User-Managed Access

UMA Work Group

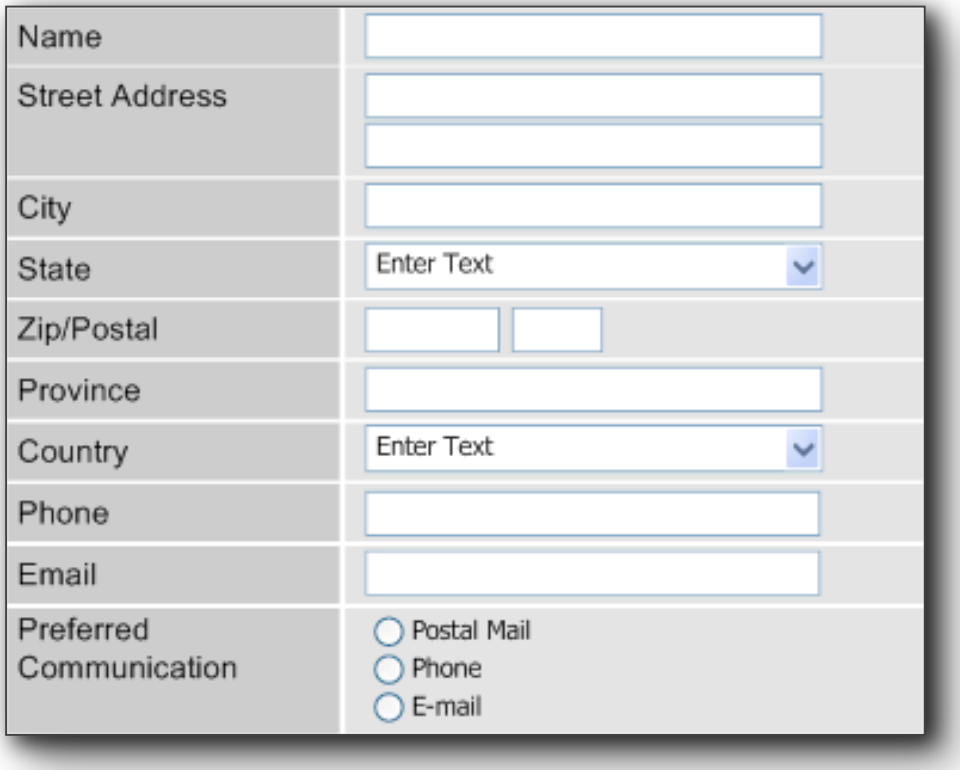
@UMAWG

tinyurl.com/umawg | tinyurl.com/umafaq

IIW 16, May 2013

The "data price" for online service is too high: typing…

- Provisioning by hand
- Provisioning by value
- Oversharing
- Lying!



The "data price" for online service is too high: connecting…

- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oblivious oversharing

The "data price" for online service is too high: private URLs…

- Handy but insecure
- Unsuitable for really sensitive data

Most data "sharing" today is back-channel and unconsented

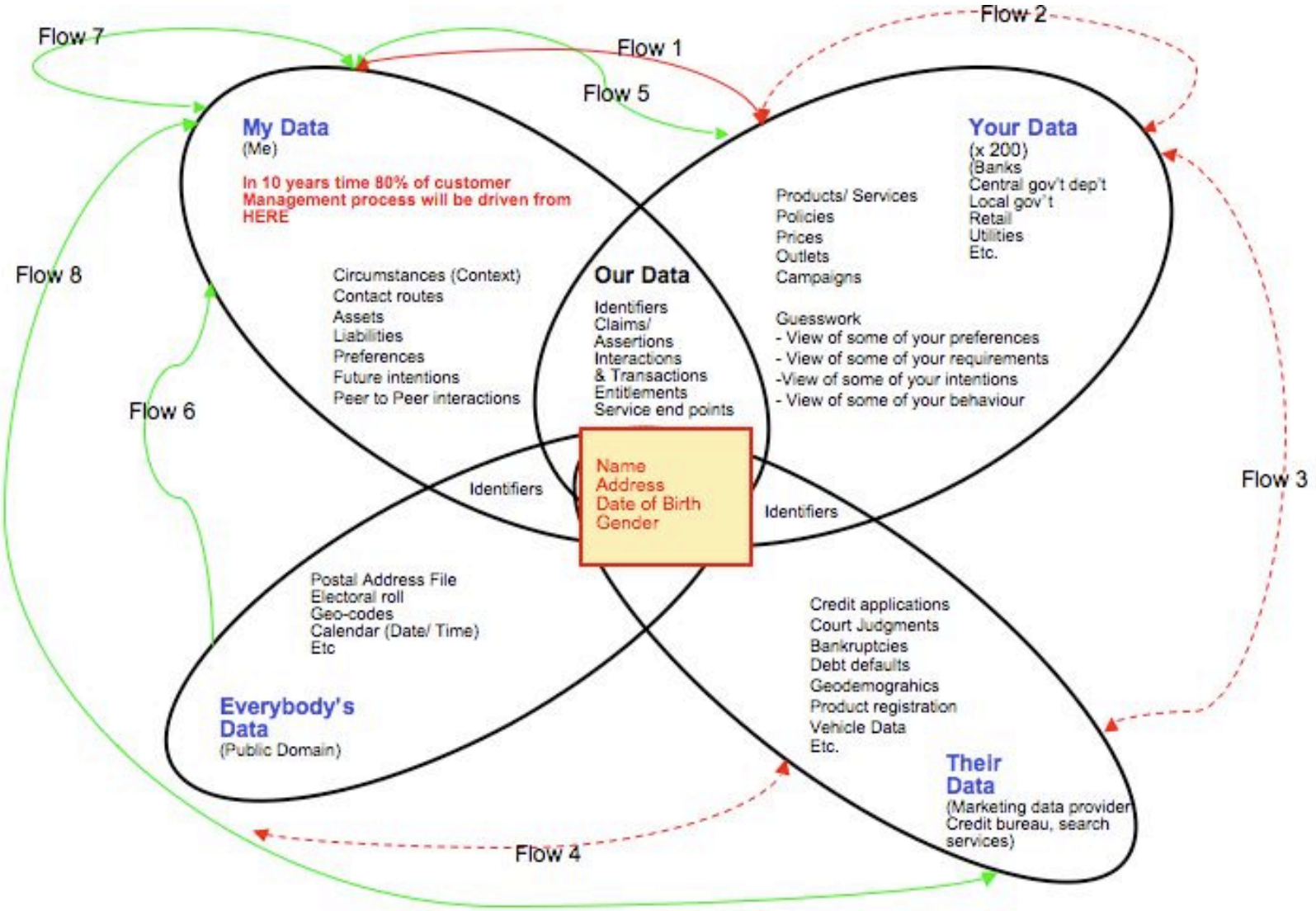


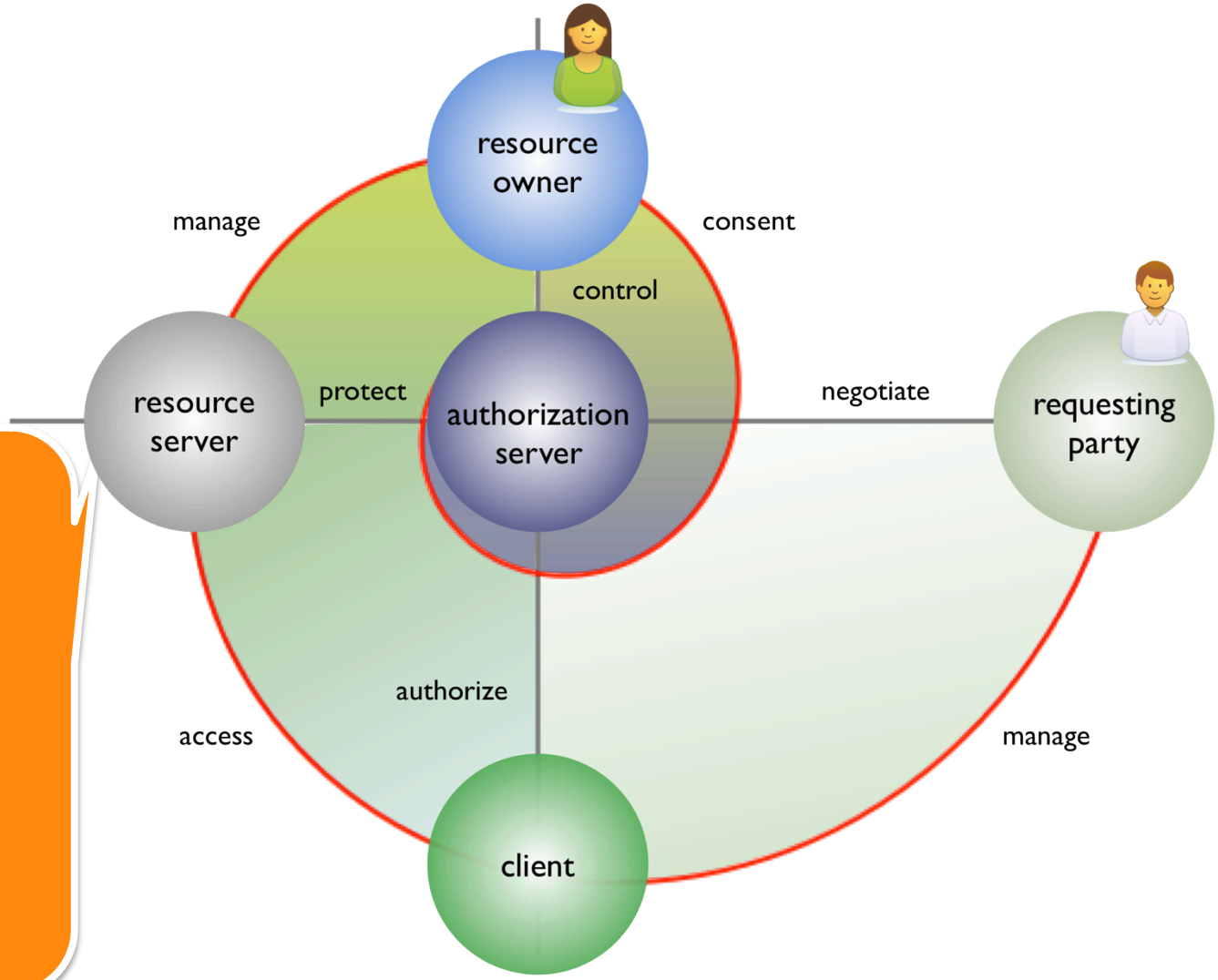
Image source: http://informationanswers.com/?p=283

Privacy is about context, control, choice and respect – so UMA enables a "digital footprint control console"

- *Web 2.0 access control is inconsistent and unsophisticated*
- *To share with others, you have to list them literally*
- *You have to keep rebuilding your "circles" in new apps*
- *You can't advertise content without giving it away*
- *You can't get a global view of who accessed what*

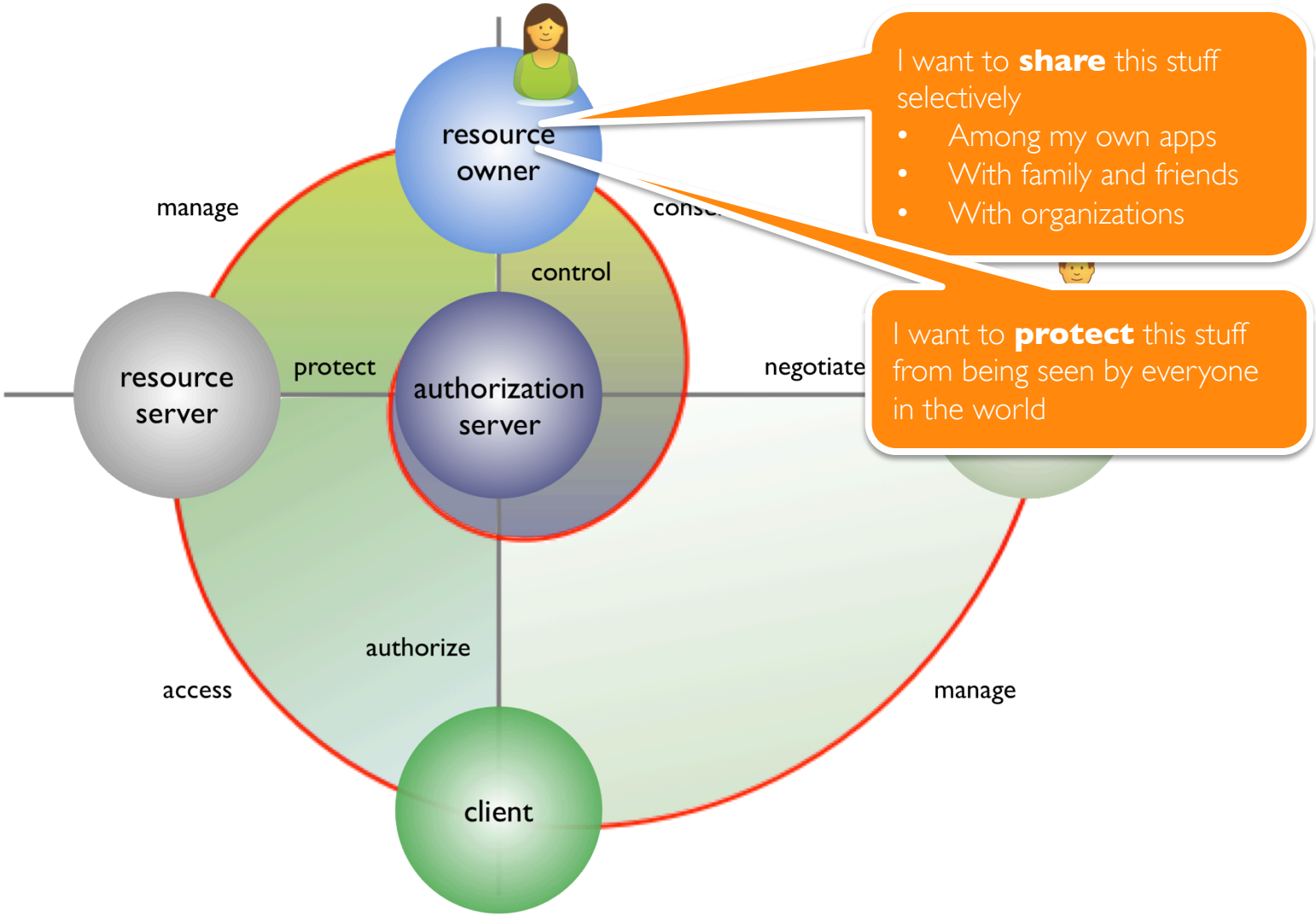
- You can **unify** access control under a single app
- Your access policies can test for **claims** like "over 18"
- You can **reuse** the same policies with multiple sites
- You can control access to stuff with **public** URLs
- You can manage and **revoke** access from one place

UMA turns online sharing into a privacy-by-design solution

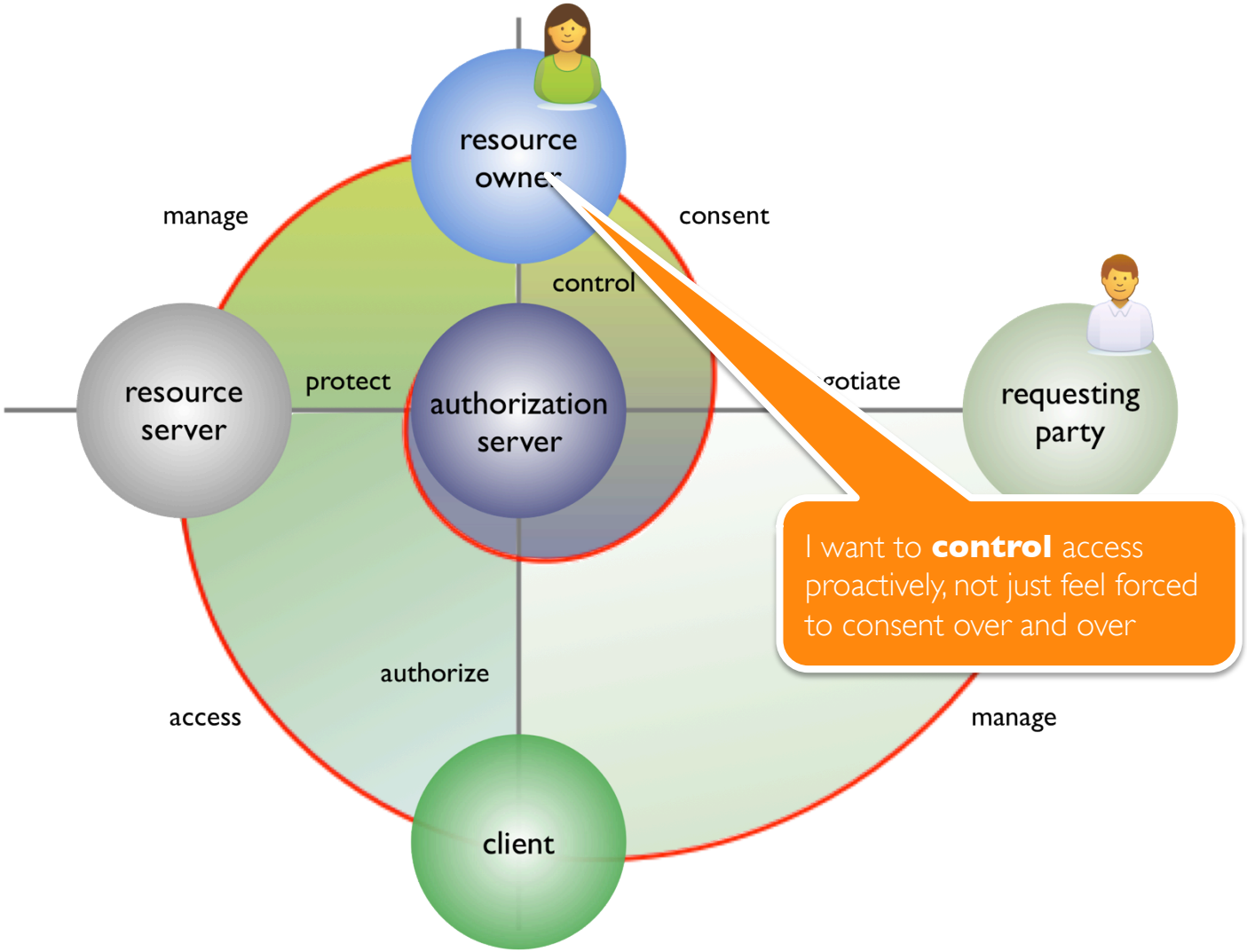


- Historical
- Municipal
- Financial
- Vocational
- Artistic
- Social
- Geolocation
- Computational
- Genealogical
- Biological
- Legal
- ...

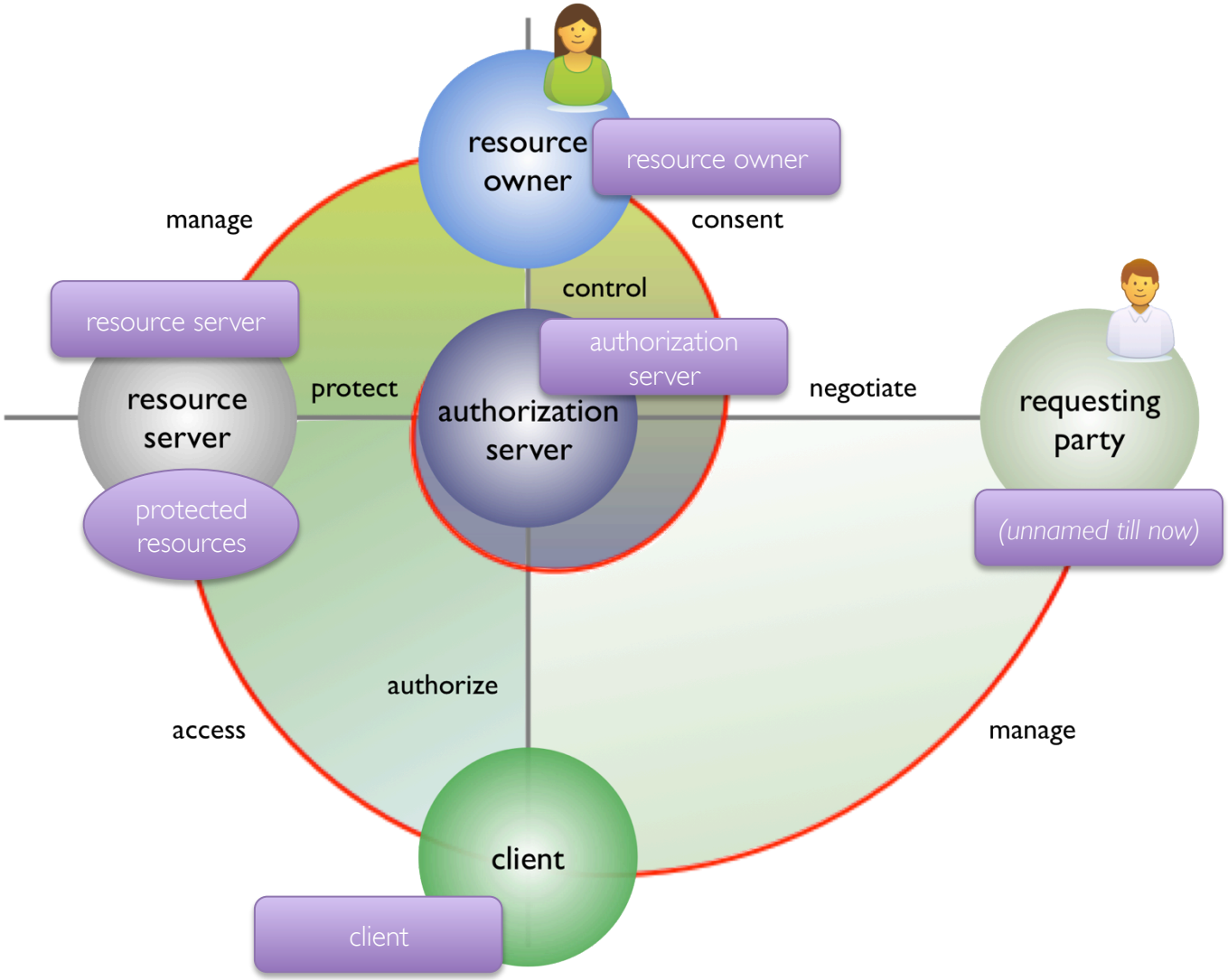
UMA turns online sharing into a privacy-by-design solution



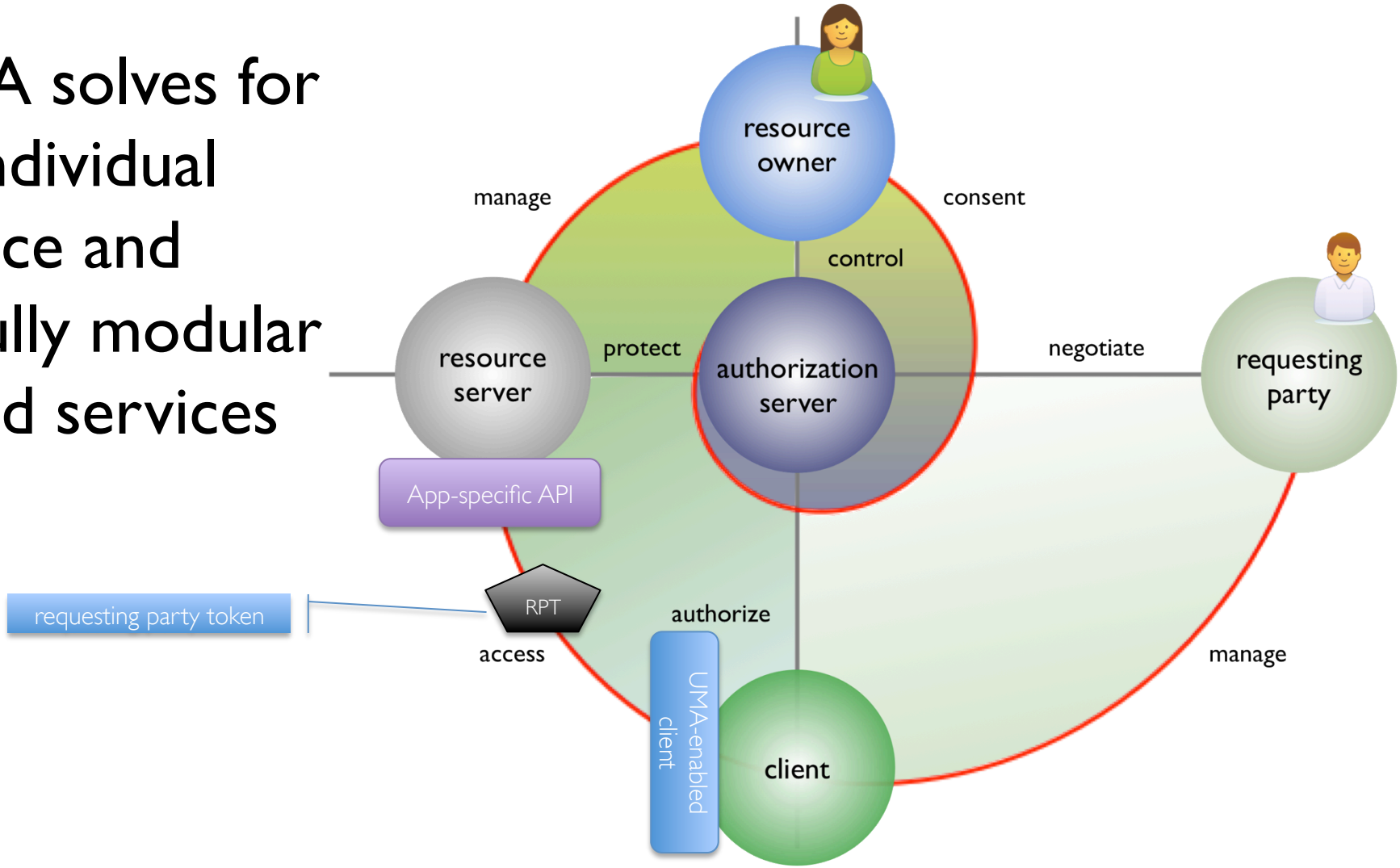
UMA turns online sharing into a privacy-by-design solution



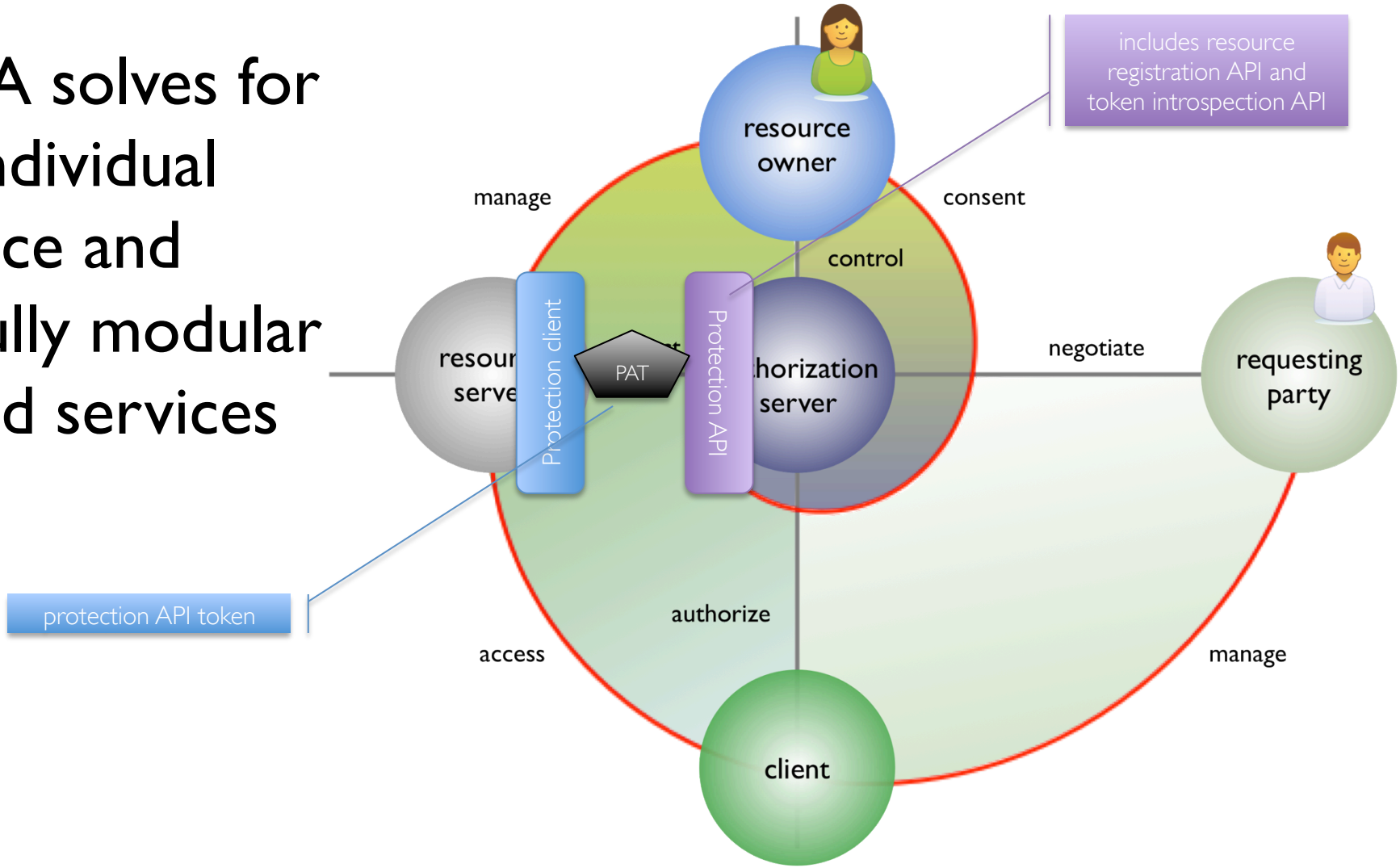
UMA is a profile of OAuth, with bits added for interop and scale



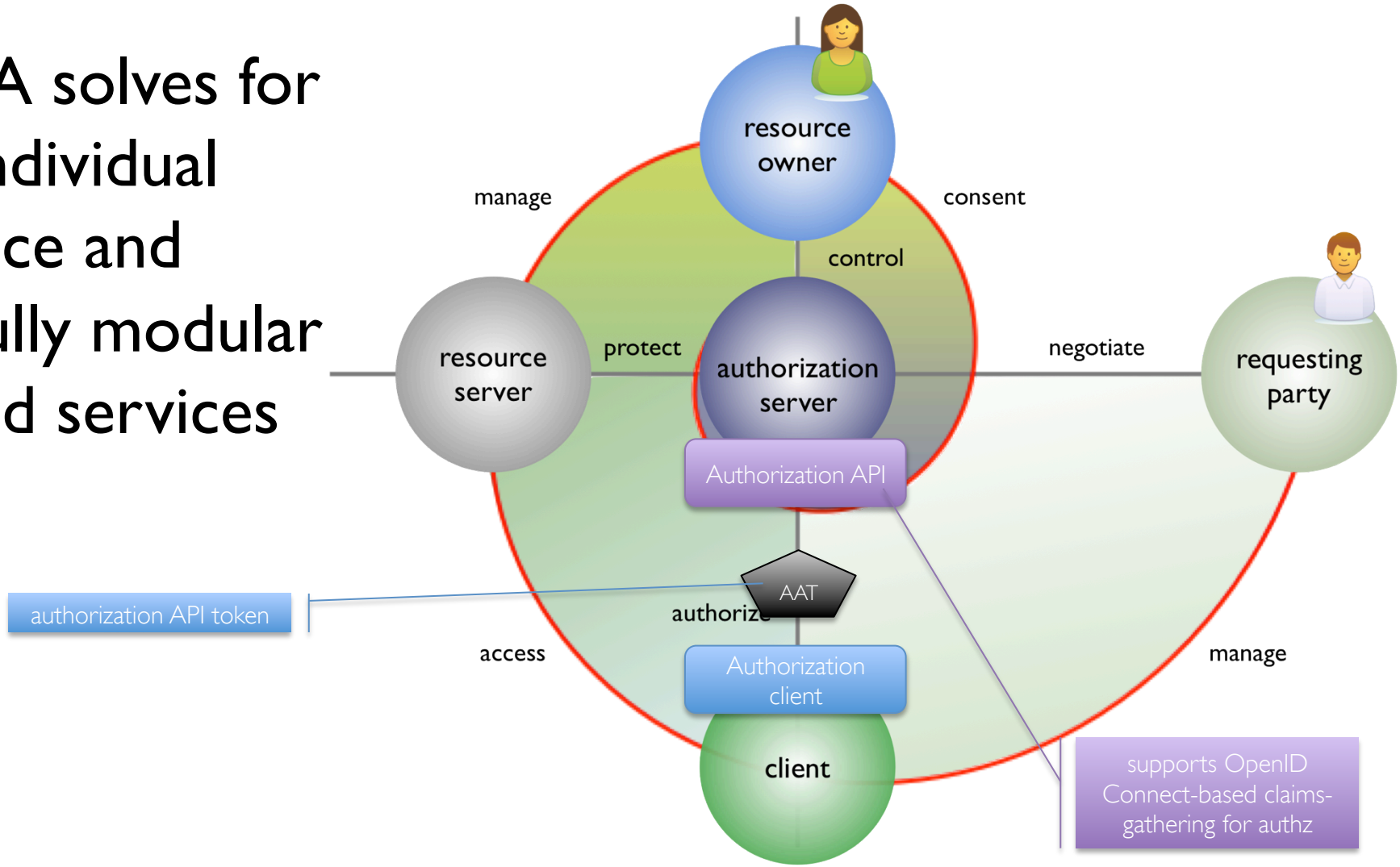
UMA solves for
1) individual choice and
2) fully modular cloud services



UMA solves for
1) individual choice and
2) fully modular cloud services



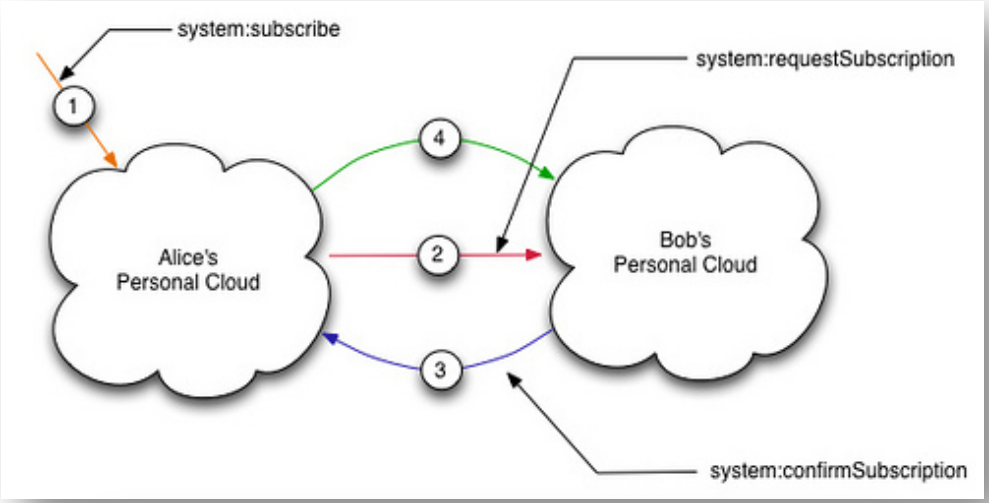
UMA solves for
1) individual choice and
2) fully modular cloud services

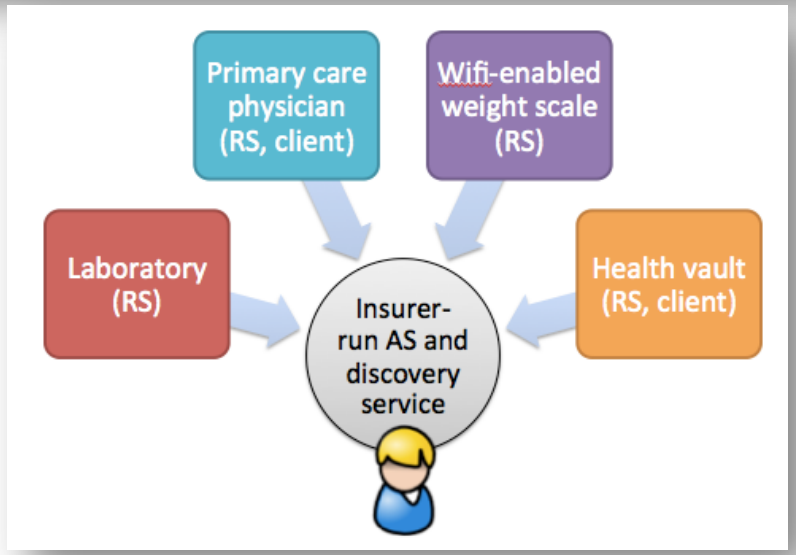


Key use cases

http://kantarainitiative.org/confluence/display/uma/Case+Studies

- Subscribing to a friend's personal cloud
- Sharing accessibility attributes ("GPII")
- E-transcript sharing ("HEAR")
- Patient-centric health data access
- Enterprise "access management 2.0"





Key implementations

http://kantarainitiative.org/confluence/display/uma/UMA+Implementations

- SMARTAM.net (running authorization service from Cloud Identity UK)
- Puma (Python libraries for RS- and client-enabling web apps) from ditto
- Fraunhofer AISEC open-source implementation in Java
- Gluu OX open-source implementation for Access Management 2.0 use cases

Next steps

- Work on optimization opportunities when UMA and OpenID Connect are used together
- Issue "Implementor's Draft"
- Continue to work with AXN, Scalable Privacy, and others in "trusted identities in cyberspace" ecosystem
- Profile UMA for higher ed, accessibility attribute sharing, healthcare use cases
- We welcome your involvement and contributions
  - Become an UMAnitarian!
  - Follow @UMAWG on Twitter and UserManagedAccess on FB

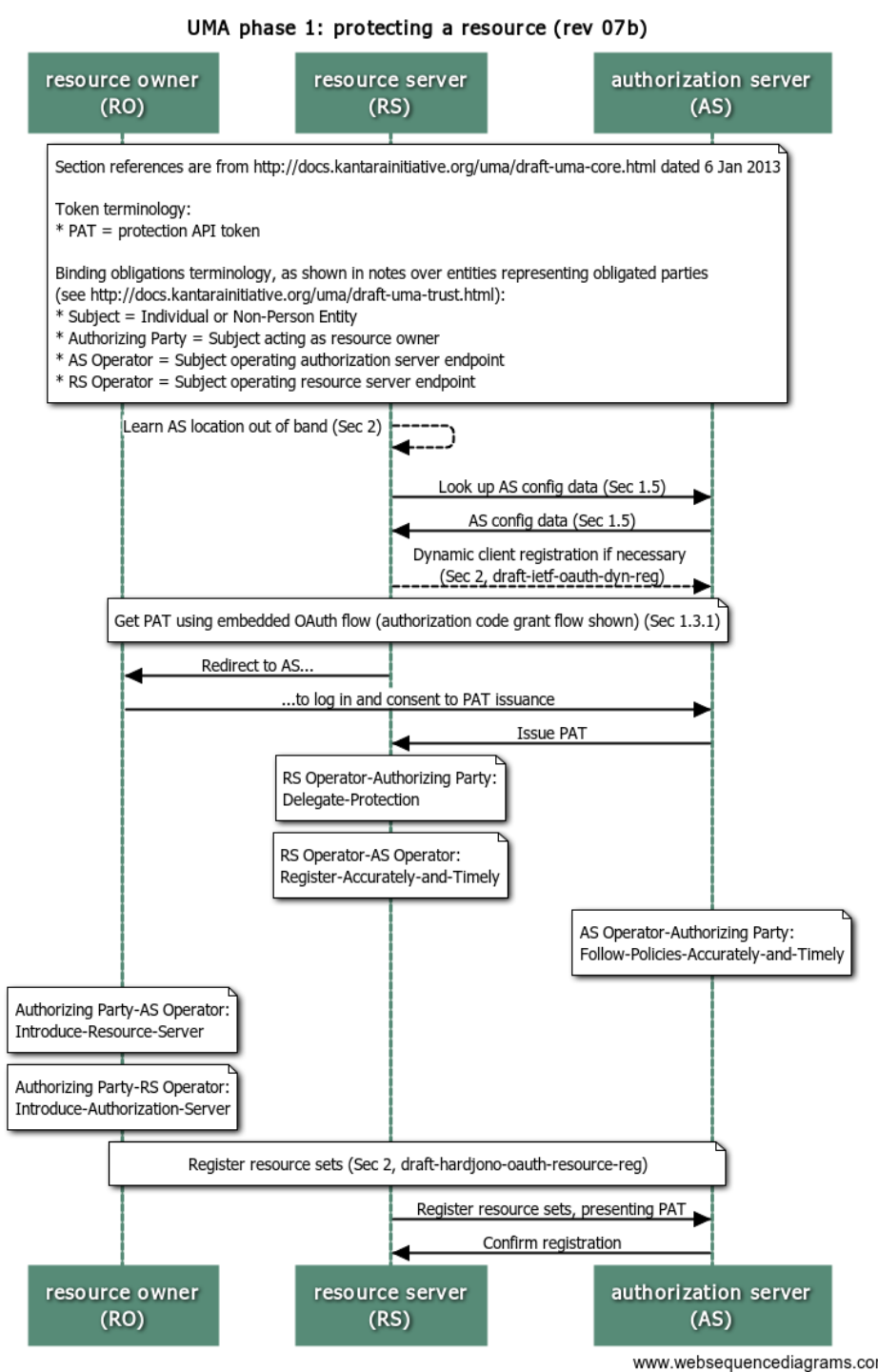
Questions?
Thank you

@UMAWG

tinyurl.com/umawg | tinyurl.com/umafaq

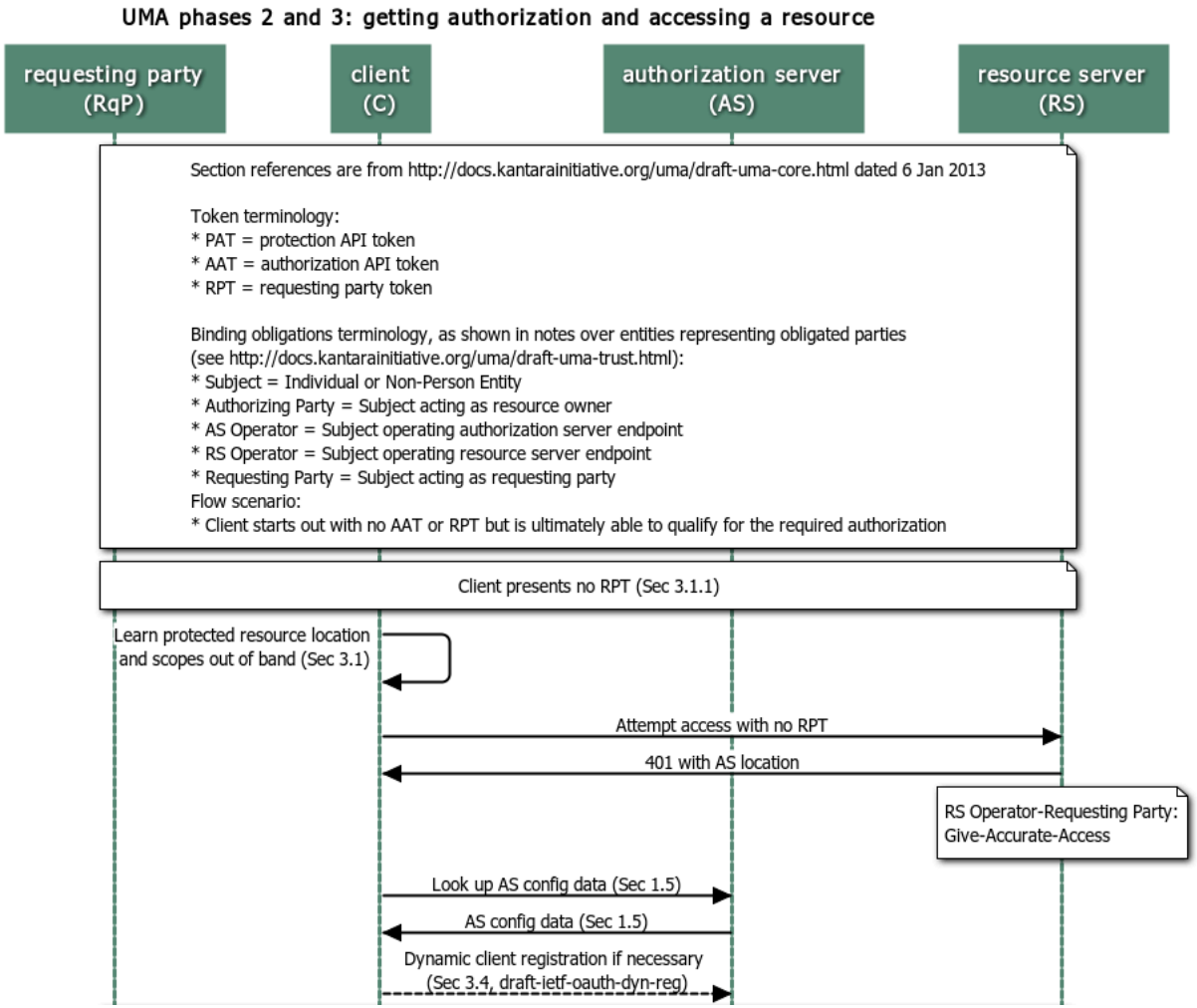
IIW 16, May 2013

Phase 1: protect a resource



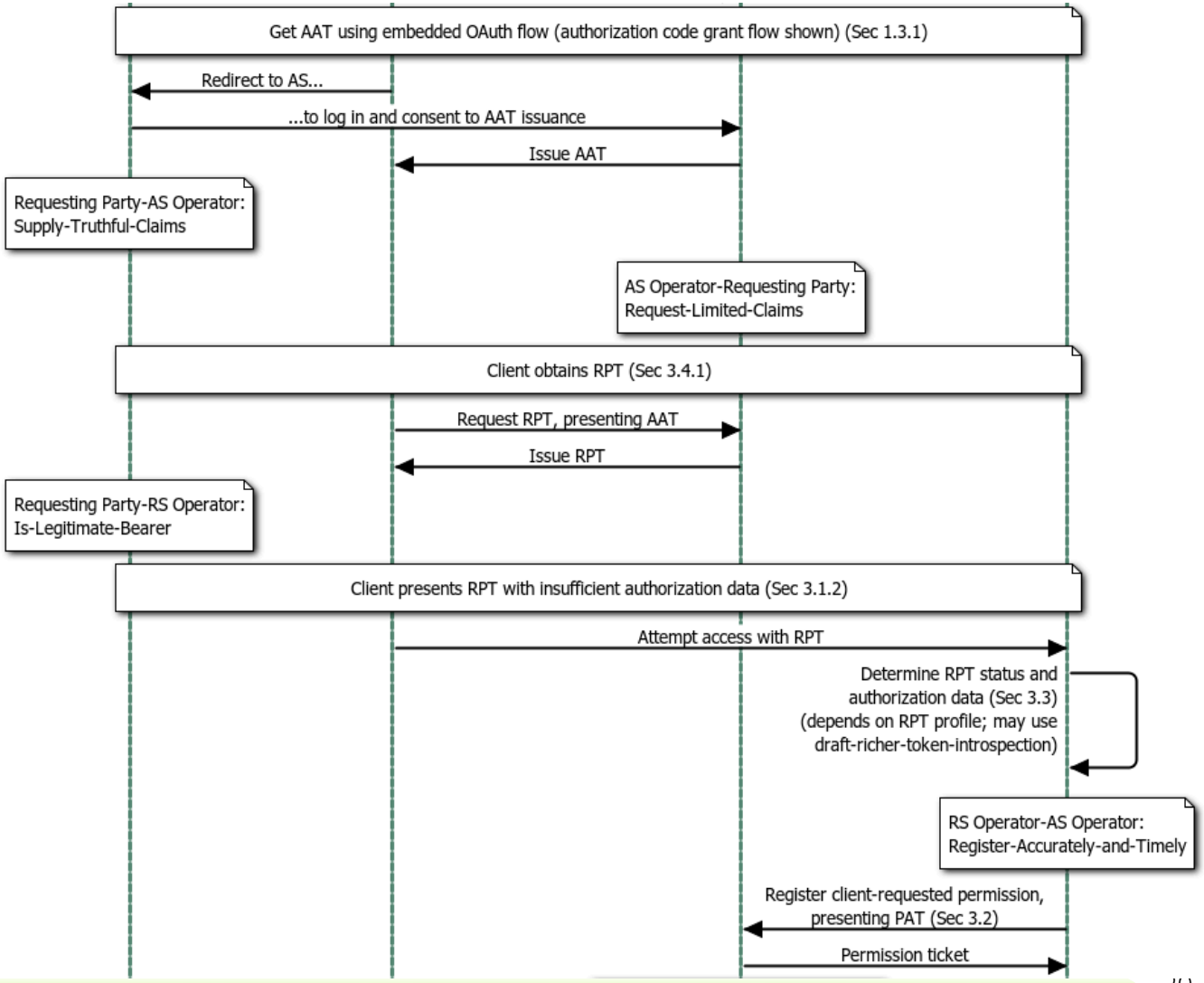
Phases 2 and 3: get authorization and access resource

1 of 3



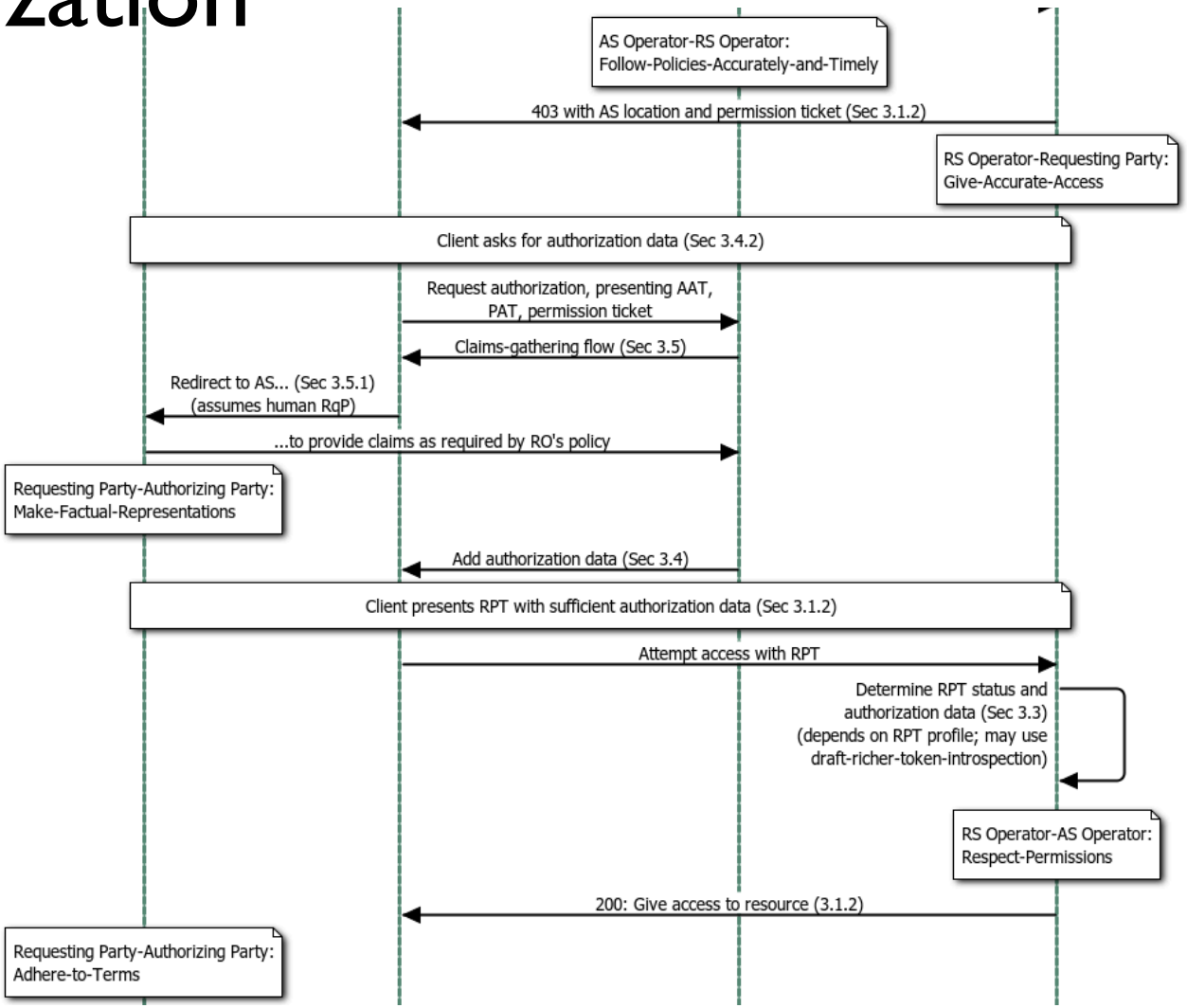
Phases 2 and 3: get authorization and access resource

2 of 3

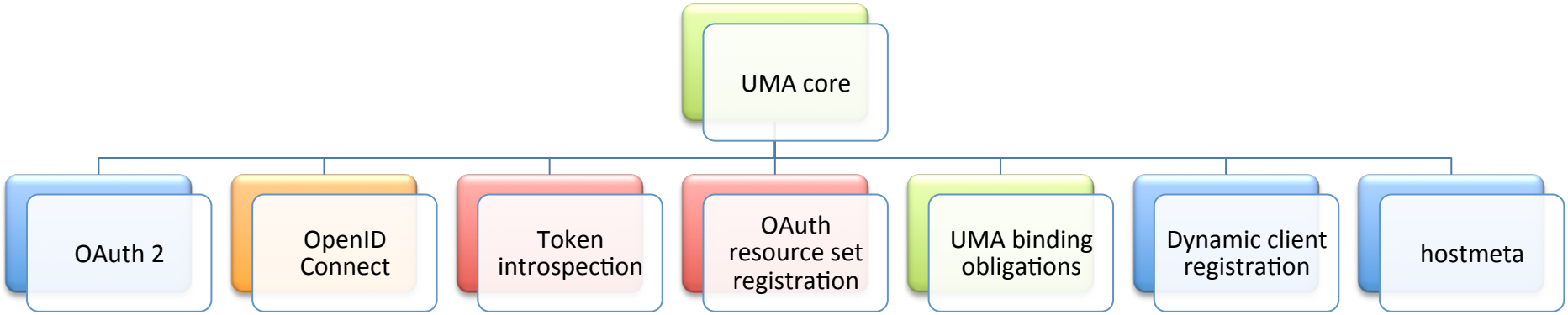


Phases 2 and 3: get authorization and access resource

1 of 3



Spec call tree for the UMA profile of OAuth



UMA native spec

Required external component

Optional external component

Individual IETF I-D