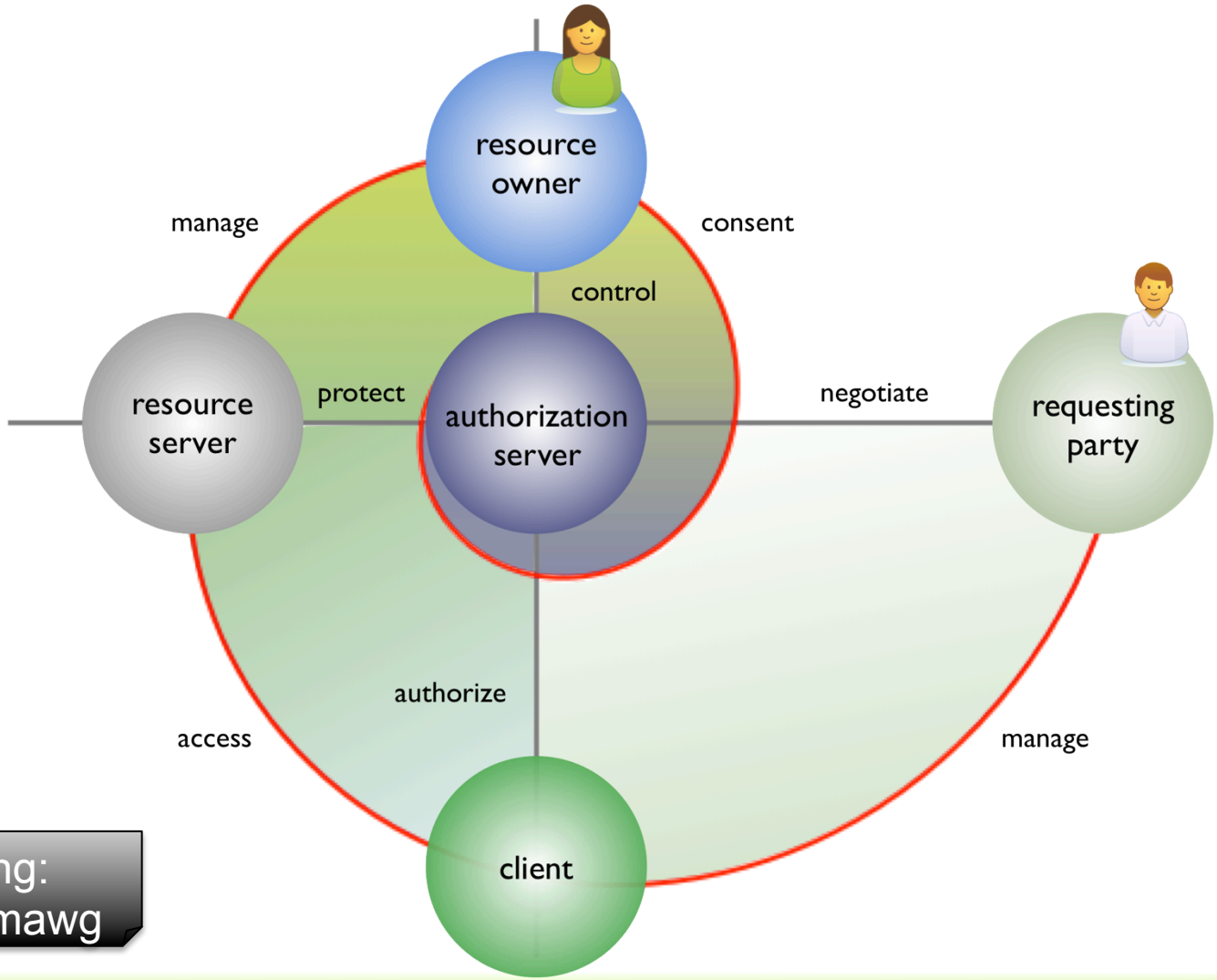
Protecting “Personal Clouds” with UMA and OpenID Connect

@UMAWG
#UMApcloud *for questions*
19 June 2014
tinyurl.com/umawg *for slides, recording, and more*

The marvelous spiral of controlled personal data sharing



Further reading:
tinyurl.com/umawg

Agenda

- The realities and challenges of personal data sharing
- “UMA for humans 101”
- A walk through personal cloud models
- Use cases
- How UMA leverages OpenID Connect – with demo
- Next steps

Thanks to MIT-KIT for sponsoring this webinar and taking part!

Thanks to Kantara for supporting the UMA work!

Thanks to our additional webinar participants!

The realities and challenges of personal data sharing

What is personal data?

Personal Data is the Life Blood of the Information Age

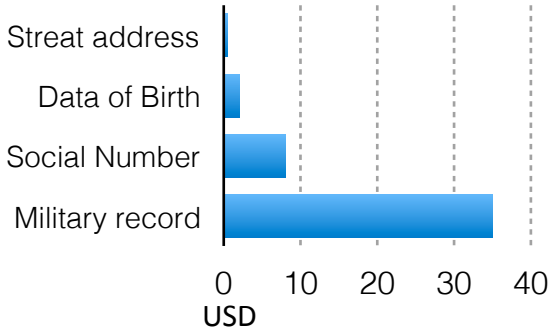
Personal Data is the New "***Oil of the Internet***"

Personal Data is the new **currency**

Ways to measure the value of personal data

- Market capitalization
- Revenue per record/user
- Market Price
- Cost of data breach
- Pay to protect

$112 per user record



SONY

Data breach cost $171M

USD 1.7 per record

Source: OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value"

Personal data risks

"72% of European citizens are concerned that their personal data may be misused…"

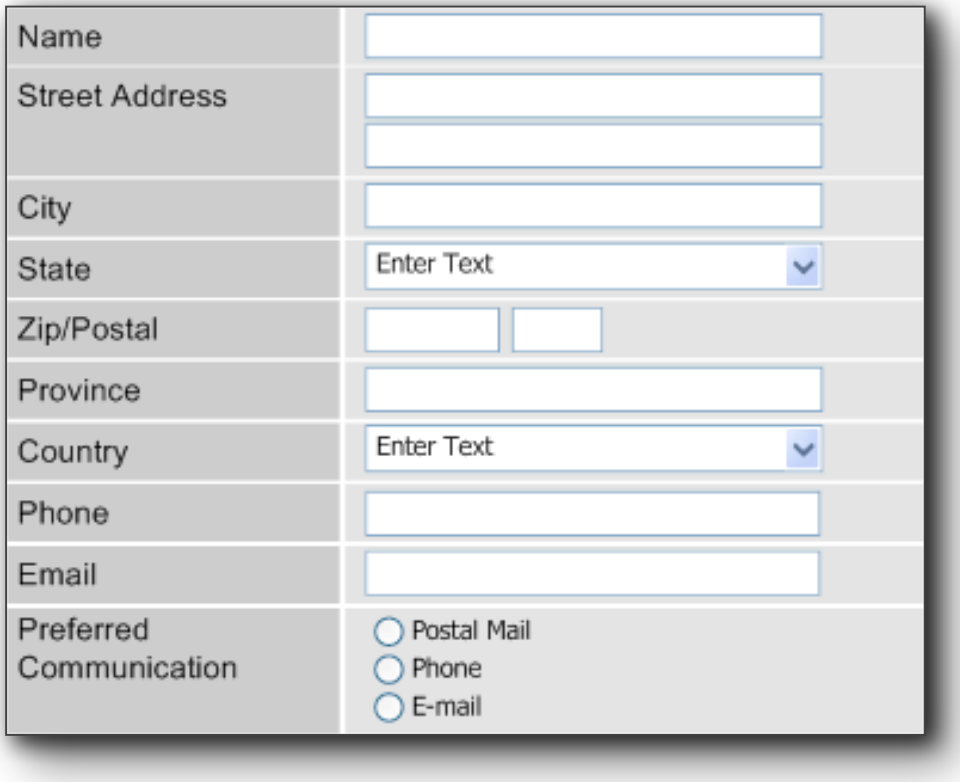
Individuals have little visibility into the practices of the organizations they are putting their trust in – until their data is breached or misused.

Risks: Loss of Trust

EU commission survey 2012

The “personal data price” for online service is too high: typing…

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



The “personal data price” for online service is too high: connecting…

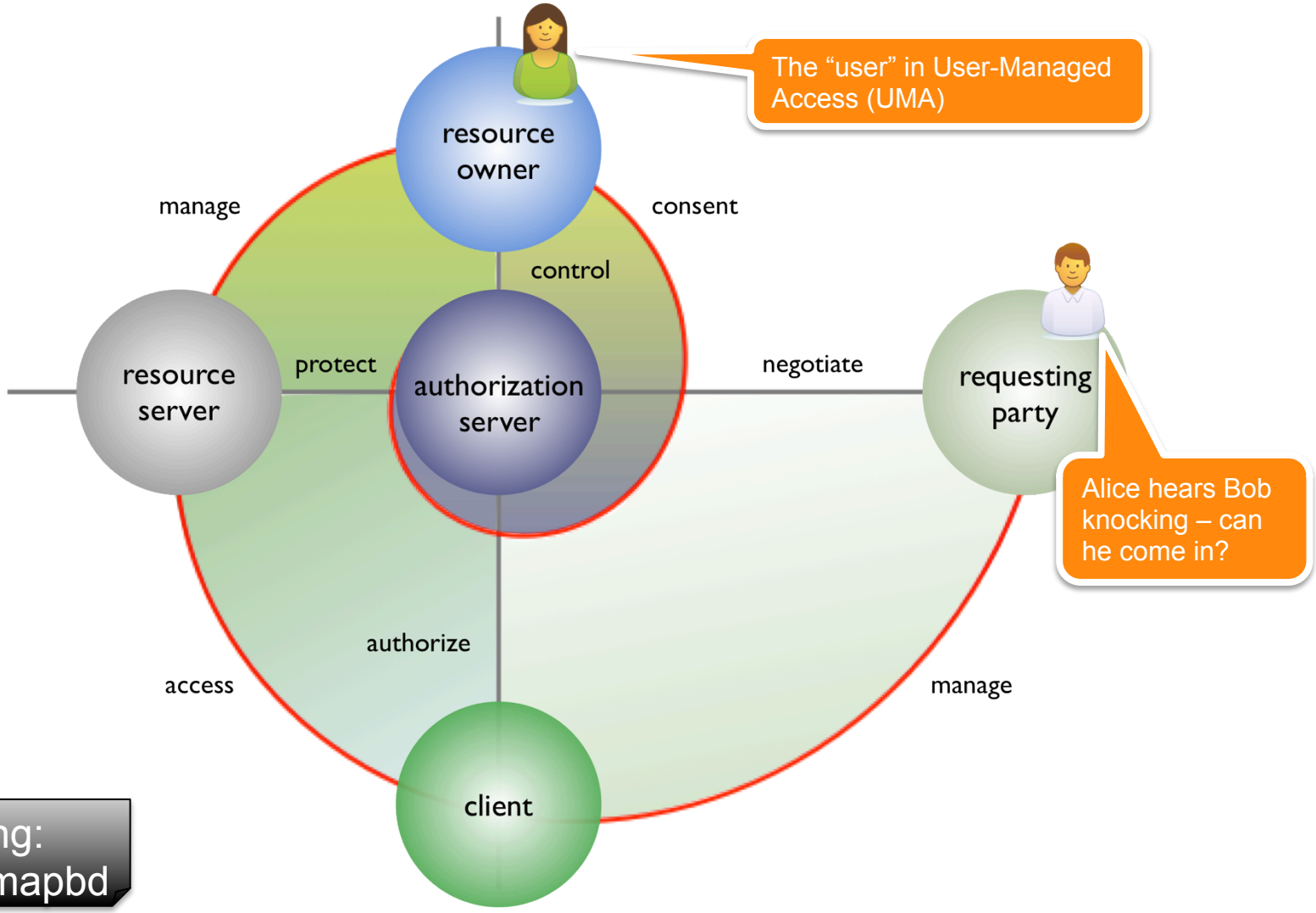
- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oblivious oversharing

The “personal data price” for online service is too high: private URLs…

- Handy but insecure
- Unsuitable for really sensitive data

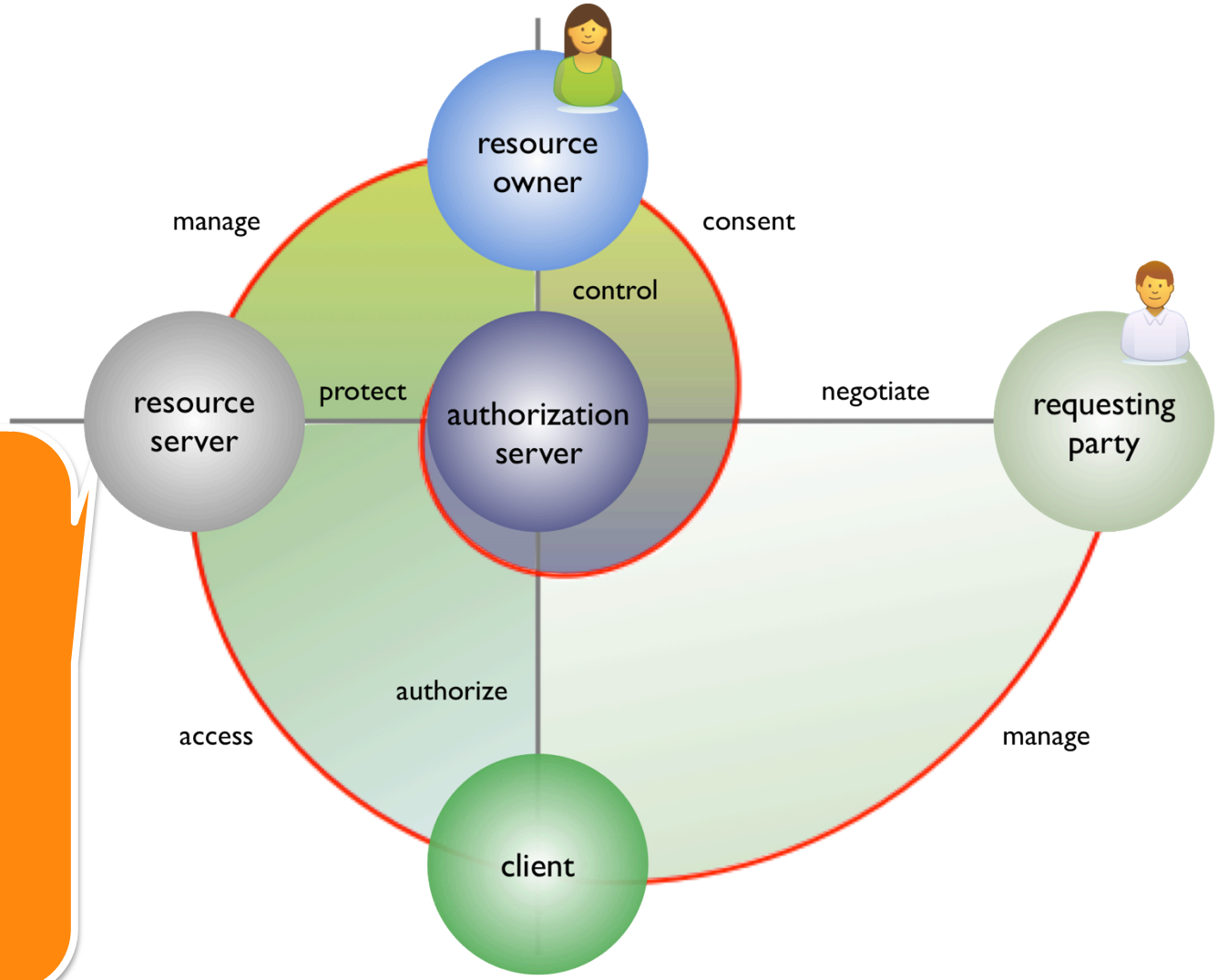
“UMA for humans 101”

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



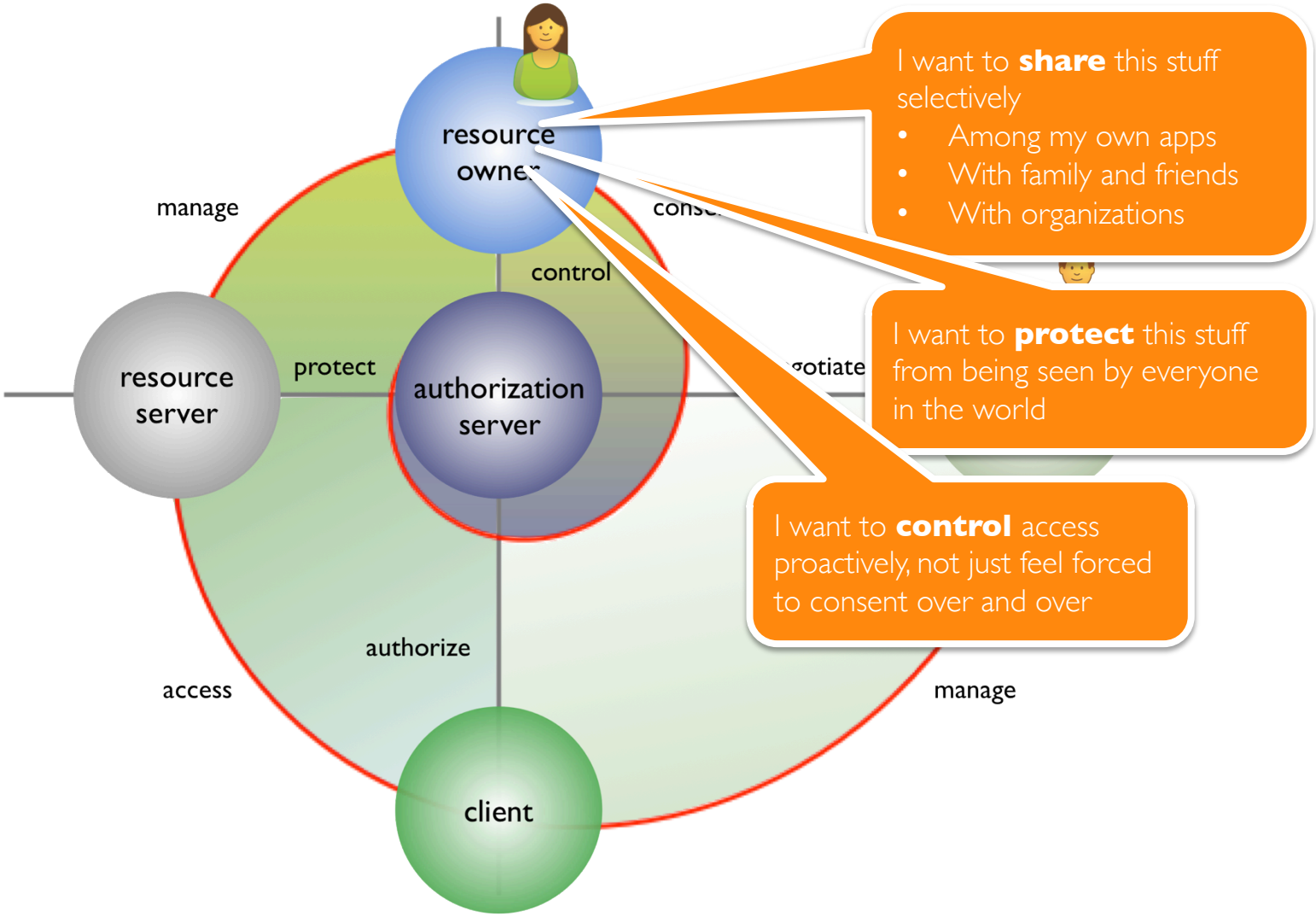
Further reading:
tinyurl.com/umapbd

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

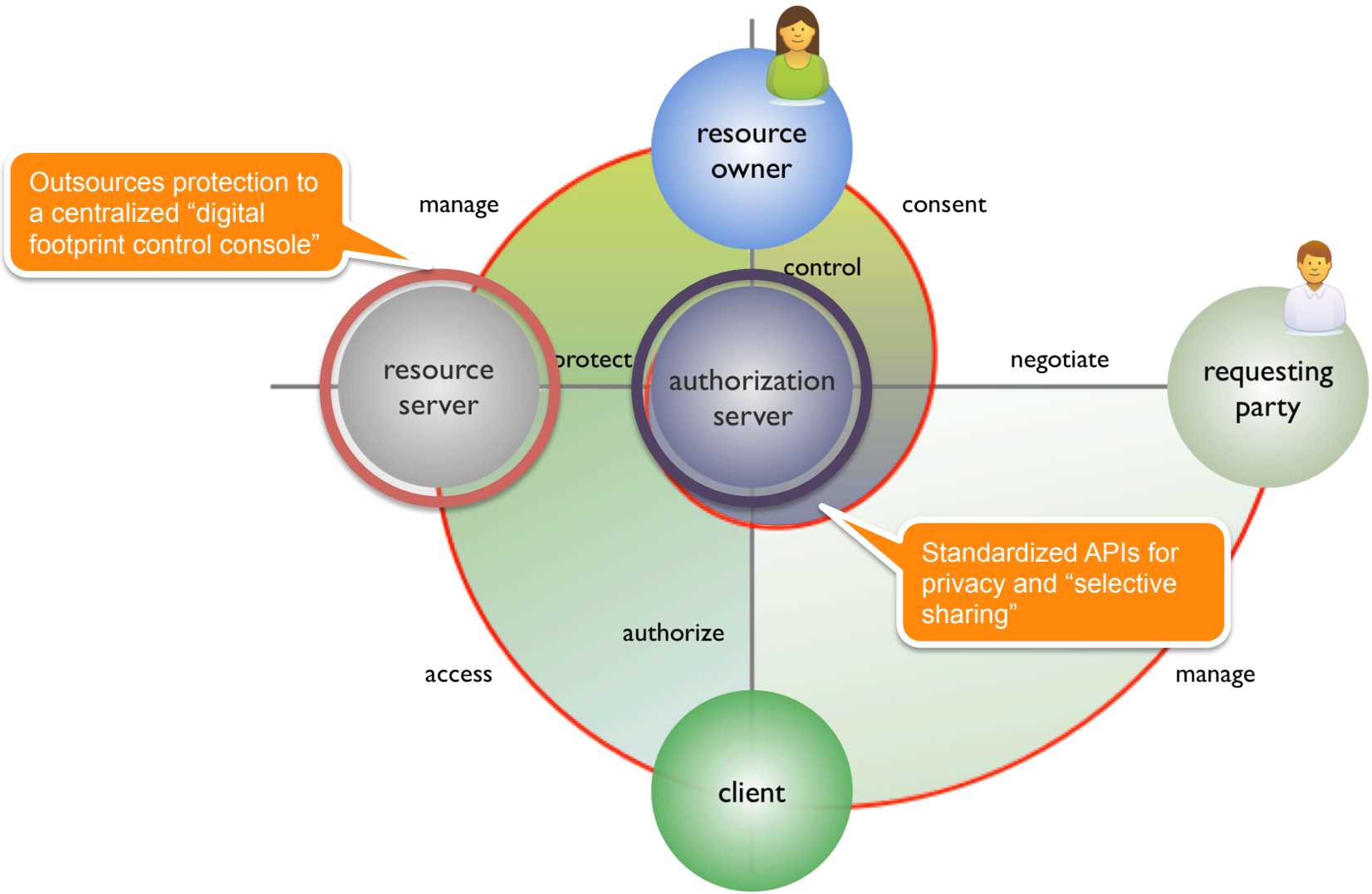


- Historical
- Municipal
- Financial
- Vocational
- Artistic
- Social
- Geolocation
- Computational
- Genealogical
- Biological
- Legal
- ...

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

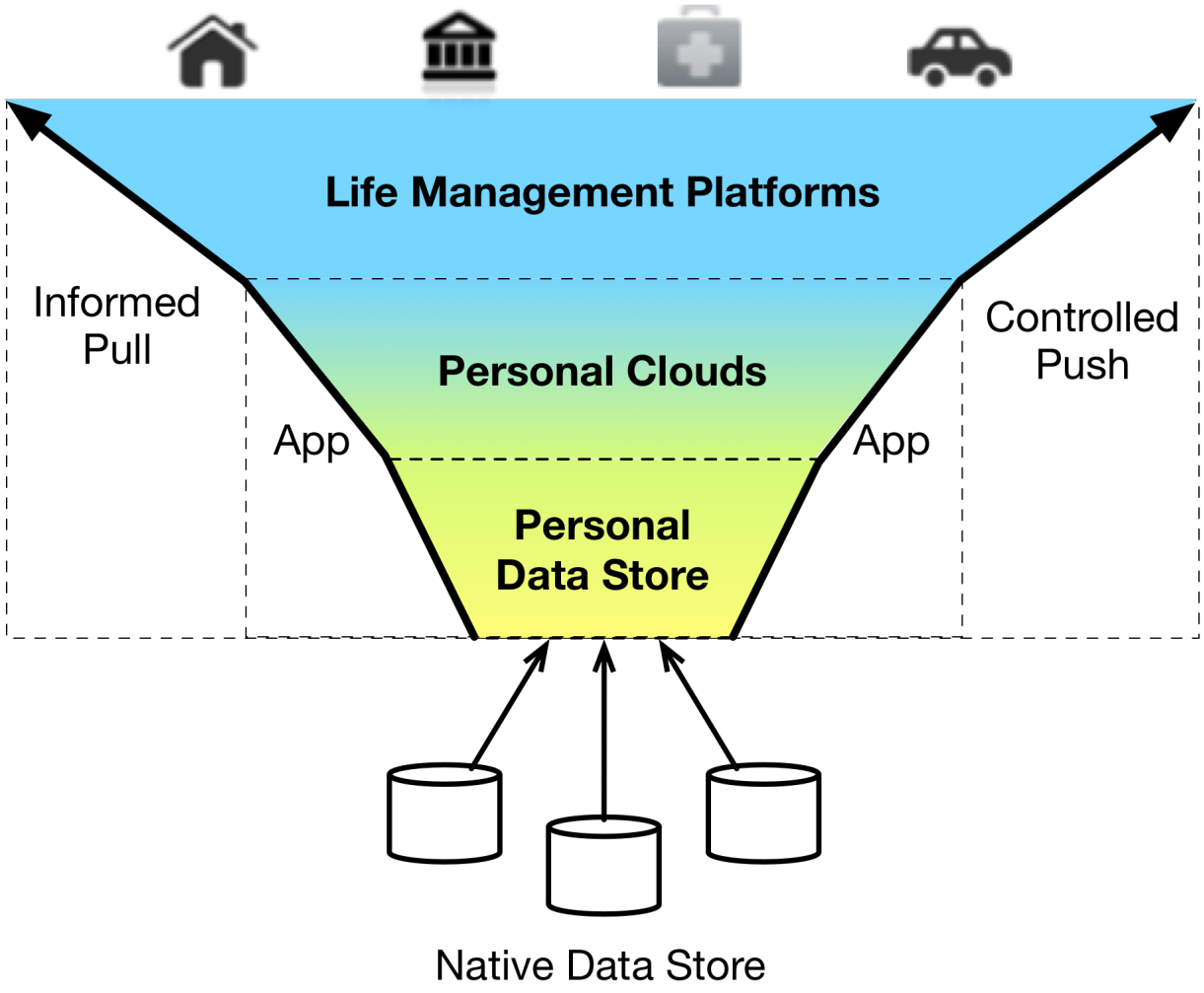


UMA turns online sharing into a privacy-by-design solution

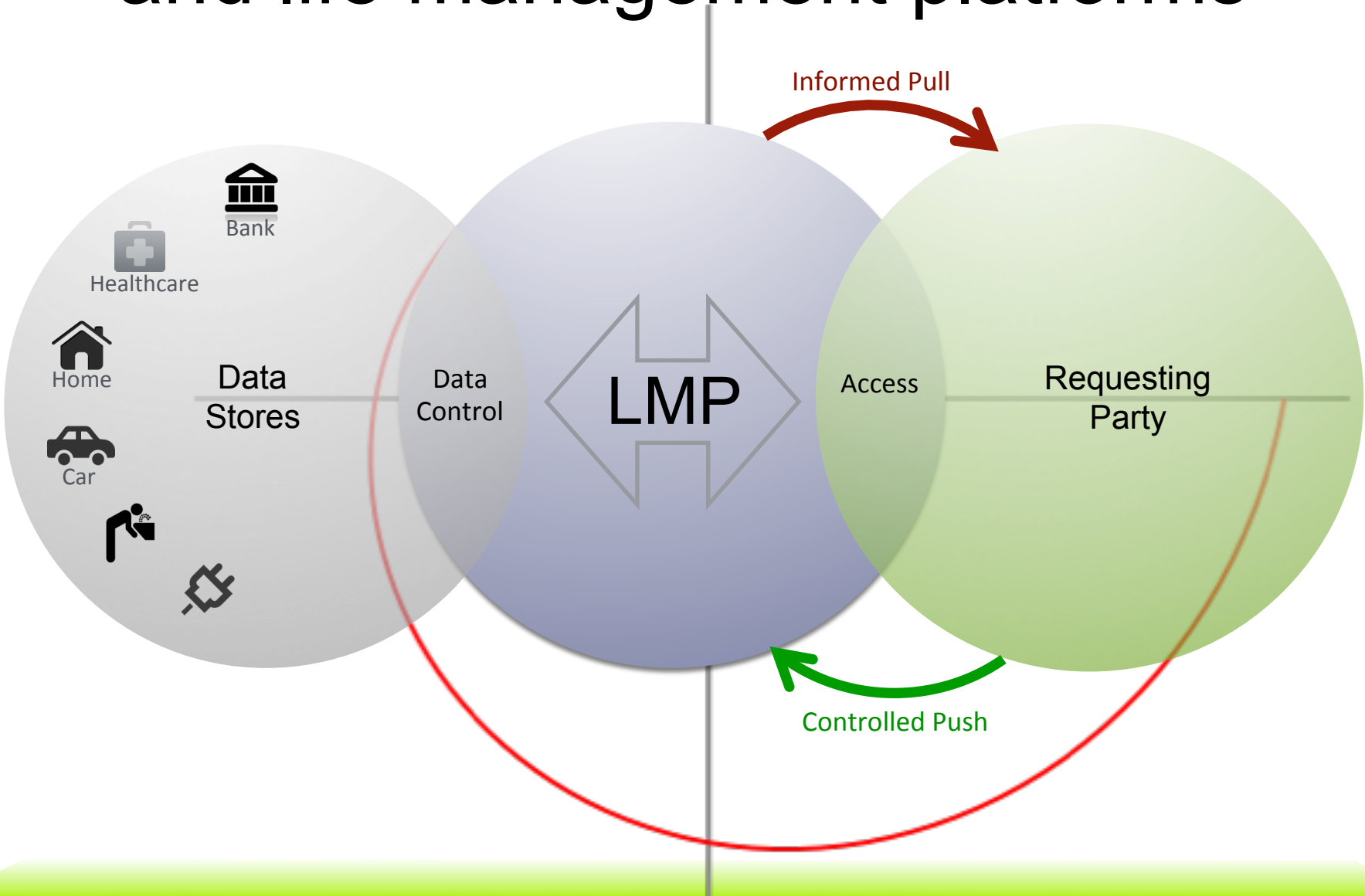


A walk through personal cloud models

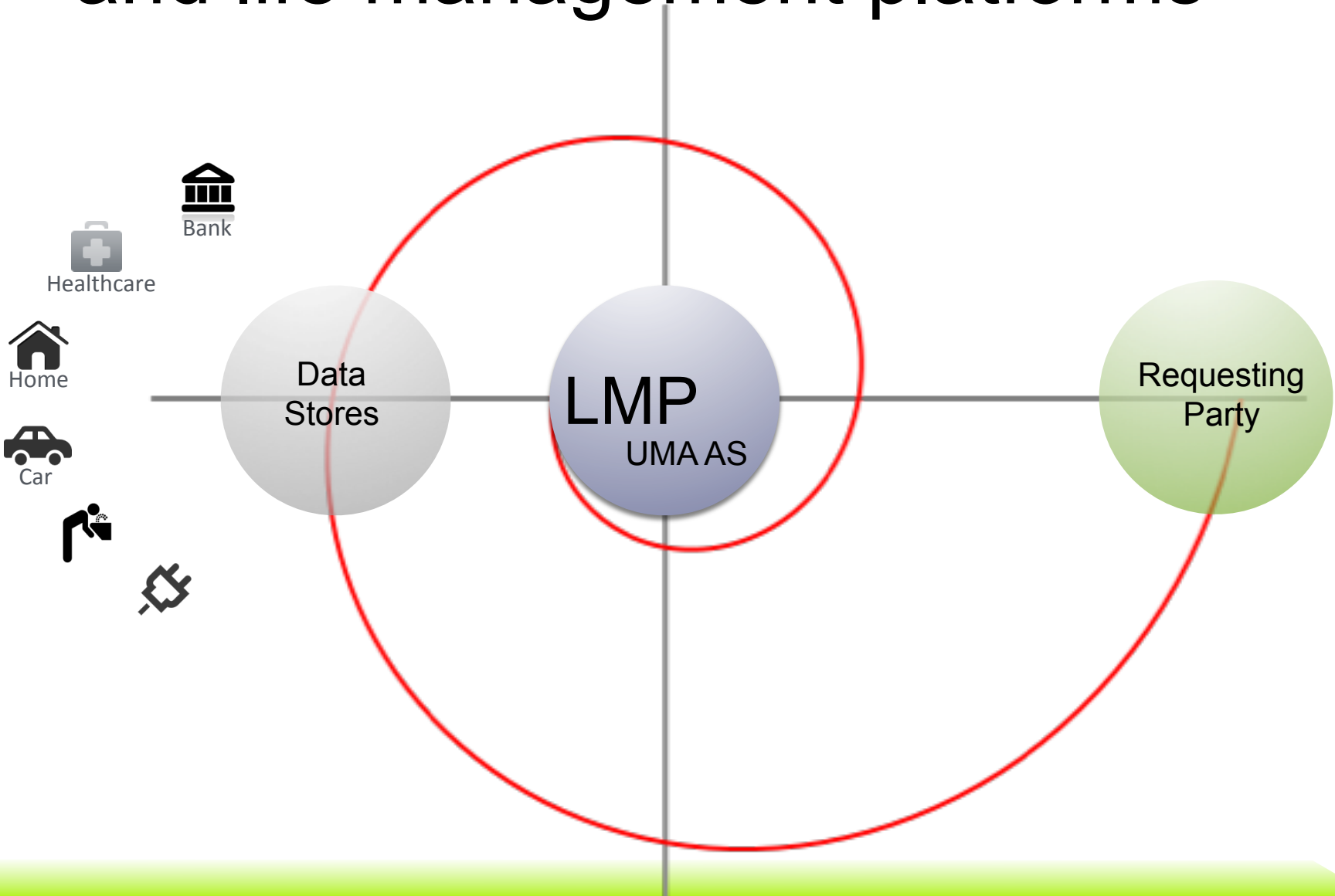
Personal data ecosystem emerging trends



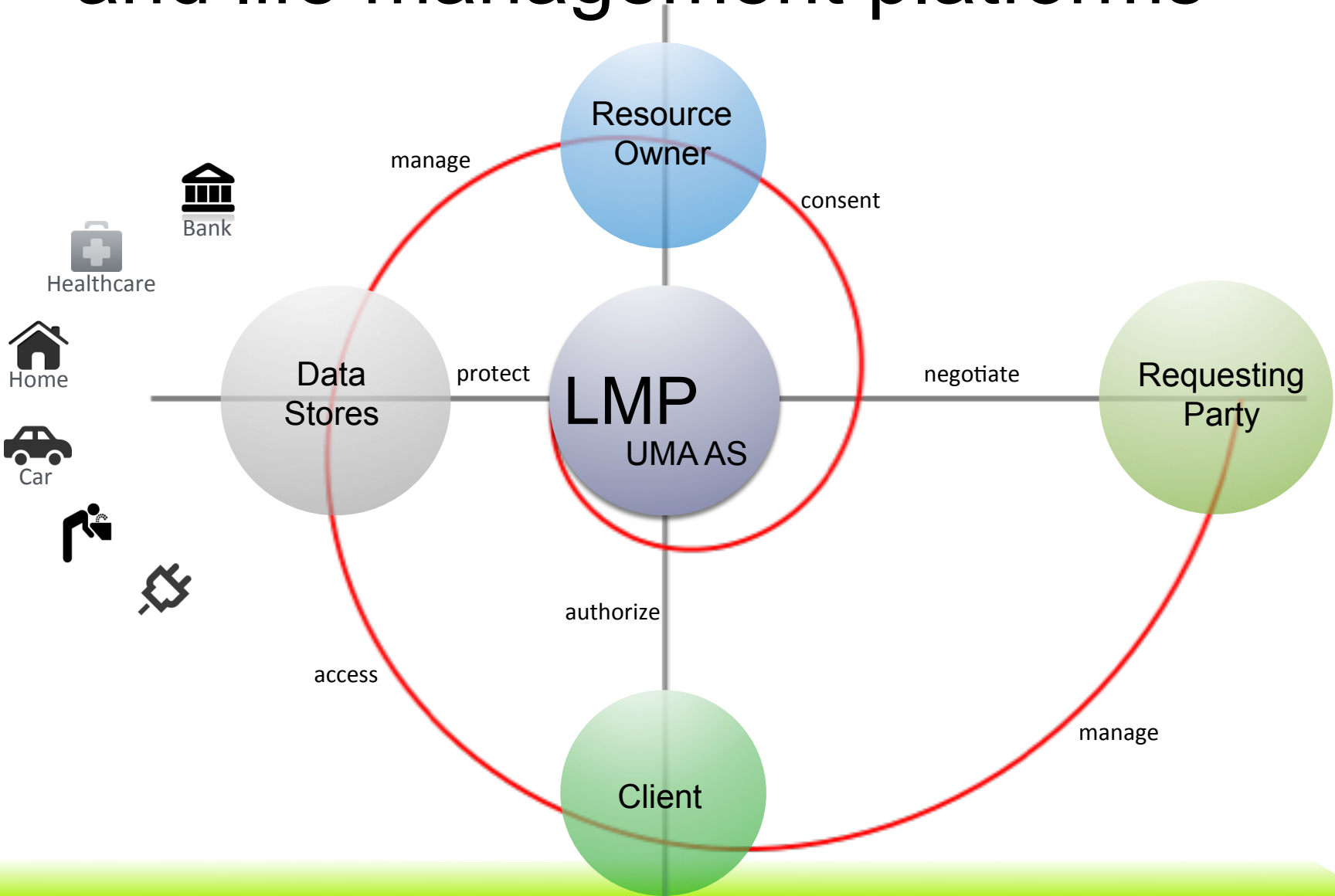
Mapping UMA to personal clouds and life management platforms



Mapping UMA to personal clouds and life management platforms



Mapping UMA to personal clouds and life management platforms



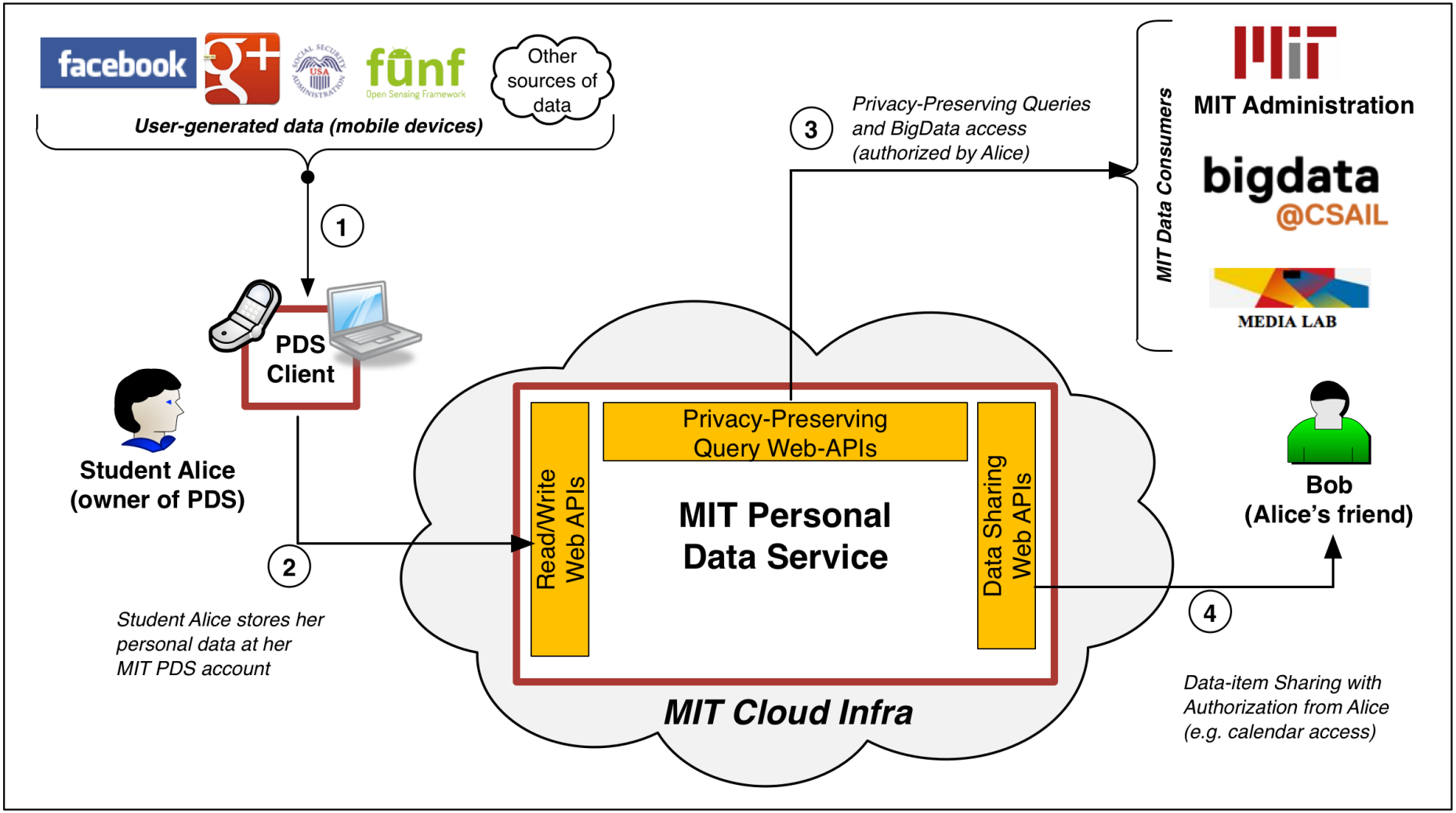
Use cases

Case studies for…

- Management and sharing of personal accessibility needs and preferences
- Secure sharing of university e-transcripts
- Healthcare relationship locator service and patient-centric consent directives
- Access management 2.0 for the enterprise (previous webinar)
- …
- Protecting the personal data stores of everyone at MIT

Further reading:
tinyurl.com/umacase

Protected personal data stores: MIT's view



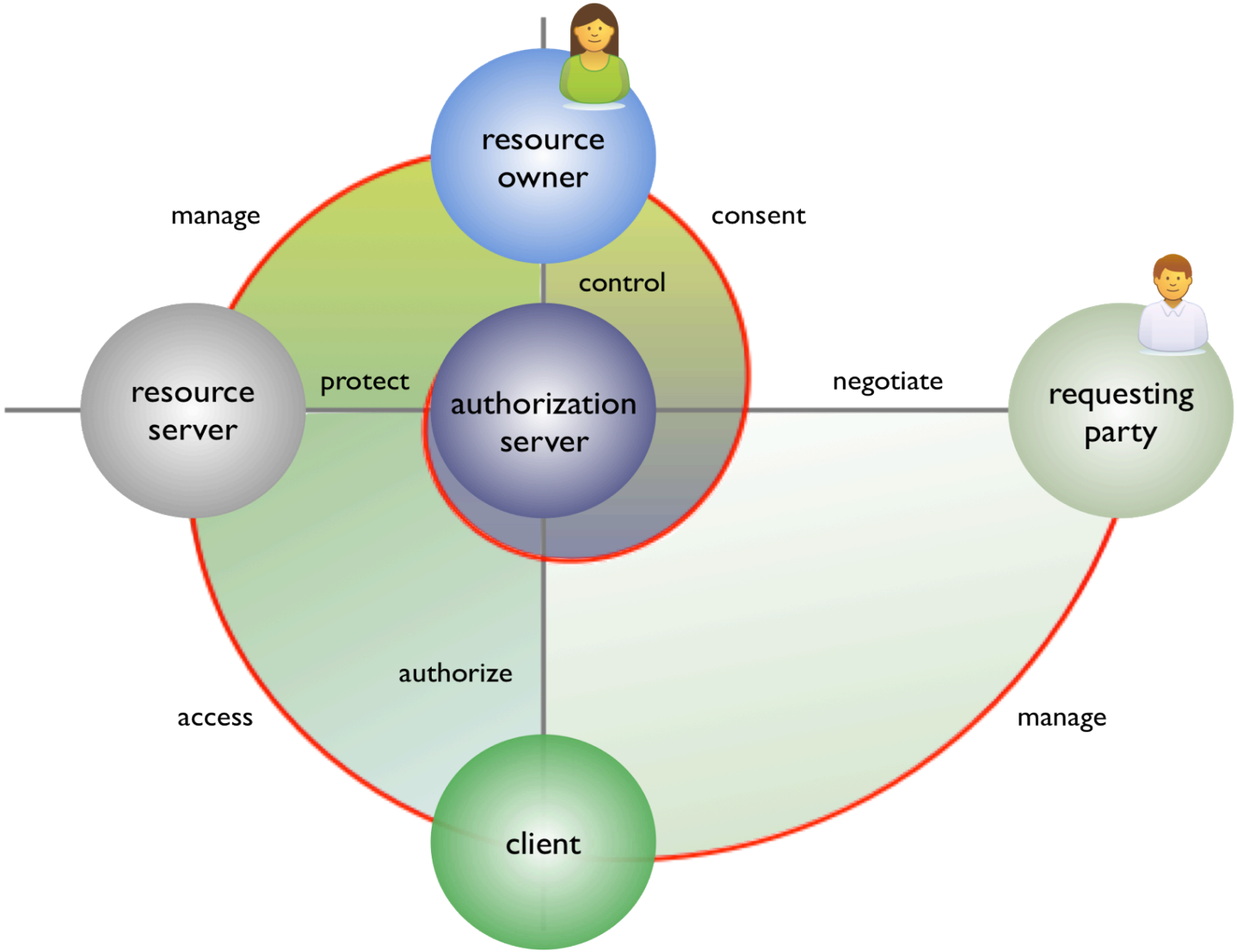
How UMA leverages OpenID Connect

Use case: Transcript of Records sharing

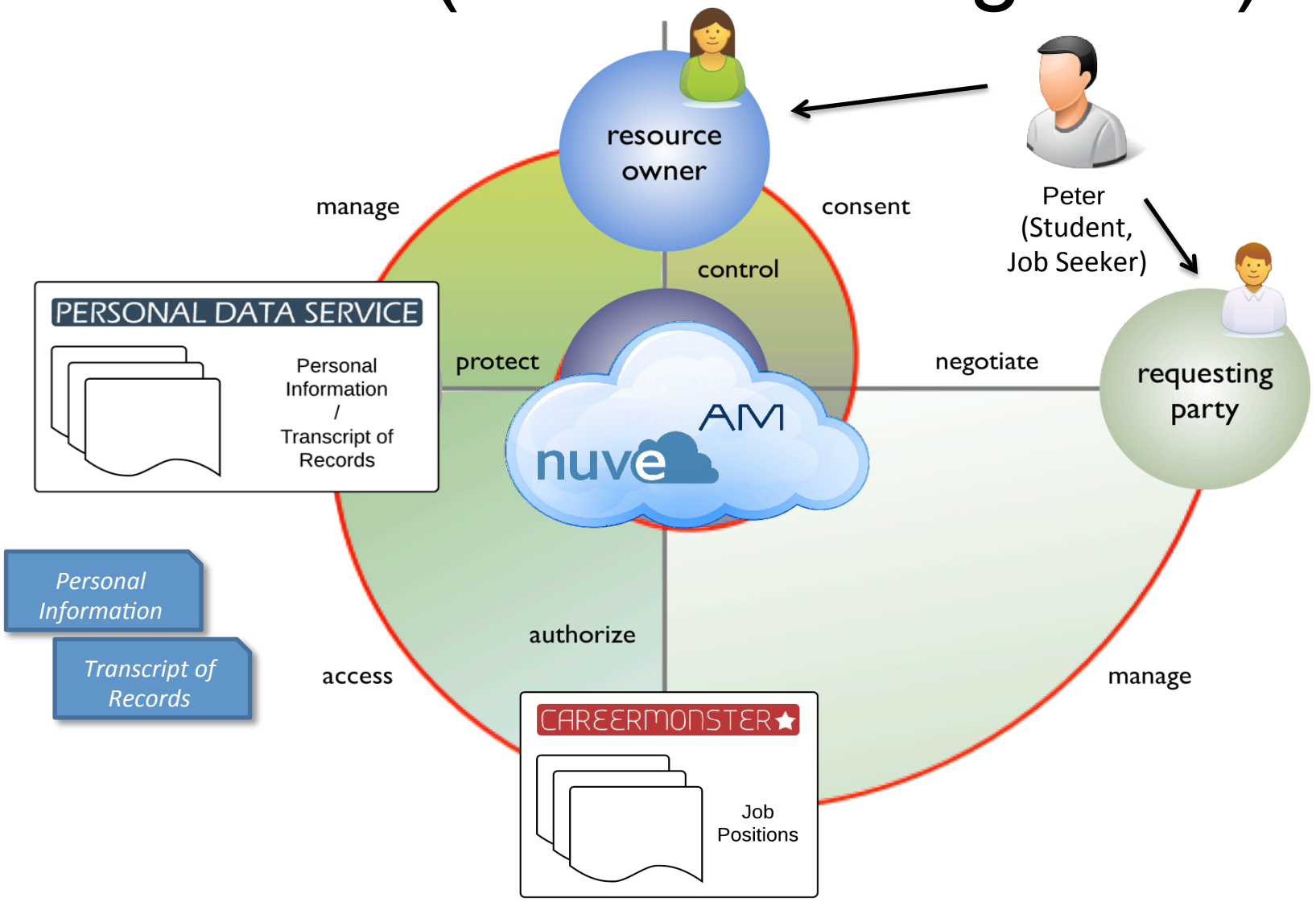
- Student interacts with an online job application system
- Student fills in a job application form and provides:
  - Personal information
  - Transcript of Records document
- Data is transferred from the student's personal data service
  - With explicit consent
- Employer requests access to additional data
  - …and this has to be confirmed by the student

"Sharing Trustworthy Personal Data with Future Employers"
http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario

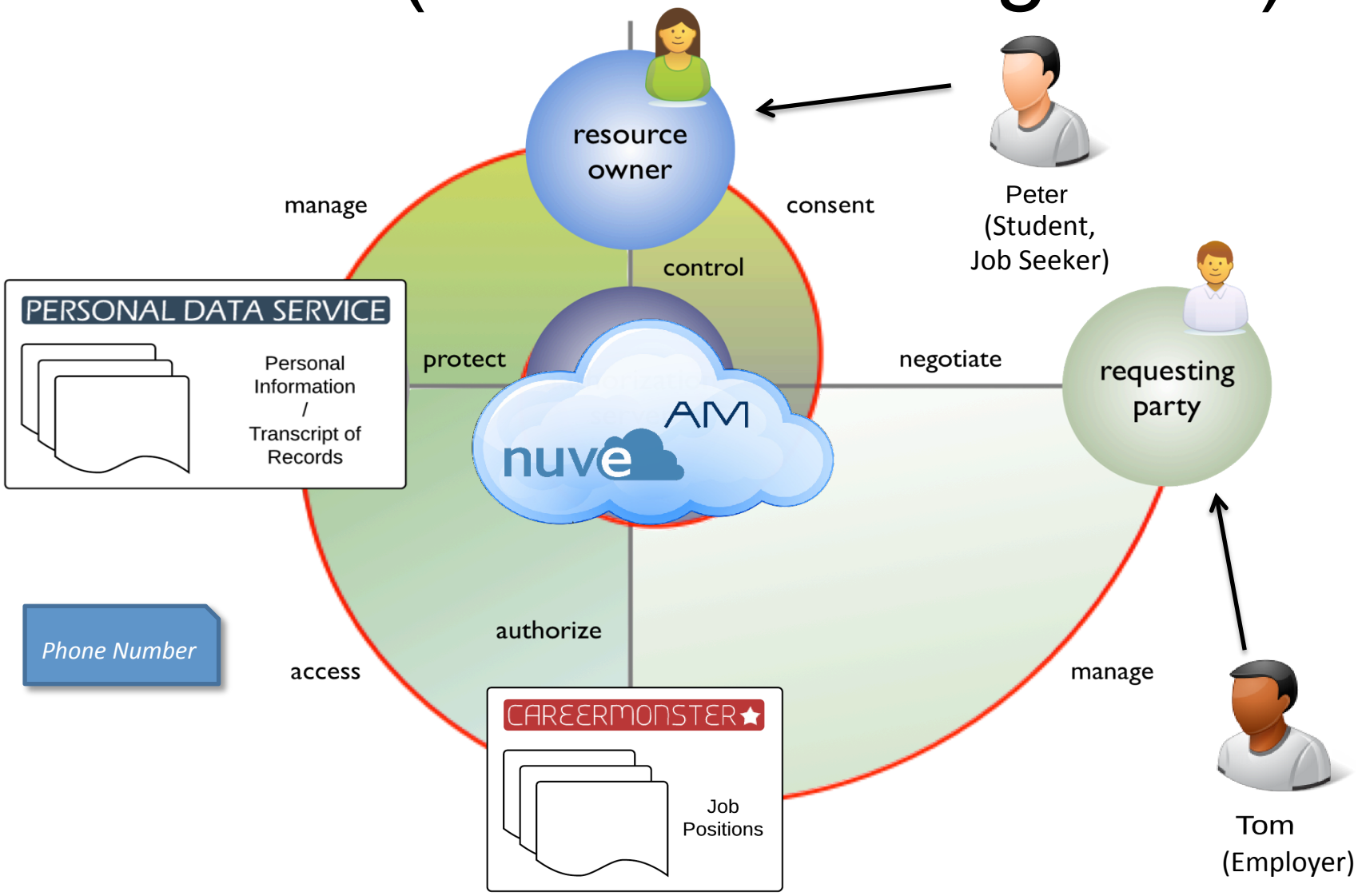
UMA model


resource owner
manage
consent
control
resource server
protect
authorization server
negotiate
requesting party
authorize
access
manage
client

Scenario (Peter sharing data)



Scenario (Tom accessing data)



Live demo

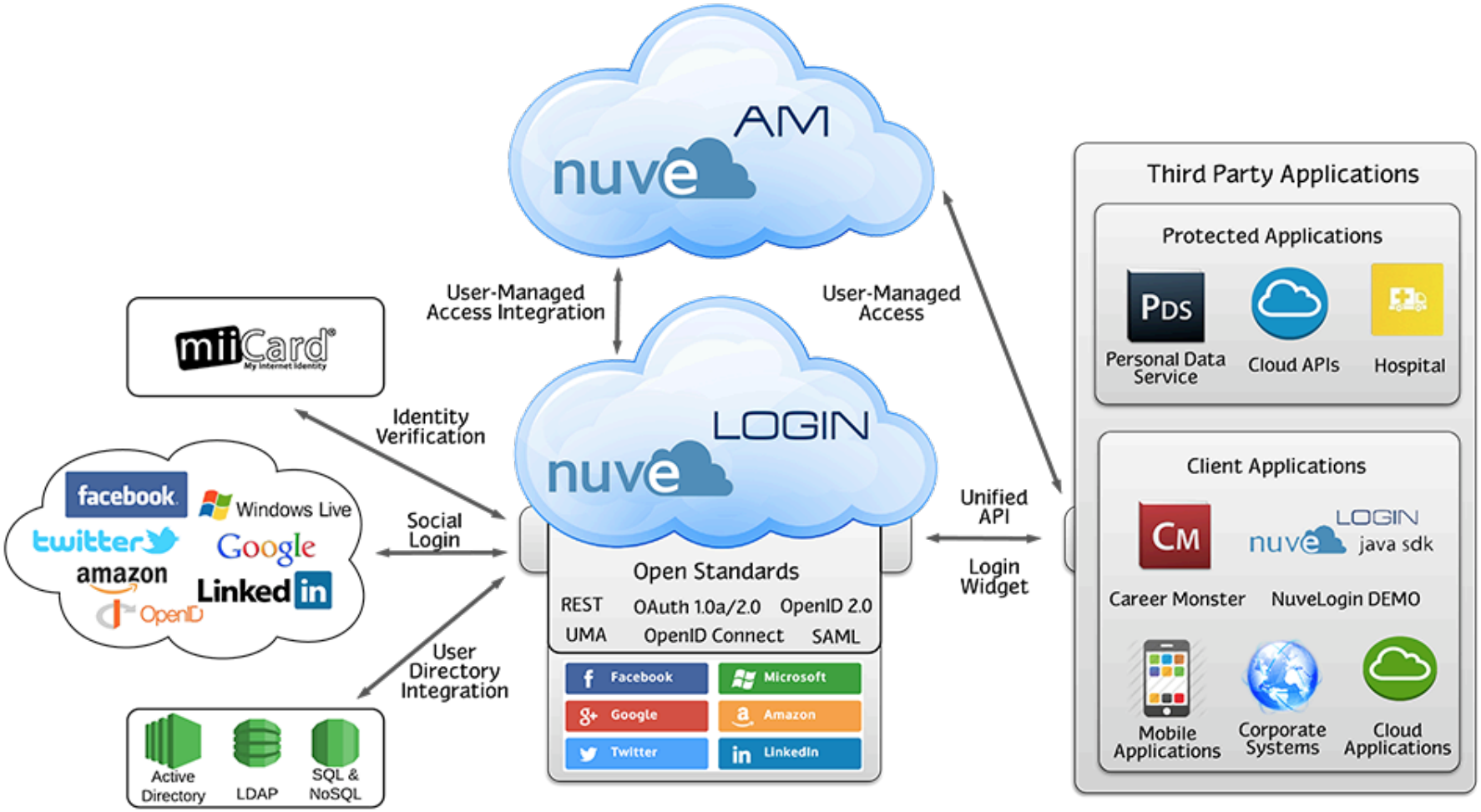
NuveAM – Authorisation Manager

- UMA-compliant Authorisation Server (AS) from Cloud Identity Limited:
  - Access control to data in the Cloud
  - API security management
  - Real-time monitoring and audit

- Use cases: **Securing Cloud-based Personal Data Services (PDS)**; Managing access to Cloud-based APIs
- Uses open standards, including: UMA, OAuth 2.0, OpenID Connect, SAML 2.0
- Open source frameworks: Java and Python

http://www.cloudidentity.co.uk/products/nuveam

Nuve User-Managed Access



cloudidentity

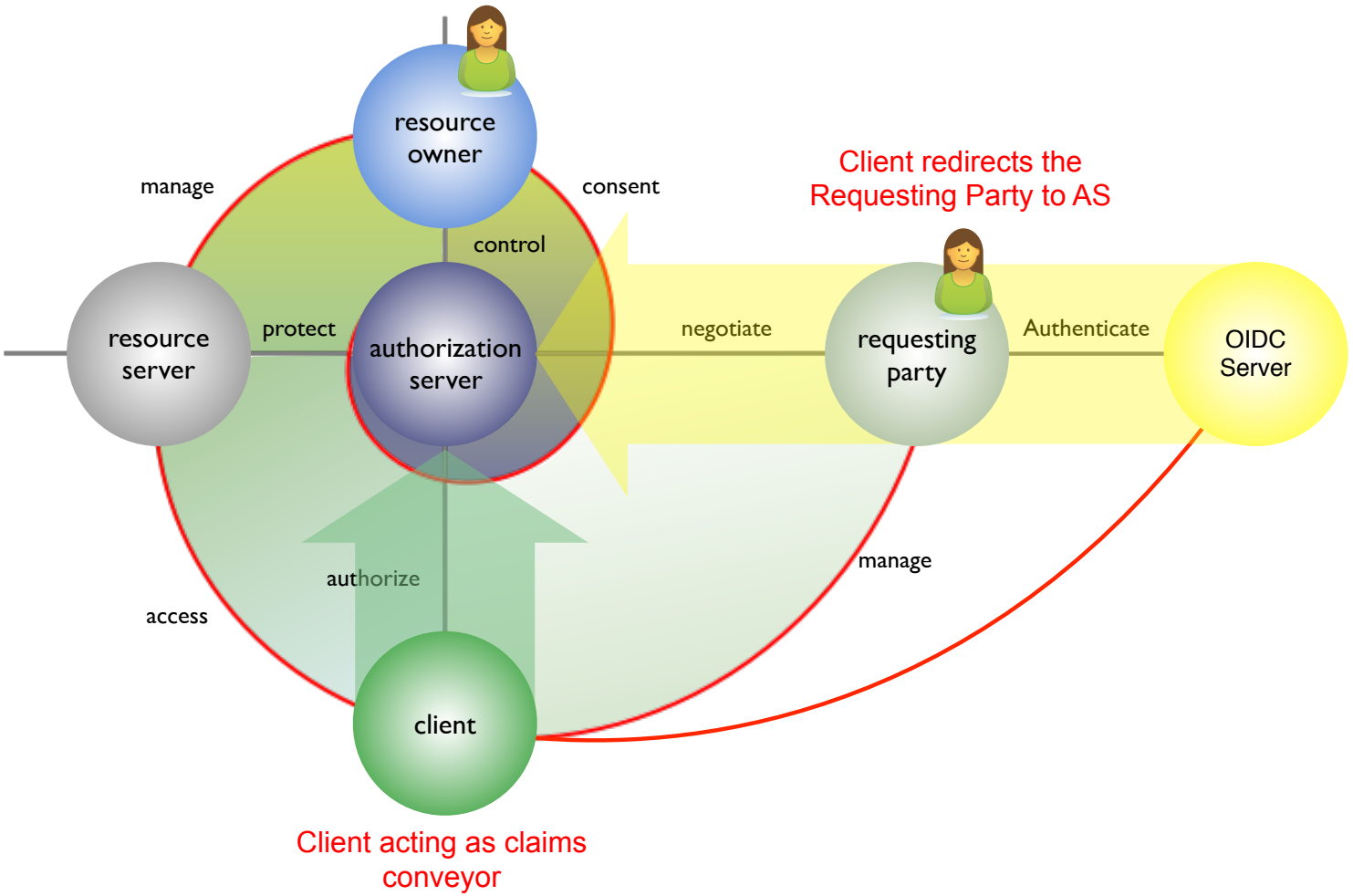
UMA claims-based authorisation

- UMA allows for the use of claims to support Claim-Based Access Control (CBAC):
  - Trusted claims from Trusted Third Parties
  - Self-asserted claims
- In CBAC, the decision to grant access to a protected resource is made based on Subject's information/ attributes, such as name, age, email address, role, location, credit score, etc.
- …or a Subject's statement (e.g. promise to adhere to licensing terms)

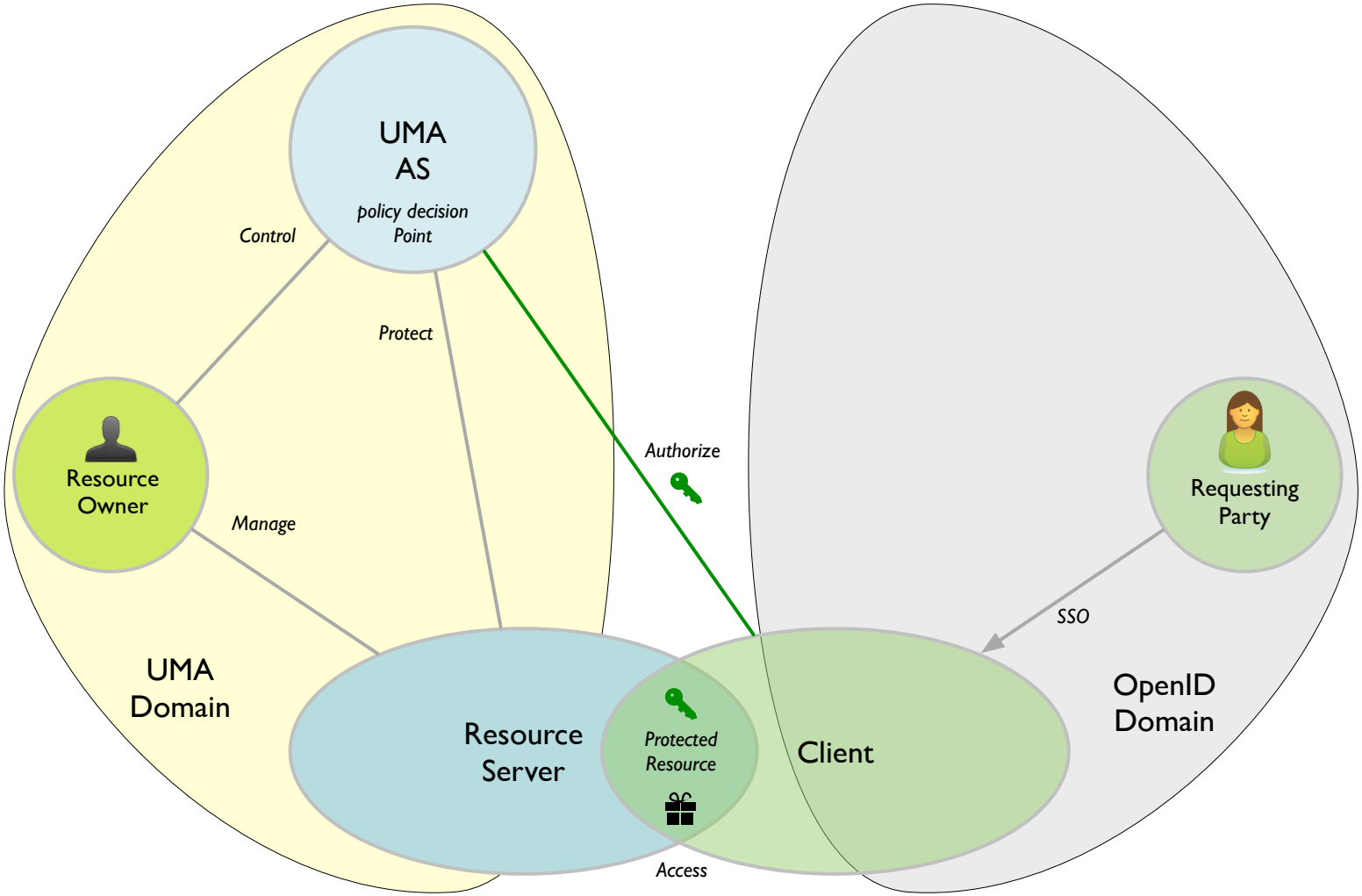
OpenID Connect role in UMA

- OpenID Connect (OIDC) provides authentication, consented attribute sharing, and attribute transmission capability
- OIDC allows third-party asserted claims from distributed sources to be collected
- UMA leverages OIDC in claims-gathering flow in one of two ways:
  - AS interacts directly with requesting parties, or
  - indirectly via clients

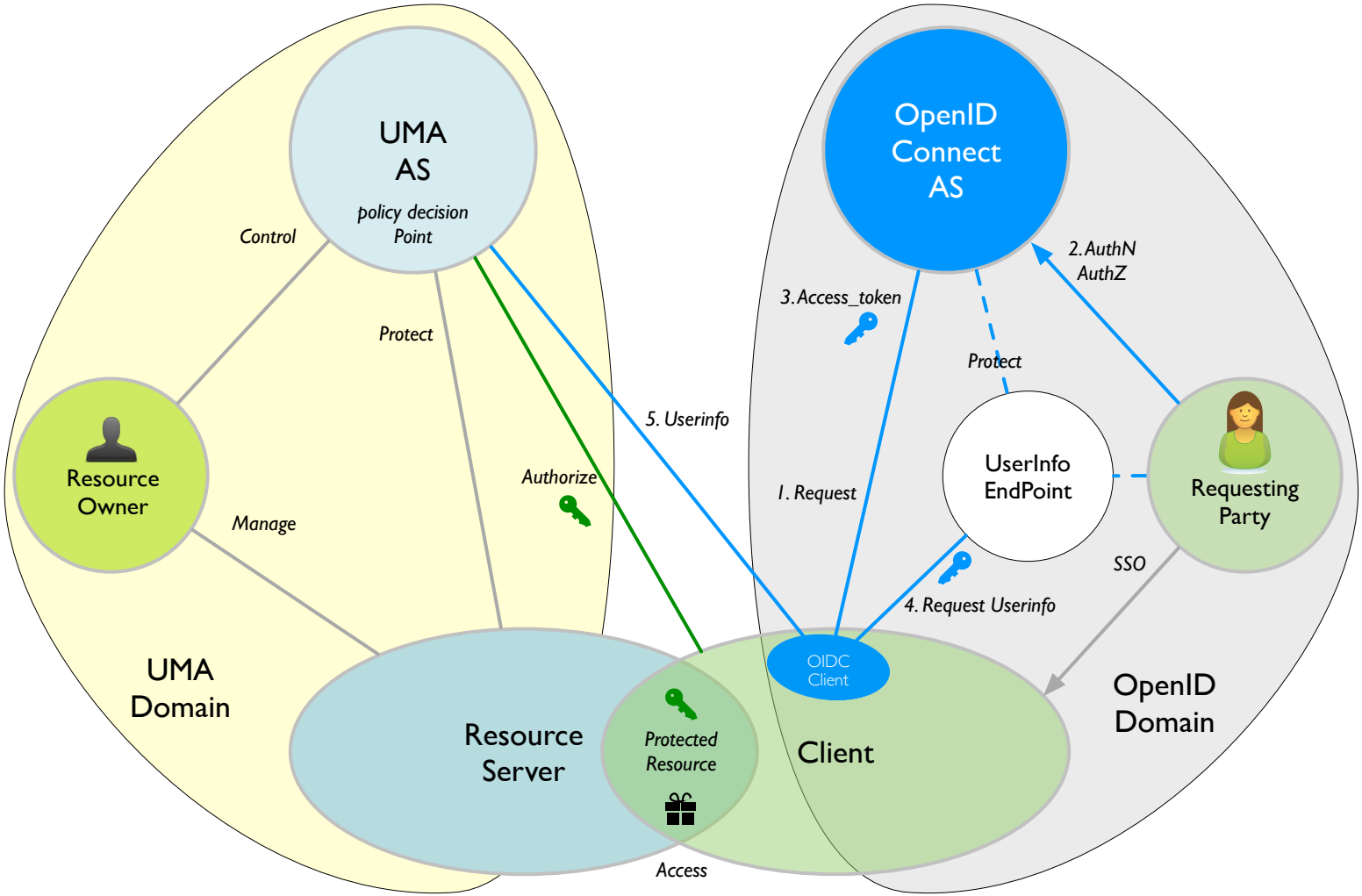
UMA AS Collecting Claims from Requesting Party



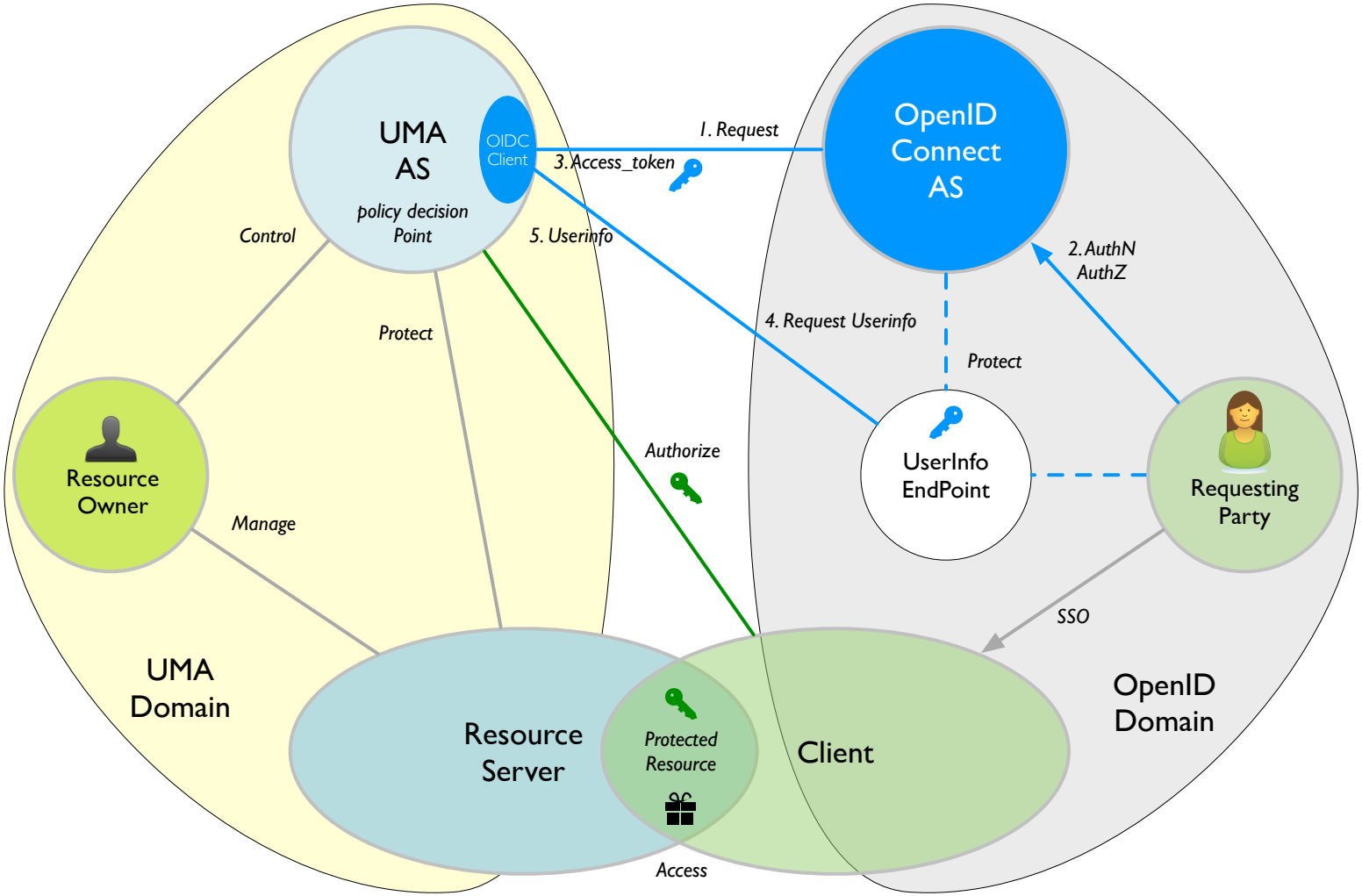
Generic UMA Model



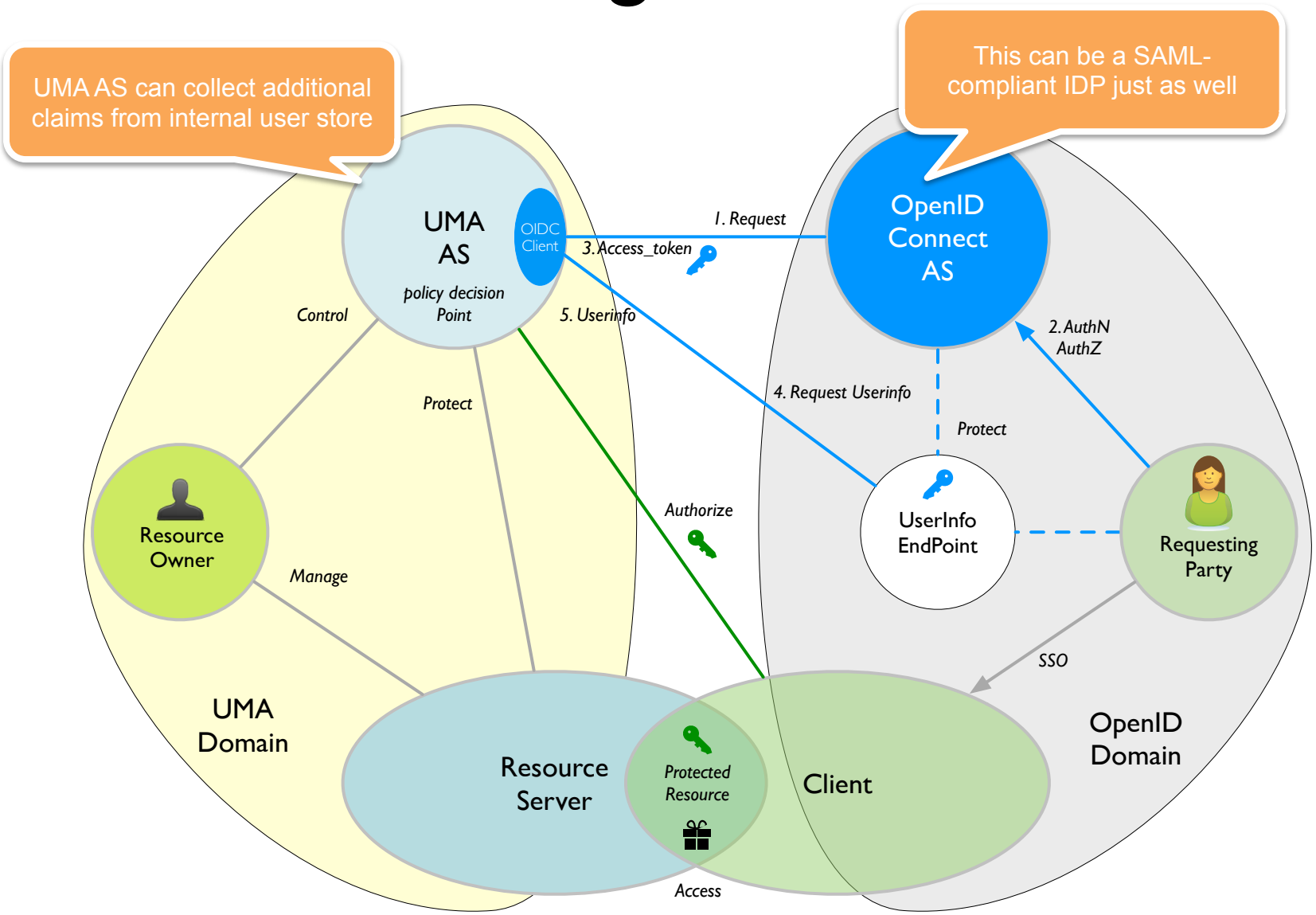
Client application conveying claims to UMA AS



UMA AS acting as Claims Client



UMA AS acting as Claims Client



Next steps

Next steps for the WG…and you

- Get involved!
  - Become an “UMAnitarian” (it’s free)
  - Participate in the interop and our implementation discussions
  - Follow and engage with @UMAWG on Twitter
- Current work:
  - Technical: claim profiling and core spec variations
  - Business: access federation trust frameworks
- Stay tuned for a webinar on UMA and Healthcare in Q3

Join at:
tinyurl.com/umawg

Questions? Thank you!

@UMAWG
#UMApcloud *for questions*
19 June 2014
tinyurl.com/umawg *for slides, recording, and more*