User-Managed Access: Why and How?

Access Control in Digital Contract Contexts

Eve Maler

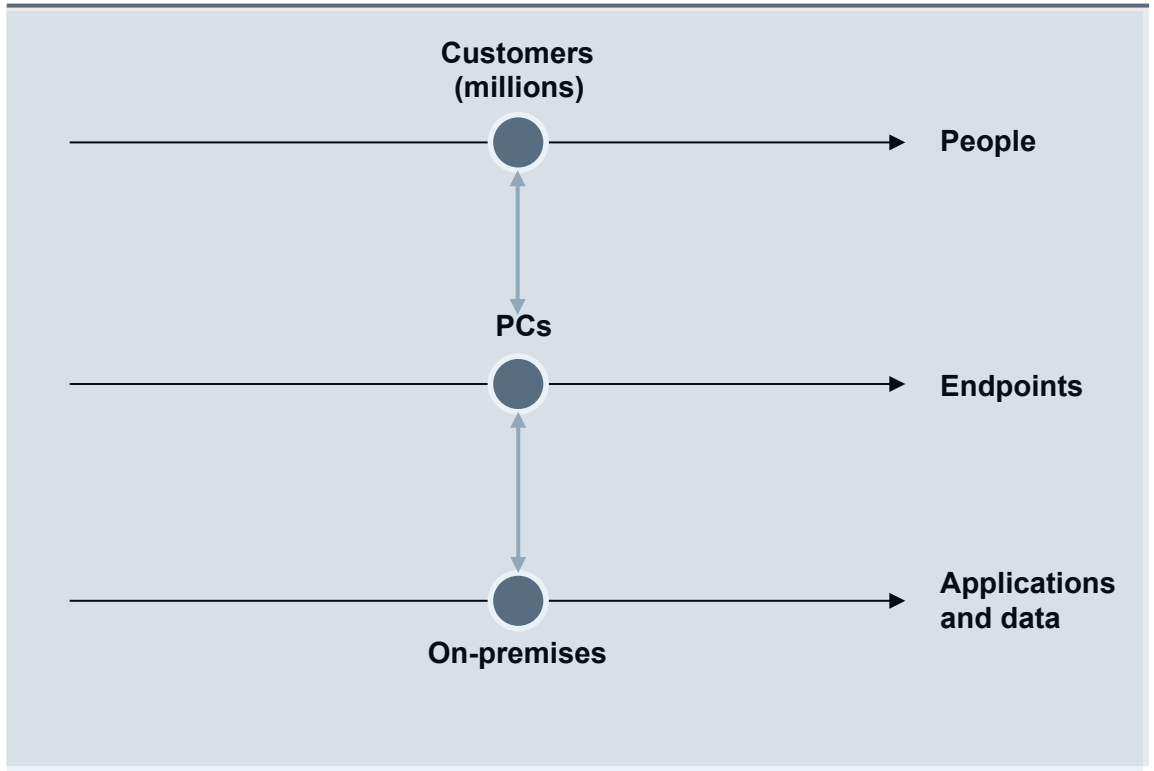
VP Innovation & Emerging Technology, ForgeRock

@xmlgrrl

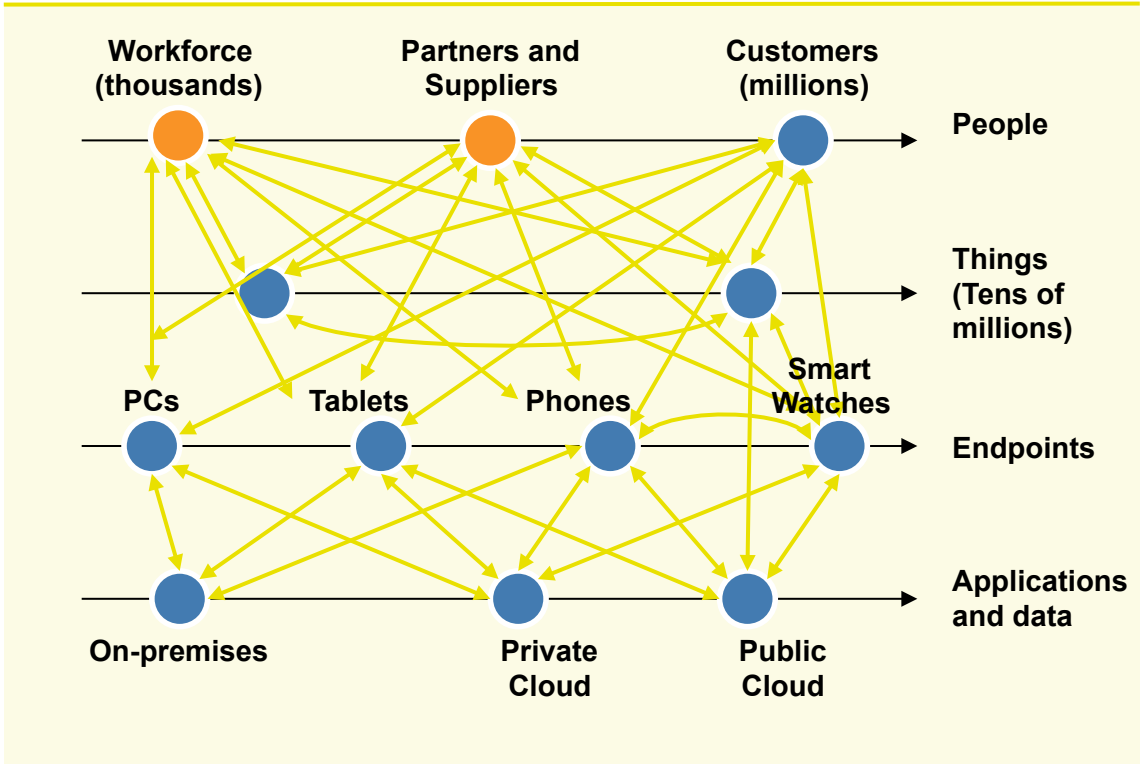
FORGEROCK

From IAM to IRM

Identity Access Management



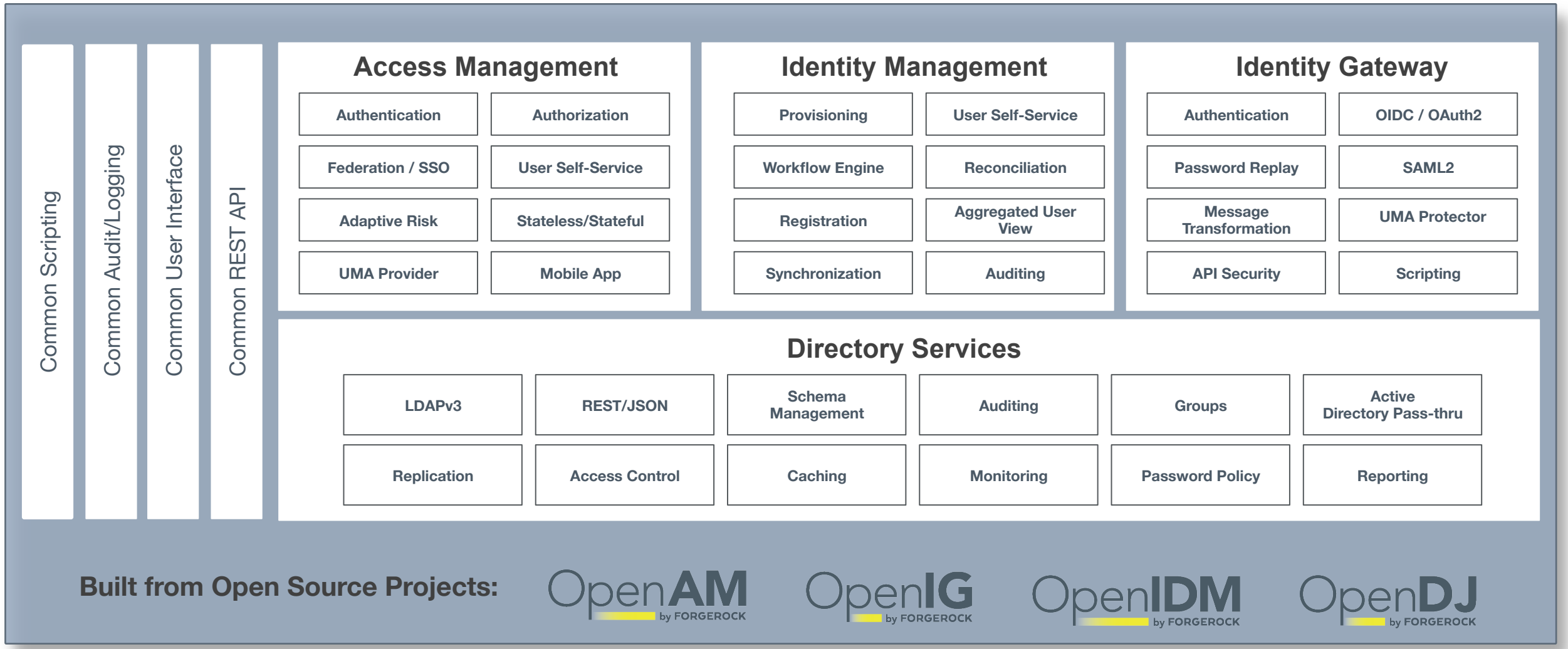
Identity Relationship Management



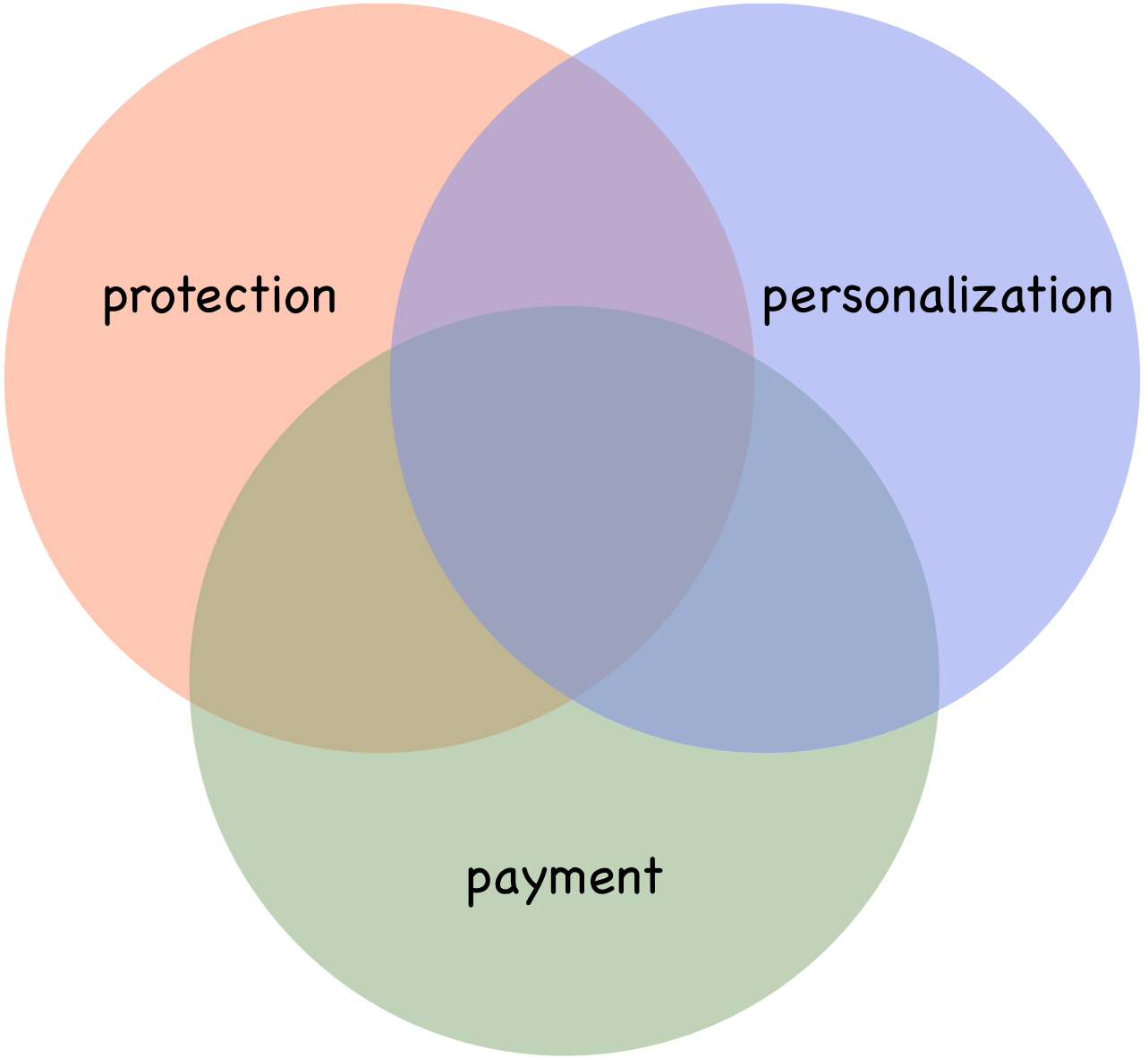
Source: Forrester Research

Digital business requires an **identity-centric** approach

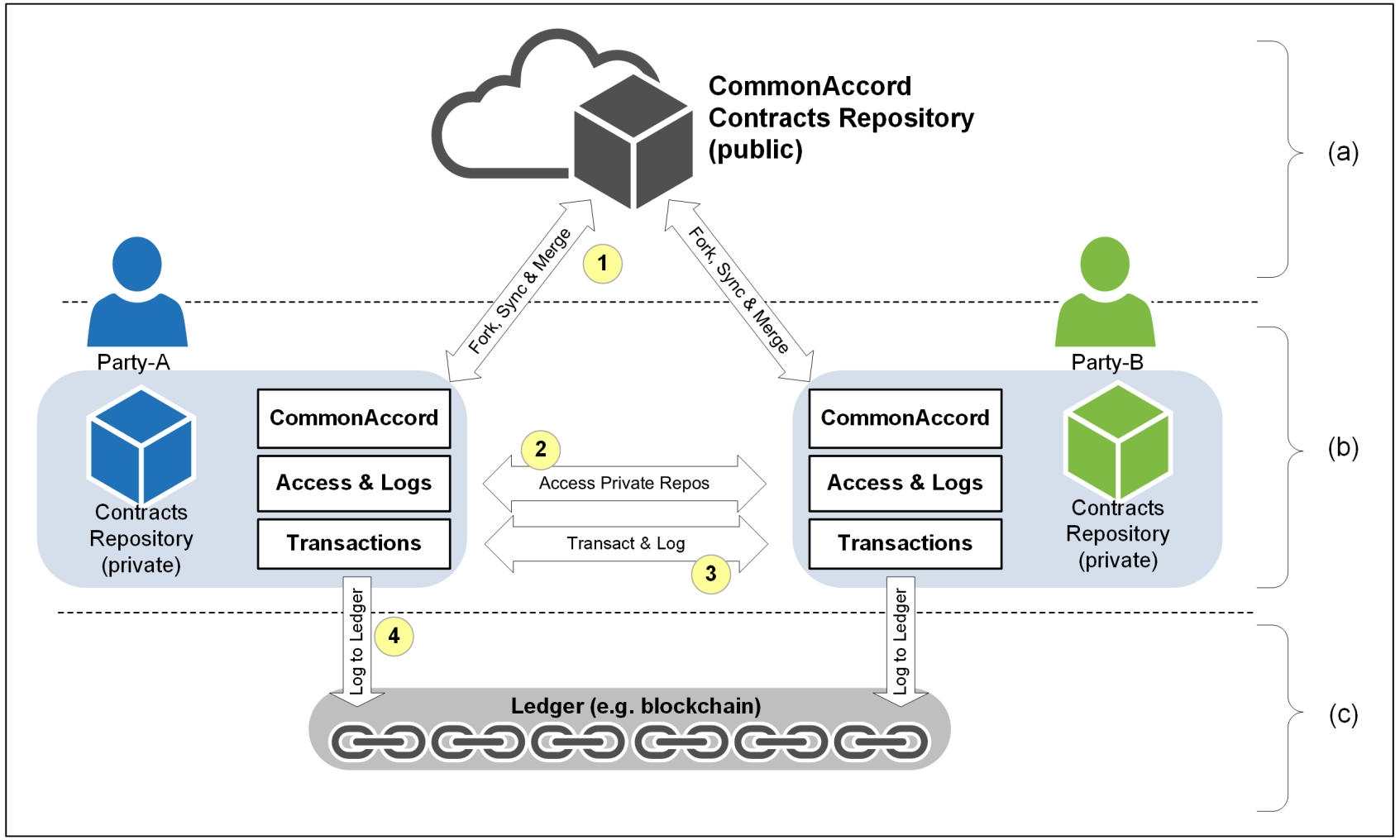
The bits and bytes of identity, access, and relationship management



We generally don’t “do identity” just for fun…



It's a rare source of information that *doesn't* require serious permissioning for access



Spotify

MEF
MOBILE ECOSYSTEM FORUM

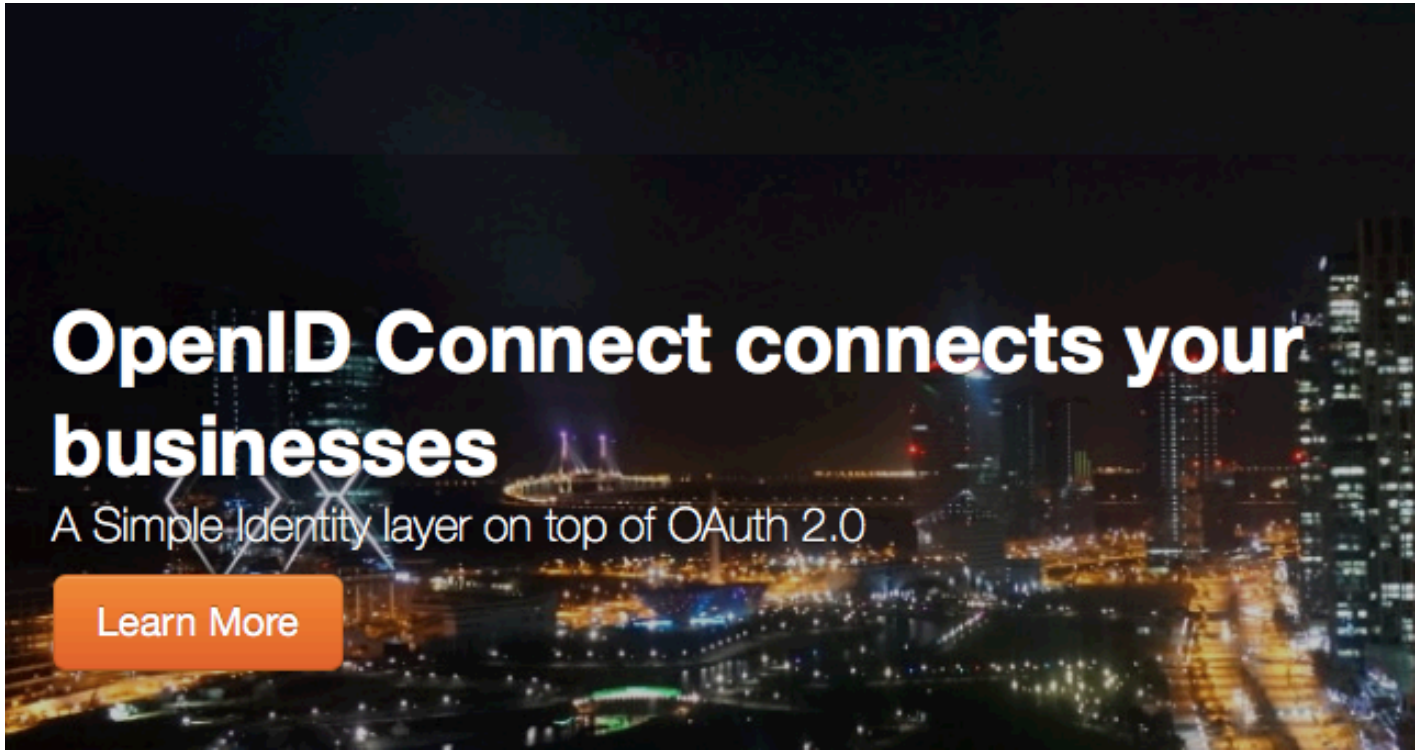
What happens when businesses *can't* form trusted digital relationships with consumers?

- Revenue loss
- Brand damage
- Loss of trust

- Missing out on opportunities

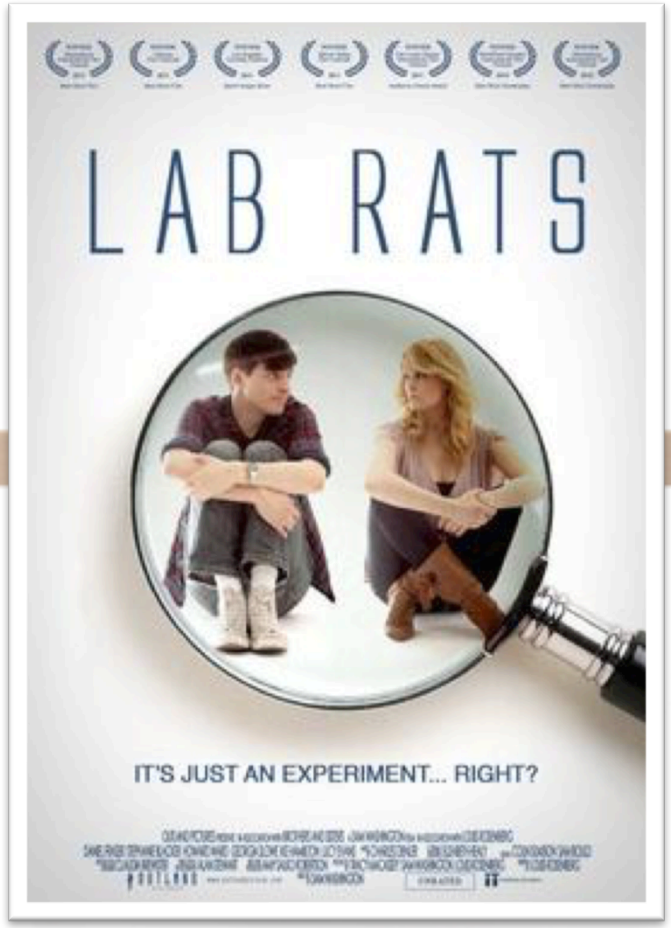
- Compliance costs and penalties?

Why enable personal data sharing?
Let's use Health Relationship Trust as an example



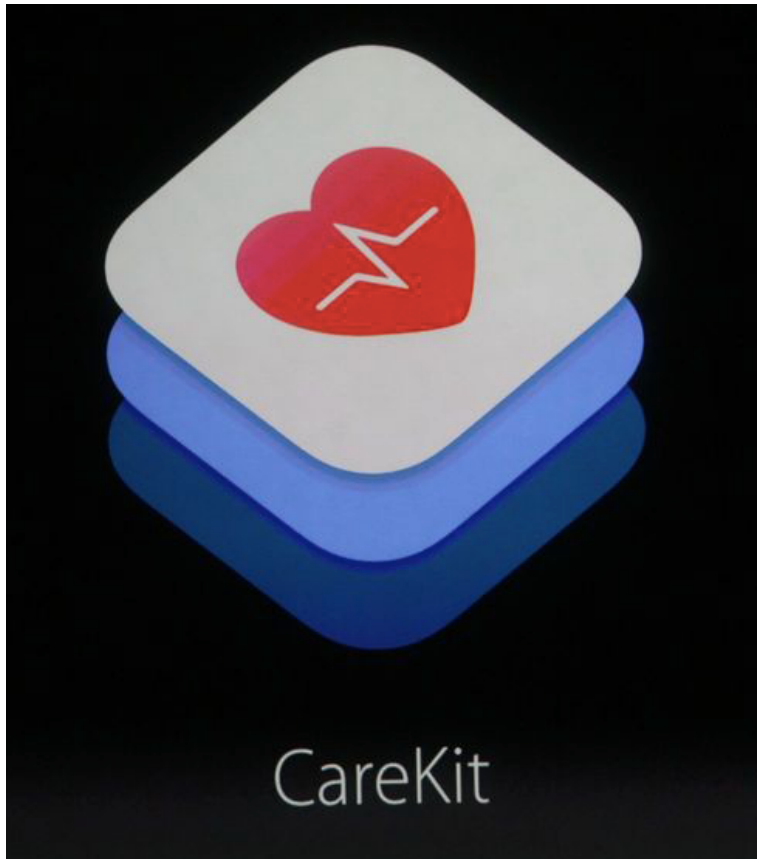
data quality
and accuracy

improved
clinical data

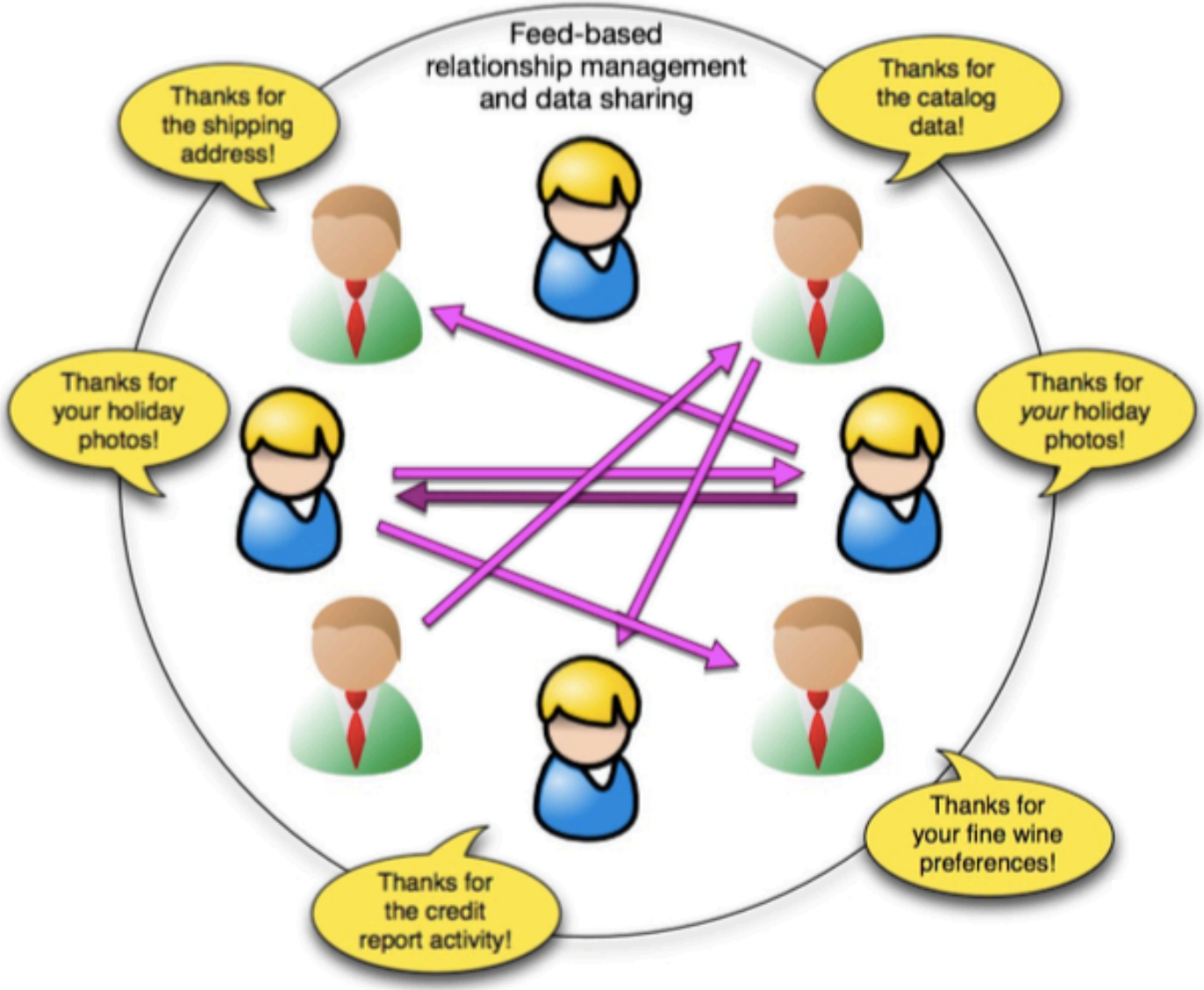


better care

Why *ensure personal control* of sharing?



To empower individuals as legal parties, give them (us) permissioning tools



To empower individuals as legal parties, give them permissioning tools

- Alice:
  - Wants to grant access to her medical power of attorney:
    - To spouse Bob: Persistently
    - To her medical professionals: When setting up and going through a procedure
    - To first responders: In an emergency situation
  - Wants to sell access to her professional high-resolution photos:
    - From a central control console: Operating across her several photo services
    - Integrating to a variety of applications: To reach the widest market
    - *Incorporating a smart contract component: To enable fair, efficient agreement*

How dire is the “consent tech” situation?

9 percent [of companies] believe current methods (i.e., check boxes, cookie acknowledgment) used to ensure data privacy and consent will be able to adapt to the needs of the emerging digital economy.

– ForgeRock global survey conducted by TechValidate, 16 Mar 2016

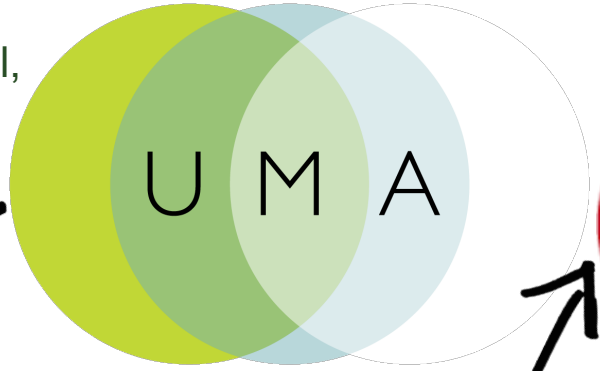
The next generation of consent standards is riding to the rescue

1. innovates coarse-grained consent withdrawal

2. leverages OAuth for portable identity

6. codifies and automates legal docs and consents

3. adds multi-party delegation, finer-grained withdrawal, central console



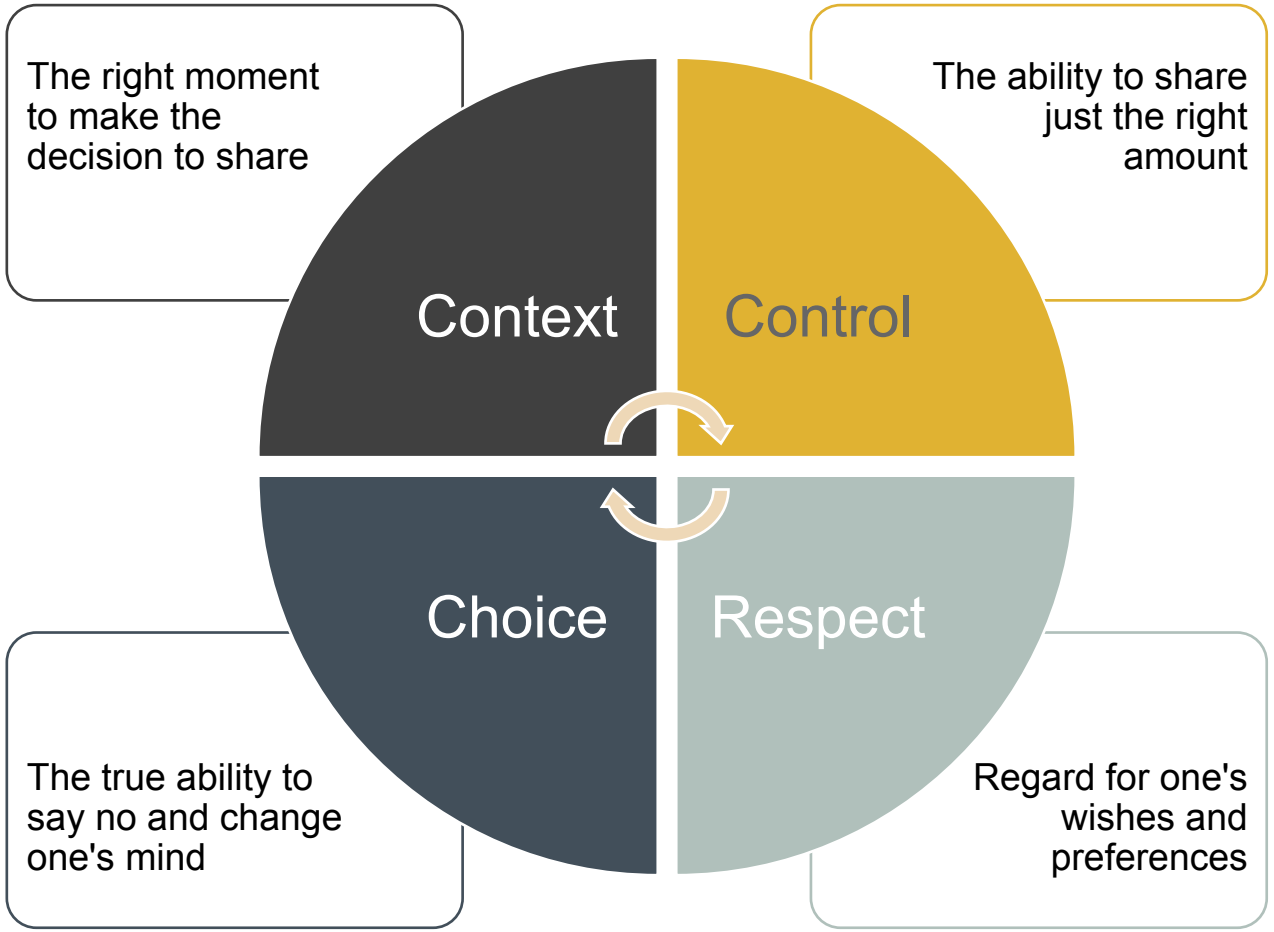
4. profiles #1, #2, #3 and the FHIR API for patient centricity

5. defines consent receipts

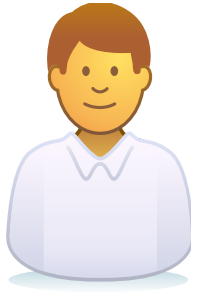
USER-MANAGED ACCESS

A new standard for data sharing and control

http://tinyurl.com/umawg
http://tinyurl.com/umalegal
@UMAWG

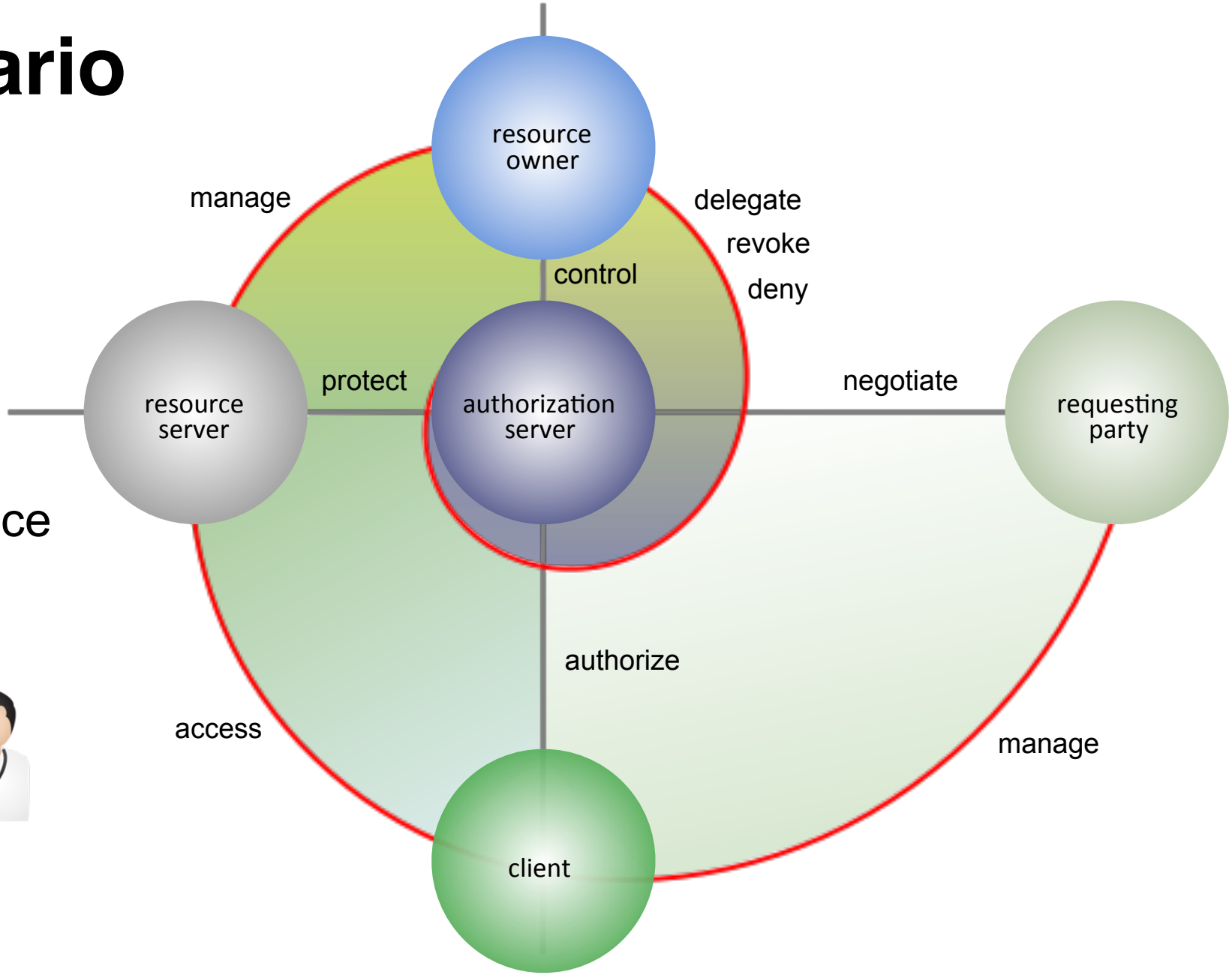


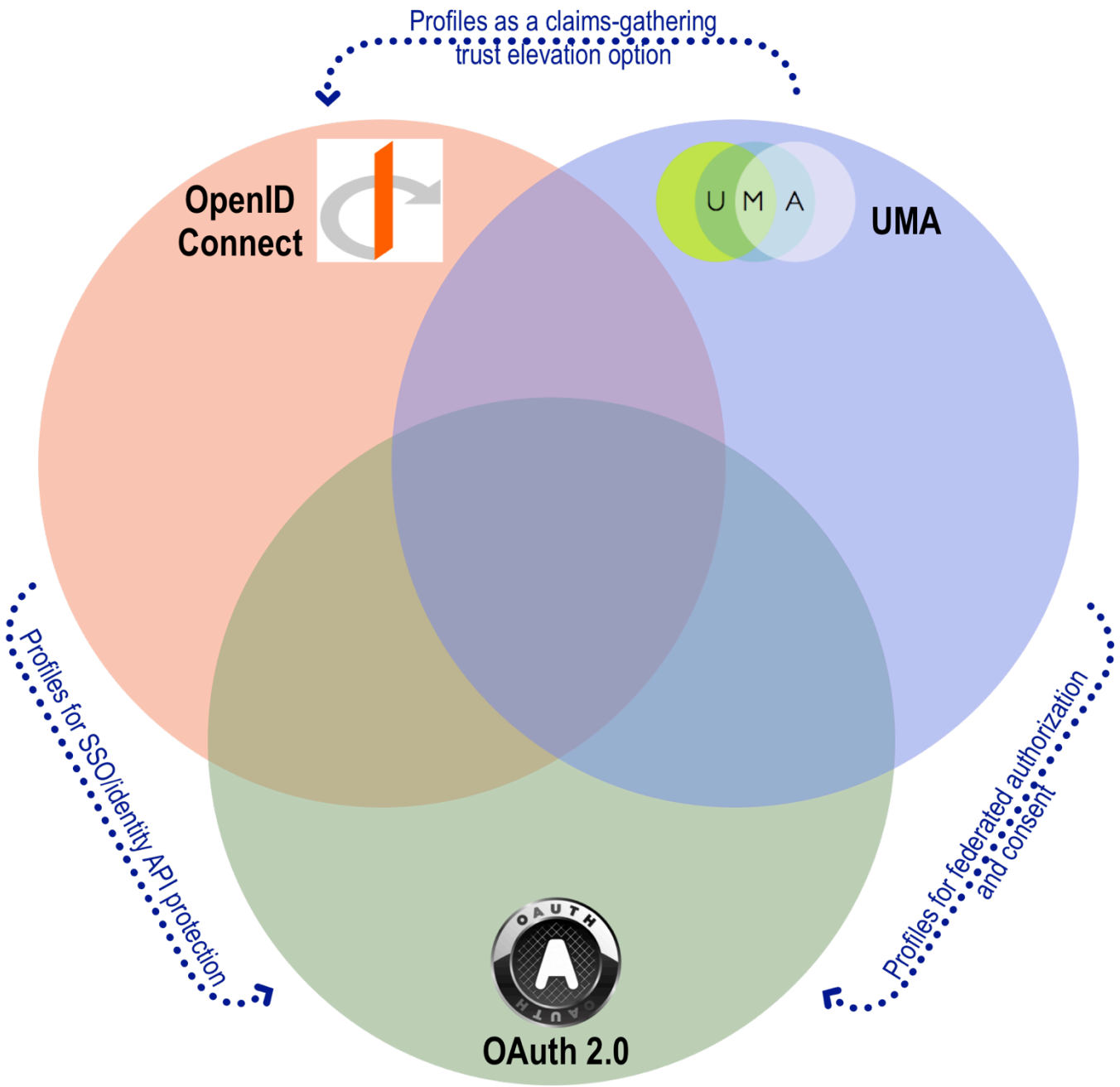
A demo scenario



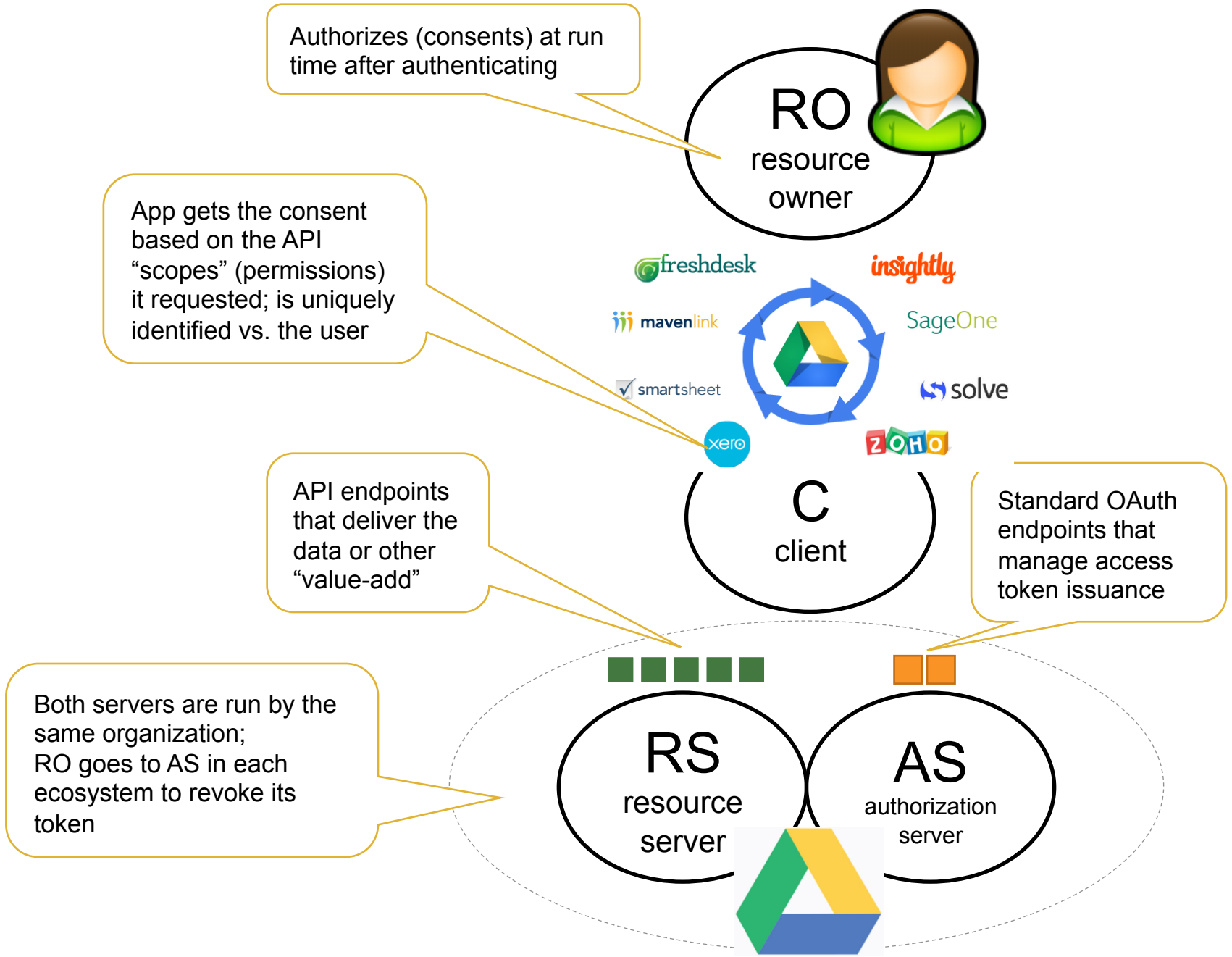
Sharing access to:

- Identity attributes
- Consumer health device
- Contract clauses
- …?





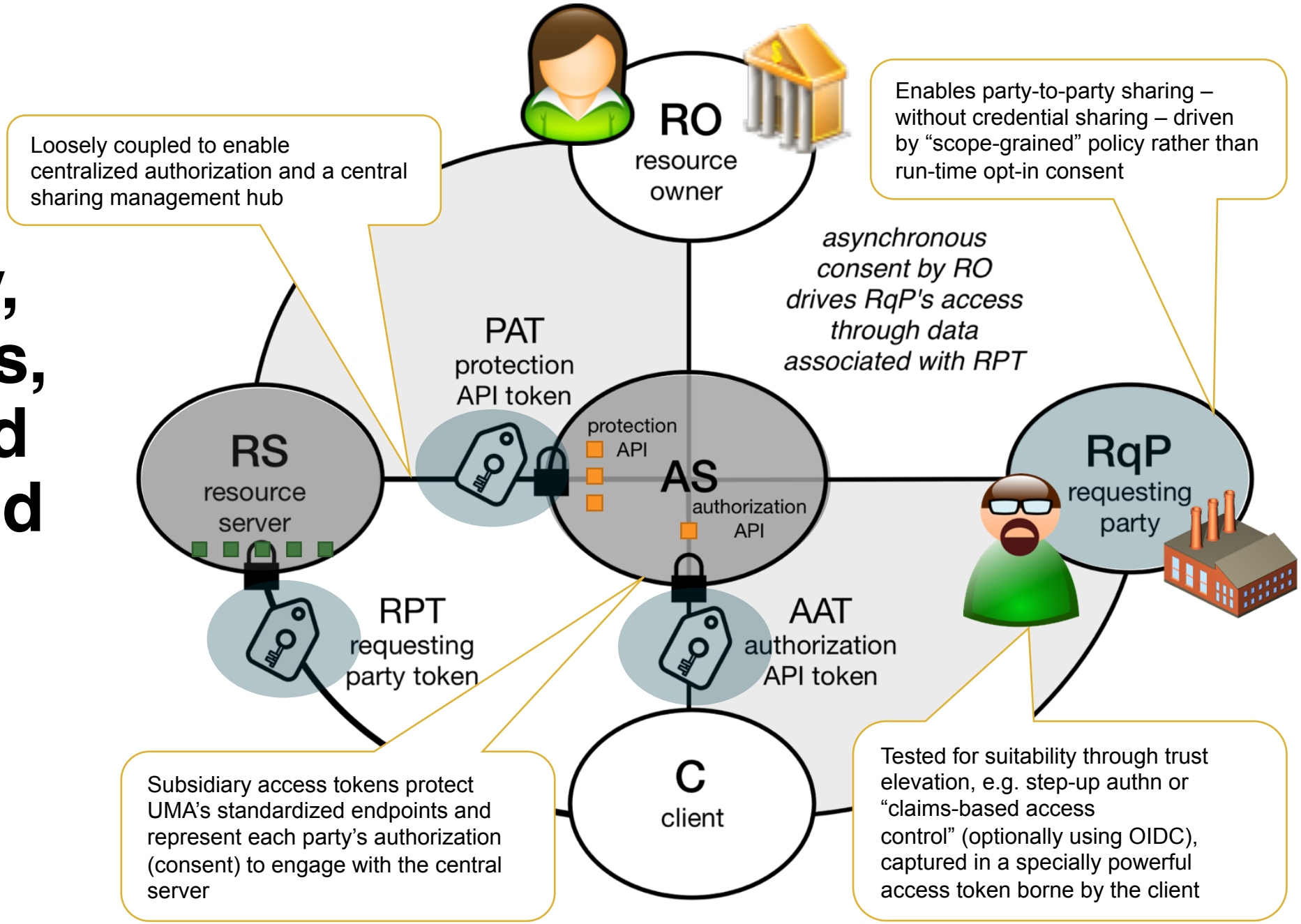
OAuth does "RESTful WS-Security," capturing user consent for app access and respecting its withdrawal

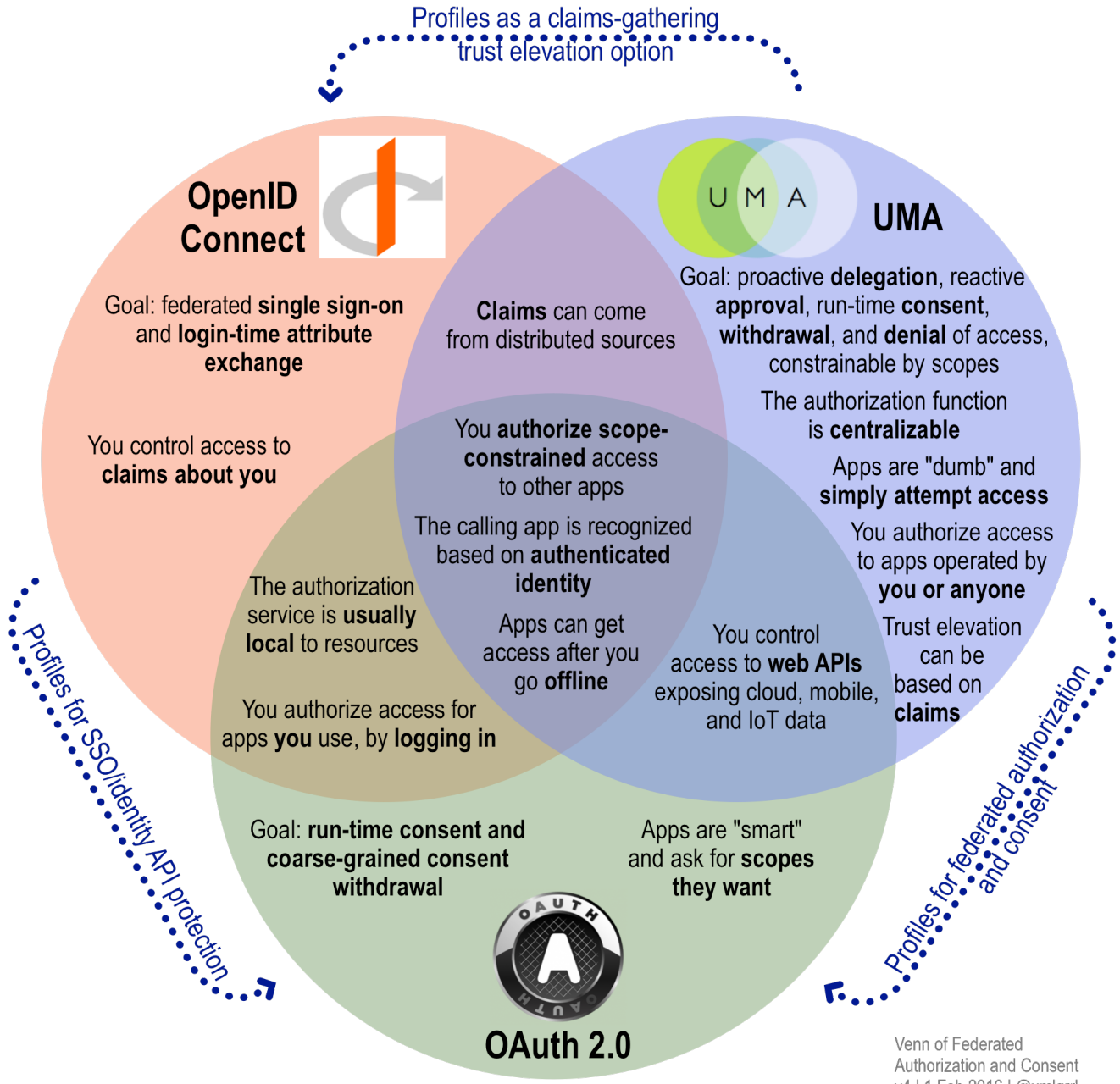


OpenID Connect Turns Single Sign-On Into an OAuth-Protected Identity API

SAML 2, OpenID 2	OAuth 2	OpenID Connect
☑ Initiating user's login session	✗ No sessions	☑ Initiating user's login session
✗ Collecting user consent	☑ Collecting user consent	☑ Collecting user consent
☑ High-security identity tokens	✗ No identity tokens per se	☑ High-security identity tokens
✗ Distributed/aggregated claims	✗ No claims per se	☑ Distributed/aggregated claims
☑ Dynamic introduction *(OpenID only)*	☑ Dynamic introduction *(new)*	☑ Dynamic introduction
✗ Session management	✗ No sessions	☑ Session management *(draft)*

UMA adds party-to-party, asynchronous, scope-grained delegation and control to OAuth





Venn of Federated Authorization and Consent
v4 | 1 Feb 2016 | @xmlgrrl

UMA technical vs. UMA legal

- The UMA protocol can accommodate many “protected sharing scenarios”
- The legal layer of trust relationships is in a parallel world where things can look markedly different
- Parties map to UMA entities that interact “on the wire”
- UMA is *leveraging* CommonAccord to create model text for accelerating “access federation” deployments

Draft definitions from

http://www.commonaccord.org/index.php?action=list&file=GH/KantaraInitiative/UMA-Text/

{Individual}
A natural person (that is, a human being) with the capacity to take on contractual duties and obligations as a participant in an {UMA} interaction.

{Legal_Person}
A legal entity to which the law ascribes the ability to contract, such as a corporation, partnership, agency or government.

{Person}
An {Individual} or {Legal_Person}. {Persons} play various roles in achieving and seeking user-managed access, and the same {Person} might serve in multiple contractual roles.

{Conformance}
Claimed adherence of a running software program or service to the requirements of one or more of the roles "authorization server", "resource server", or "client", as defined in [UMAcore]. Software components play various roles in participating in the technical interactions necessary to achieve and seek user-managed access, and the same software component might serve in multiple technical roles.

{Resource_Subject}
The {Person} to whom a digital data resource relates.

{Grantor}
The {Person} who manages access to a digital data resource, either as its {Resource_Subject} or on that {Person}'s behalf.

{Authorization_Server}
A software service that fills the "authorization server" role as defined in [UMAcore].

{Authorization_Server_Operator}
A {Person} responsible for running and operating an {Authorization_Server}.

{Resource_Server}
A software service that fills the "resource server" role as defined in [UMAcore].

{Resource_Server_Operator}
A {Person} responsible for running and operating a {Resource_Server}.

{Client}
A software application or service that fills the "client" role as defined in [UMAcore].

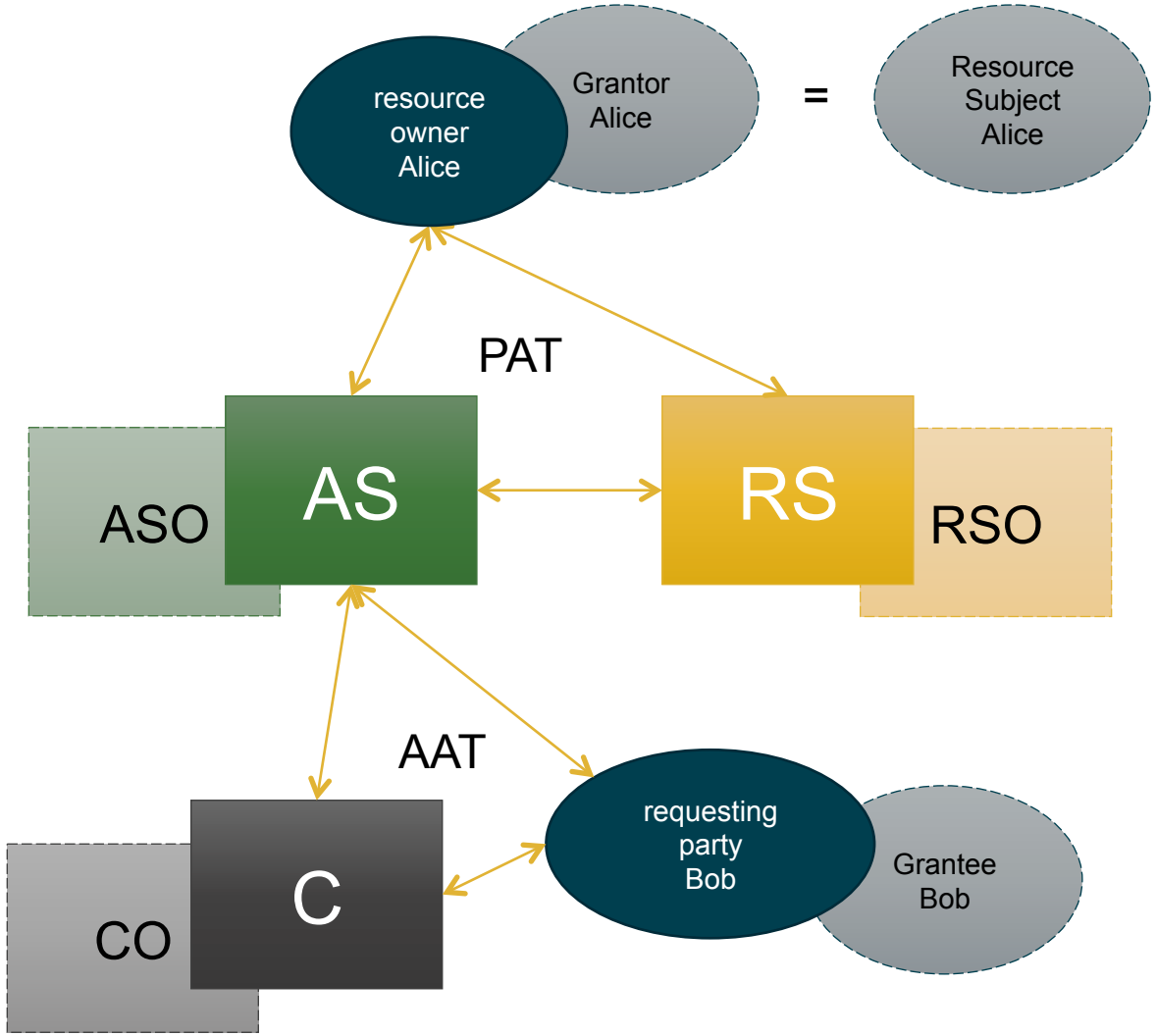
{Client_Operator}
A {Person} responsible for running and operating a {Client}.

{Requesting_Party}
A {Person} that uses a {Client} to seek access to a protected resource. This {Person} may be an {Individual} or an {Legal_Person}. The {Requesting_Party} and the {Grantor} may be the same {Person} or different {Persons}.

{Requesting_Party_Agent}
A {Person} using a {Client} to seek access to a protected resource on behalf of a {Requesting_Party}. Typically this {Person} is an {Individual} acting on behalf of an {Legal_Person}.

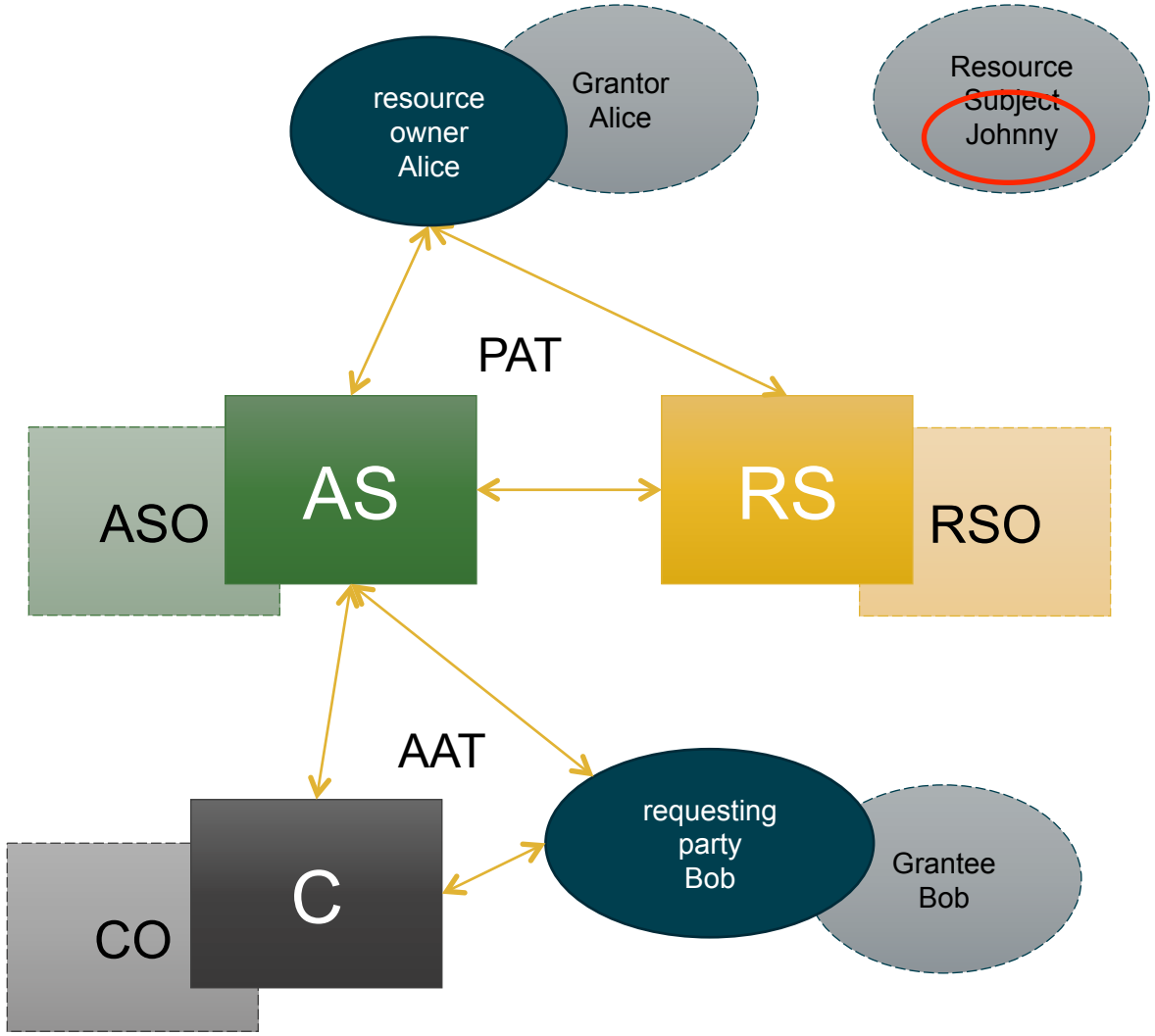
UC1: Alice is an online adult with legal capacity

- Her resources at the RS relate to her
  - So she is the Resource Subject
- She controls access to those resources herself at the AS
  - So she is also the Grantor
- She shares the resources with Bob
  - So he is a Grantee
    - More complication potentially to come here



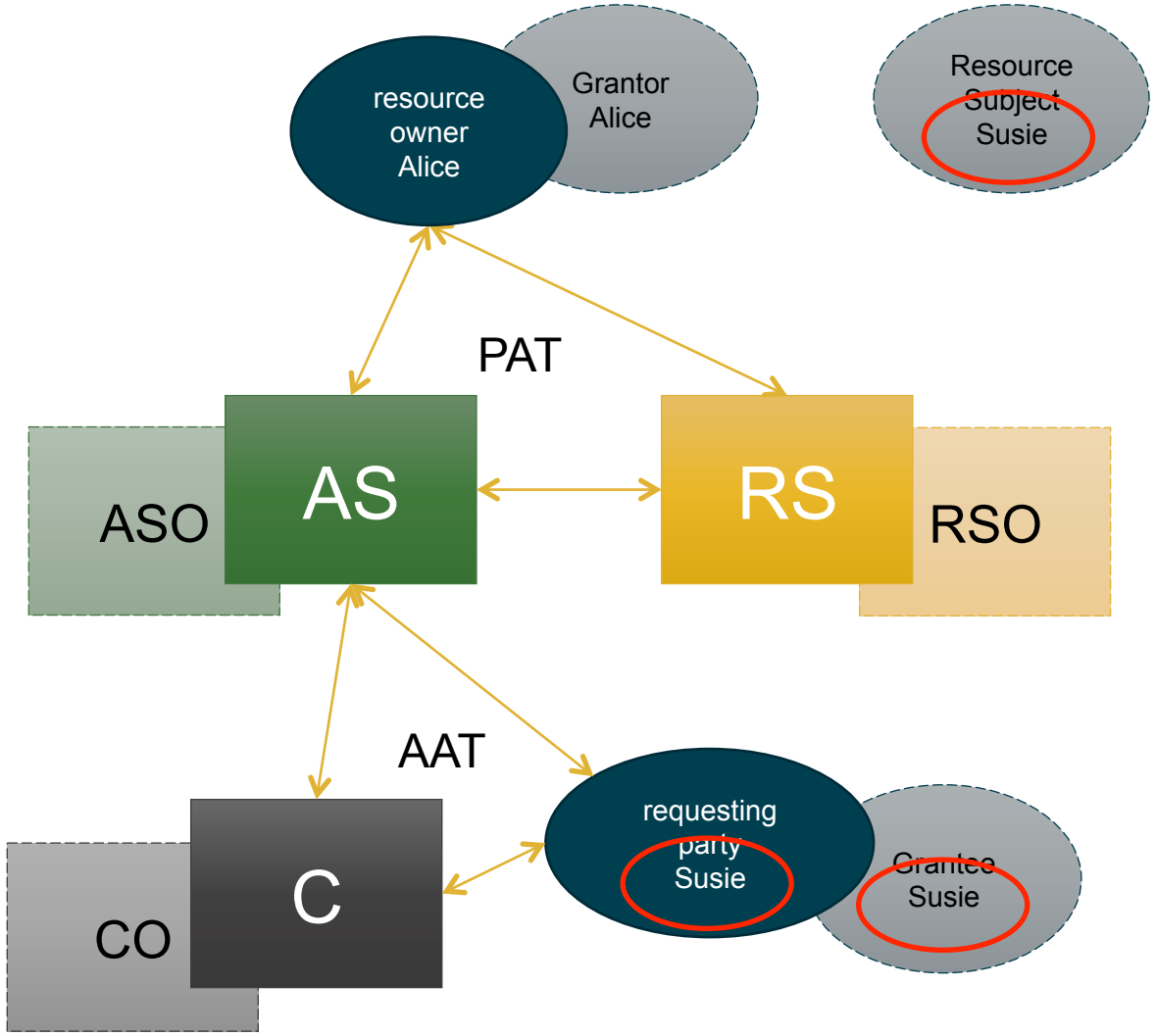
UC2: Alice is a guardian (proxy) for 2-year-old Johnny

- His resources at the RS relate to him
  - So he is the Resource Subject
- But she controls access to those resources at the AS
  - So she is the Grantor
- She wants to share the resources with Bob on Johnny's behalf
  - Johnny has no access because he is too young to do anything with them for now



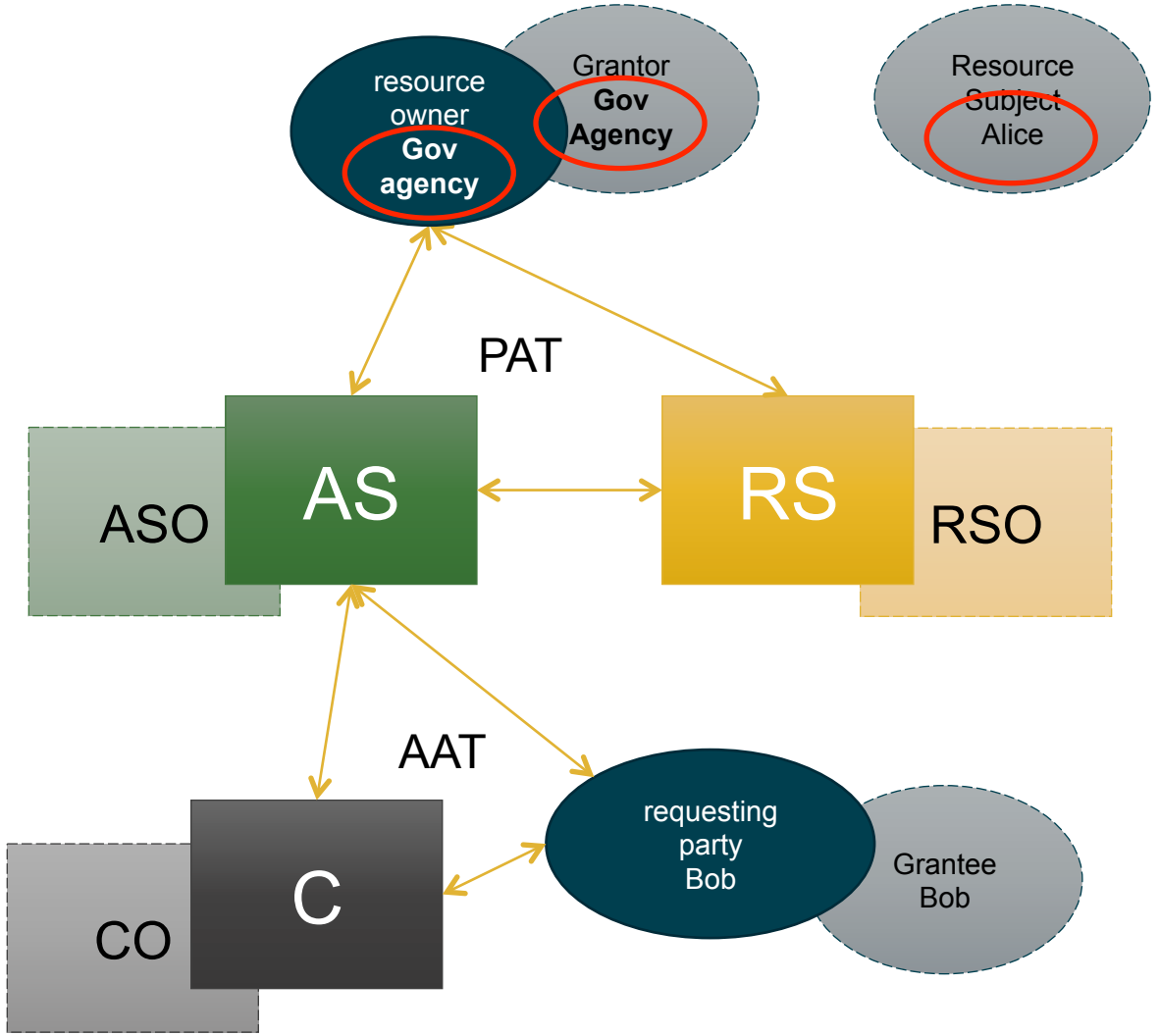
UC3: Alice oversees 12-year-old Susie's online usage

- Susie's resources at the RS relate to her
  - So she is the Resource Subject
- But Alice controls access to those resources at the AS
  - So she is the Grantor
- Alice shares the resources in constrained fashion with Susie
  - So Susie is a Grantee
  - A narrow ecosystem would help for additional downstream controls to be in place
- Susie will eventually turn 13 and will be able to control access to her own resources
  - Alice could be "kicked out" and Susie allowed to set up a direct AS relationship at that time, as a Grantor in her own right (see UC1)



UC4: Alice is offline and gives paper sharing directives to a government agency

- Alice's resources at the RS relate to her
  - So she is the Resource Subject
- The agency controls access to those resources at the AS
  - It is the Grantor, by virtue of controlling a "headless" account for Alice for this purpose (see the NZ case study)
- Alice specifies how to share resources with Bob etc.
  - The agency configures the AS for her
- If Alice wants to take online control, the agency gives her a login to the account and steps out of the way
  - No more proxying – she would become her own Grantor (see UC1)



Next challenge: model clauses enabling RSO liability management given AS instructions

- The token says don't give access:
  - When can the RS give access?
- The token says give access:
  - When can the RS deny access?
- Outside the UMA context:
  - When can RS give access?
- Plus other juicy model text work:
  - What are the reporting and notification requirements?
  - How to enable jurisdictional and sectoral hooks?
  - How to handle three-party relationships (PAT and AAT)?
  - The same subtle split in the Requesting Party as in the Resource Owner