Thanks to our webinar sponsors!

What Is User-Managed Access And Why Do We Need It?

Presented by several UMAnitarians
(participants in the Kantara UMA Work Group)
with WG chair Eve Maler as your emcee

(Questions? Contact eve@xmlgrrl.com / @xmlgrrl or maciej.machulak@cloudidentity.co.uk / @mmachulak anytime)

Introduce additional speakers: Maciej, Lukasz, Frank, Paul, Mario, Sampo, Domenico

Slides are up on the UMA wiki! And a recording of this webinar will be up within a few days.

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

Why would an organization want to UMA-enable its apps?

Existing UMA implementations

How UMA works to build technical and business trust

Q&A

Privacy is not about secrecy

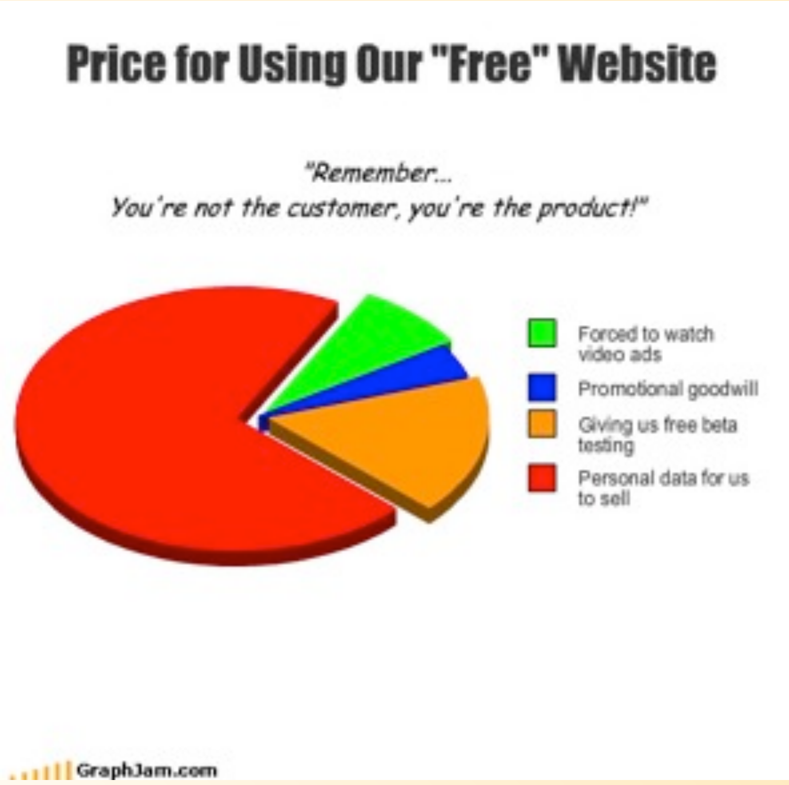
> "The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of 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

This quote from Ann Cavoukian perfectly captures the aspirations of many of us who have been working at the nexus of self-determination, identity, privacy, online data-sharing, and trust. What many people mean when they say "quickly determine" is to "quickly find out" – to "be disclosed to". With our work on User-Managed Access, we're trying to expand it to mean to "quickly control" – to "have an effect on". This is a big leap. It's not easy, but we've made a lot of progress.

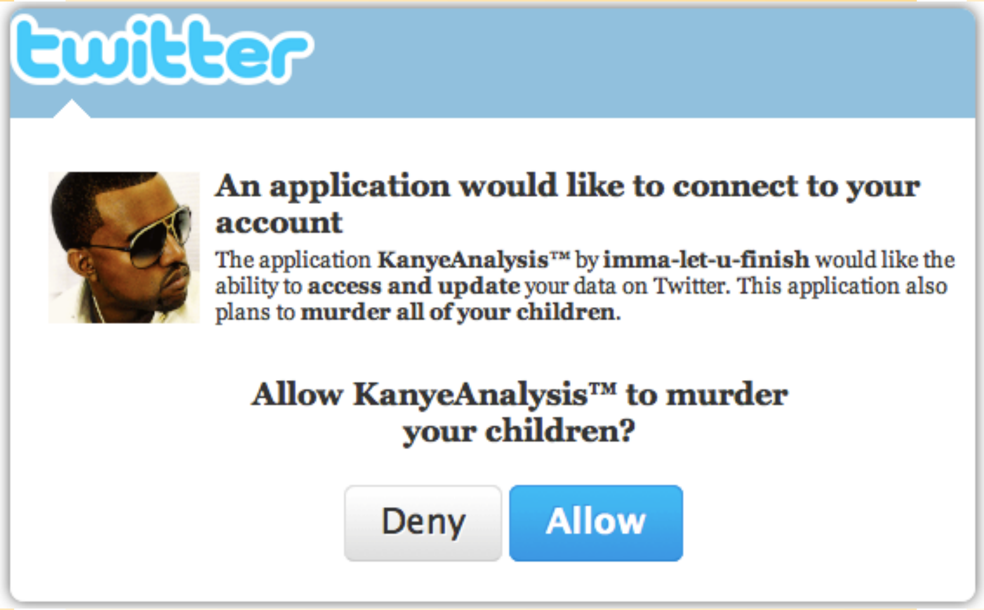
The price for sharing access to our data is too high

Either we have to do all the work ourselves



...often in the role of the "product," not the "customer"

Or we have to agree to install large data pipelines



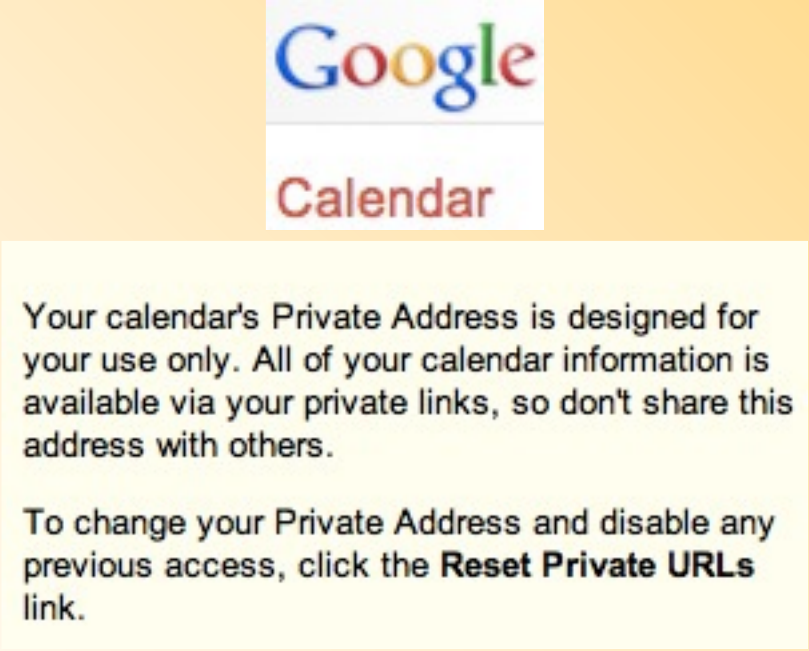
An application would like to connect to your account

The application **KanyeAnalysis™** by **imma-let-u-finish** would like the ability to **access and update** your data on Twitter. This application also plans to **murder all of your children.**

Allow KanyeAnalysis™ to murder your children?

...resulting in oversharing of high-quality data and a "too many subscriptions" problem

Or we share with friends through "secret links"



Your calendar's Private Address is designed for your use only. All of your calendar information is available via your private links, so don't share this address with others.

To change your Private Address and disable any previous access, click the **Reset Private URLs** link.

...rebuilding friend lists over and over – and hoping they won't give away the store

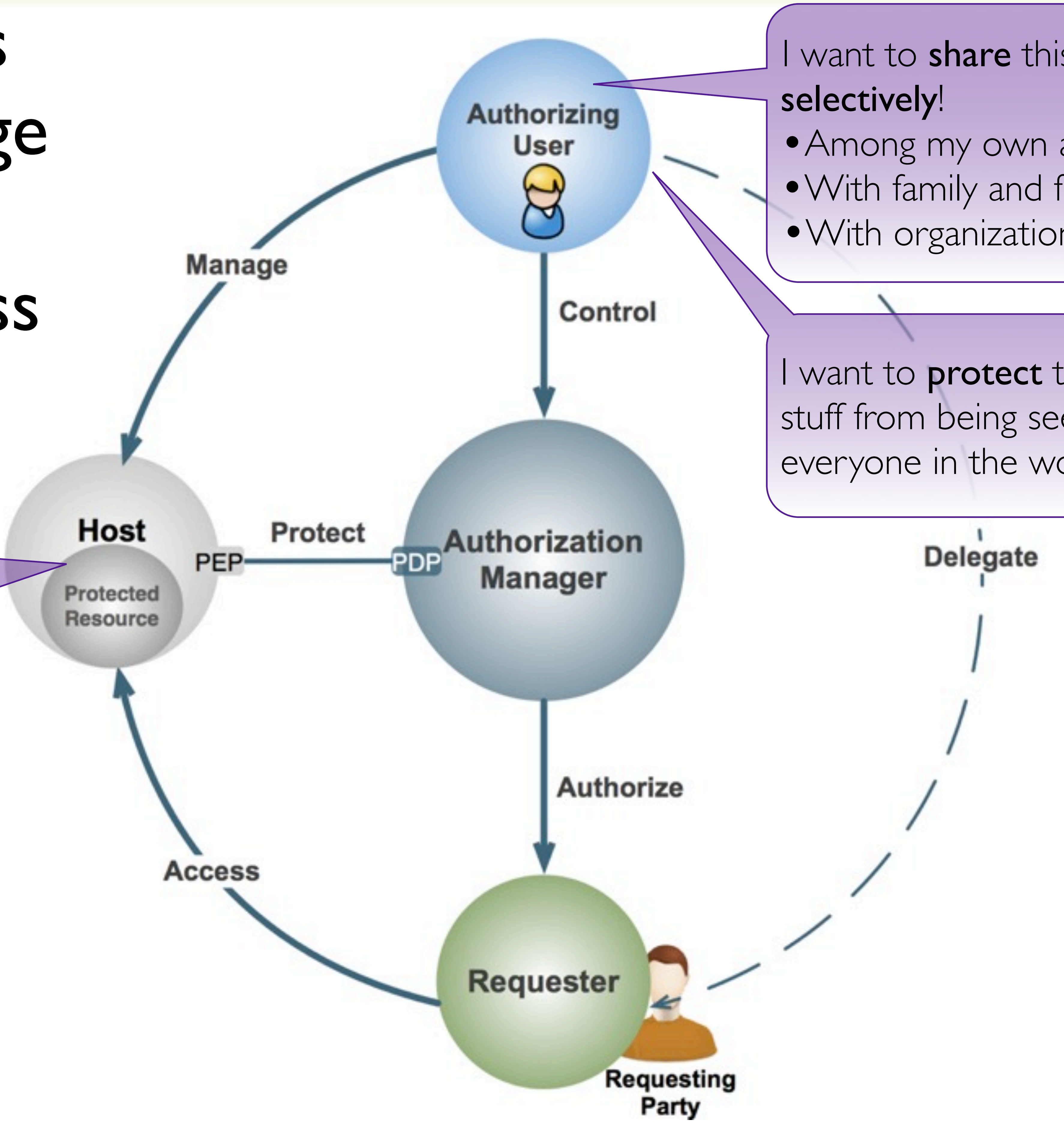
Most websites:
Provisioning by hand (annoying) of data by value (goes stale)
Oversharing (thus, lying): the pushmi-pullyu problem of assurance: RPs want lots of good data; users want reasonable privacy/protection
77% of domain registrations filled with rubbish; 2/3 of cases seem to be people "unaware or unwilling to hand over their identifying details" (The Reg, 17 Feb 2010)

UMA is...

(see also the FAQ)

- A web protocol that lets you control access to all your online stuff from one place
- A set of draft specifications, free for anyone to implement
- Undergoing multiple implementation efforts
- A Work Group of the Kantara Initiative, free for anyone to **join** and contribute to
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly
- Contributed to the IETF for consideration: draft-hardjono-oauth-umacore-02
- Heading towards interoperability testing and increased OpenID Connect integration in early 2012

UMA enables you to manage sharing and protect access from a single hub



I want to **share** this stuff **selectively**!

- Among my own apps
- With family and friends
- With organizations

I want to **protect** this stuff from being seen by everyone in the world!

Historical
Biographical
Reputation
Vocational
Artistic/user-generated
Social
Location/geolocation
Computational
Genealogical
Biological/medical
Legal
...

Today we see individuals sharing data with themselves, so to speak, by connecting two applications that operate on the same person's behalf. For example, Twitter enables this when you allow third-party applications like Backupify or Tweetizen to do things with your Twitter stream. It uses OAuth to accomplish this between application pairs.

We also see people sharing things like calendars and photo albums selectively with friends by having the web app email so-called private URLs to these people. This is effective as far as it goes, but not very secure.

We need a unified way to **securely and meaningfully control,** and get a **global view** on, sharing in all these cases – and more, including sharing with organizations such as health care providers, family members, and e-commerce companies. UMA does this by building on top of the OAuth technology already in wide use.

UMA gives users a digital footprint dashboard

Web 2.0 access control today is inconsistent and unsophisticated

You have to name known people in order to share with others

You must be online in order to authorize access

You can't "advertise" your content without giving it away

You can't get a global view of all your sharing relationships

Source: http://www.flickr.com/photos/paraflyer/2749336420/

You can unify access control under one AM

Your AM can test for claims like "over 18"

You can set up policies that work while you're away

You can control access to stuff with public URLS

You can manage and revoke access from one place

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

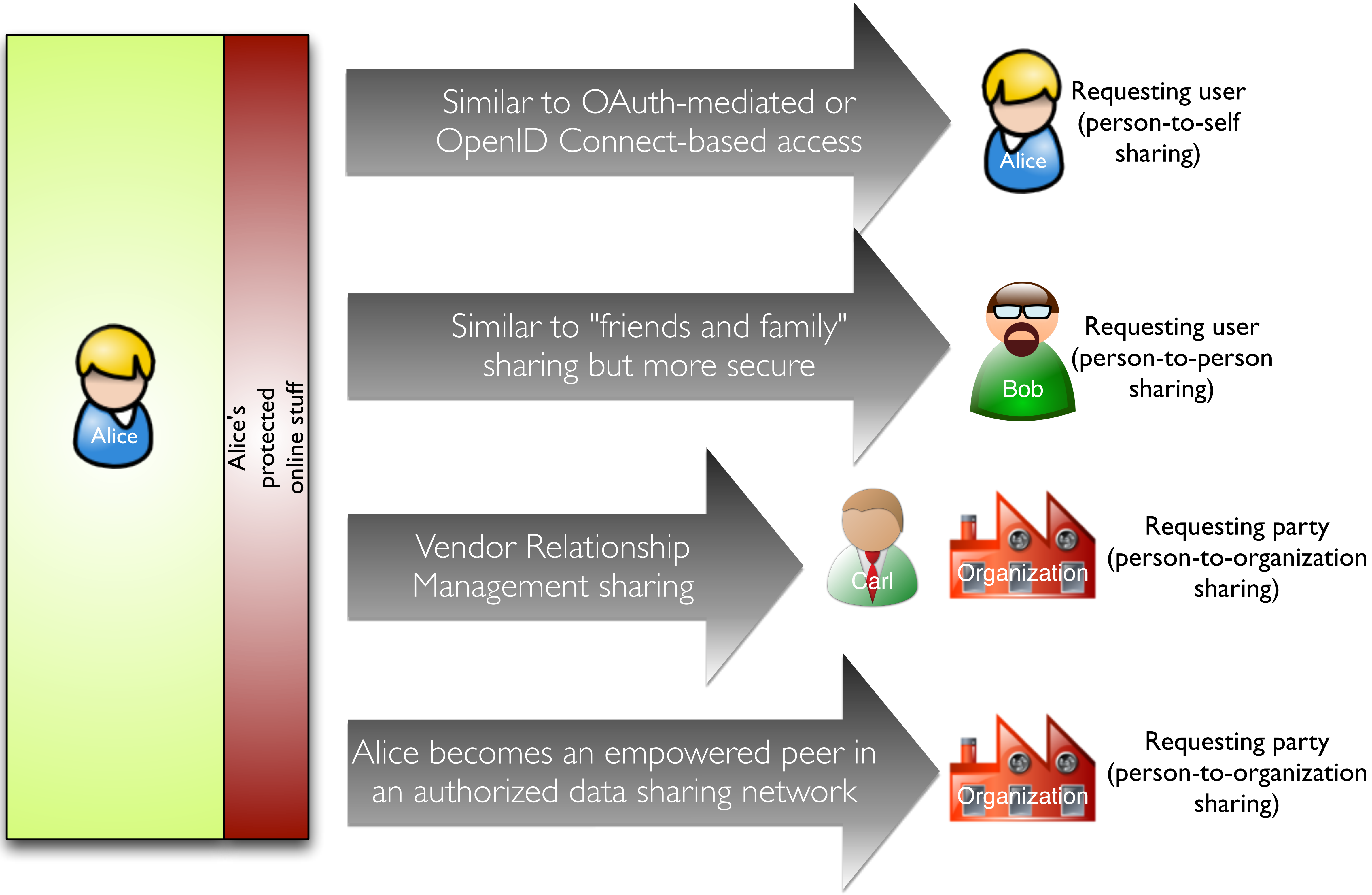
Why would an organization want to UMA-enable its apps?

Existing UMA implementations

How UMA works to build technical and business trust

Q&A

UMA data sharing constellations



Similar to OAuth-mediated or OpenID Connect-based access

Requesting user (person-to-self sharing)

Similar to "friends and family" sharing but more secure

Requesting user (person-to-person sharing)

Vendor Relationship Management sharing

Requesting party (person-to-organization sharing)

Alice becomes an empowered peer in an authorized data sharing network

Requesting party (person-to-organization sharing)

speaker: Eve

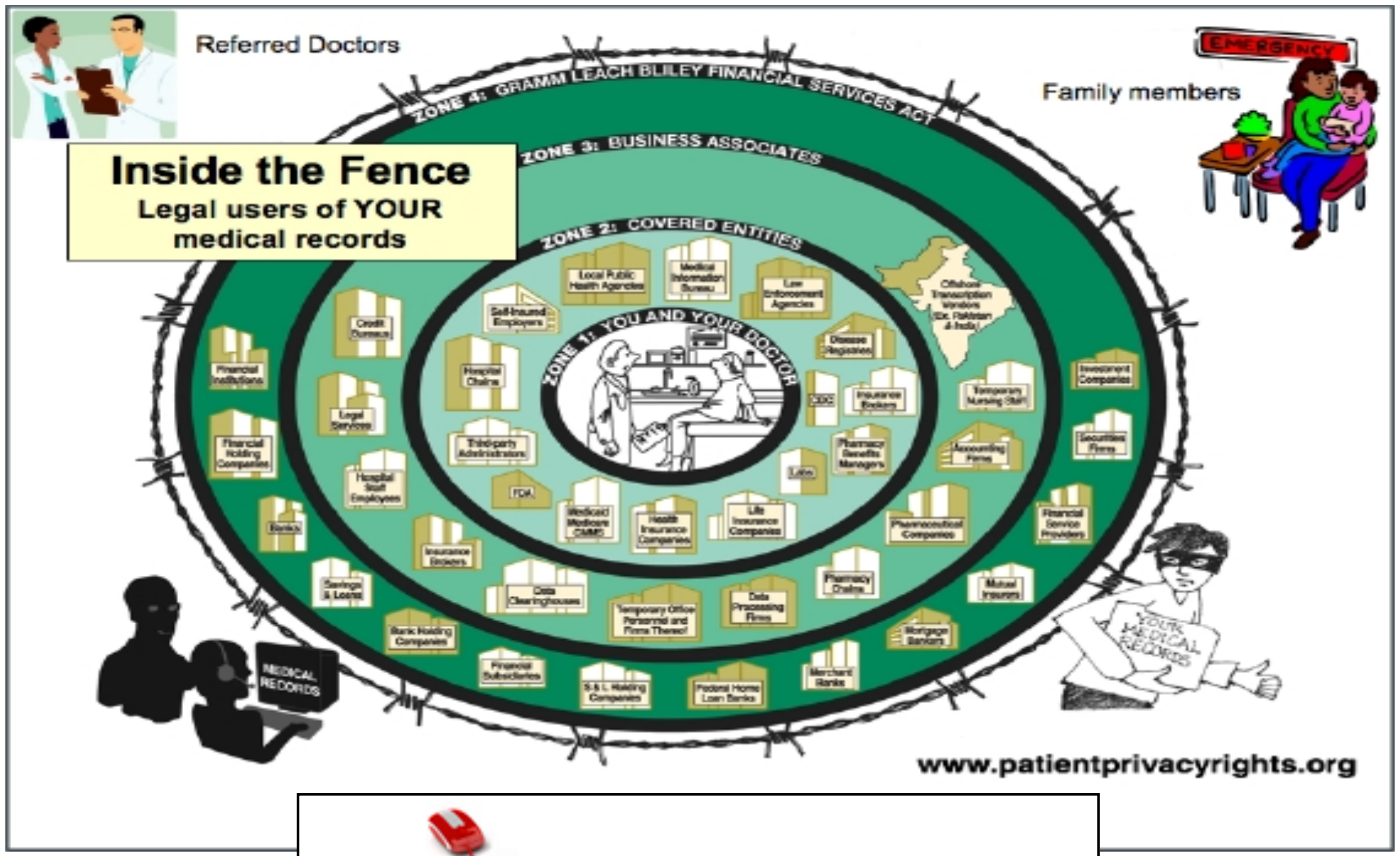
Use case: Sharing trusted identity attributes with anyone

- The NSTIC initiative is striving to "make online transactions safer, faster, and more private"
- The Street Identity/LMNOP project is experimenting with authorizing access to verified street addresses
- UMA helps you manage such access and share with others besides just "apps with you sitting behind them"
    - Possibly requiring the requesting party to promise to adhere to your contractual requirements: NDAs, embargoes, payment...
- For true online safety, contracts must be enforceable (see the UMA Trust Model – and stay tuned for more to come)

speaker: Eve, inviting Maciej to comment

Use case: Protecting hData electronic health records (EHRs)

- EHR technologies are at the heart of health care debates in many countries
- ProjecthData.org is a new approach in answer to these debates



speaker: Frank

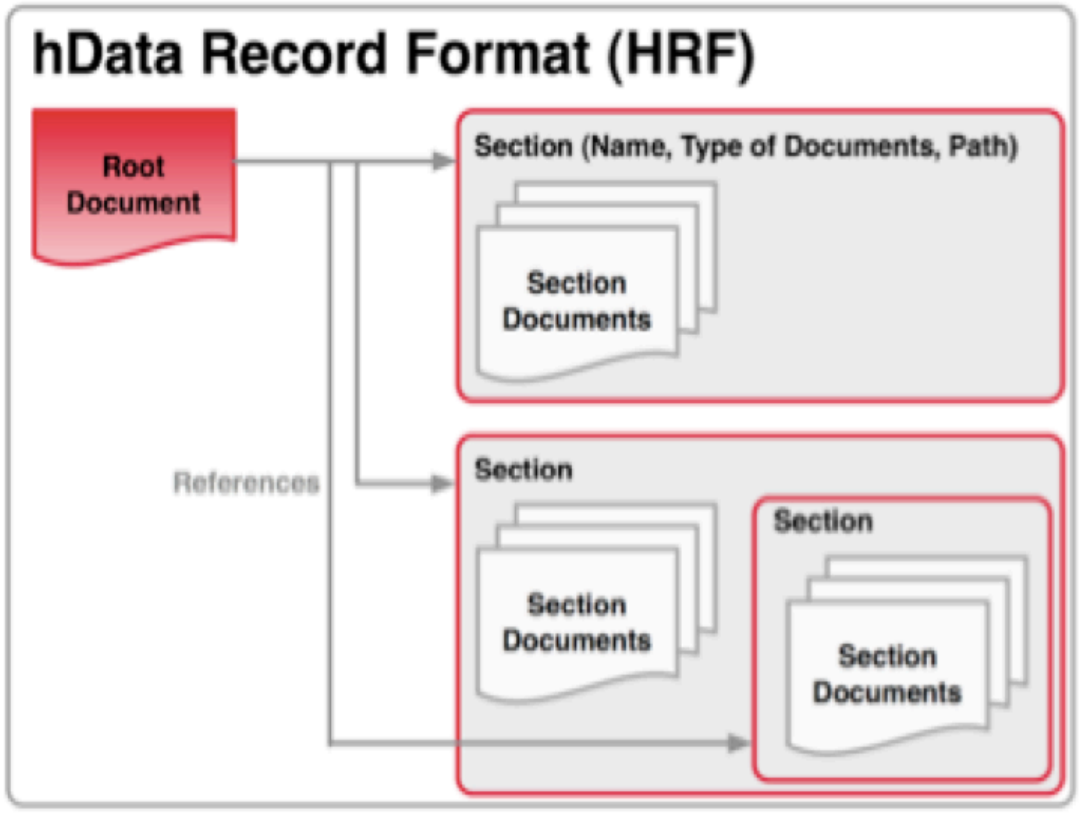
I became interested in UMA about a year ago because I found several use cases and opportunities in allowing users more control over their data.

While analyzing which use cases could have the most impact, I realized that Health Data, its misuse, and the costs for maintaining privacy requirements make this a perfect candidate.

Electronic Health Record technologies are at the heart of health care debates in many countries

Use case: Protecting hData electronic health records (EHRs)

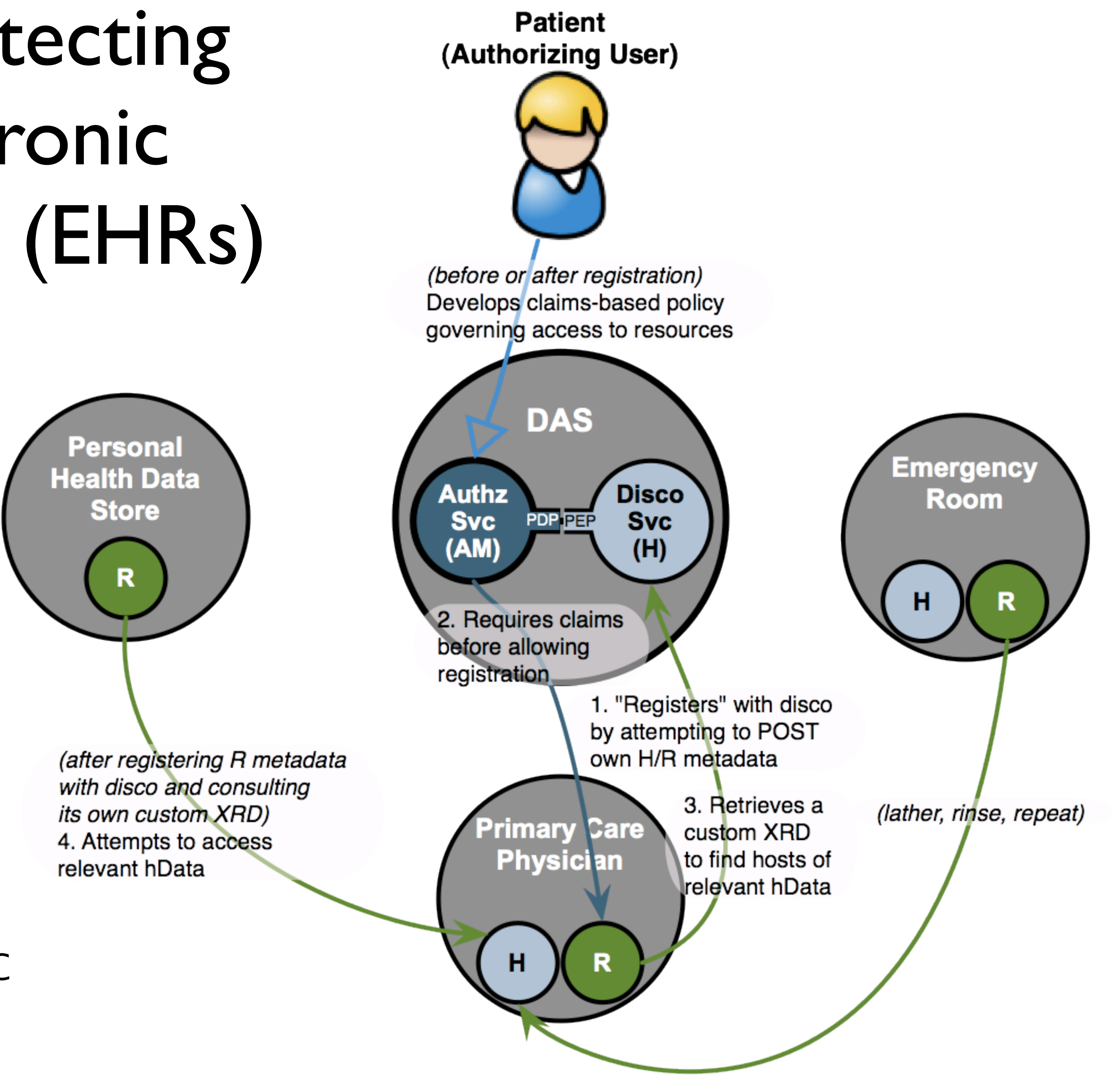
- The hData specification requires the ability for patients to protect their health records based on their authorization
- UMA allows patients to share their EHRs based on their authorization



hData allows a RESTful exchange of health records conforming to the hData specification. hData requires the ability for patients to protect their health records, as they are exchanged over public networks in a secure manner and based on the patients authorization.
Just as hData is the answer to Electronic Health Record Management, UMA is the answer to hData's need to allow a secure, patient authorized exchange of health records

Use case: Protecting hData electronic health records (EHRs)

- A dual challenge: high security plus dynamic introduction of parties
- This challenge can be solved with the help of OpenID Connect's Dynamic Discovery method


Patient
(Authorizing User)
(before or after registration)
Develops claims-based policy governing access to resources
DAS
Authz Svc (AM)
PDP
PEP
Disco Svc (H)
Personal Health Data Store
R
Emergency Room
H
R
2. Requires claims before allowing registration
1. "Registers" with disco by attempting to POST own H/R metadata
(after registering R metadata with disco and consulting its own custom XRD)
4. Attempts to access relevant hData
3. Retrieves a custom XRD to find hosts of relevant hData
(lather, rinse, repeat)
Primary Care Physician
H
R

A use case has been documented at the UMA Kantara site for more information.
Although UMA solves almost all of patient authorization cases found in hData, an area not covered by UMA natively, is the concept of dynamic introduction of parties.
As with other use cases, dynamic discovery of parties is important to the hData eco-system, so a need to solve for this became very important. Thankfully, the introduction of OpenID Connect's Dynamic Discovery specification can be leveraged in this respect

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

Why would an organization want to UMA-enable its apps?

Existing UMA implementations

How UMA works to build technical and business trust

Q&A

Web apps that become UMA hosts can easily offer "context, control, choice, and respect"

- You can provide sophisticated protection and sharing of any user content or data that isn't meant to be fully public
- You can outsource the entire job to third parties (AMs)
- You can ensure that the protection of sensitive resources is stronger than the "private URL trick"
- You can build trust more readily with users who are "privacy fundamentalists"
- You can integrate these features using lightweight OAuth, JSON, HTTP, and REST paradigms and a freely implementable protocol

speaker: Eve, inviting Paul

Identity providers that become UMA AMs can centrally coordinate sharing of anything to anyone

- The separation between IdPs and other attribute providers has long been acknowledged – you can never be the sole trusted source of all interesting user data
- OpenID Connect is solving how you as an IdP can act as a discovery hub for OAuth-mediated access to attributes
- UMA complements it by solving how you as an IdP can now act as an authorization hub for access by "others besides Alice" to:
  - Trusted attributes
  - User-generated content
  - APIs

speaker: Eve, inviting Maciej

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

Why would an organization want to UMA-enable its apps?

Existing UMA implementations

How UMA works to build technical and business trust

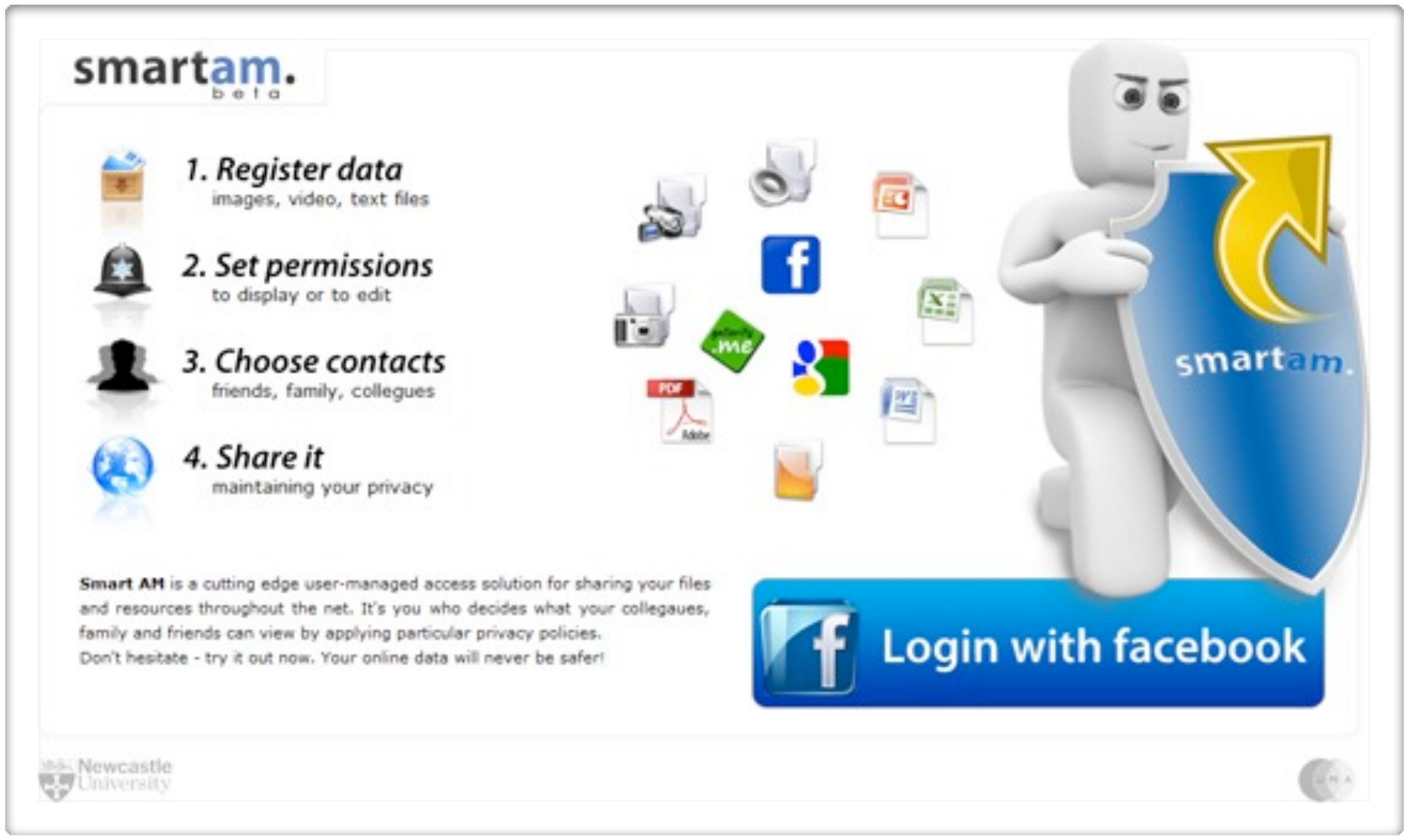
Q&A

Major implementation work to date

- The SMART project begun at Newcastle University
- Fraunhofer AISEC photo-sharing project
- Synergetics TAS^3/UMA integration

speaker: Eve

The SMARTAM.org project



1. *Register data*
images, video, text files

2. *Set permissions*
to display or to edit

3. *Choose contacts*
friends, family, collegues

4. *Share it*
maintaining your privacy

Smart AM is a cutting edge user-managed access solution for sharing your files and resources throughout the net. It's you who decides what your collegaues, family and friends can view by applying particular privacy policies.
Don't hesitate - try it out now. Your online data will never be safer!

See also the SMARTAM implementation FAQ

Hand the ball to speaker Maciej or Lukasz

UMA Reference Implementation

Use Case: Controlling Photo Sharing

Fraunhofer
AISEC

UMA Reference Implementation
Use Case: Controlling Photo Sharing

Contact: **Fraunhofer AISEC**
Mario Hoffmann
Parkring 4
85748 Garching (near Munich)
Germany

Mario.Hoffmann@aisec.fraunhofer.de,
Alam.Mohammad@aisec.fraunhofer.de

MOTIVATION

Protecting your Privacy

- **Empowering Users**
- **Controlling Web Resources**
- **Unifying Authorization**

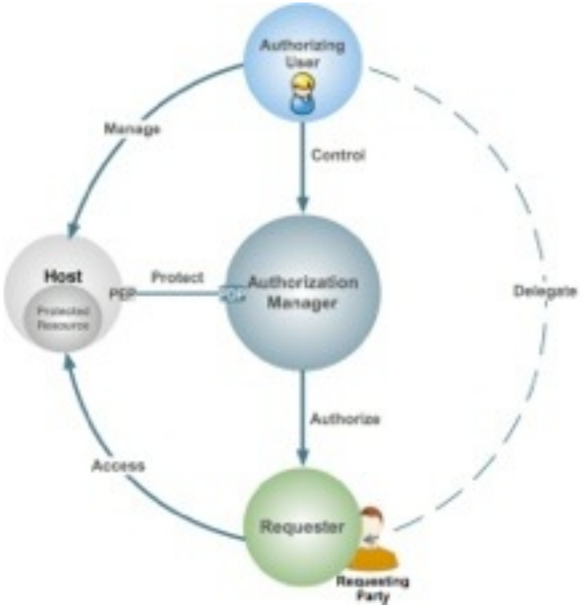
Use Case: Controlling Photo Sharing

- User can easily **share photos** from their mobile devices with family, friends, and world.
- Upload to **UMA-enabled** photo sharing services (e.g. Cloud services), also accessible from their mobile devices
- With simple **policies** whom to share (me, participants, and world)
- Requester should **authenticate** in order to access any photos
- **Showed** at Fraunhofer AISEC Opening Event (Sep 2011) and WWRF Conference, Düsseldorf (Oct 2011)

Hand the ball back to Eve
speaker: Mario

UMA Reference Implementation

Use Case: Controlling Photo Sharing



Contact:
Mario.Hoffmann@aisec.fraunhofer.de
Alam.Mohammad@aisec.fraunhofer.de

Mario

Host
Stores photos in gallery.

Eve

User
Controls access to her photo(s)

Mario's boss

Requester
Would like to gain access to photo(s)

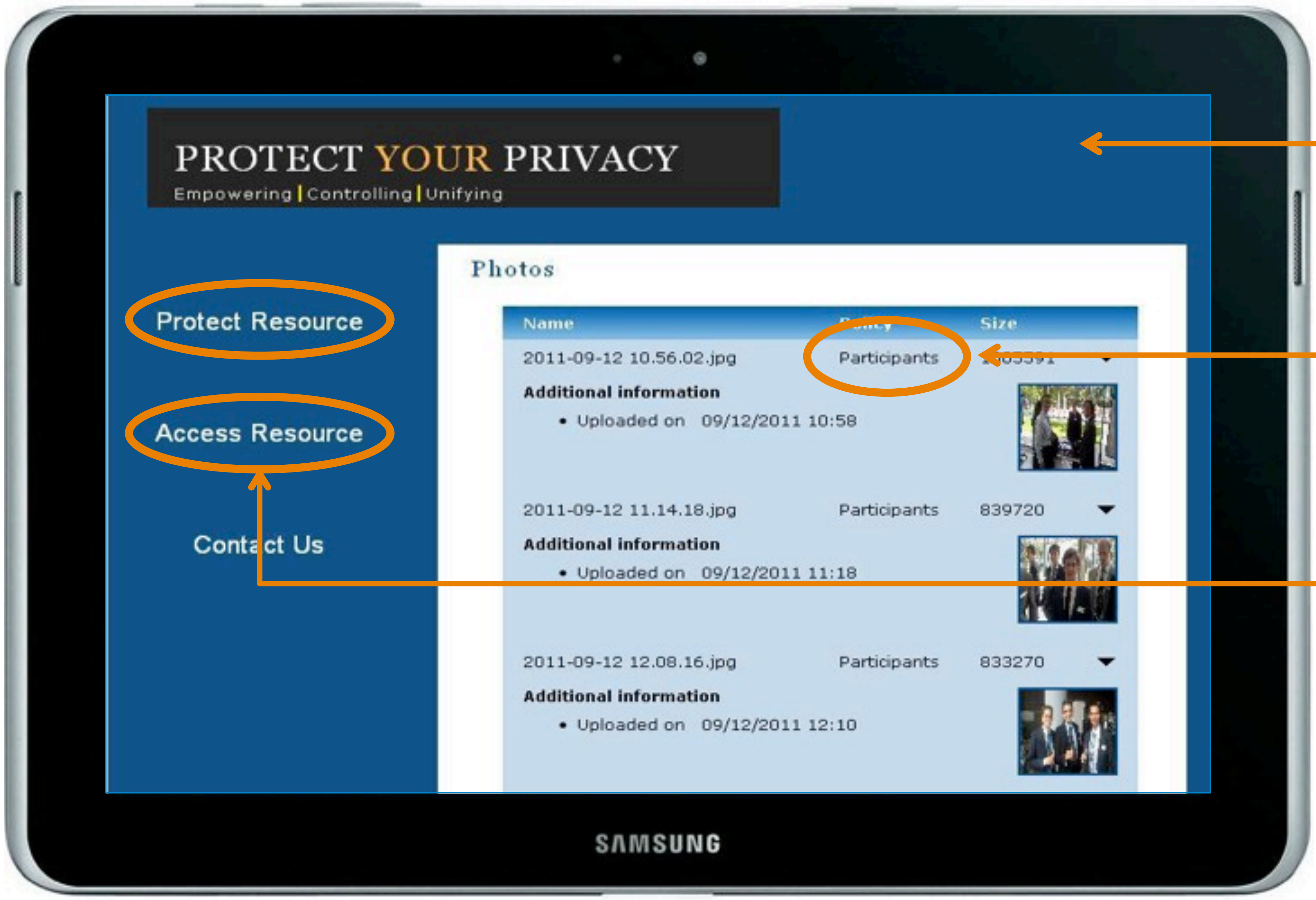
Setting the scene

1. Mario takes a photo of Eve at a conference.
2. Eve agrees on uploading the photo to AISEC's photo gallery service.
3. Before uploading Eve chooses the sticky policy determining who might get access to the photo. Here, default policies are:
   a) *Only the user her-/himself*
   b) *Participants of the conference*
   c) *Internet – free download*
4. According to the policy (a) the photo will be uploaded restricted to Eve's eyes only.
5. Mario's boss checks the gallery for available photos but he cannot see Eve's photo.

UMA Reference Implementation

Use Case: Controlling Photo Sharing

Fraunhofer
AISEC



PROTECT YOUR PRIVACY
Empowering | Controlling | Unifying

Protect Resource

Access Resource

Contact Us

Photos

Name	Policy	Size
2011-09-12 10.56.02.jpg	Participants	1003591
2011-09-12 11.14.18.jpg	Participants	839720
2011-09-12 12.08.16.jpg	Participants	833270

2011-09-12 10.56.02.jpg

Additional information

- Uploaded on 09/12/2011 10:58

2011-09-12 11.14.18.jpg

Additional information

- Uploaded on 09/12/2011 11:18

2011-09-12 12.08.16.jpg

Additional information

- Uploaded on 09/12/2011 12:10

UMA-enabled Photo Sharing Web-Service hosted at Fraunhofer AISEC's Cloud

Photo gallery with user defined sticky policy attached to each photo.

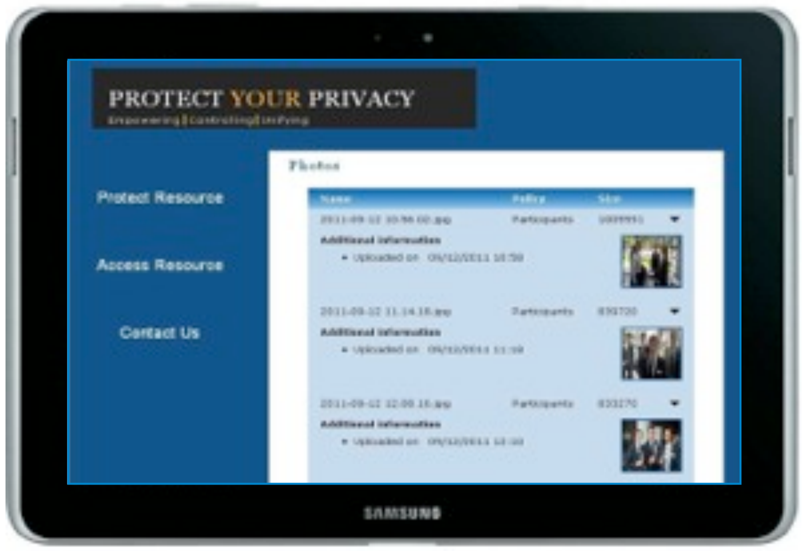
Functionality of AISEC's photo sharing service

Contact:
Mario.Hoffmann@aisec.fraunhofer.de
Alam.Mohammad@aisec.fraunhofer.de

UMA Reference Implementation

Use Case: Controlling Photo Sharing

Fraunhofer
AISEC



Contact:
Mario.Hoffmann@aisec.fraunhofer.de
Alam.Mohammad@aisec.fraunhofer.de

FAQ Research & Development

- Which parts of the UMA protocol have been **implemented**?

  Introduction & registration of host and AM, scope and resource registration, policy administration, third-party login at AM and HOST.

- What are the **key technologies used**?

  Java, JSP, Spring 3.0, Apache Tomcat, iBatis, PostgreSQL, Navicat, Dreamweaver, Restfull, JSON

- What have been the **key challenges** implementing UMA?

  Scope registration acted according to the policy at AM.

- What is the current status of the **Open Source** approach?

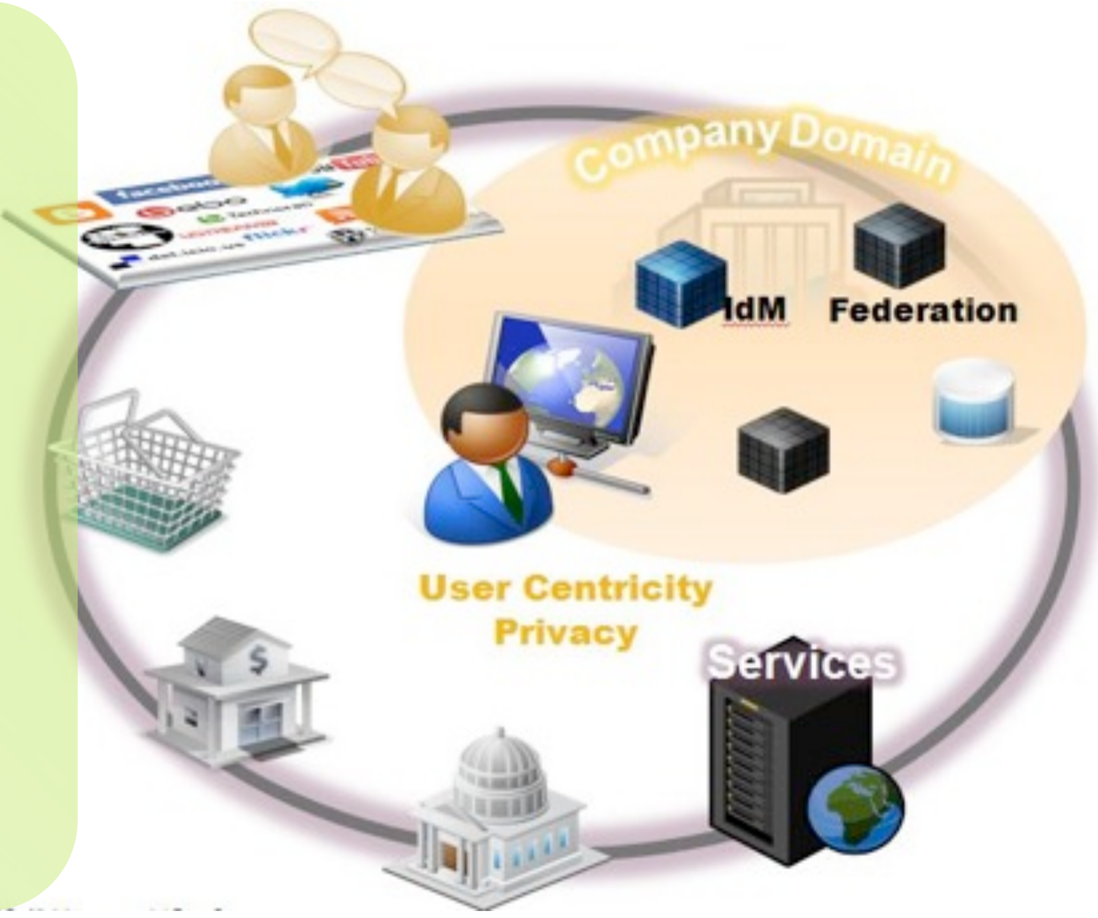
  Should be open source, but where to publish not yet clear.

- What are the **next steps** regarding our reference implementation?
  - Extending resource management including personal information -> kind of I-card.
  - Managing PI and build reputational system -> kind of R-card .
  - AM - Personal data backup and synchronization in a Cloud (AM as a Service)
  - AM-lite for mobile devices (Android, iPhone -> Web-based vs App)
  - Integration of OpenID-Connect
  - PayPal Access (Identity and attribute provider product) Integration

Synergetics project: TAS³ is getting an UMA connector

Trusted Architecture for Securely Shared Services

> “The TAS³ project is working to produce an architecture in which data can be shared and reused securely and safely within a trusted environment. Most importantly, it puts users in control of what happens to their data and allows them to see when and by whom it has been accessed. For more information visit www.tas3.eu or www.zxid.org.



Synergetics is now developing the UMA connector to its end-to-end trust assurance framework, which otherwise focuses primarily on machine-to-machine and deep web service calls

Hand the ball to speaker Sampo

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

Why would an organization want to UMA-enable its apps?

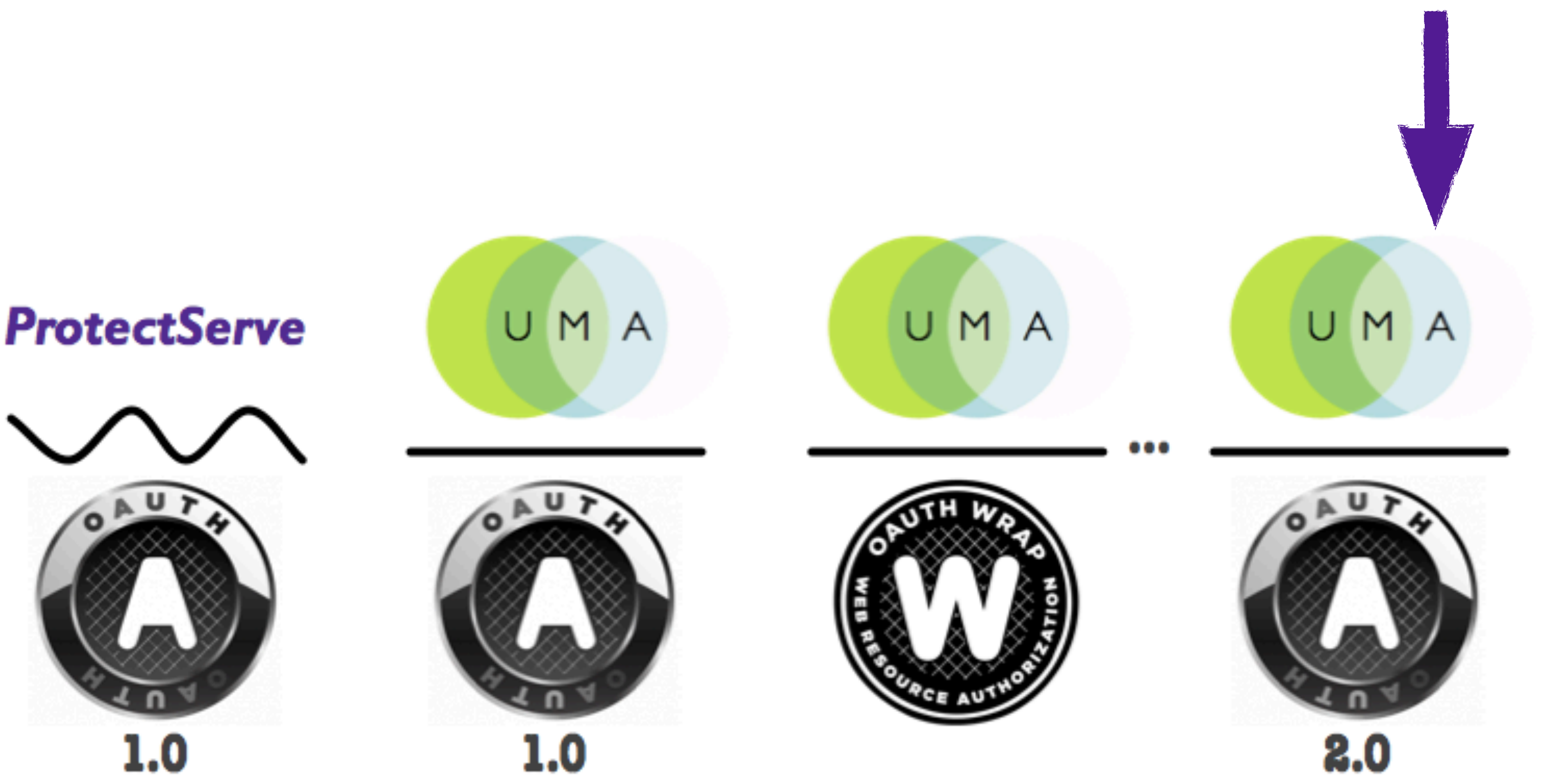
Existing UMA implementations

How UMA works to build technical and business trust

Q&A

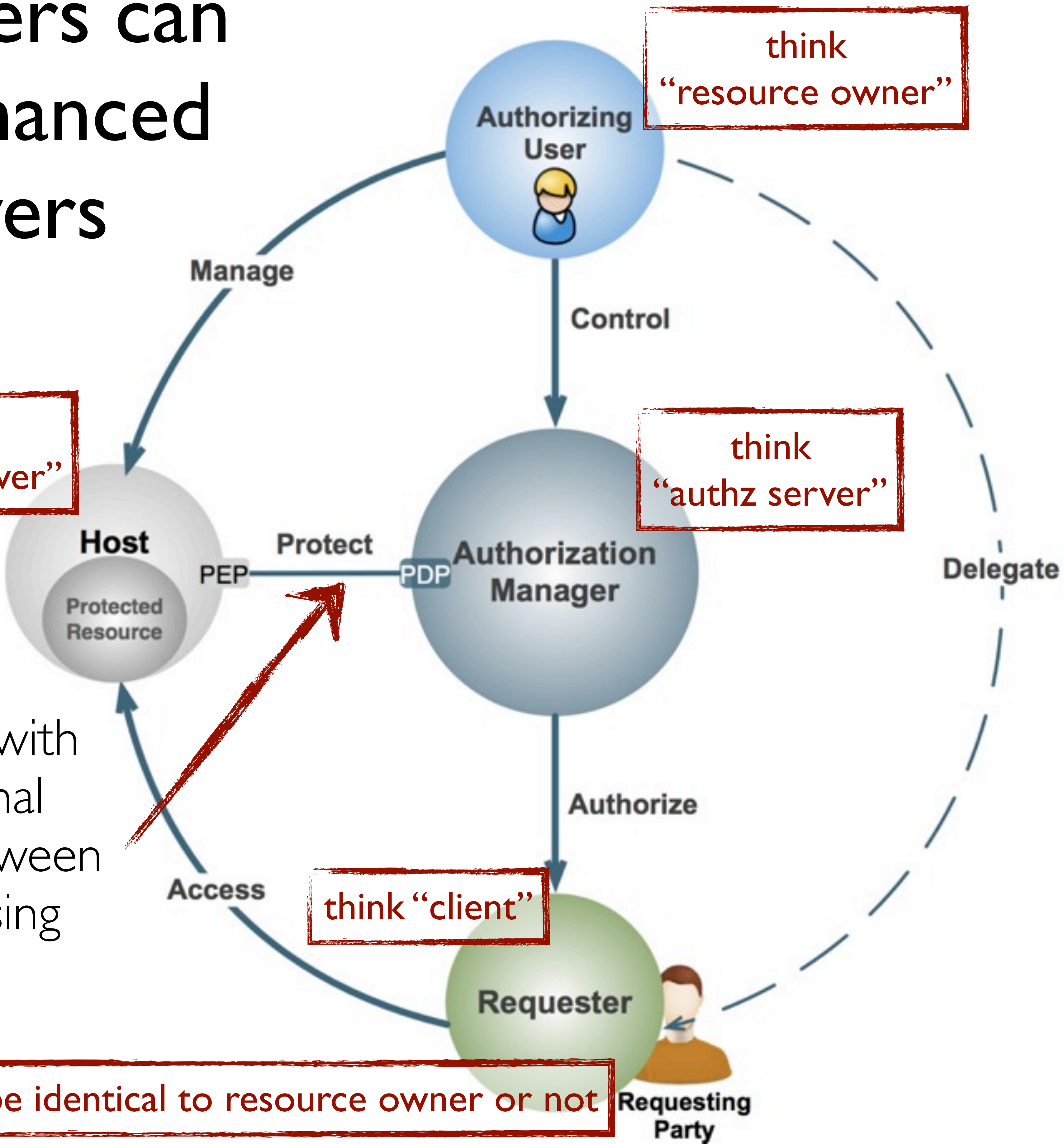
Hand the ball back to Eve

Here is UMA's history with OAuth



we're right about here

The UMA players can be seen as enhanced OAuth players



think "resource owner"

think "resource server"

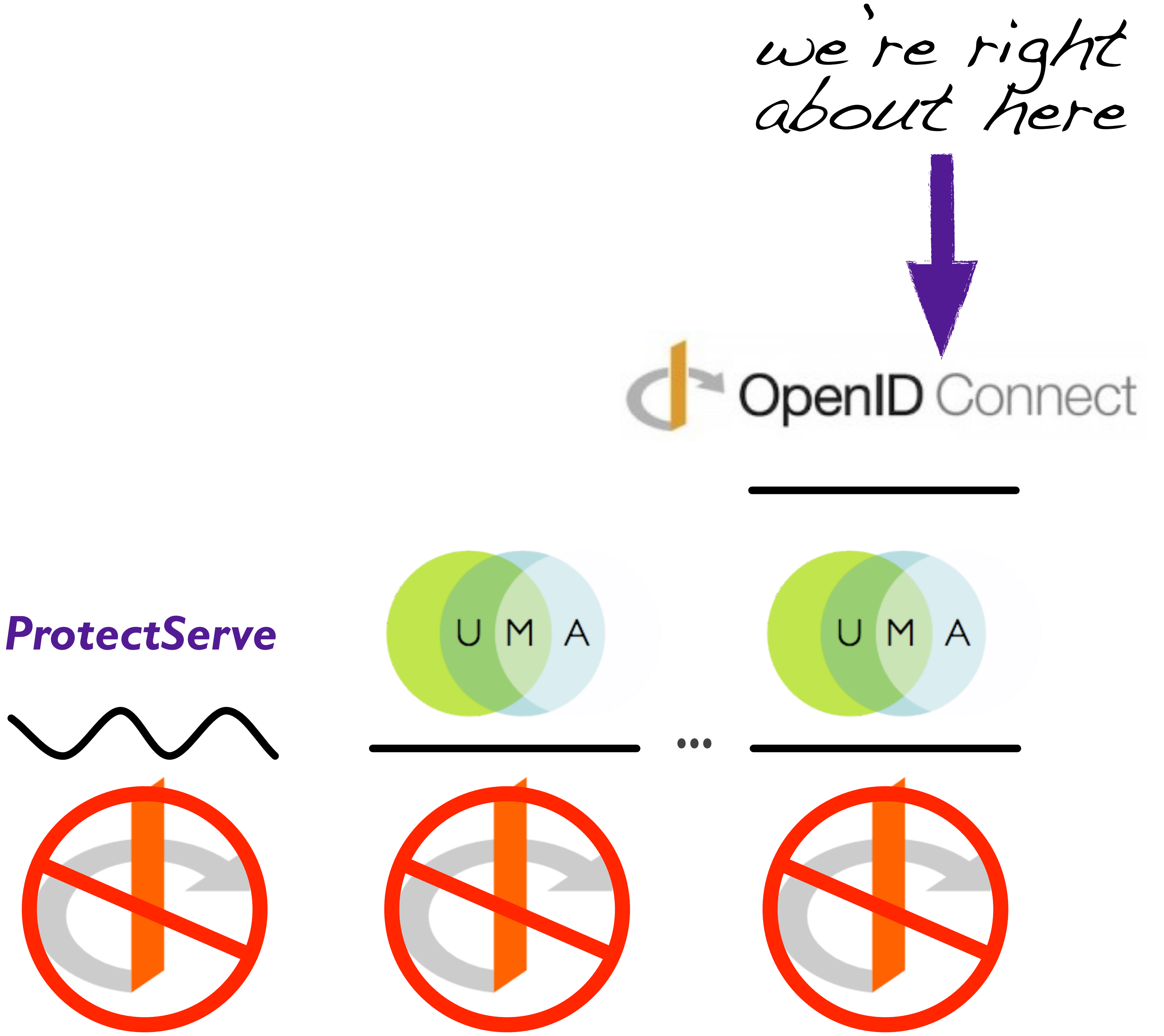
think "authz server"

think "client"

could be identical to resource owner or not

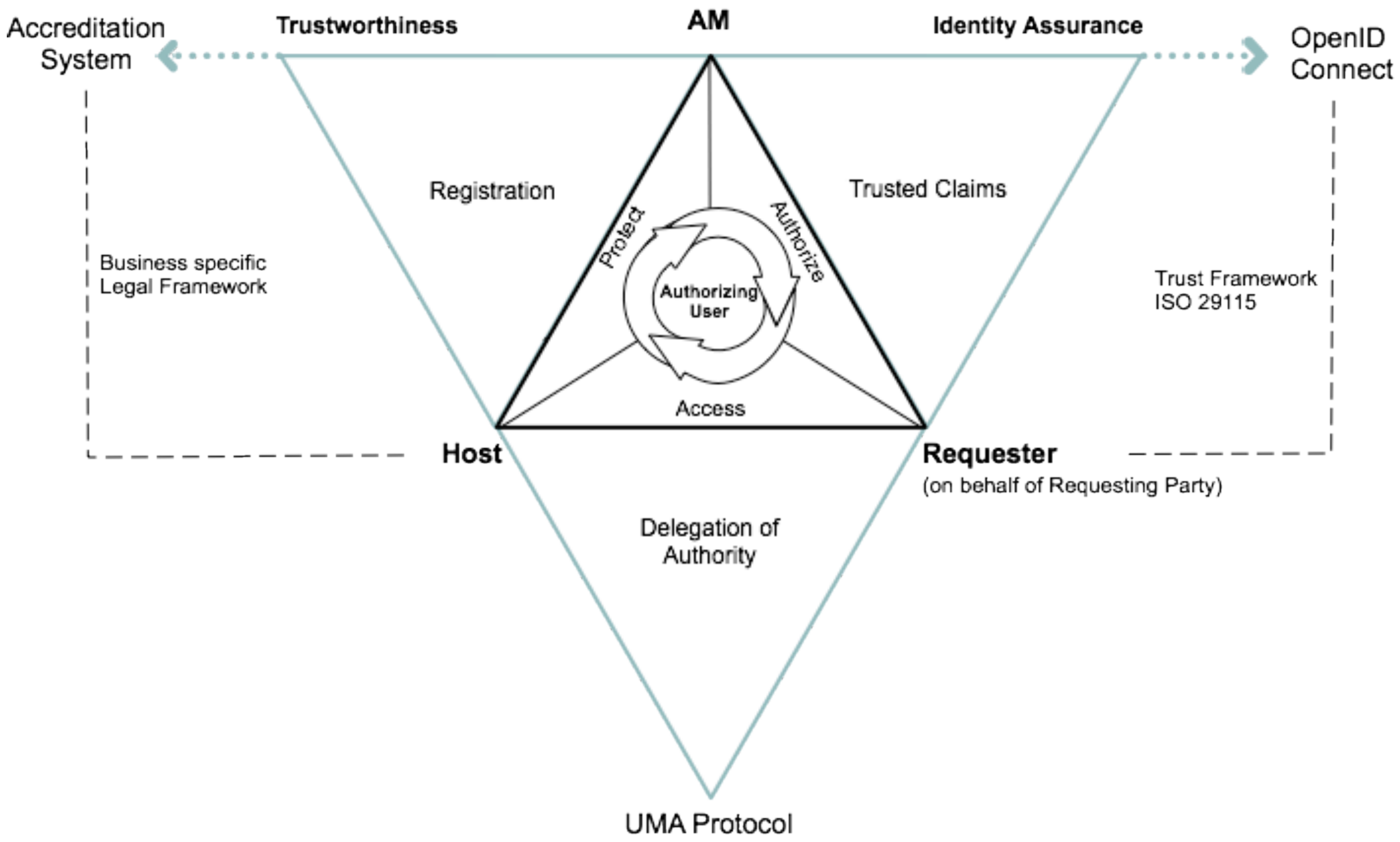
Technical trust begins with UMA defining a formal protected interface between the host and AM – using OAuth

By contrast, here is UMA's history with OpenID



UMA also has what might be called an explicit history with OpenID. Another one of UMA's design principles is to be agnostic as to the identifier systems it works with, so, for example, it can't have any dependencies on OpenID as one such system. This is an outgrowth of UMA being focused on authorization and wanting to work with websites and web apps as they work today, even if they don't use OpenID or indeed any third-party authentication approach. But we have a strong interest in OpenID Connect, as we'll explain.

Business trust has many moving parts; claims-based authorization is one key

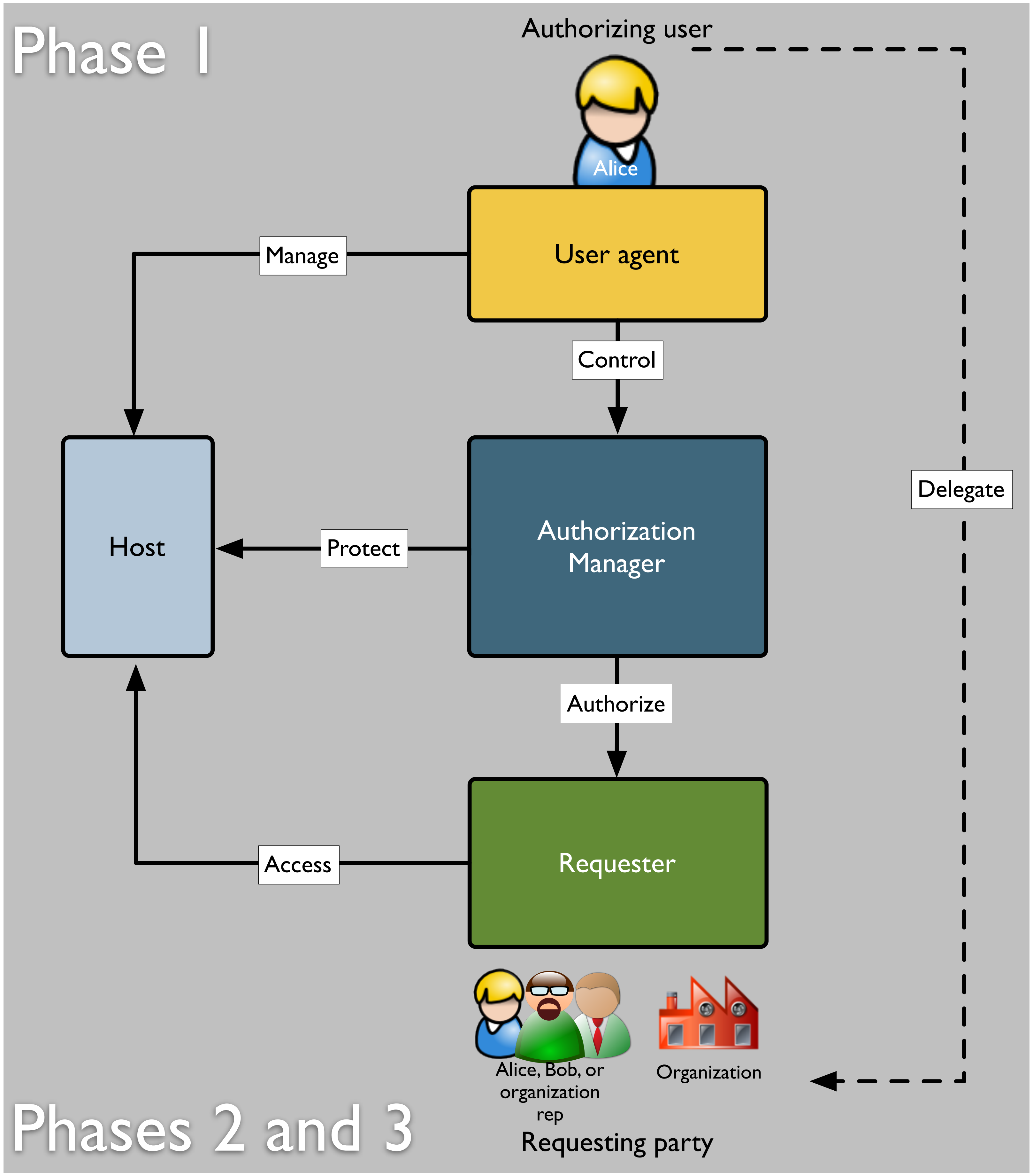


speaker: Domenico

UMA has three phases

1. Protect a resource

2. Get authorization
3. Access a resource



speaker: Eve

Agenda

Introduction: What is UMA, why do we need it, and how far along is it?

Use cases illustrating UMA's unique strengths

Why would an organization want to UMA-enable its apps?

Existing UMA-conforming implementations

How UMA works to build technical and business trust

Q&A

Thanks again to our webinar sponsors!

Thanks for joining us today

Become an UMAnitarian!

Webinar recording will appear soon!

Visit http://tinyurl.com/umawg

On behalf of and with thanks to the UMA Work Group

14 December 2011

(Questions? Contact eve@xmlgrrl.com / @xmlgrrl or maciej.machulak@cloudidentity.co.uk / @mmachulak anytime)