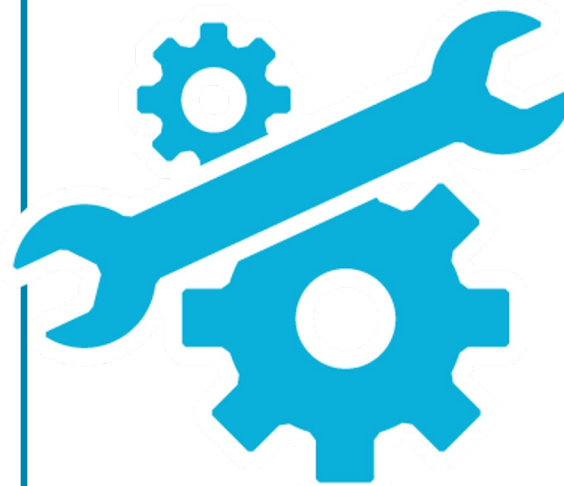
True secure delegation; no password sharing



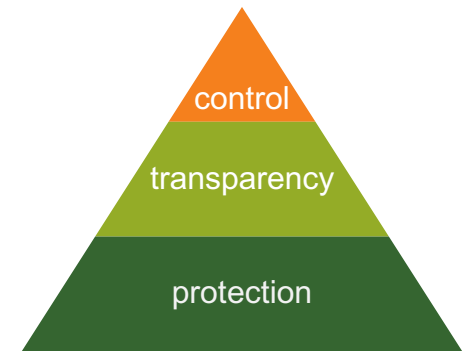
Scale permissioning through self-service



API-first protection strategy

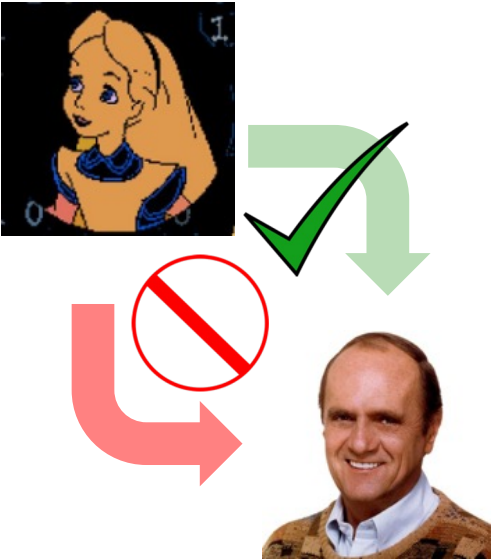


Foster compliance through standards

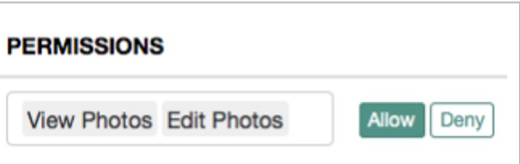


Benefits for patients and end users

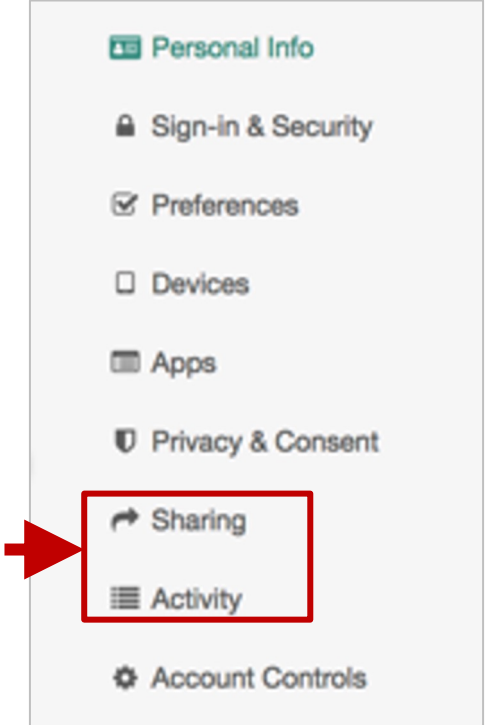
Choice in sharing with other parties



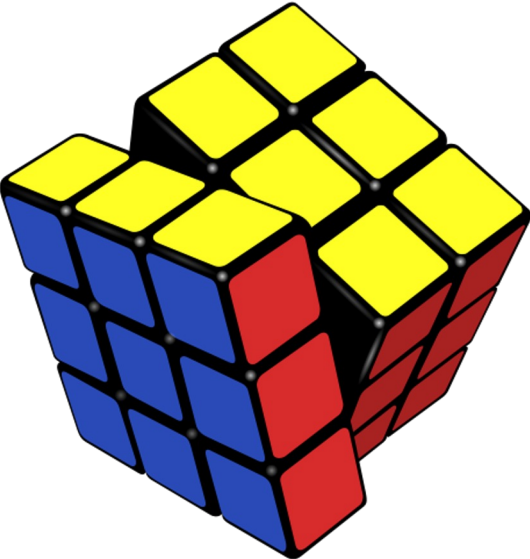
Convenient sharing/approval with no outside influence



Centralizable monitoring and management



Control of who/what/how at fine granularity





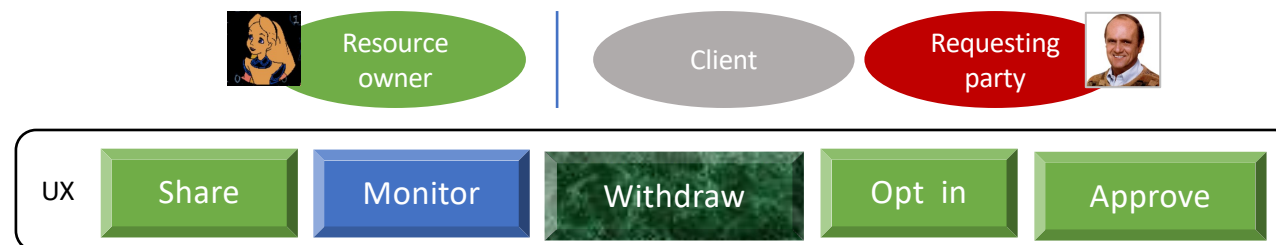
UMA Specs



The UMA extension grant adds...

<https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html>

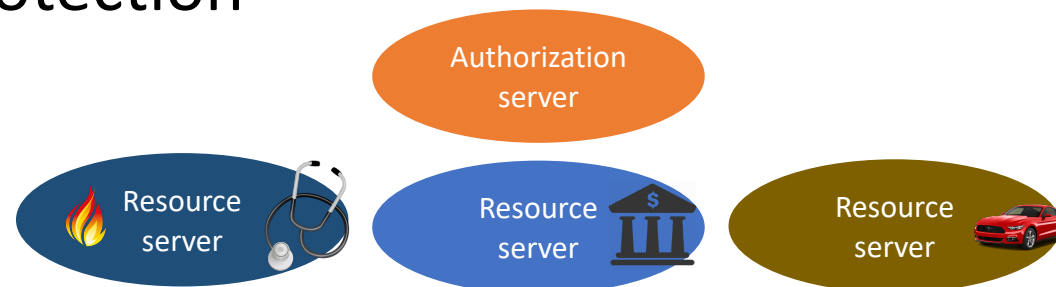
- **Party-to-party:** Resource owner authorizes protected-resource access to clients used by requesting parties
- **Asynchronous:** Resource owner interactions are asynchronous with respect to the authorization grant
- **Policies:** Resource owner can configure an AS with rules (policy conditions) for the grant of access, vs. just authorize/deny
 - Such configurations are outside UMA's scope



UMA federated authorization adds...

<https://docs.kantarinitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html>

- **1-to-n:** Multiple RS's in different domains can use an AS in another domain
 - “Protection API” automates resource protection
 - Enables resource owner to monitor and control grant rules from one place
- **Scope-grained control:** Grants can increase/decrease by resource and scope
- **Resources and scopes:** RS registers resource details at the AS to manage their protection



Known implementations

(more details [here](#))

- ForgeRock – financial, healthcare, IoT, G2C...
- Gravitee – API protection, financial
- Gluu (open source) – API protection, enterprise, G2C...
- HIE of One / Trustee (open source) – healthcare
- IDENTOS – healthcare, G2C
- Patient Centric Solutions – healthcare
- Pauldron (open source) – healthcare
- RedHat Keycloak (open source) – API protection, enterprise, IoT...
- WSO2 (open source) – enterprise...

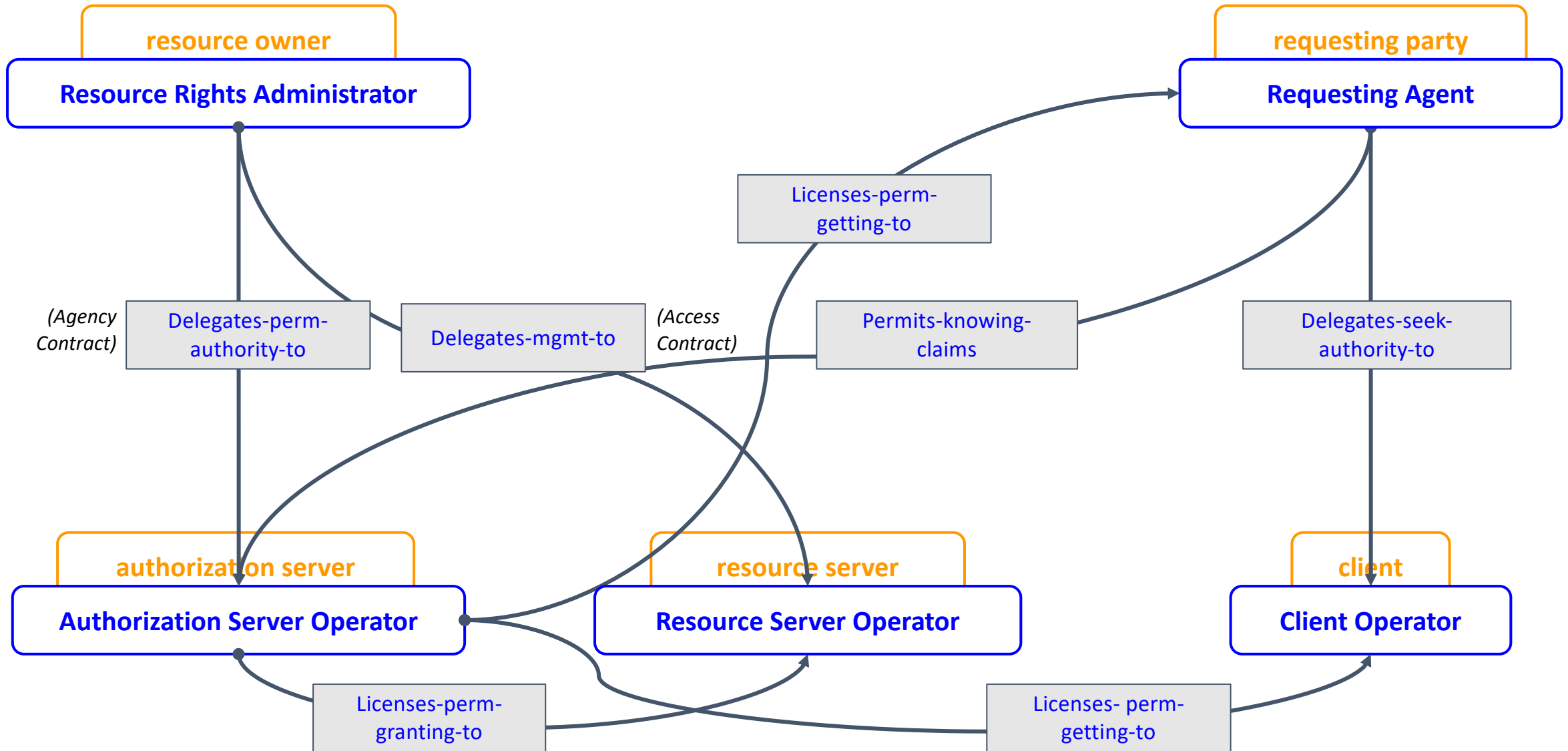
Privacy and “BOLTS” implications

Business, **O**perational, **L**egal, **T**echnical and **S**ocietal factors
(Don Thibeau)

Relevance for privacy

- Features relevant to privacy regulations (GDPR, CCPA, OB, PSD2, CDR, HHS ONC info blocking rules...):
 - Asynchronous resource owner control of grants
 - Enabling resource owner to monitor and manage grants from a “dashboard”
 - Auditability of grants (consent) and PAT-authorized AS-RS interactions
- Work is well along on an UMA business model
 - Modeling real-life data-sharing relationships and legal devices
 - Technical artifacts are mapped to devices
 - Goal: tear down artifacts and build up new ones in response to state changes

(Most) legal relationships in the business model



UMA implications - BOLTS

...for the client

- Simpler next-step handling at every point

...for the RS

- Standardize management of protected resources

...for the RO

- Control data sharing/device control
- Truly delegate access to other parties using clients

...for the AS

- Offer interoperable authorization services
- Don't have to touch data to protect it

...for the RqP

- Seek access to a protected resource as oneself

...for the client operator

- Distinguish identities of resource owners from mere users

...for the resource server operator

- Externalize authorization while still owning API/scopes

...for the resource rights admin

- Manage sharing on behalf of data subjects, not just for oneself

...for the authorization server operator

- Prove what interactions took place or didn't

...for the requesting agent

- Revoke access (or request it) to someone else's assets

What is the UMA WG up to?

- Recent work:
 - [Patient-centered Data Sharing with UMA](#)
 - Julie Adam's use-case report – describes how UMA can be applied to complex patient centric data sharing, from Child to Adult
 - Published in early 2023
- Current work:
 - Pension Dashboard use-case report - Financial-sector
- Queued work:
 - IDPro Body of Knowledge article(s) on UMA
 - UMA alignment with other specs – FHIR/UDAP, FAPI, GNAP



Join us!
Thank you!
Questions?

Kantara Initiative UMA Working Group
<https://kantara.atlassian.net/wiki/spaces/uma/wg-uma@kantarainitiative.org>

Alec Laws
WG Chair

Steve Venema
WG Vice-chair

IIWXXXVI | 18Apr2023

