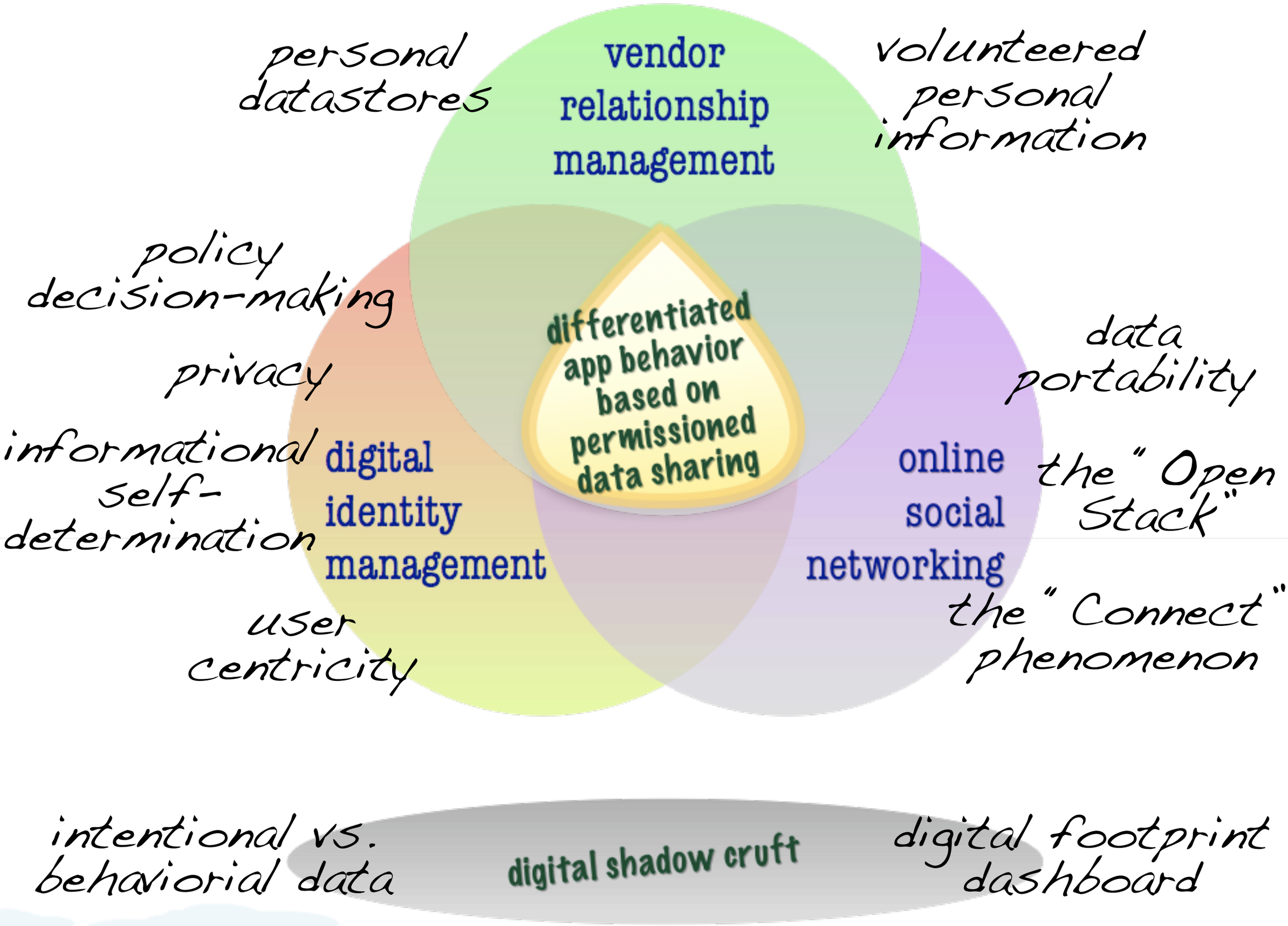
Making the World Safe for User-Managed Access

Eve Maler
PayPal Identity Services
Cloud Identity Summit 21 July 2010

Privacy is not about secrecy

> The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be”
>
> – Ann Cavoukian, Information and Privacy Commissioner of Ontario, **Privacy in the Clouds** paper

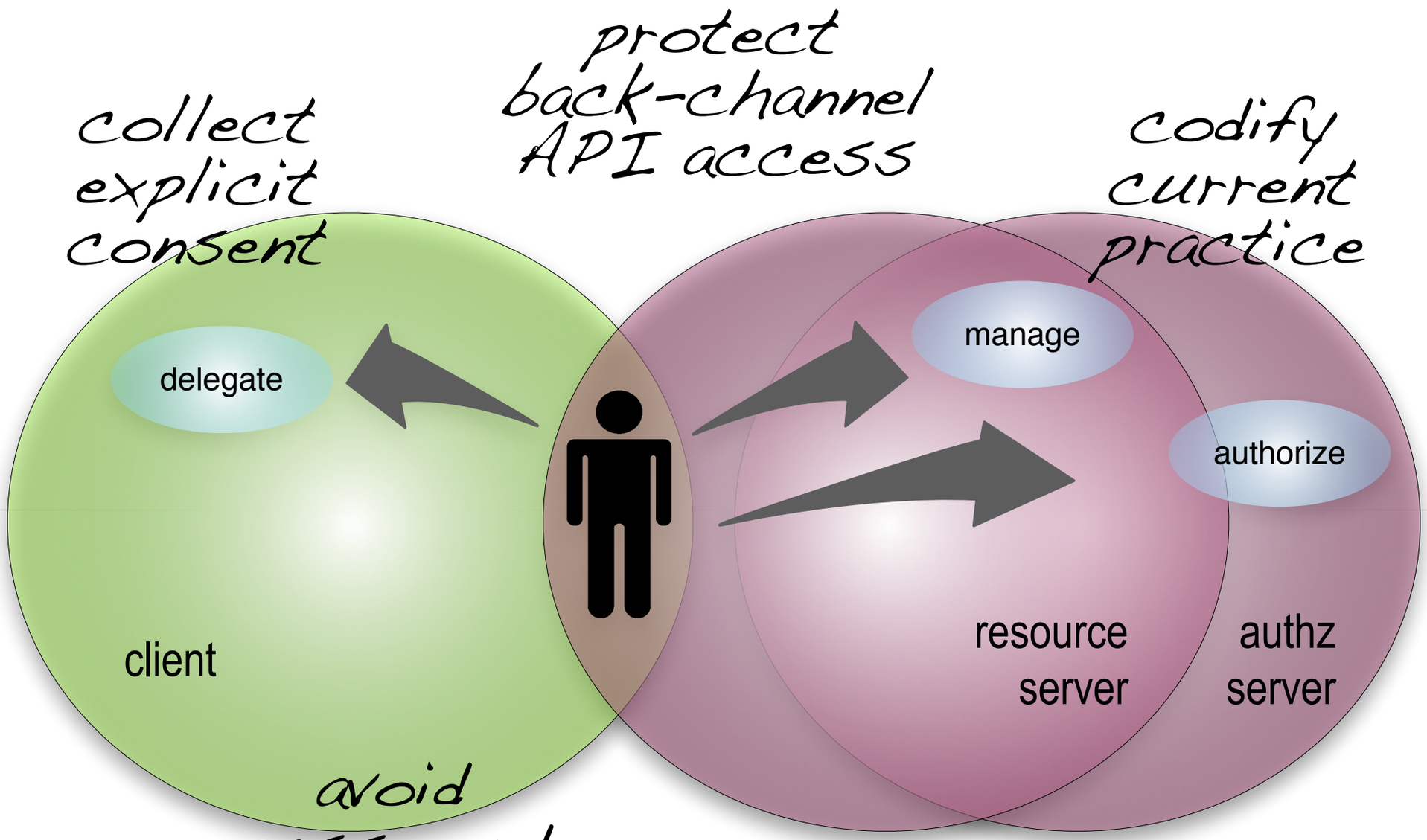
It’s about context, control, choice, and respect


personal datastores
vendor relationship management
volunteered personal information
policy decision-making
privacy
informational self-determination
digital identity management
differentiated app behavior based on permissioned data sharing
data portability
the "Open Stack"
online social networking
the "Connect" phenomenon
user centricity
intentional vs. behavioral data
digital shadow cruft
digital footprint dashboard

UMA is...

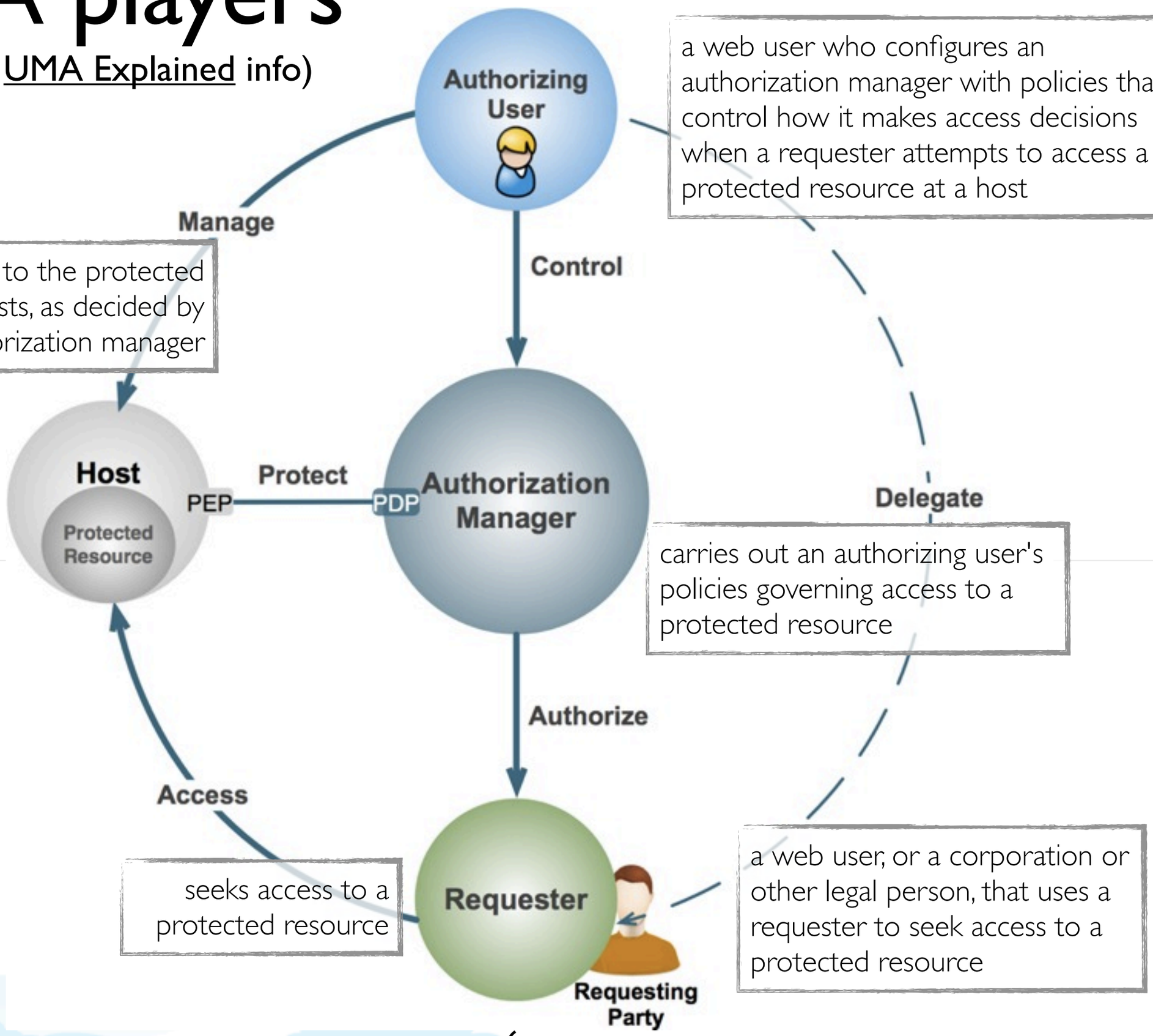
- A web protocol that lets you control authorization of data sharing and service access made on your behalf
- A Work Group of the Kantara Initiative that is free for anyone to **join** and contribute to
- A set of draft specifications that is free for anyone to implement
- Undergoing multiple implementation efforts
- Slated to be contributed to the IETF
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly

OAuth themes



UMA players

(see also UMA Explained info)



a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host

enforces access to the protected resources it hosts, as decided by an authorization manager

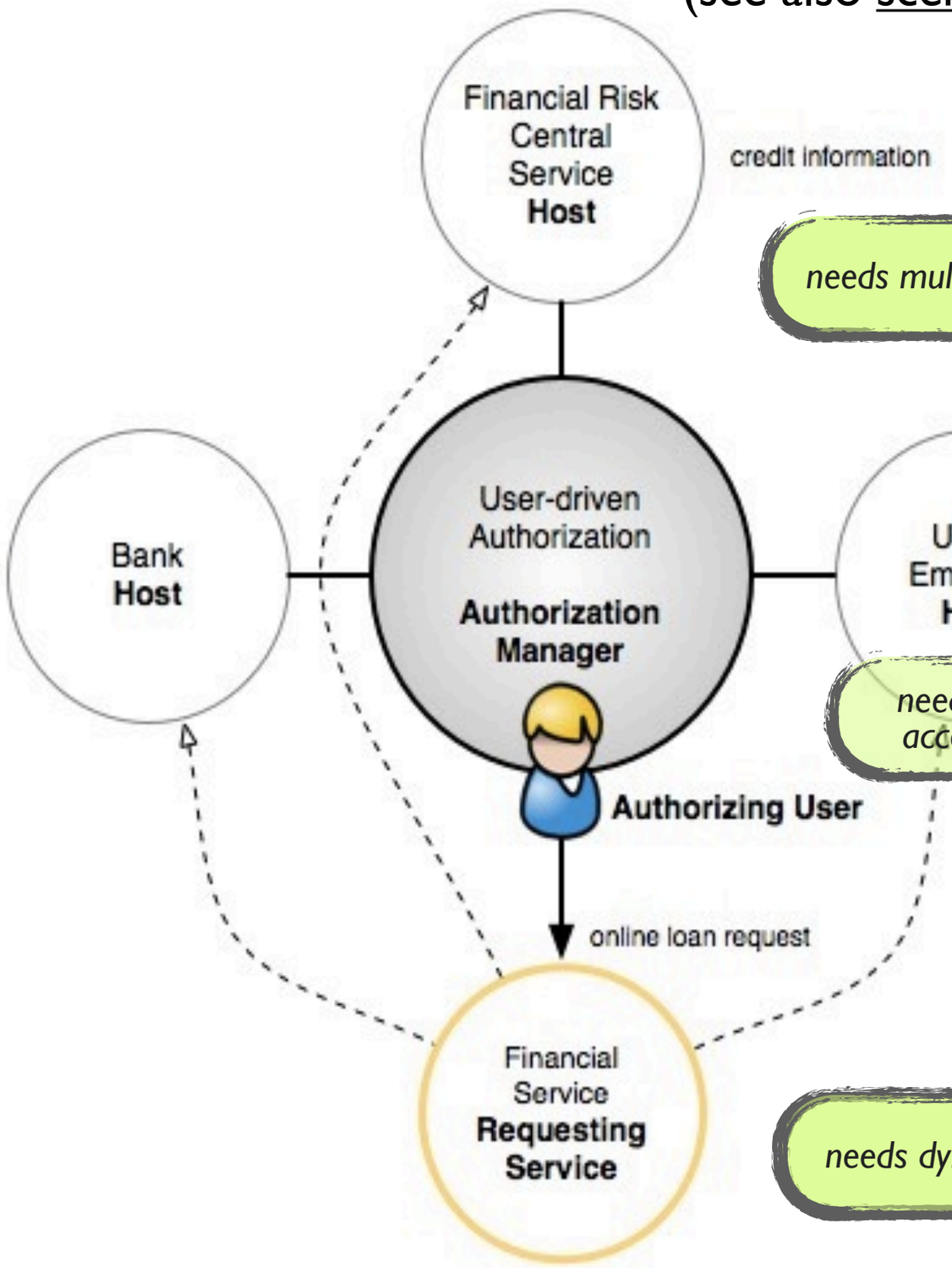
carries out an authorizing user's policies governing access to a protected resource

seeks access to a protected resource

a web user, or a corporation or other legal person, that uses a requester to seek access to a protected resource

Sample scenarios

(see also scenarios and use cases doc)



- Sharing a calendar with both vendors and friends
- Packaging resources for e-commerce vendors
- **Online personal loan request**
- Distributed social graphs
- Offering photos if recipient agrees to licensing
- CV sharing with future Employers
- Controlling access to health data

person to service

needs multi-sourced data

person to person

third-party authoritative

needs dynamic access criteria

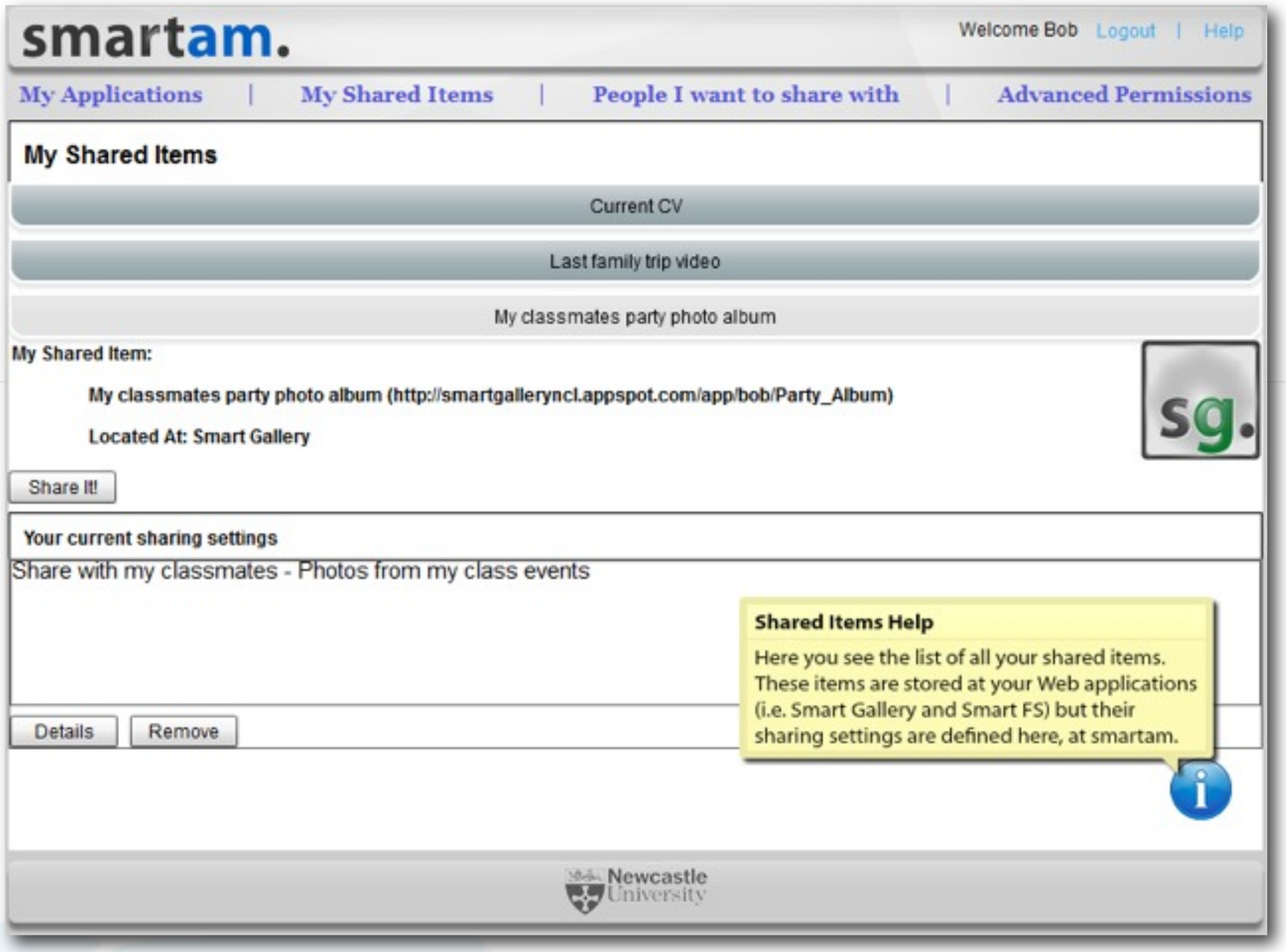
social

needs dynamic discovery

sensitive and regulated

Data-sharing relationship management is bigger than protocols

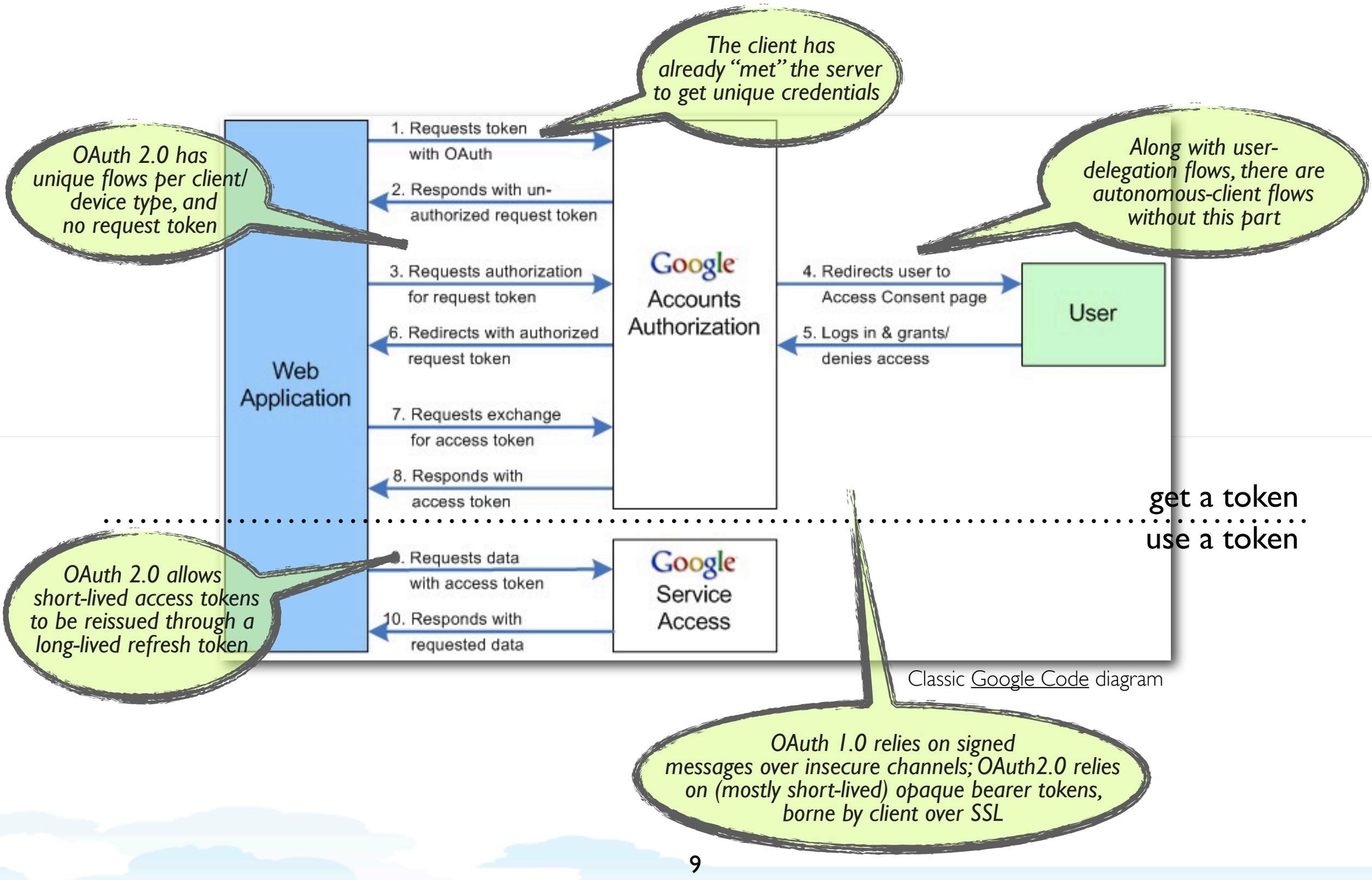
(see also UX and implementation pages)



Newcastle University

Student-Managed Access to Online Resources (SMART)

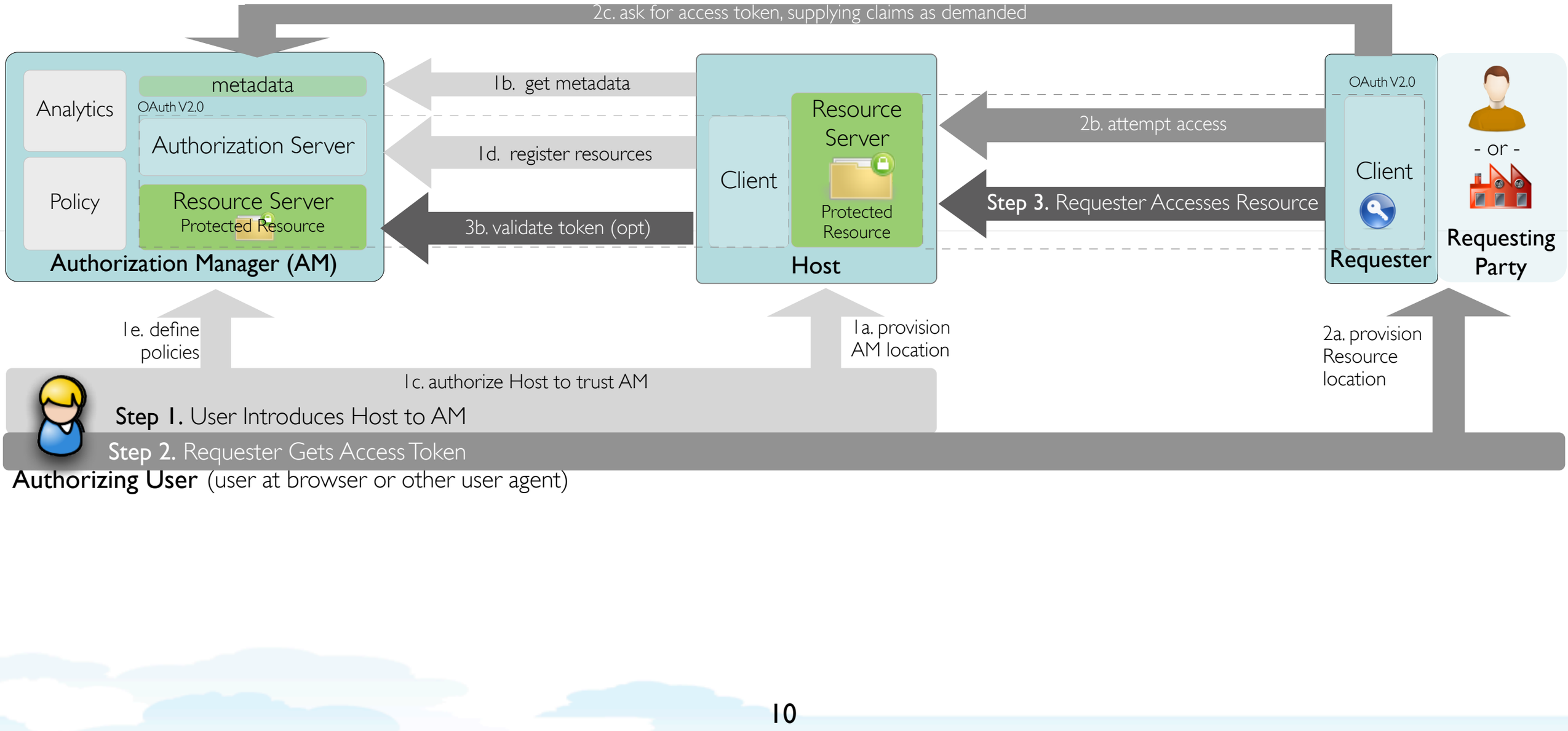
OAuth works roughly like this



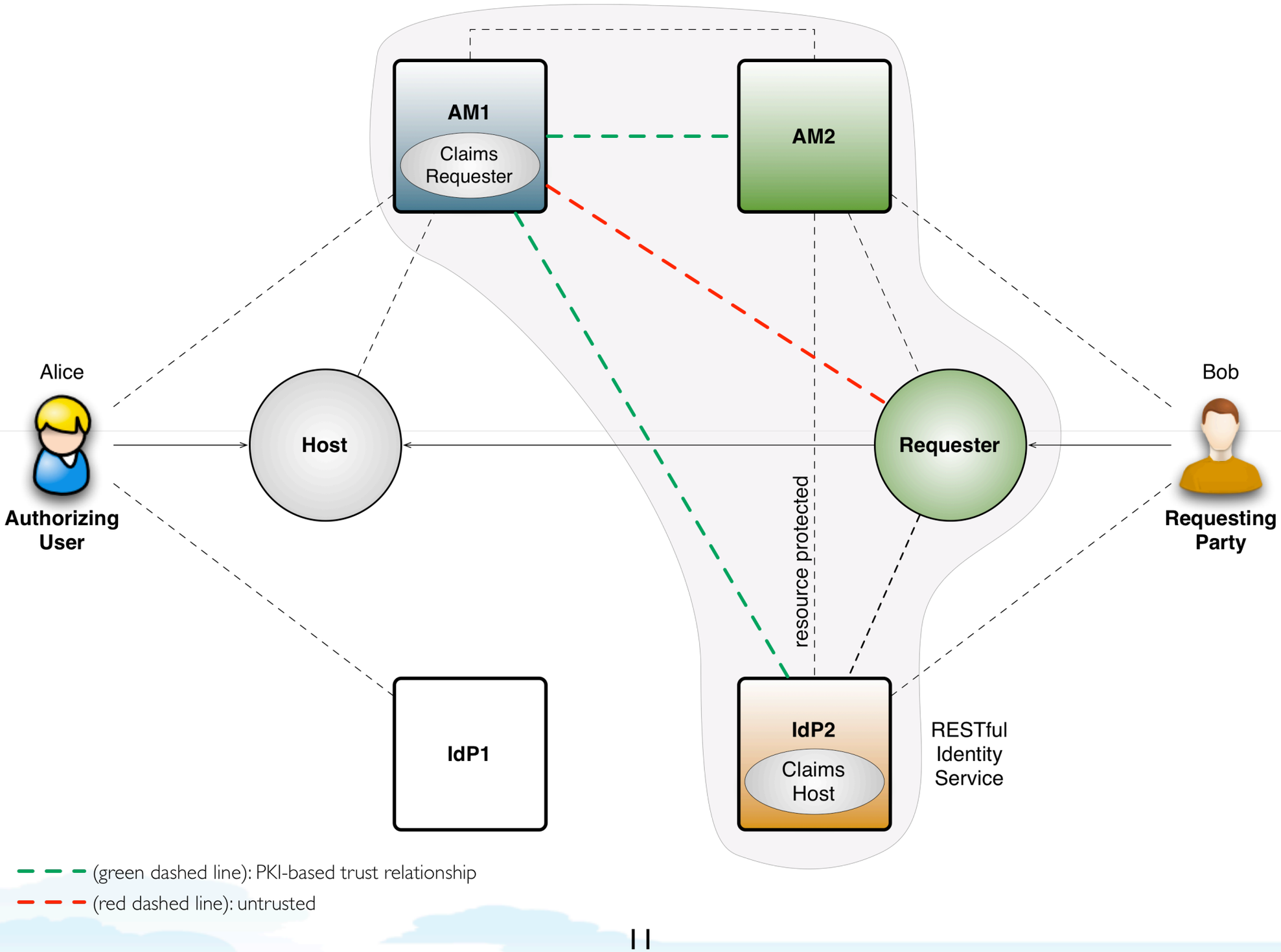
Classic Google Code diagram

The UMA protocol in a nutshell: trust a token, get a token, use a token

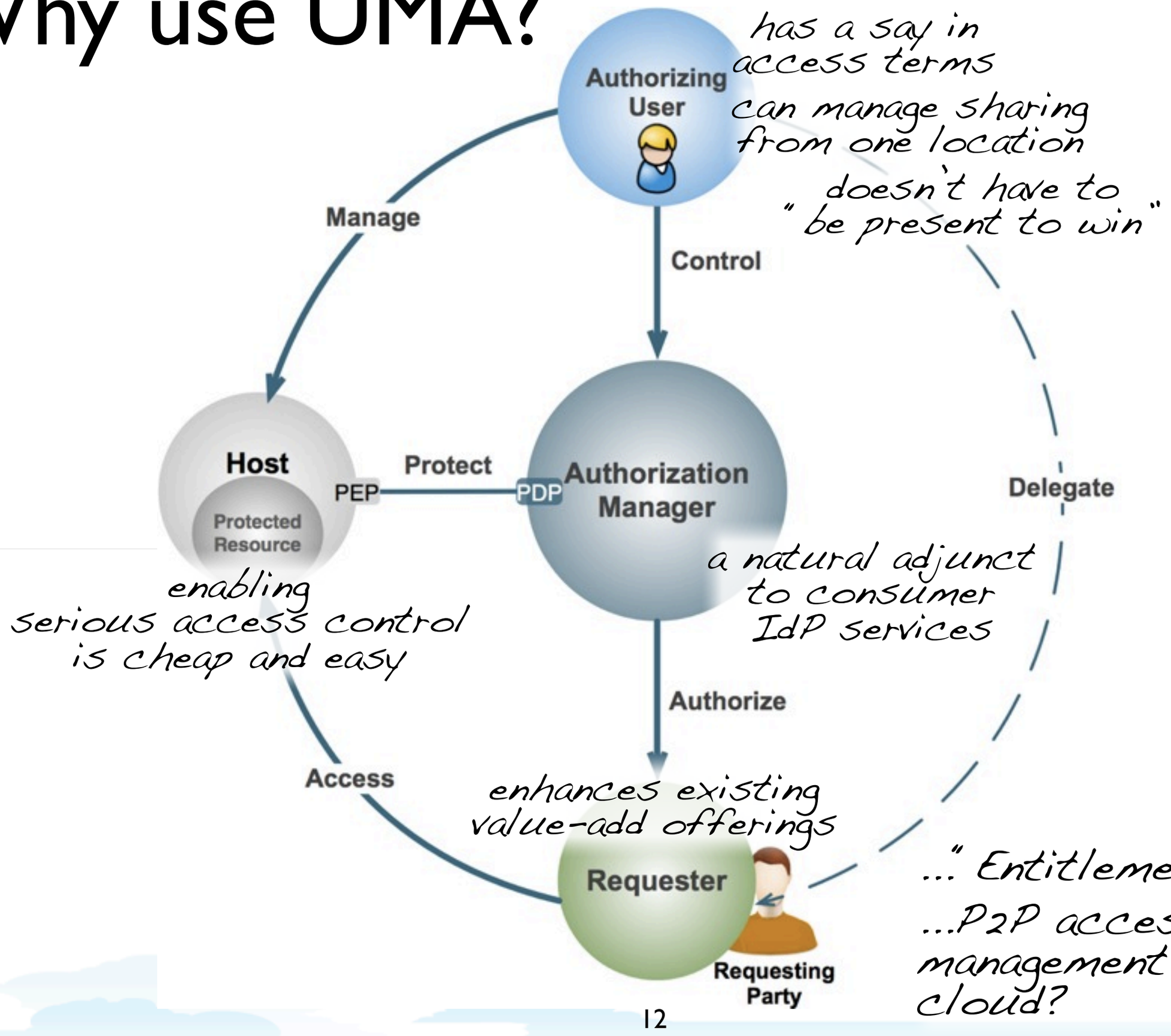
(see also spec working drafts)

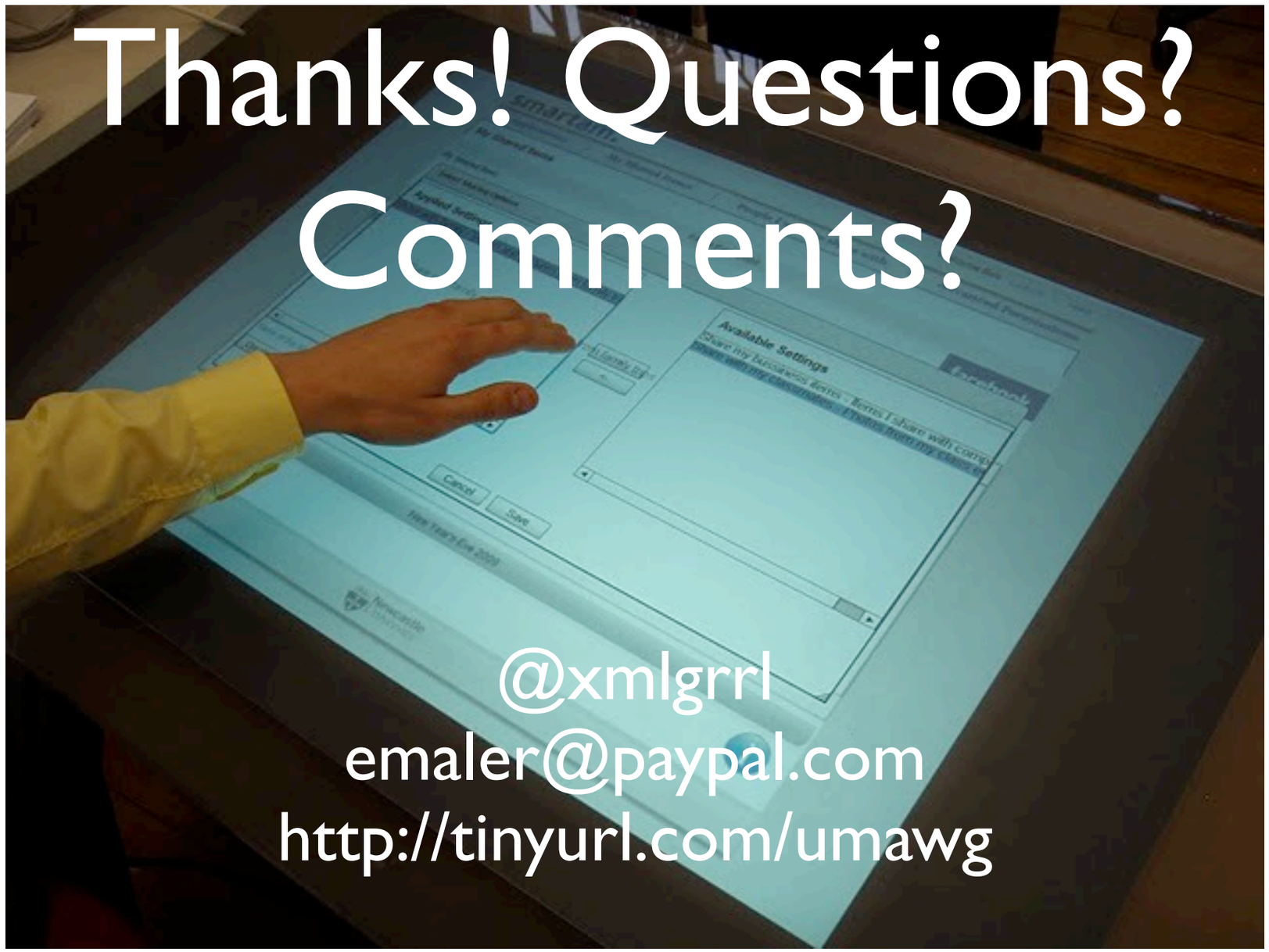


A potential claims trust model: make them UMA-protected resources



Why use UMA?


Authorizing User
has a say in access terms
can manage sharing from one location
doesn't have to "be present to win"
Manage
Control
Delegate
Host
Protected Resource
PEP
Protect
PDP
Authorization Manager
enabling serious access control is cheap and easy
a natural adjunct to consumer IdP services
Authorize
Access
enhances existing value-add offerings
Requester
Requesting Party
..."Entitlements 2.0"?
...P2P access management in the cloud?


Thanks! Questions?
Comments?
@xmlgrrl
emaler@paypal.com
http://tinyurl.com/umawg

PayPal™