

Take control of your Personal Data

User-Managed Access (UMA)

Domenico Catalano

Oracle Community For Security

22 June 2011



Agenda

Today's Challenges

UMA Concepts and Benefits

Use cases

SmartAM.org Project

Trust Model

Q&A

Digital life

“Everything you do in life leads to a digital slime trail”

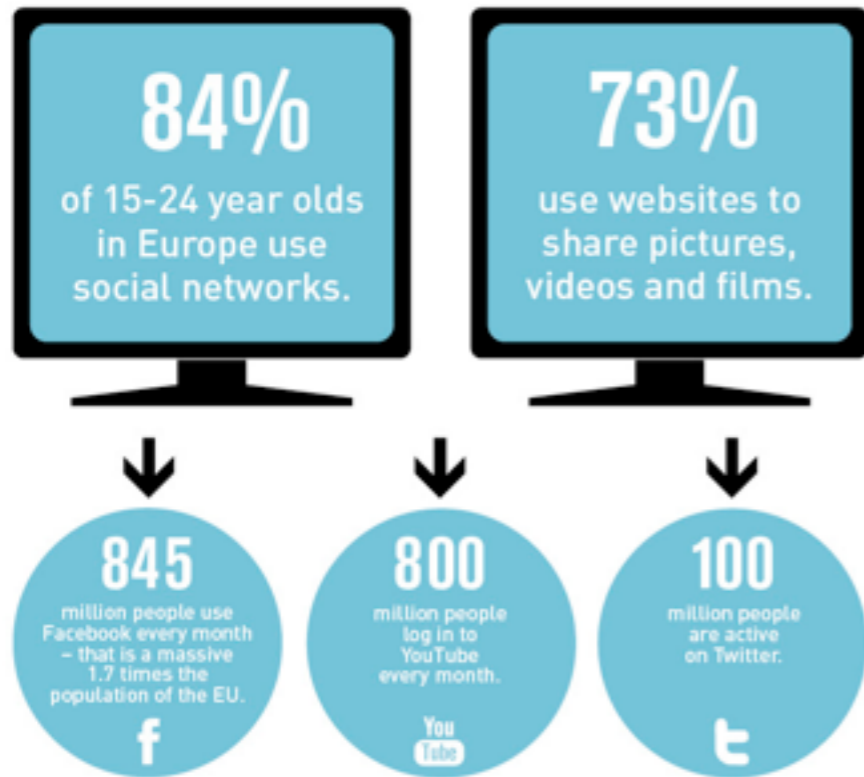


Today's Challenges

- Social Network
- Emerging Personal Cloud, PDS
- Participatory Personal data



Data Sharing in the Internet



Are you in **Control** of your **Personal Data**?

What do **People Share** online?

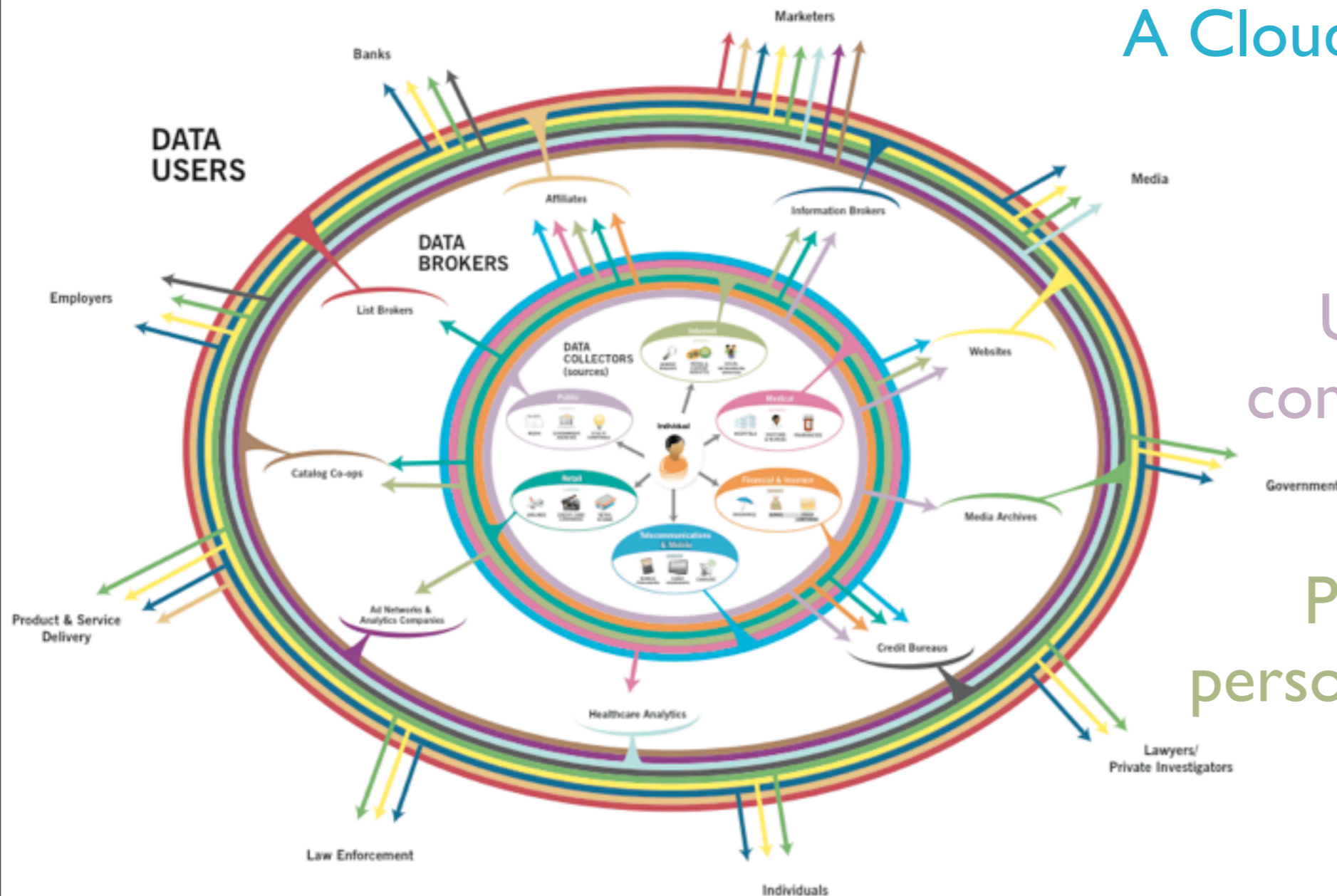


Emerging Personal Data Store

A Cloud Service for storing personal life bits

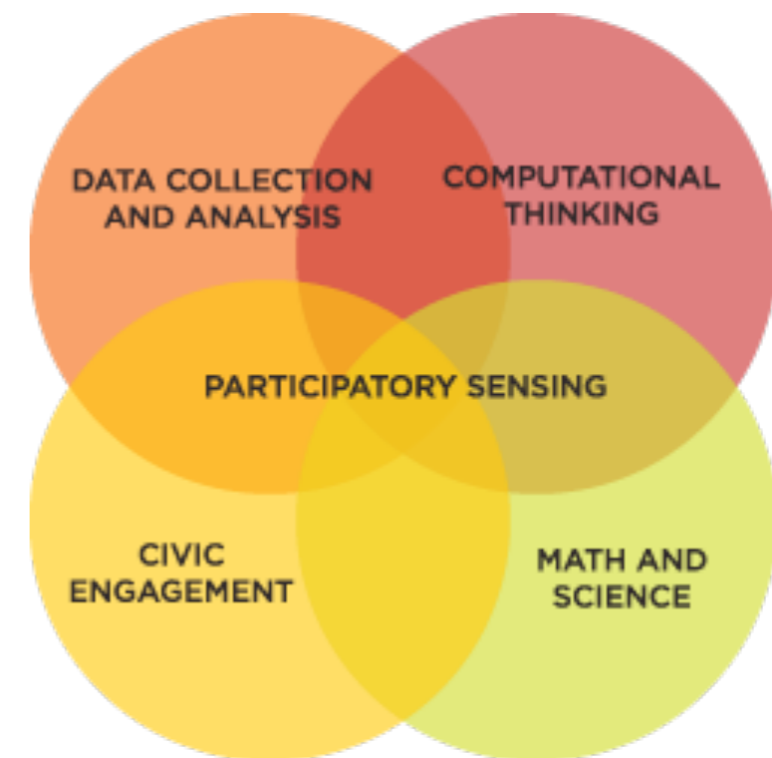
Under the complete control of an individual

Provide portability of personal data across PDS



Participatory Personal Data

- Participatory personal data refers to aggregation of representations of measurements collected by people, about people.
- These data are part of a coordinated activity;
- Captured, processed, analyzed, displayed and shared.



Agenda

Introduction and Business Driver

UMA Concepts and Benefits

Use cases

SmartAM.org Project

Trust Model

Q&A

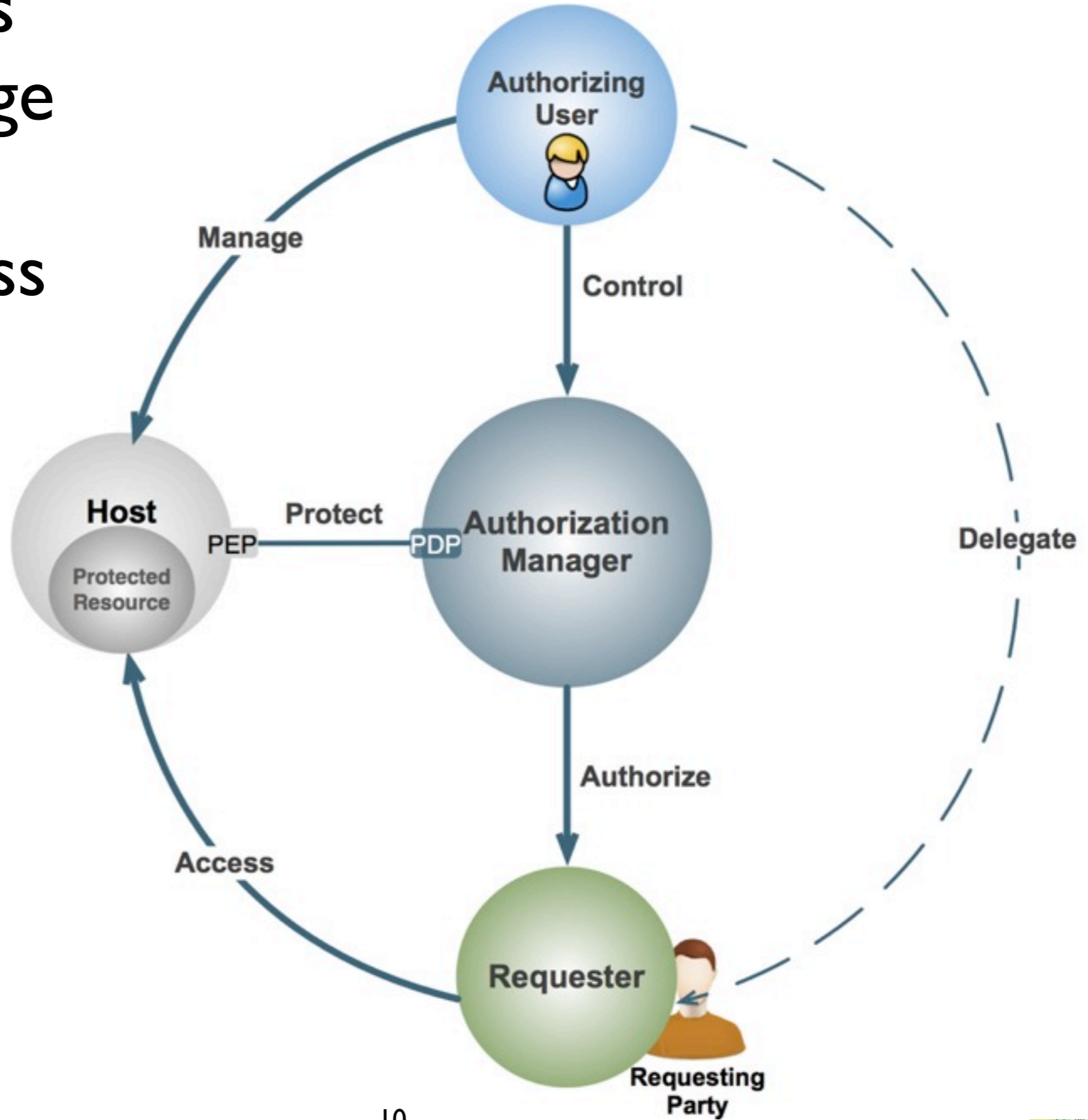
Privacy is not about secrecy

“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”

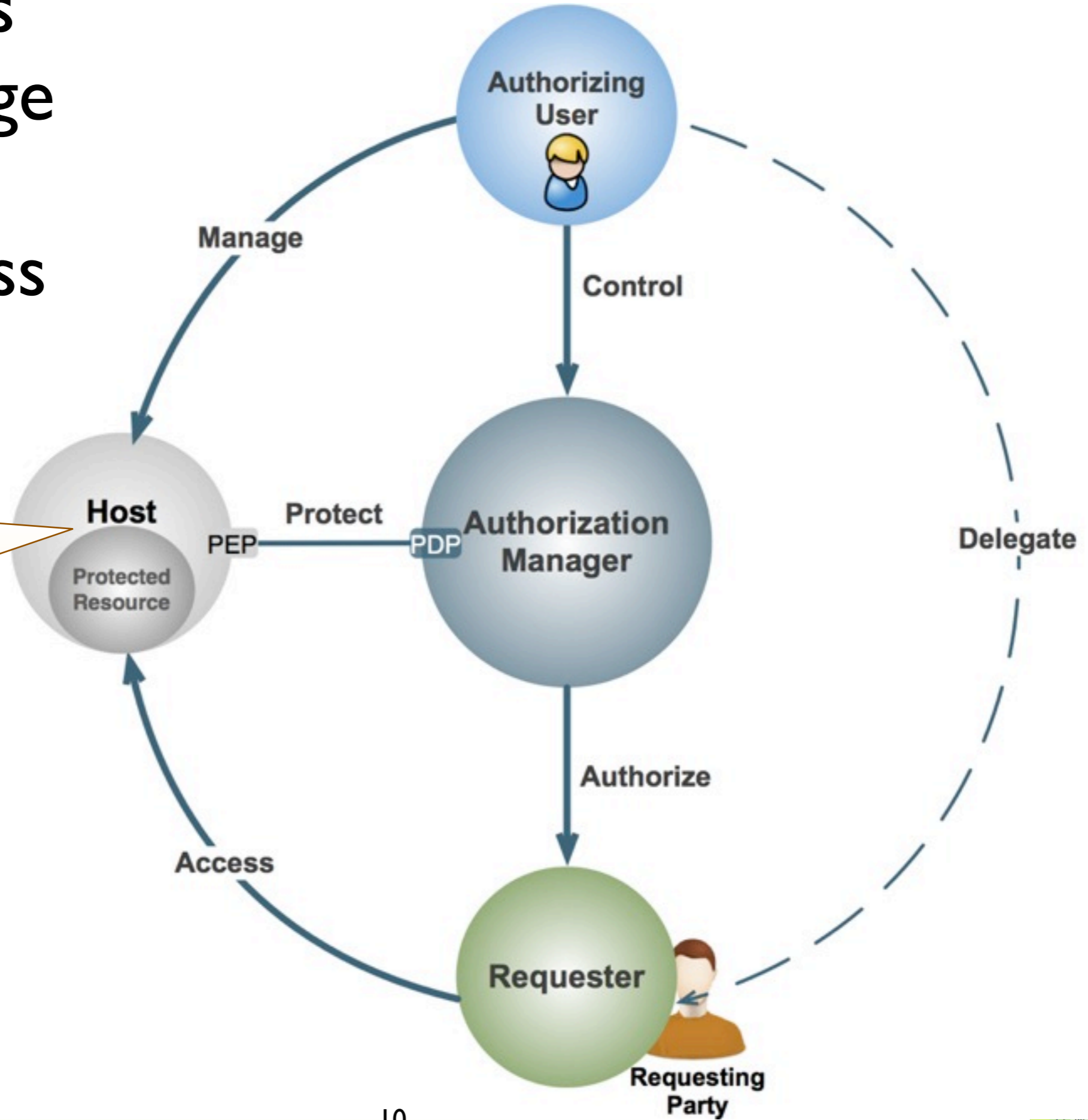
– Ann Cavoukian, Information and Privacy Commissioner of Ontario,
Privacy in the Clouds paper

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

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

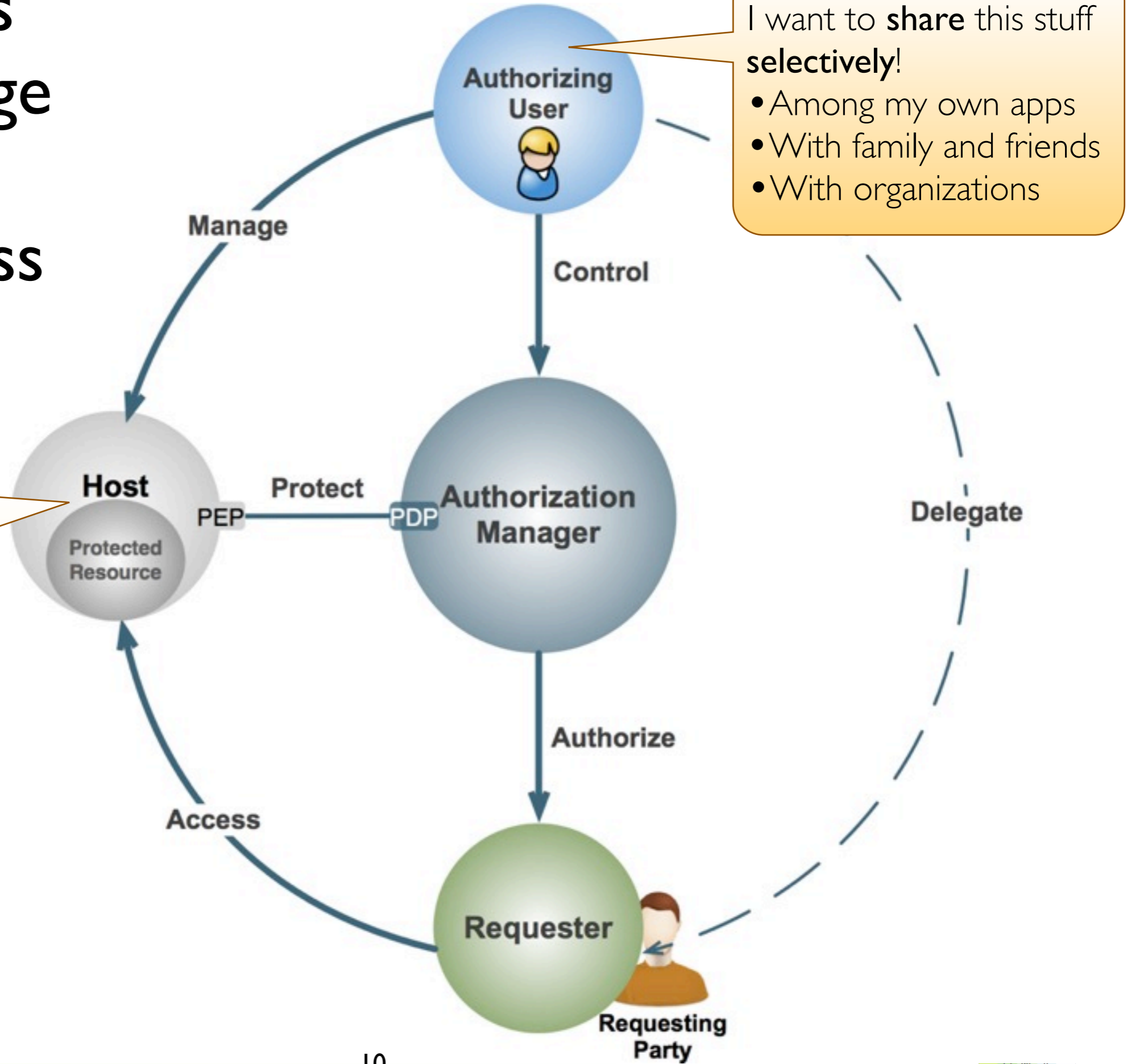


UMA enables you to manage sharing and protect access from a single hub



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

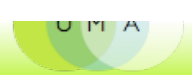
UMA enables you to manage sharing and protect access from a single hub



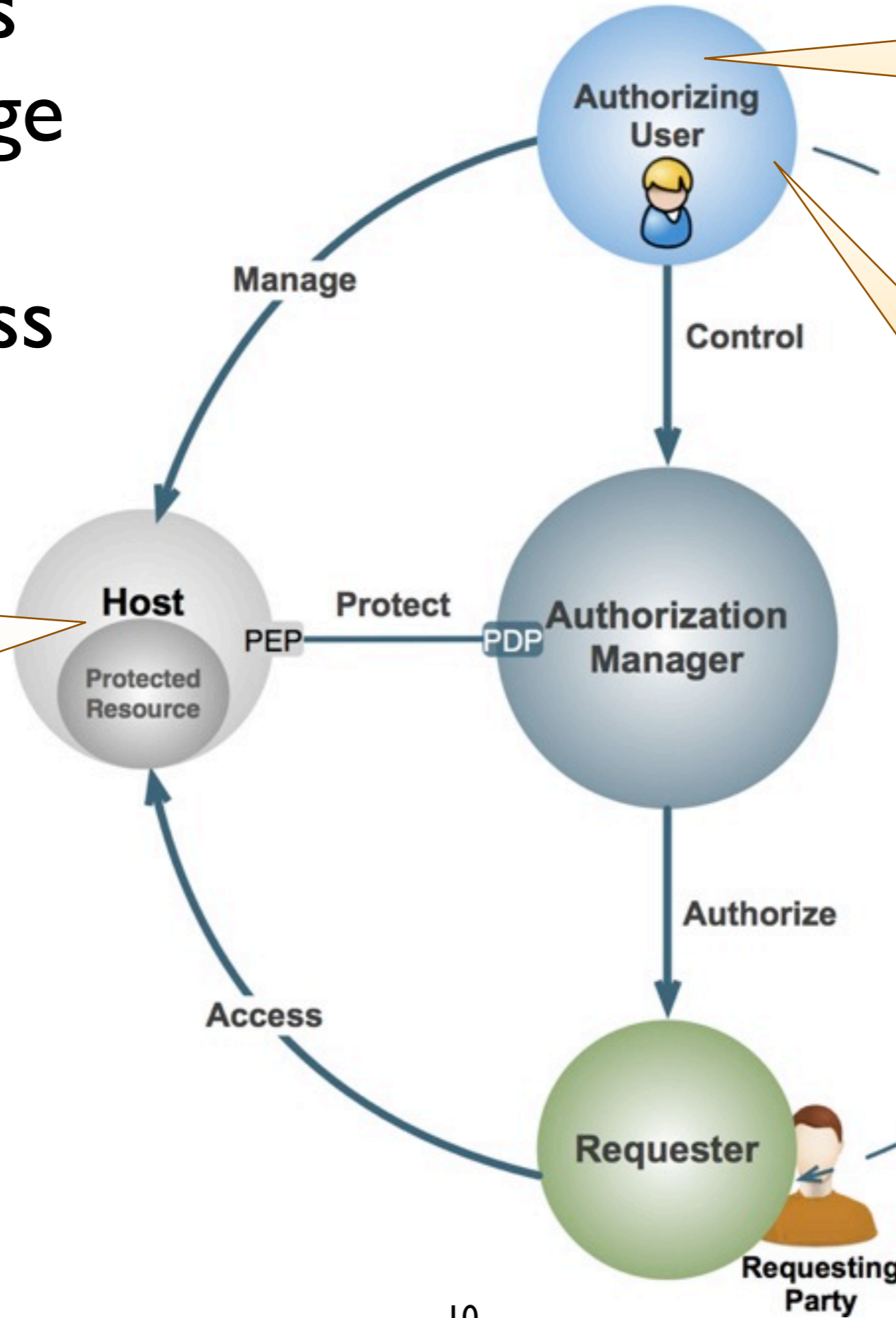
I want to **share** this stuff **selectively!**

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

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



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/health
- Legal
- ...



UMA is...

- A web protocol that lets you control access by anyone 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
- Simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly
- Contributed to the IETF for consideration: draft-hardjono-oauth-umacore
- Currently undergoing interop testing and increased OpenID Connect integration

UMA and Privacy Controls benefits

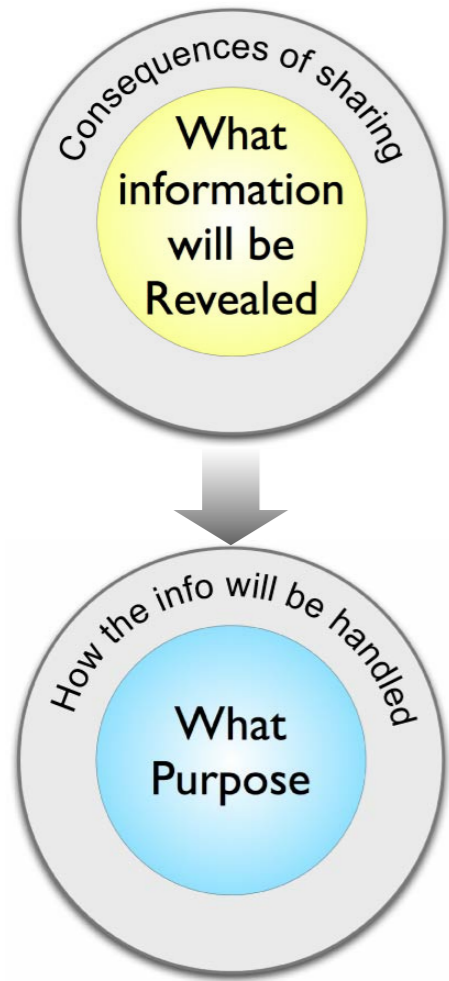


UMA and Privacy Controls benefits



- Subject registers the resource which is collecting the personal data with a centralized Authorization Manager.
- It allows to maintain a centralized view of what data is being collected.

UMA and Privacy Controls benefits



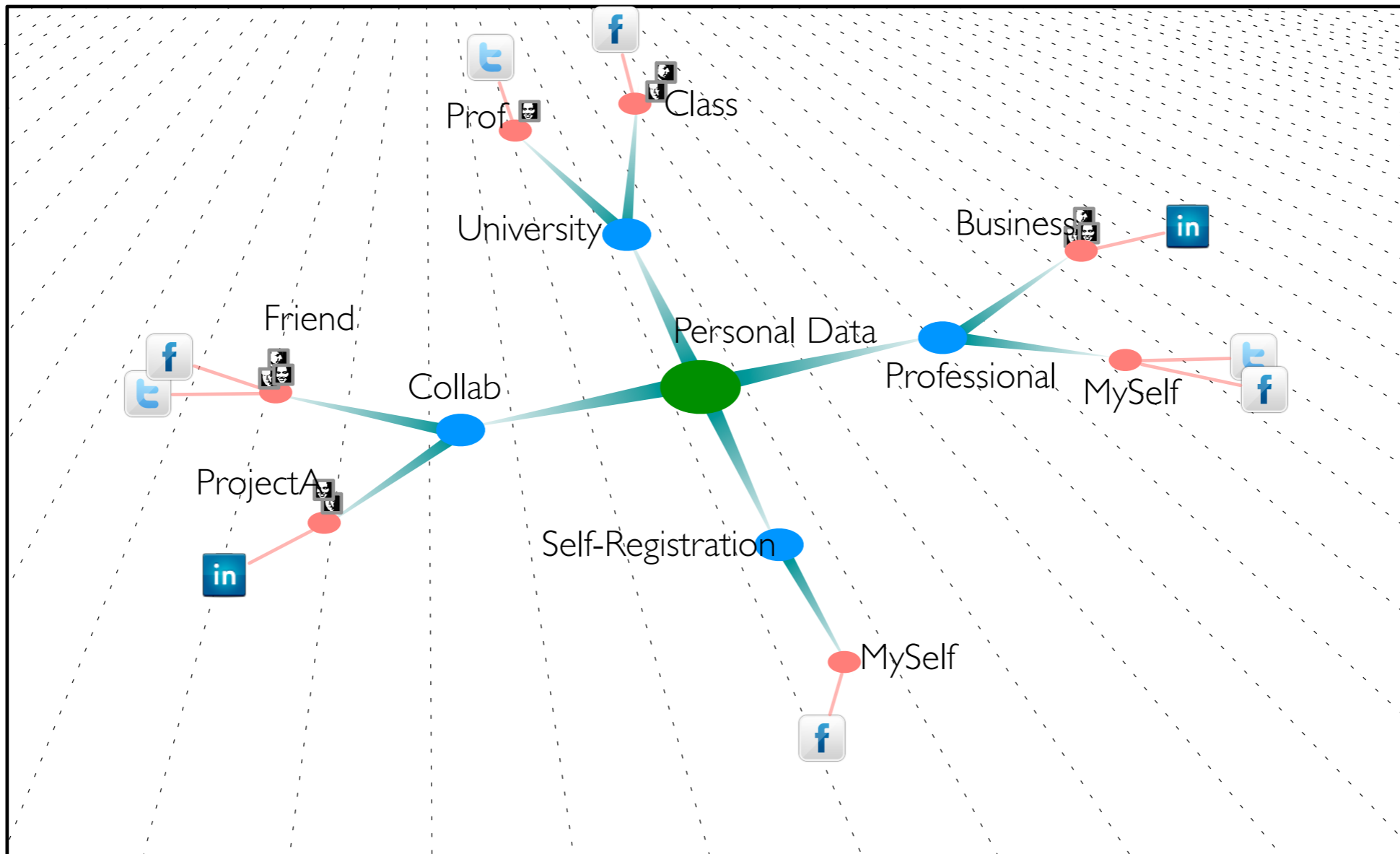
- Subject registers the resource which is collecting the personal data with a centralized Authorization Manager.
- It allows to maintain a centralized view of what data is being collected.
- Individuals are an active part of defining the how the personal information will be handled in the data sharing process.
- A sharing policy (or connection) defines for what purposes personal data is shared.
- Possibility to disable or cancel any connection at any time.

UMA and Privacy Controls benefits



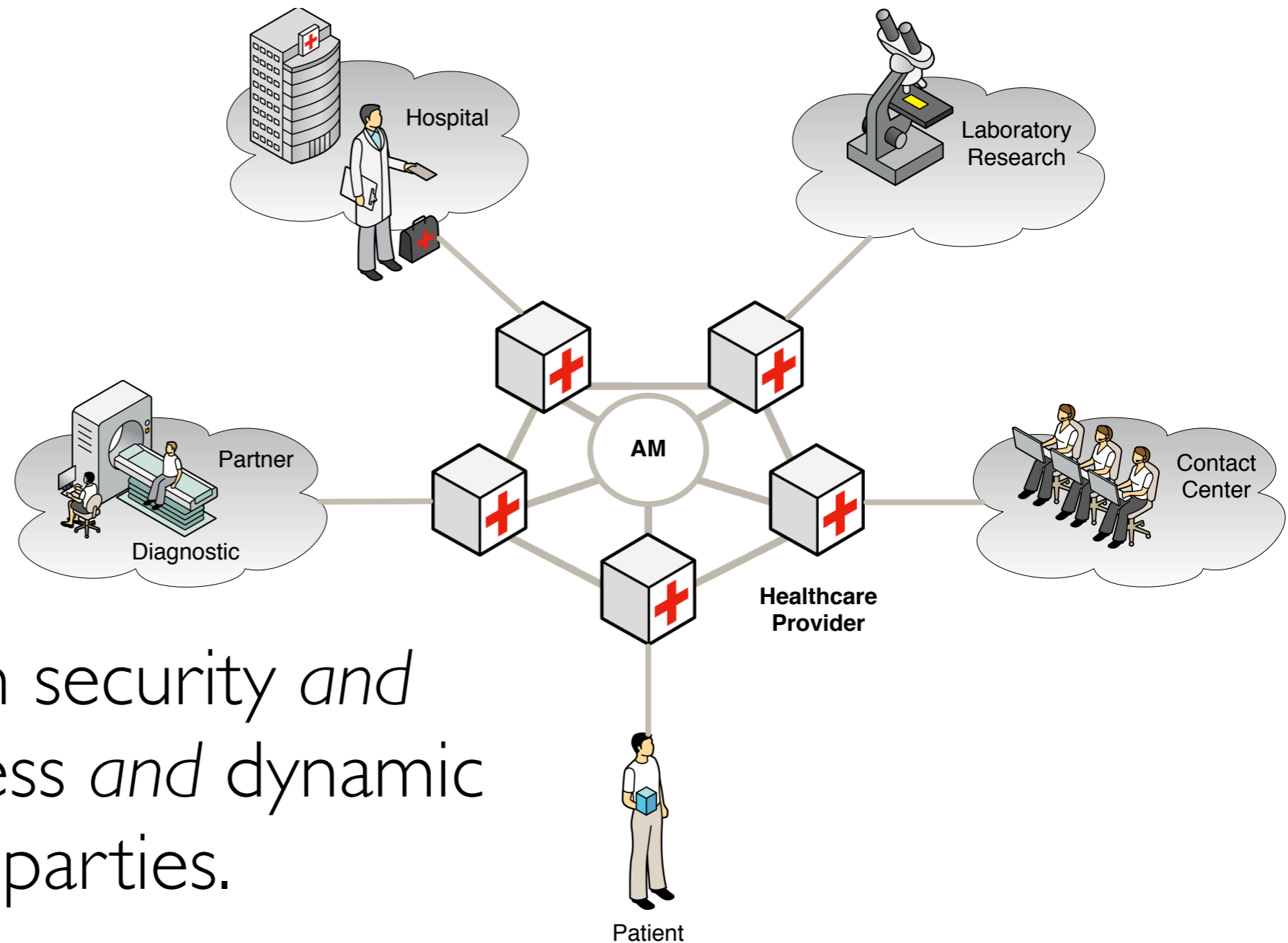
- Subject registers the resource which is collecting the personal data with a centralized Authorization Manager.
- It allows to maintain a centralized view of what data is being collected.
- Individuals are an active part of defining the how the personal information will be handled in the data sharing process.
- A sharing policy (or connection) defines for what purposes personal data is shared.
- Possibility to disable or cancel any connection at any time.
- Policy Enforcement Point at Host site allows to intercept any request to access to personal data.
- Explicit User consent.
- Trusted Claims allow to discriminate the Requesting Party.

Maintain control on Information that will be revealed



Human Interface study for SmartAM at Newcastle University

Protecting electronic health records



EHRs need high security *and* third-party access *and* dynamic introduction of parties.

Agenda

Introduction and Business Driver

UMA Concepts and Benefits

Use cases

SmartAM Project

Trust Model

Q&A

SmartAM Project

- User-Managed Access in Higher Education - Project conducted at Newcastle University.
- Reference UMA Implementation in Java.
- Smart Authorization Manager.
- UMA/j and PUMA (Python) framework for building UMA-enabled application.
- To be deployed at Newcastle and integrated with UK Federation.
- <https://smartjisc.wordpress.com>

The SMARTAM project

smartam.
beta

- 1. Register data**
Images, video, text files
- 2. Set permissions**
to display or to edit
- 3. Choose contacts**
friends, family, colleagues
- 4. Share it**
maintaining your privacy

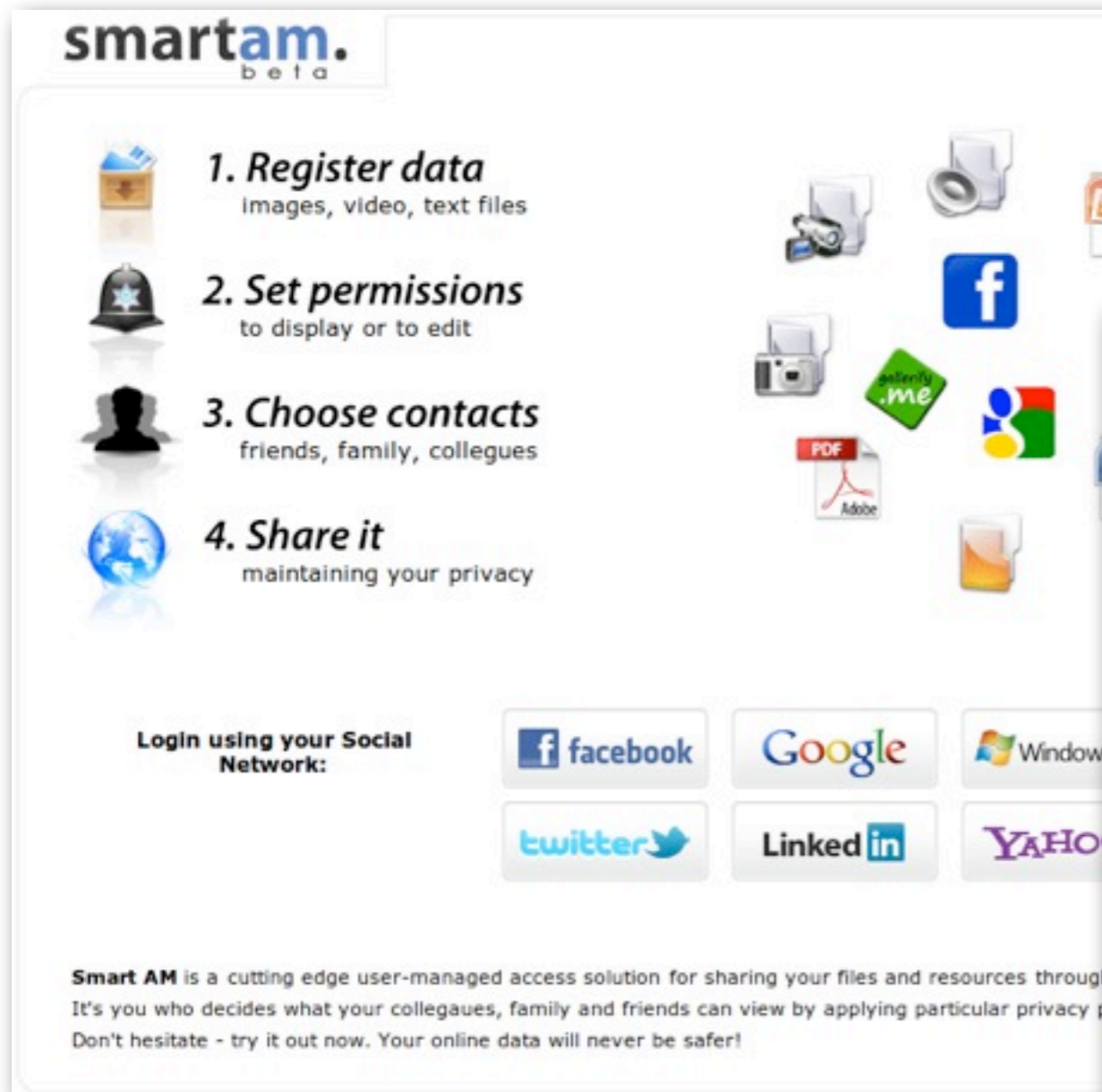
Login using your Social Network:

- facebook
- Google
- Windows Live
- twitter
- LinkedIn
- YAHOO!

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 colleagues, 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](#)

The SMARTAM project



The screenshot shows the SMARTAM beta website interface. At the top left is the logo "smartam. beta". Below it are four numbered steps: 1. Register data (Images, video, text files), 2. Set permissions (to display or to edit), 3. Choose contacts (friends, family, colleagues), and 4. Share it (maintaining your privacy). To the right of these steps are various file and social media icons including a folder, a camera, a document, a Facebook 'f' icon, a .me domain icon, a Google 'G' icon, a PDF icon, an Adobe logo, and a folder icon. Below the steps is a "Login using your Social Network:" section with buttons for Facebook, Google, Windows, Twitter, LinkedIn, and YAHOO. At the bottom, there is a short paragraph of text: "Smart AM is a cutting edge user-managed access solution for sharing your files and resources through... It's you who decides what your colleagues, family and friends can view by applying particular privacy... Don't hesitate - try it out now. Your online data will never be safer!"



See also the [SMARTAM implementation FAQ](#)

Agenda

Introduction and Business Driver

UMA Concepts and Benefits

Use cases

SmartAM.org Project

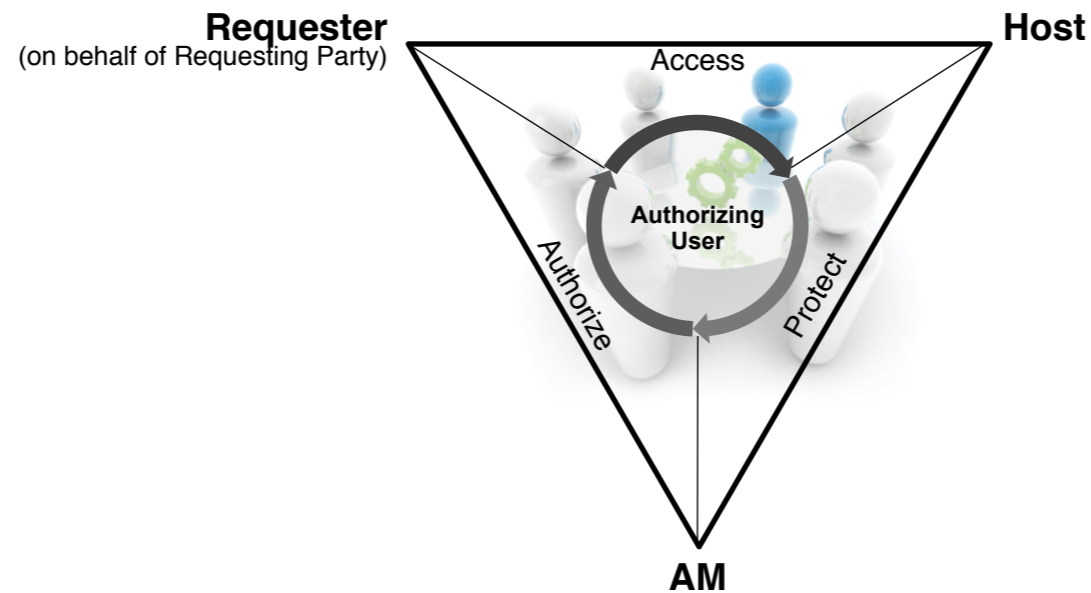
Trust Model

Q&A

Trust in a distributed Authorization System

Build a trusted ecosystem among Individual, Service Providers and Requester services.

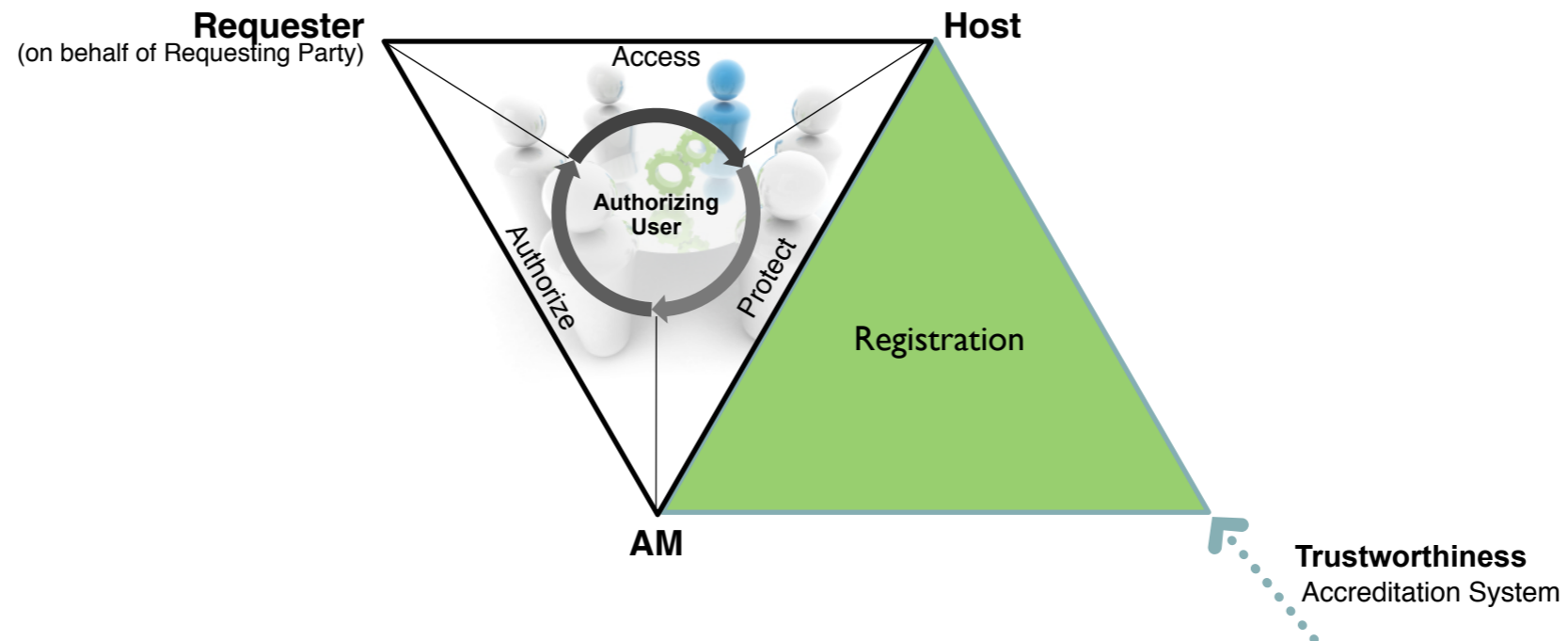
UMA Trust Model
<http://tinyurl/umatrust>



Trust in a distributed Authorization System

Build a trusted ecosystem among Individual, Service Providers and Requester services.

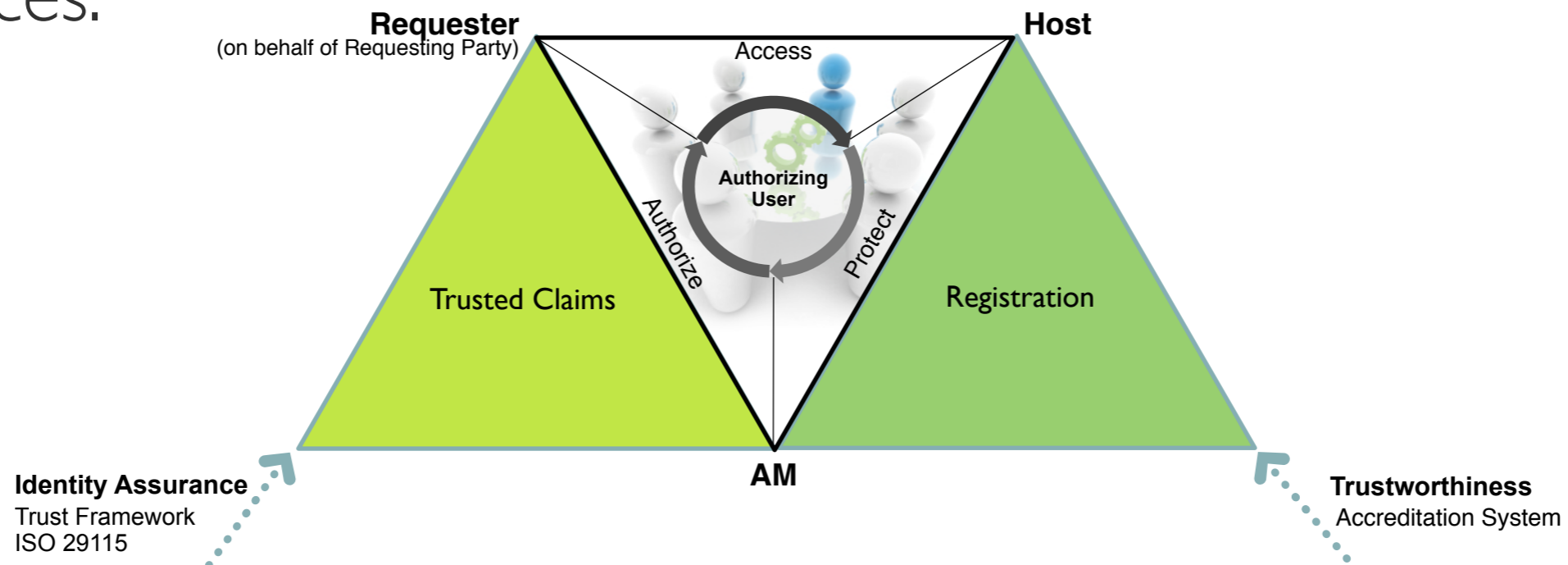
UMA Trust Model
<http://tinyurl/umatrust>



Trust in a distributed Authorization System

Build a trusted ecosystem among Individual, Service Providers and Requester services.

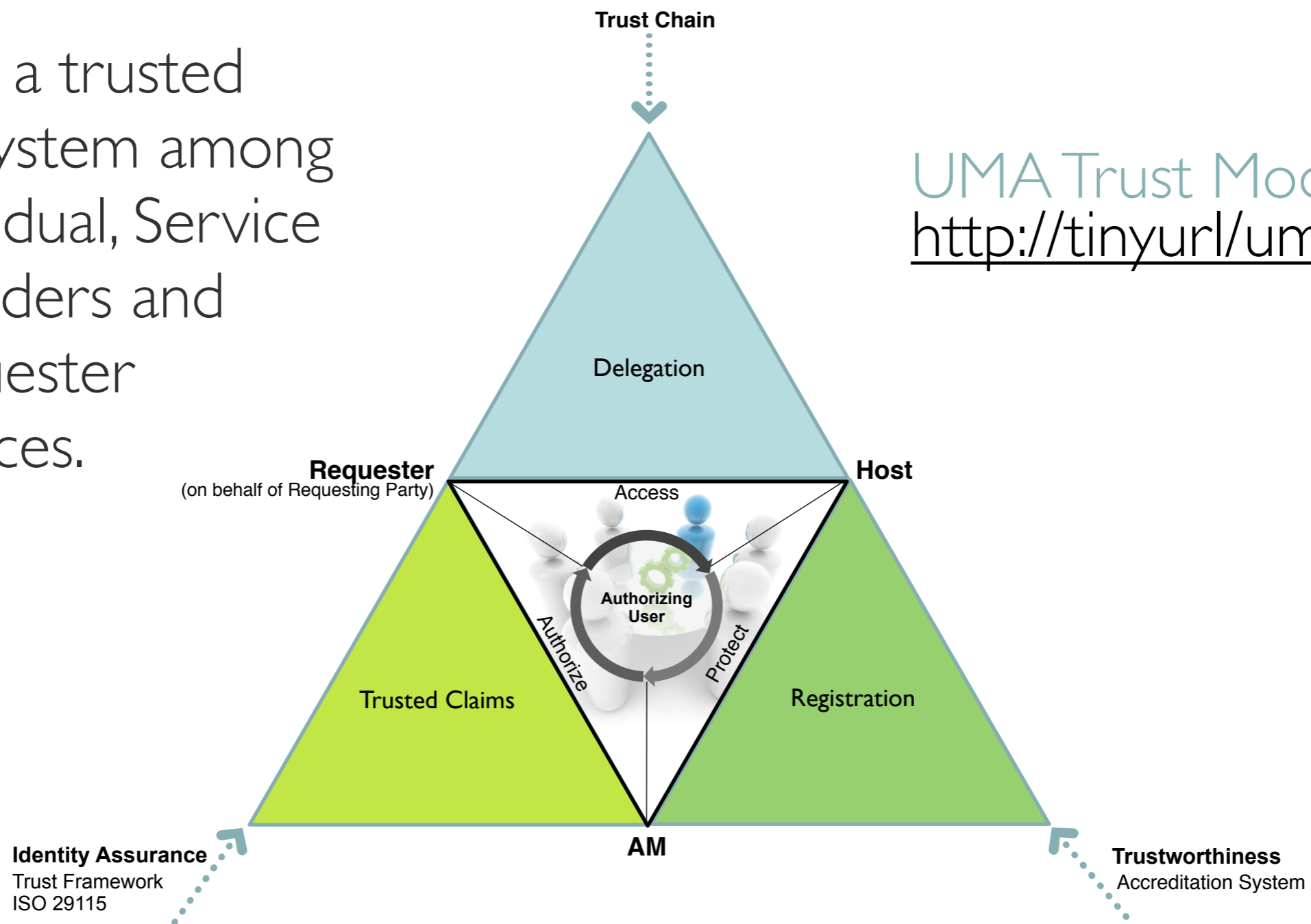
UMA Trust Model
<http://tinyurl/umatrust>



Trust in a distributed Authorization System

Build a trusted ecosystem among Individual, Service Providers and Requester services.

UMA Trust Model
<http://tinyurl/umatrust>



Thanks

Become an UManitarian!

Thanks to Eve Maler and Maciej Machulak for their assistance

