# User-Managed Access (UMA)

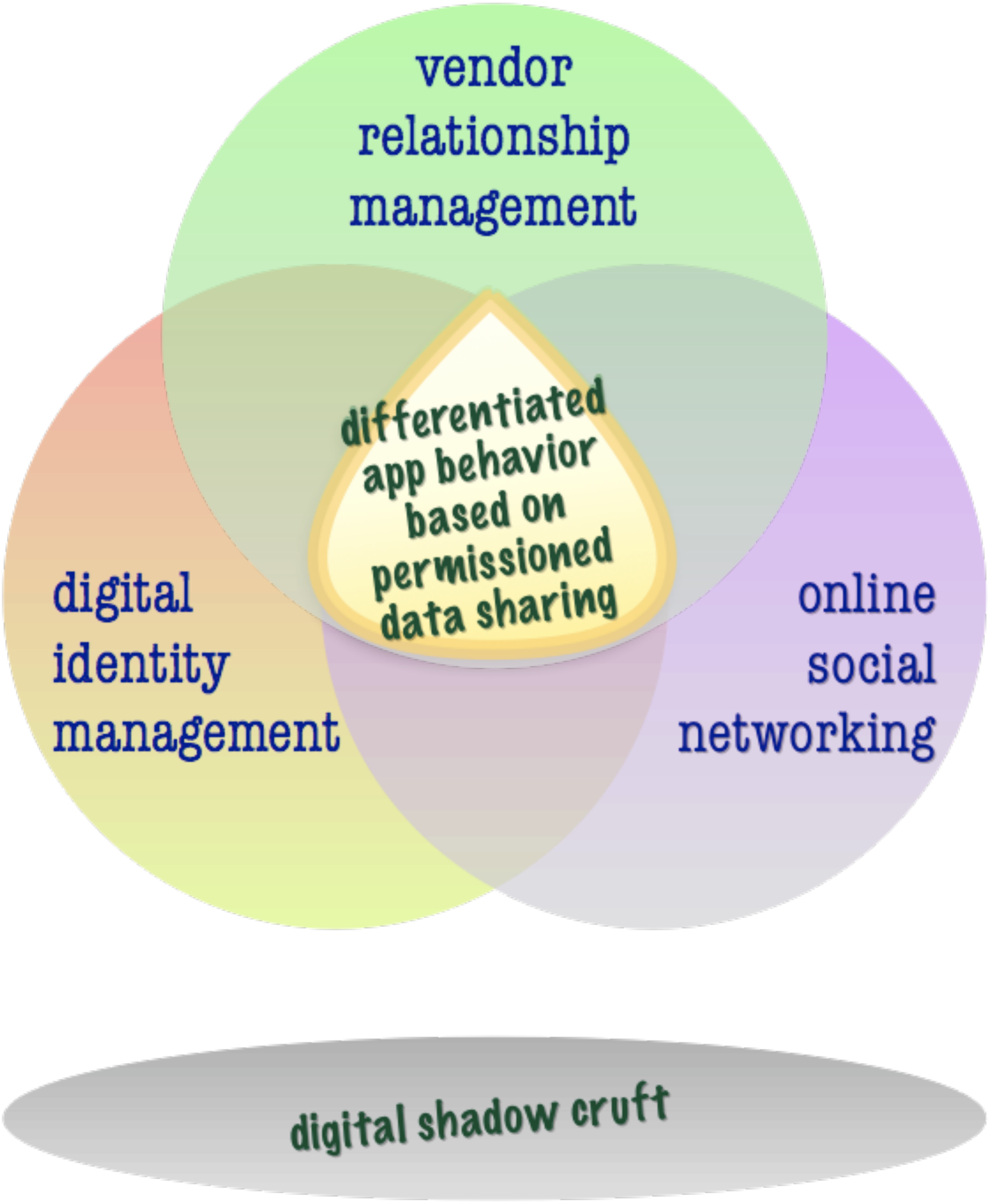
Joni Brennan, Kantara Managing Director
Eve Maler, PayPal, UMA WG chair
ITU-T Q10/17 Identity Summit
10 December 2010

*(feel free to send questions to @xmlgrrl)*

# 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



vendor relationship management

digital identity management

online social networking

differentiated app behavior based on permissioned data sharing

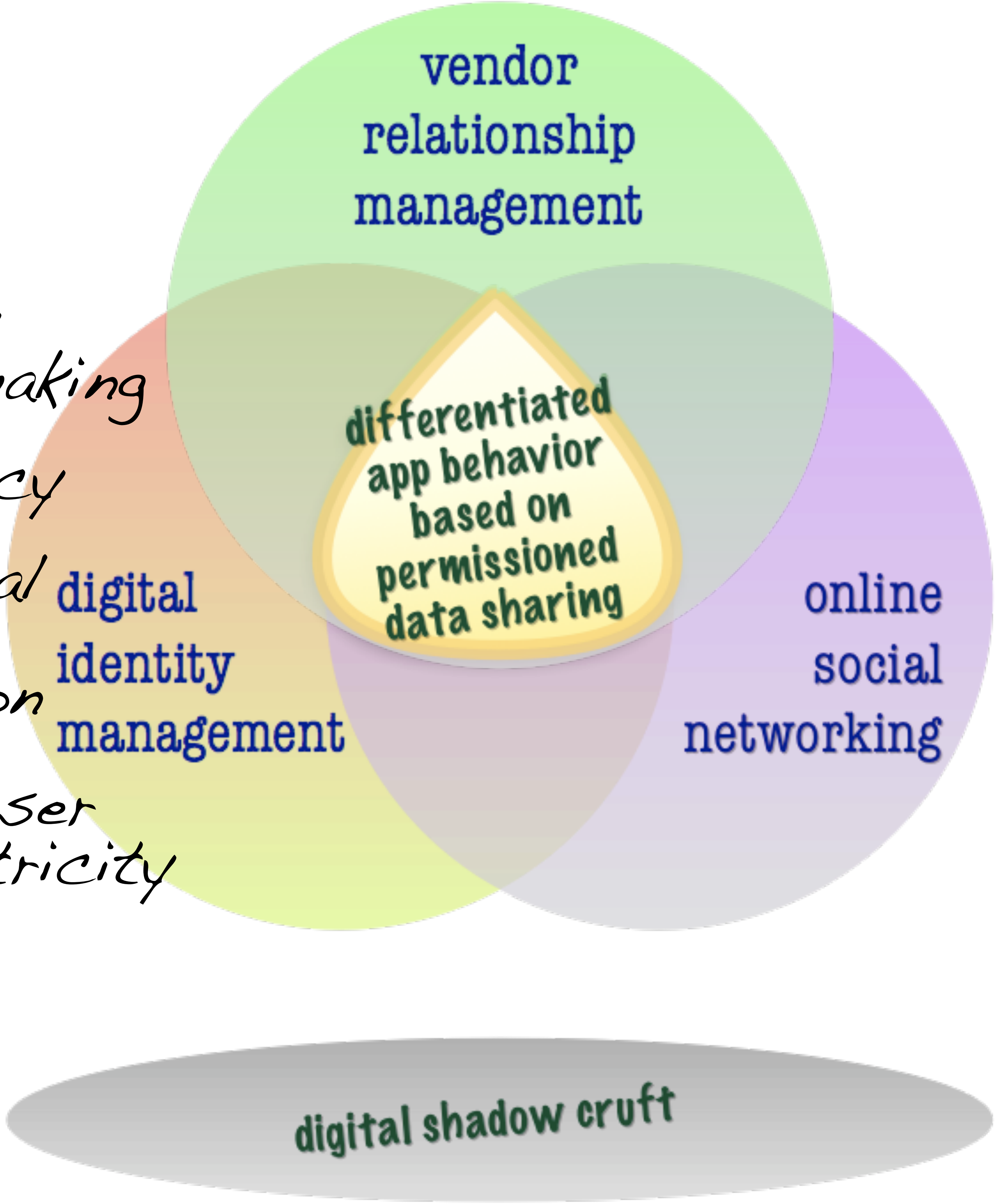
digital shadow cruft

policy
decision-making

privacy

informational
self-
determination

user
centricity



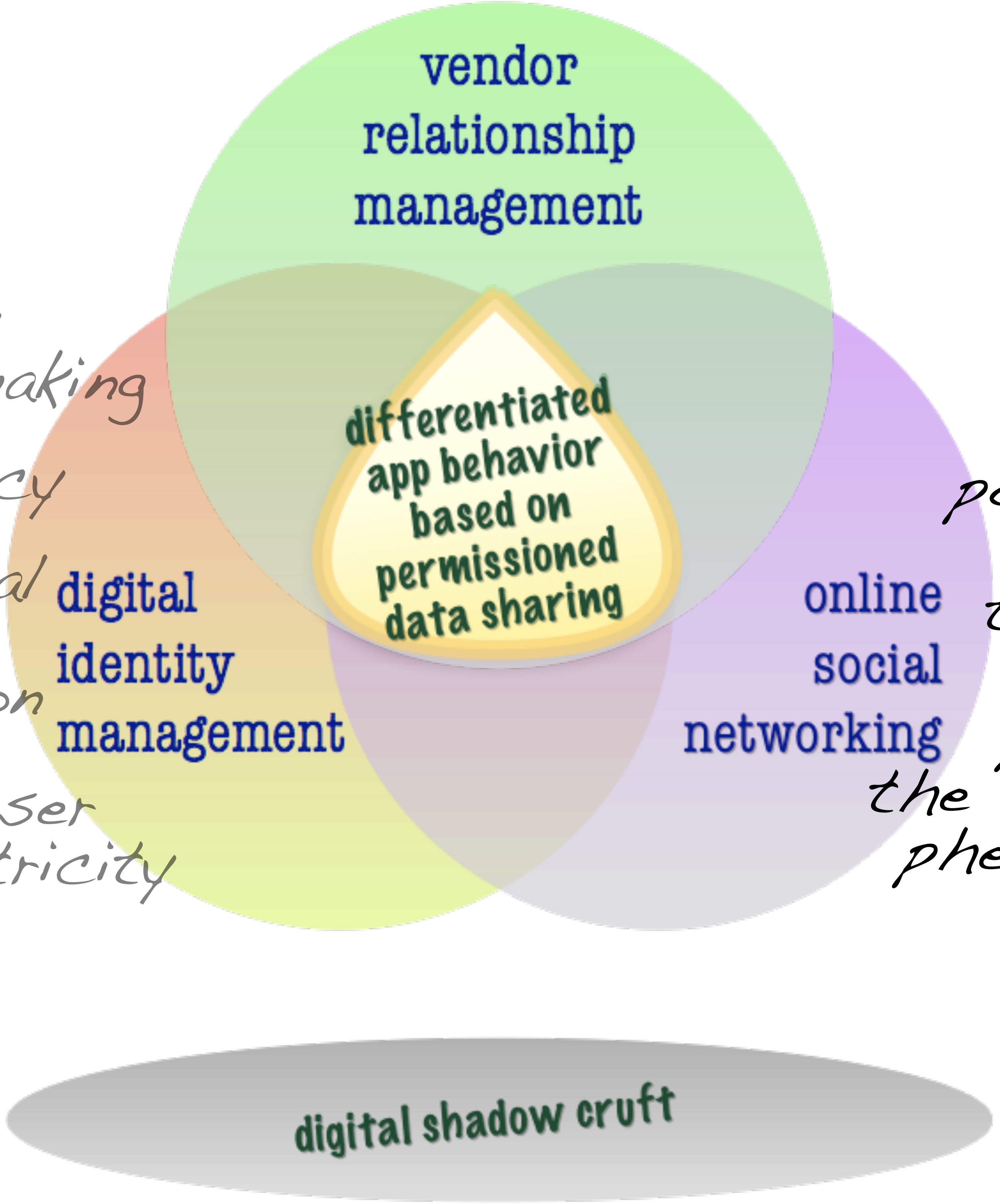
vendor
relationship
management

digital
identity
management

online
social
networking

differentiated
app behavior
based on
permissioned
data sharing

digital shadow cruft



vendor relationship management

digital identity management

online social networking

differentiated app behavior based on permissioned data sharing

digital shadow cruft

policy decision-making

privacy

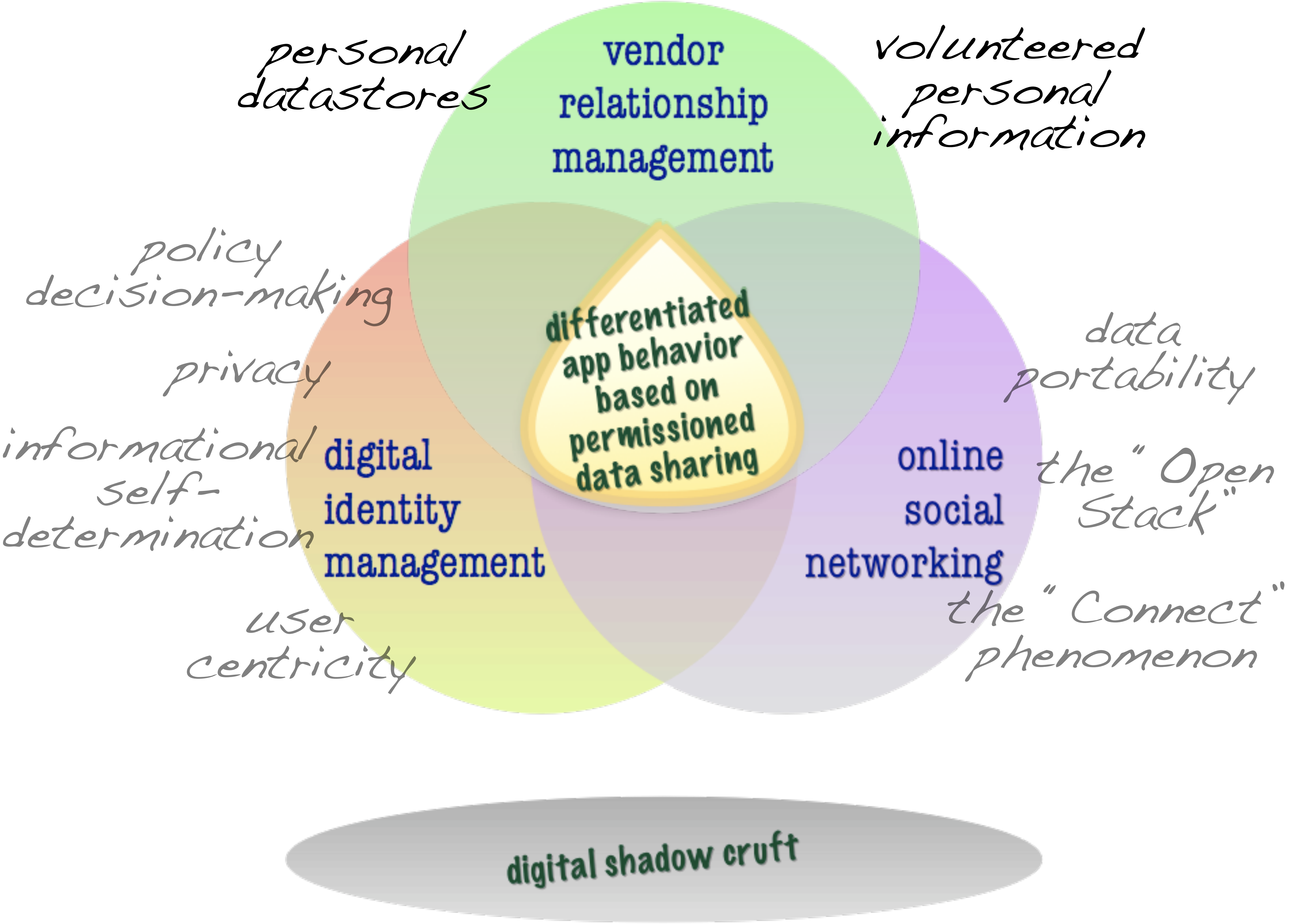
informational self-determination

user centricity

data portability

the " Open Stack"

the " Connect" phenomenon



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

online social networking

data portability

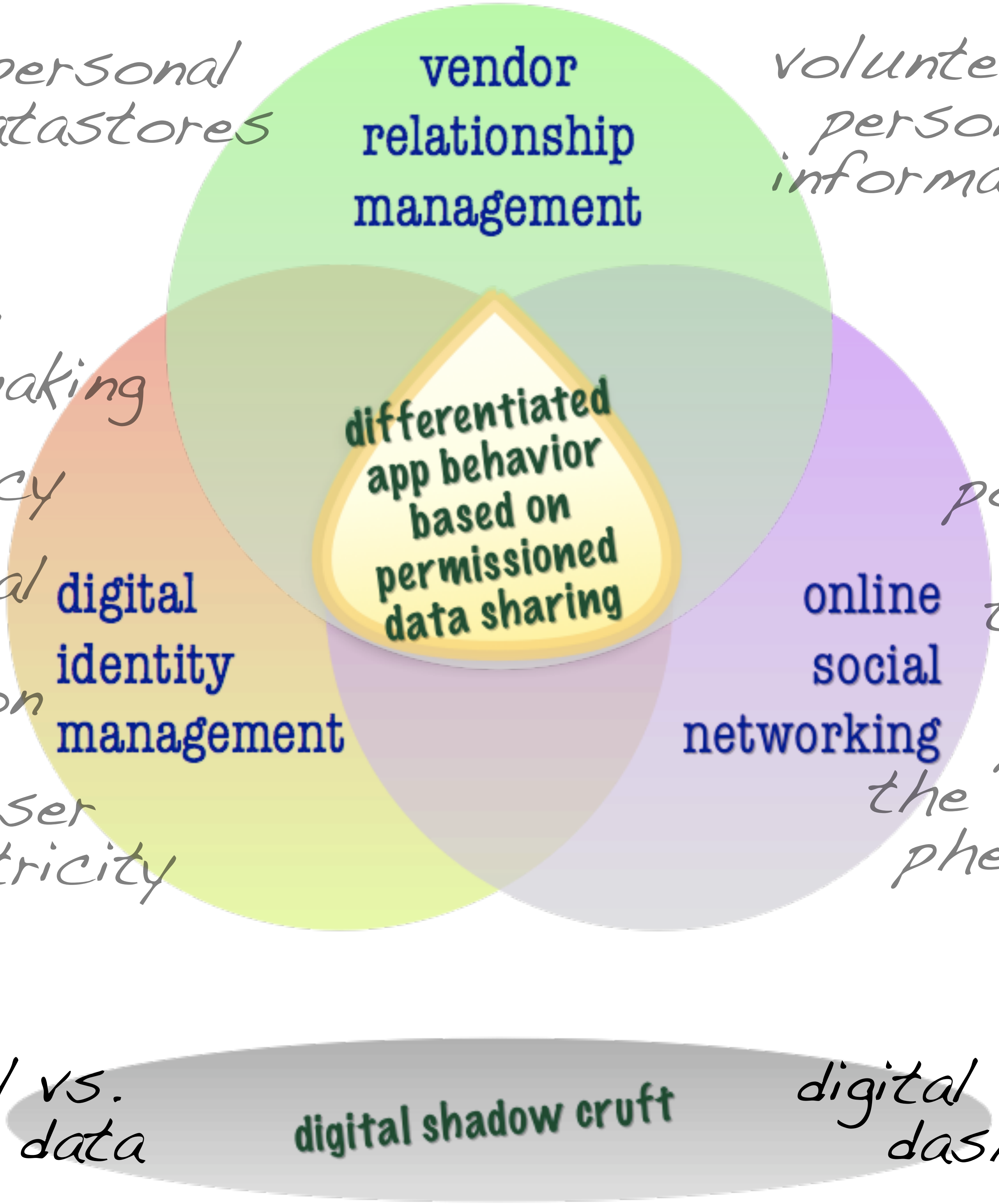
the "Open Stack"

the "Connect" phenomenon

user centricity

digital shadow cruft

personal
datastores



vendor
relationship
management

digital
identity
management

online
social
networking

differentiated
app behavior
based on
permissioned
data sharing

digital shadow cruft

volunteered
personal
information

policy
decision-making

privacy

informational
self-
determination

user
centricity

data
portability

the "Open
Stack"

the "Connect"
phenomenon

intentional vs.
behaviorial data

digital footprint
dashboard

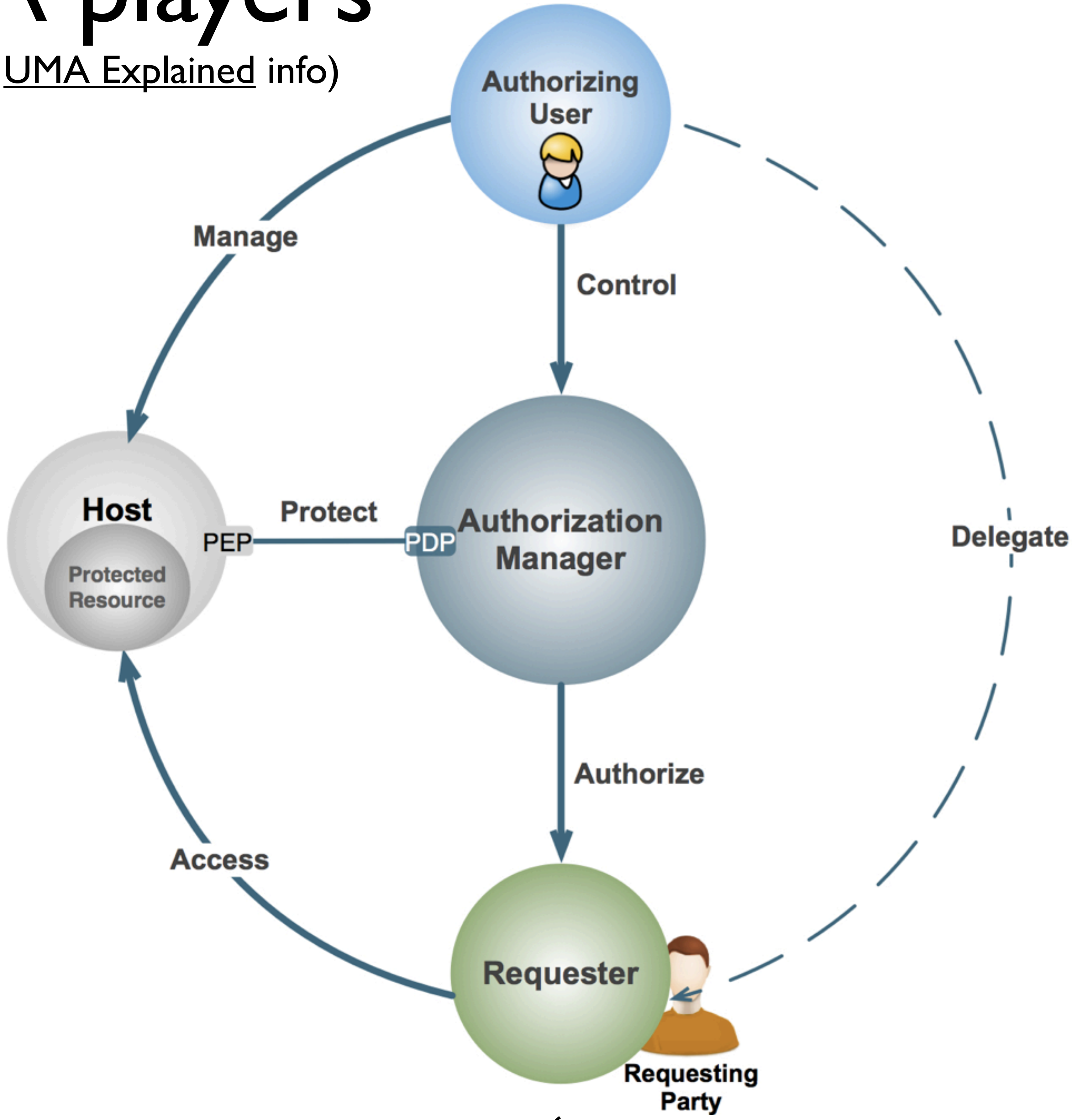
# UMA is...

- 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

| Selective sharing shortcomings | User-Managed Access solutions |
|---|---|
| Little sophistication and consistency in Web 2.0 access control – e.g., Google Calendar vs. Flickr vs. TripIt | A way for any web app to provide sophisticated access control merely by outsourcing it, à la SSO |
| Rules for selective sharing can't be applied to different apps – the "family" ACL has to keep being rebuilt | Selective-sharing policies can be mapped to content at multiple hosts |
| Selective sharing is largely identity-based and static | Conditions for access can be "claims-based", with claims tested when access is attempted – e.g., "anyone over 18" |
| Individual is only in a position to consent to sharing and to site terms of service, not dictate terms of access | Sharing policies form a barrier; requesting parties have to agree to terms or otherwise prove suitability |
| Individual can't get a global view of every party they've said can get access to their data and content | Sharing policies and sharing authorizations all come out of a single "hub" application |
| OAuth today only enables the protection of singular API endpoints for web services | Any Web resource with a URL, and any access scope on it, can be protected – e.g., sharing a status update API or a single tweet |

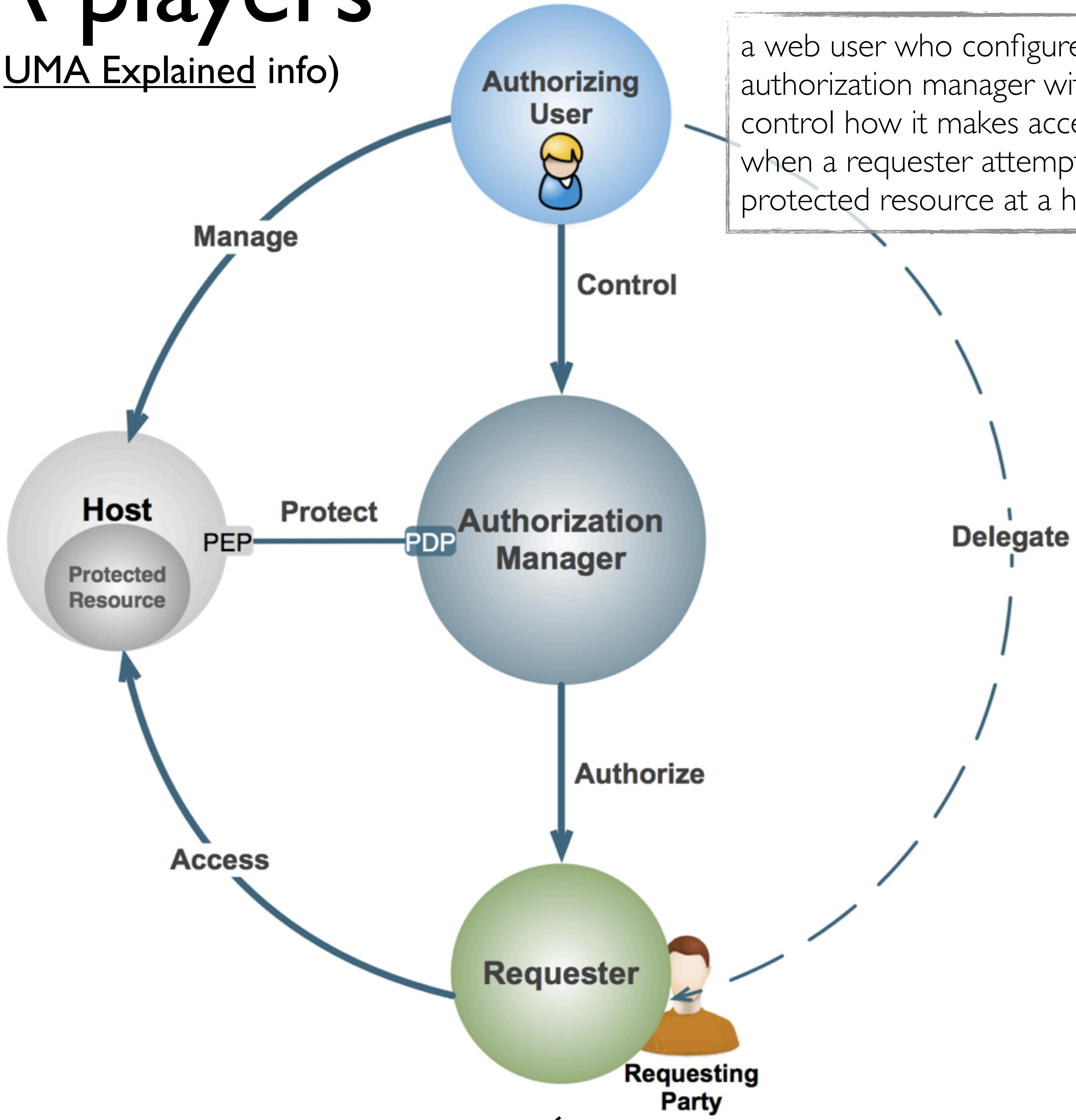
# UMA players

(see also UMA Explained info)



# UMA players

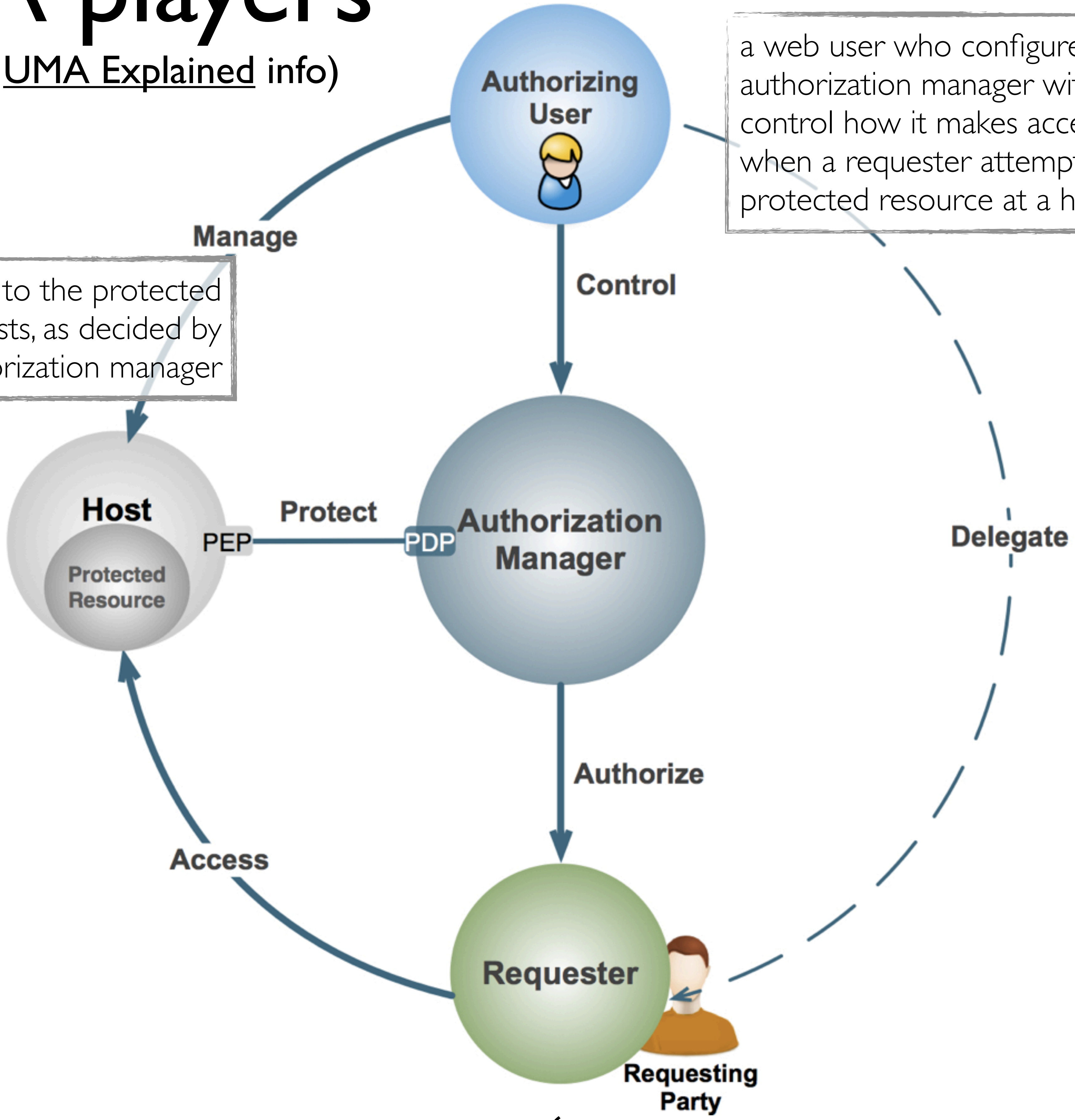
(see also UMA Explained info)



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

# UMA players

(see also UMA Explained info)

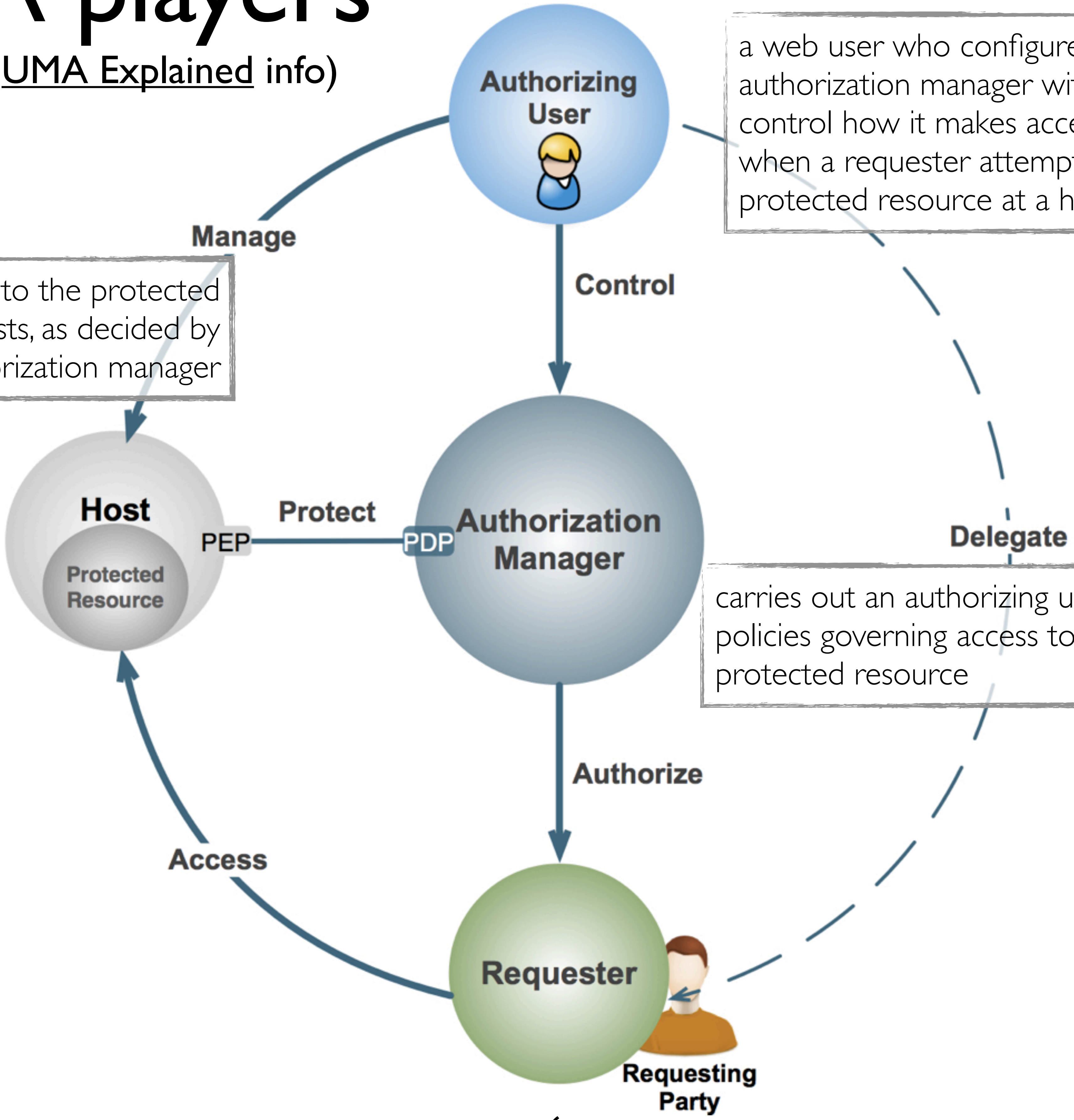


a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host

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

# UMA players

(see also UMA Explained info)



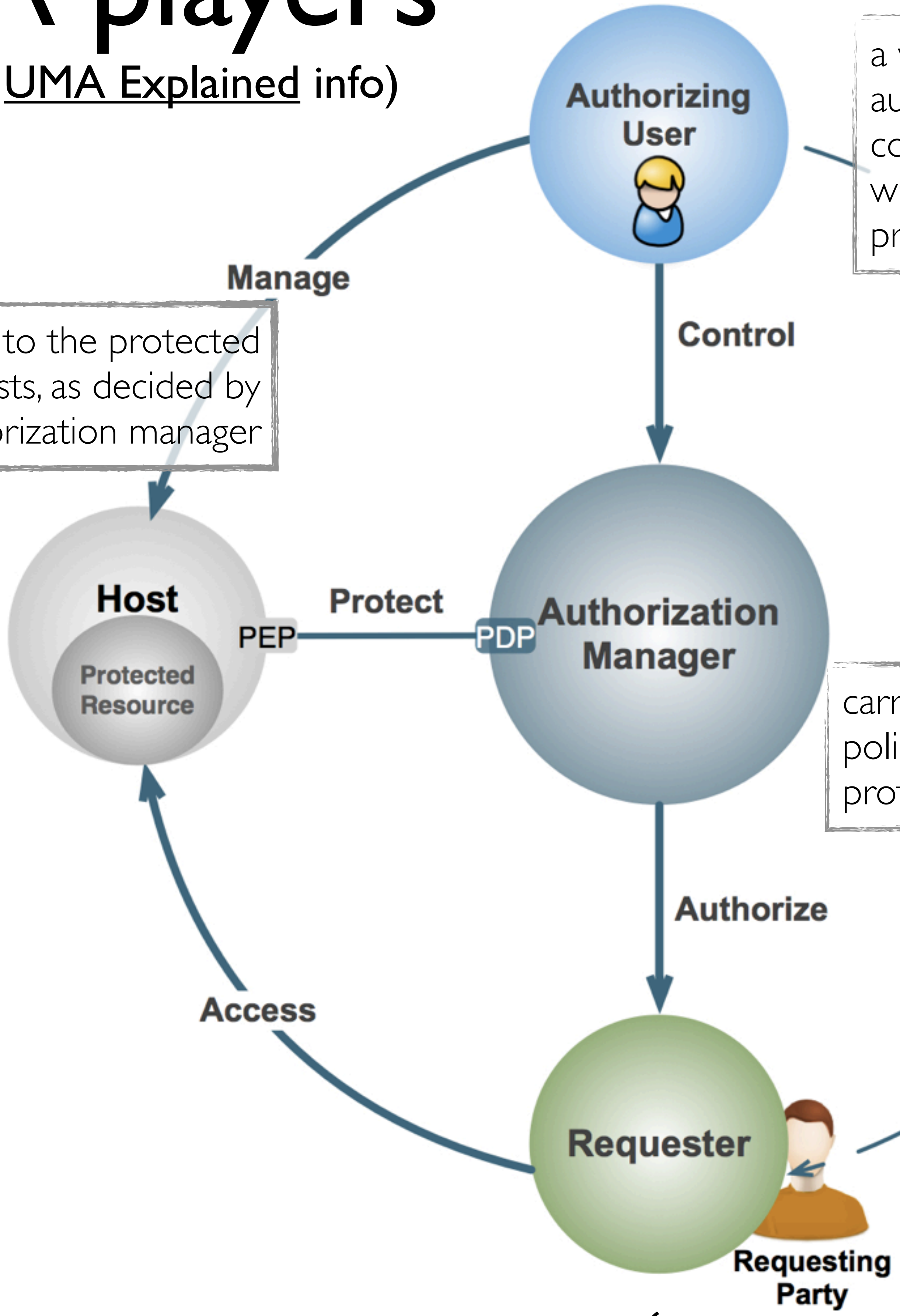
a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host

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

# 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

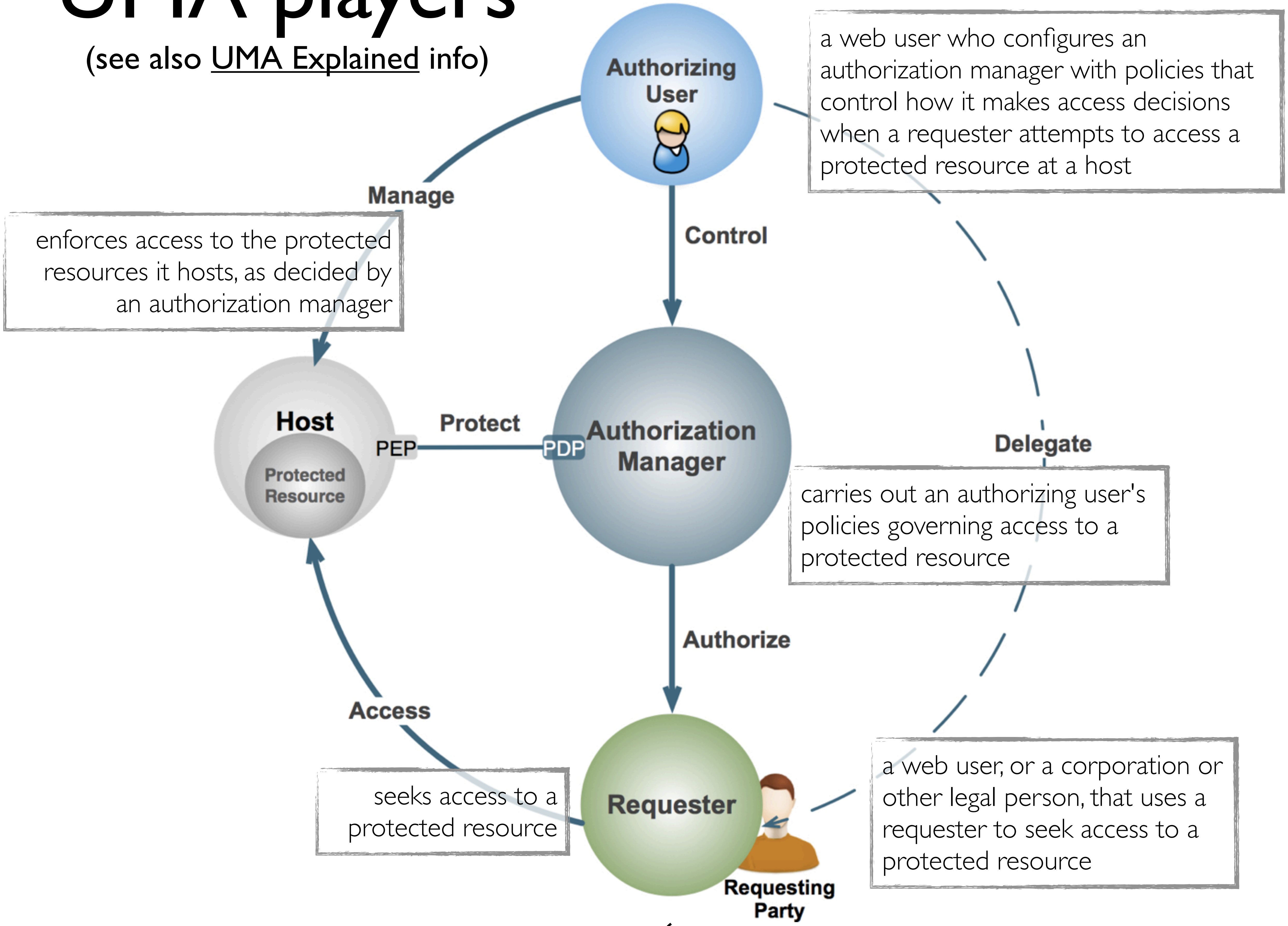
enforces access to the protected resources it hosts, as decided by an authorization manager

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

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

# 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

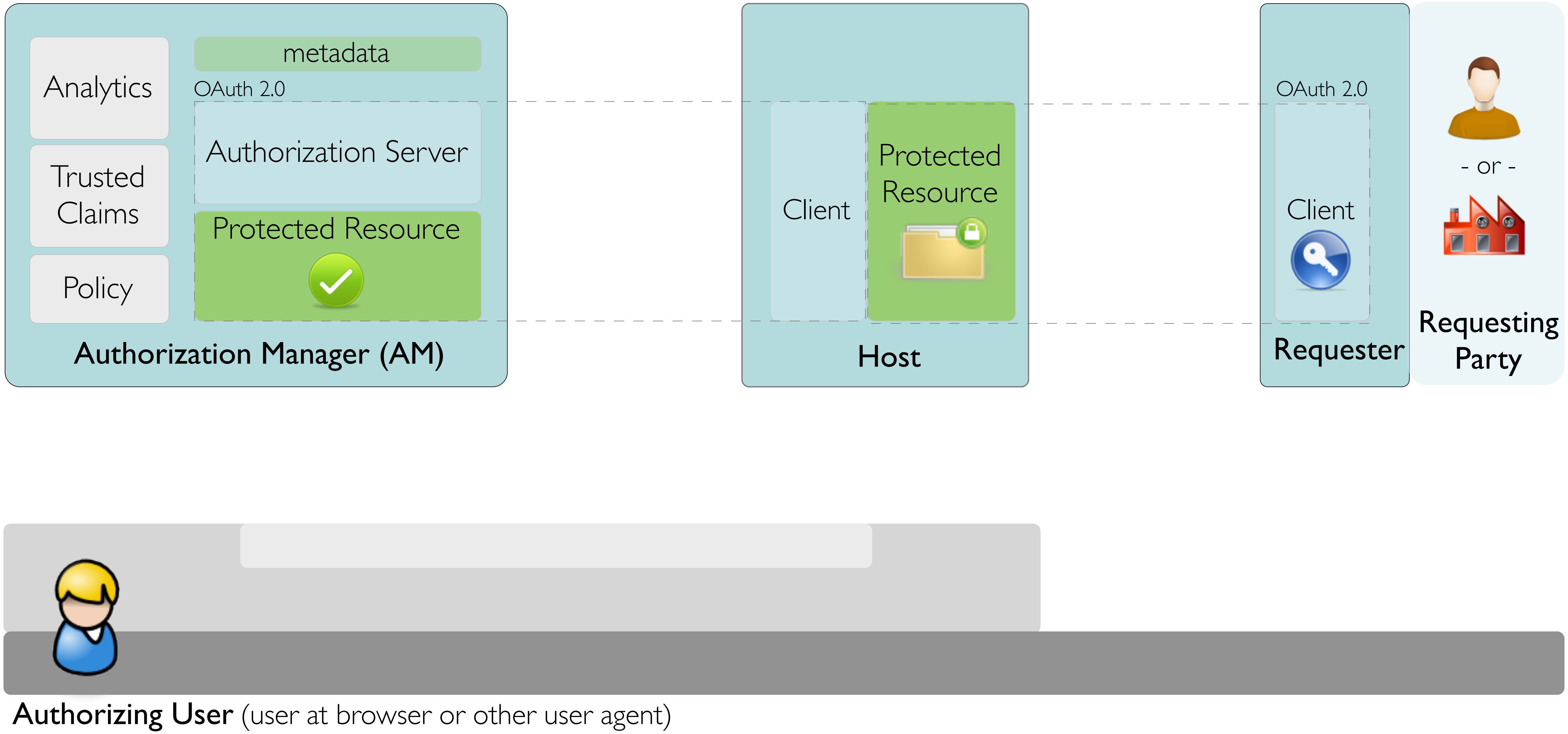
seeks access to a protected resource

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

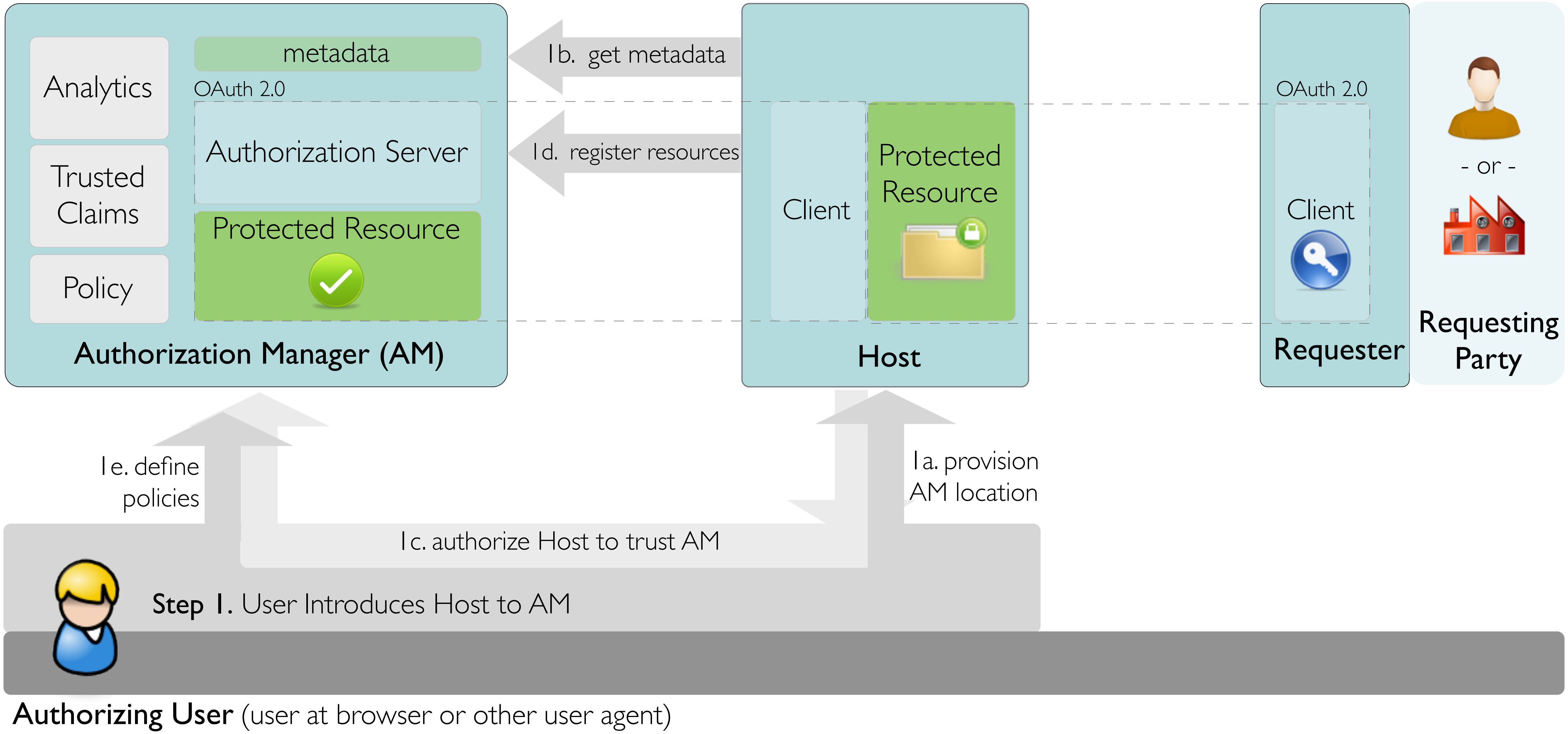
# UMA has three steps

1. Trust a token
   - Alice introduces her Calendar host to CopMonkey: "When CopMonkey says whether to let someone in, do what he says"
2. Get a token
   - A travel marketing company tries to subscribe to Alice's calendar but it has to agree to her terms of use: "All right, all right, I'm clicking the 'I Agree' button"
3. Use a token
   - The marketing company now has an OAuth access token to use at the Calendar host: "This means Alice thinks it's okay"

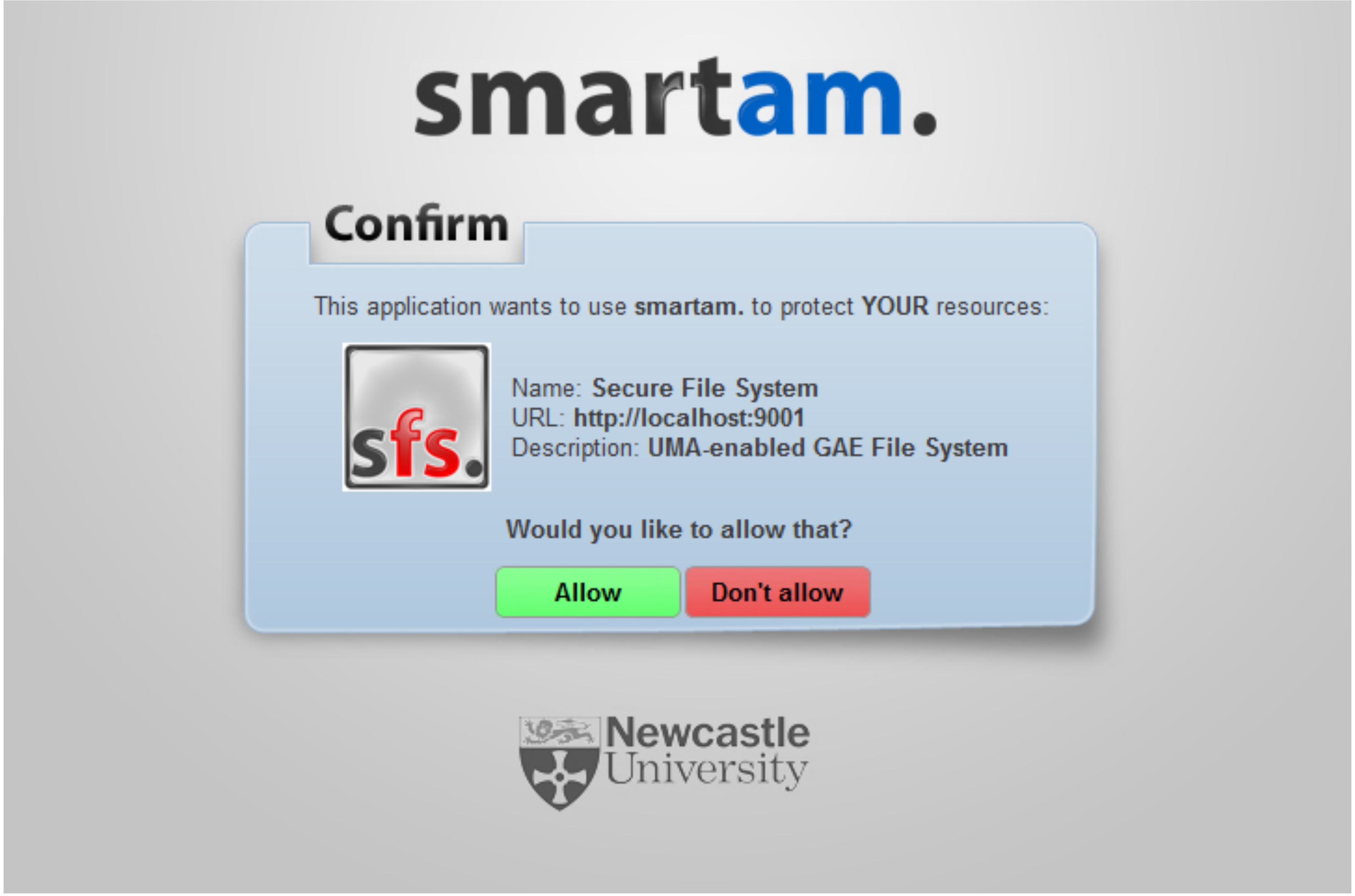
# The players again



# Step 1 protocol flow



# A possible UX for host-AM introduction



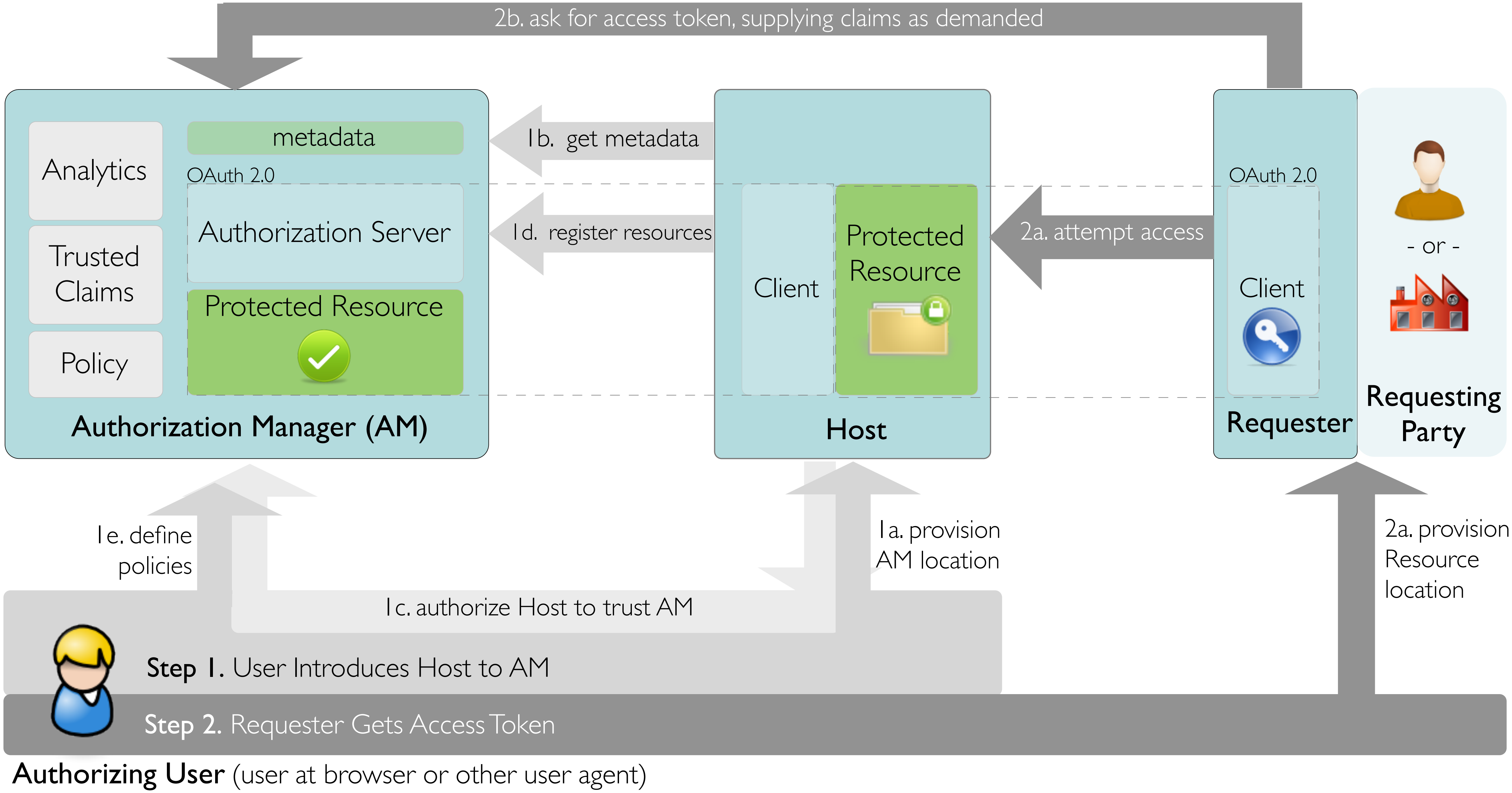
Confirm

This application wants to use **smartam.** to protect **YOUR** resources:

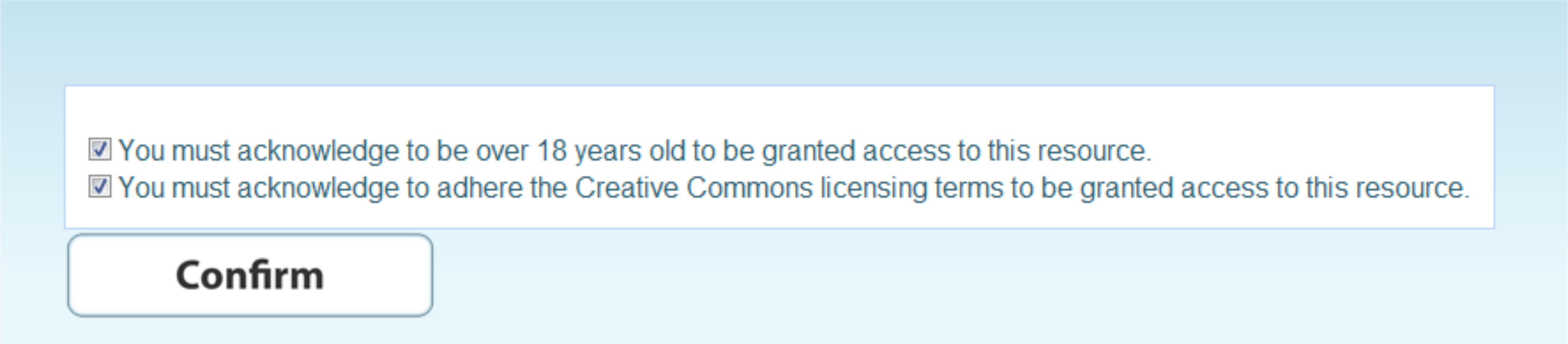
Name: **Secure File System**
URL: **http://localhost:9001**
Description: **UMA-enabled GAE File System**

**Would you like to allow that?**

# Step 2 protocol flow


2b. ask for access token, supplying claims as demanded
Analytics
Trusted Claims
Policy
metadata
OAuth 2.0
Authorization Server
Protected Resource
Authorization Manager (AM)
1b. get metadata
1d. register resources
Client
Protected Resource
Host
2a. attempt access
OAuth 2.0
Client
Requester
- or -
Requesting Party
1e. define policies
1a. provision AM location
2a. provision Resource location
1c. authorize Host to trust AM
Step 1. User Introduces Host to AM
Step 2. Requester Gets Access Token
Authorizing User (user at browser or other user agent)

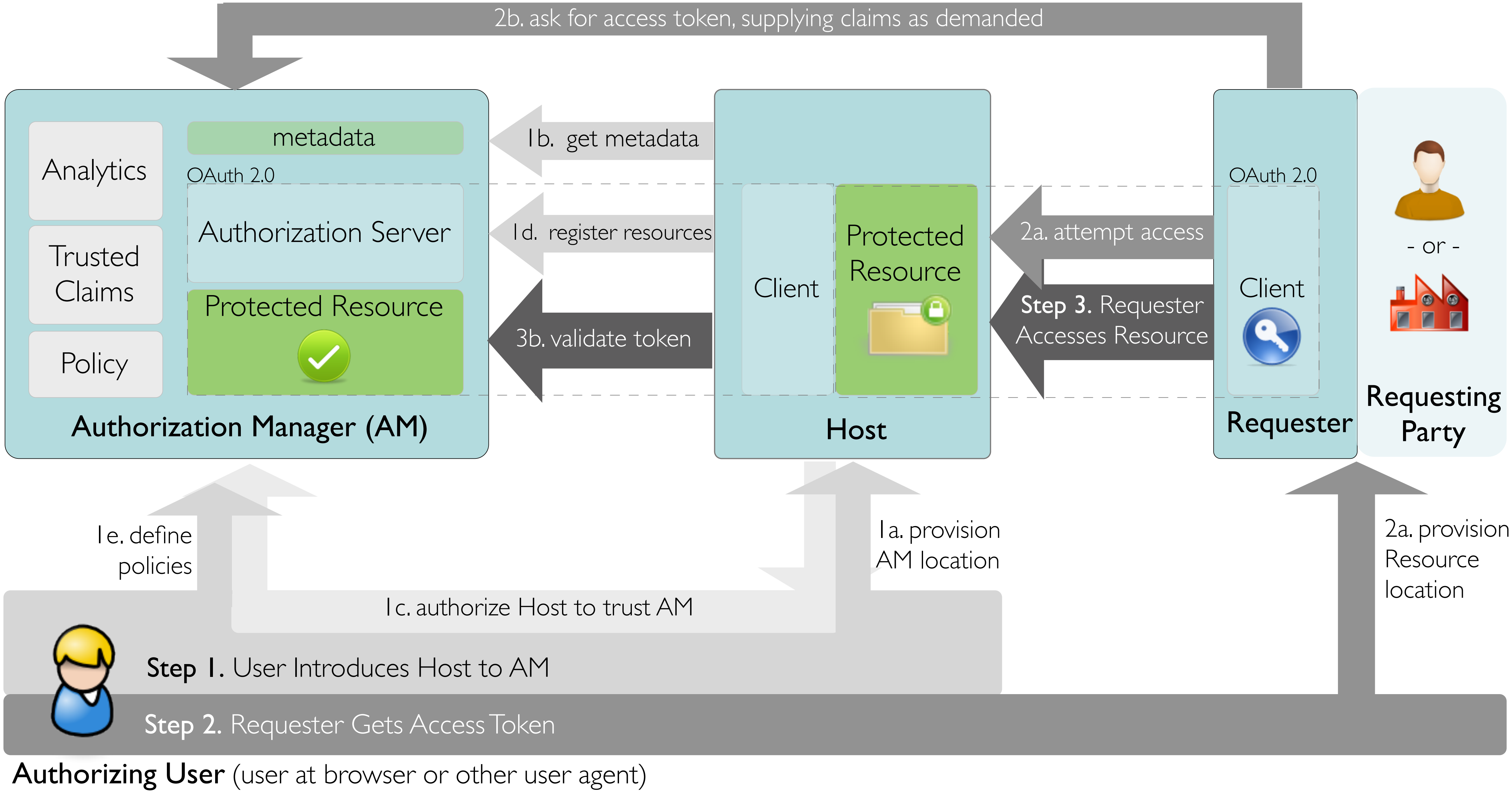
# A possible UX for self-asserted "promise" claims



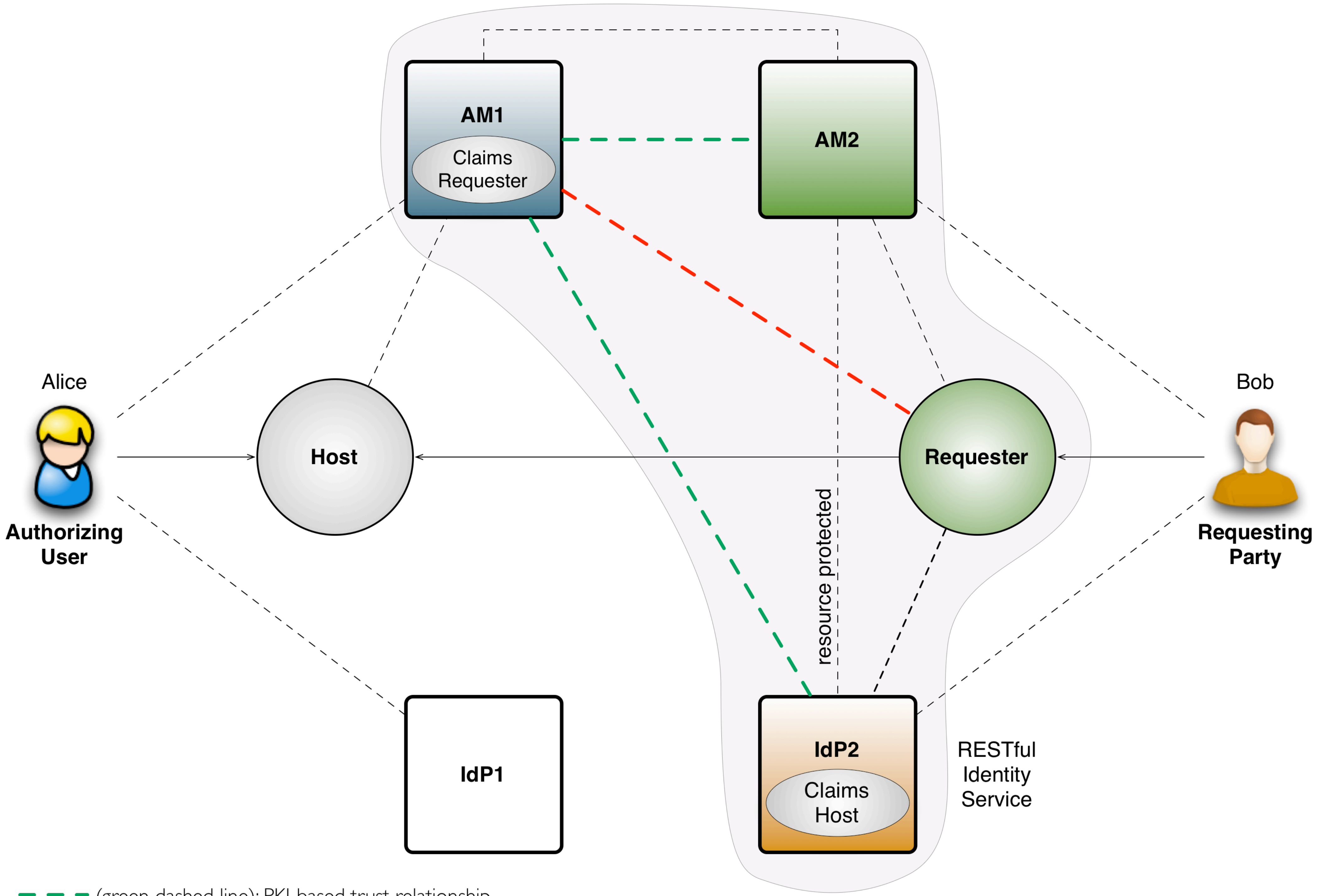
☑ You must acknowledge to be over 18 years old to be granted access to this resource.

☑ You must acknowledge to adhere the Creative Commons licensing terms to be granted access to this resource.

# Step 3 protocol flow


2b. ask for access token, supplying claims as demanded
Analytics
Trusted Claims
Policy
metadata
OAuth 2.0
Authorization Server
Protected Resource
Authorization Manager (AM)
1b. get metadata
1d. register resources
3b. validate token
Client
Protected Resource
Host
2a. attempt access
Step 3. Requester Accesses Resource
OAuth 2.0
Client
Requester
- or -
Requesting Party
1e. define policies
1a. provision AM location
2a. provision Resource location
1c. authorize Host to trust AM
Step 1. User Introduces Host to AM
Step 2. Requester Gets Access Token
Authorizing User (user at browser or other user agent)

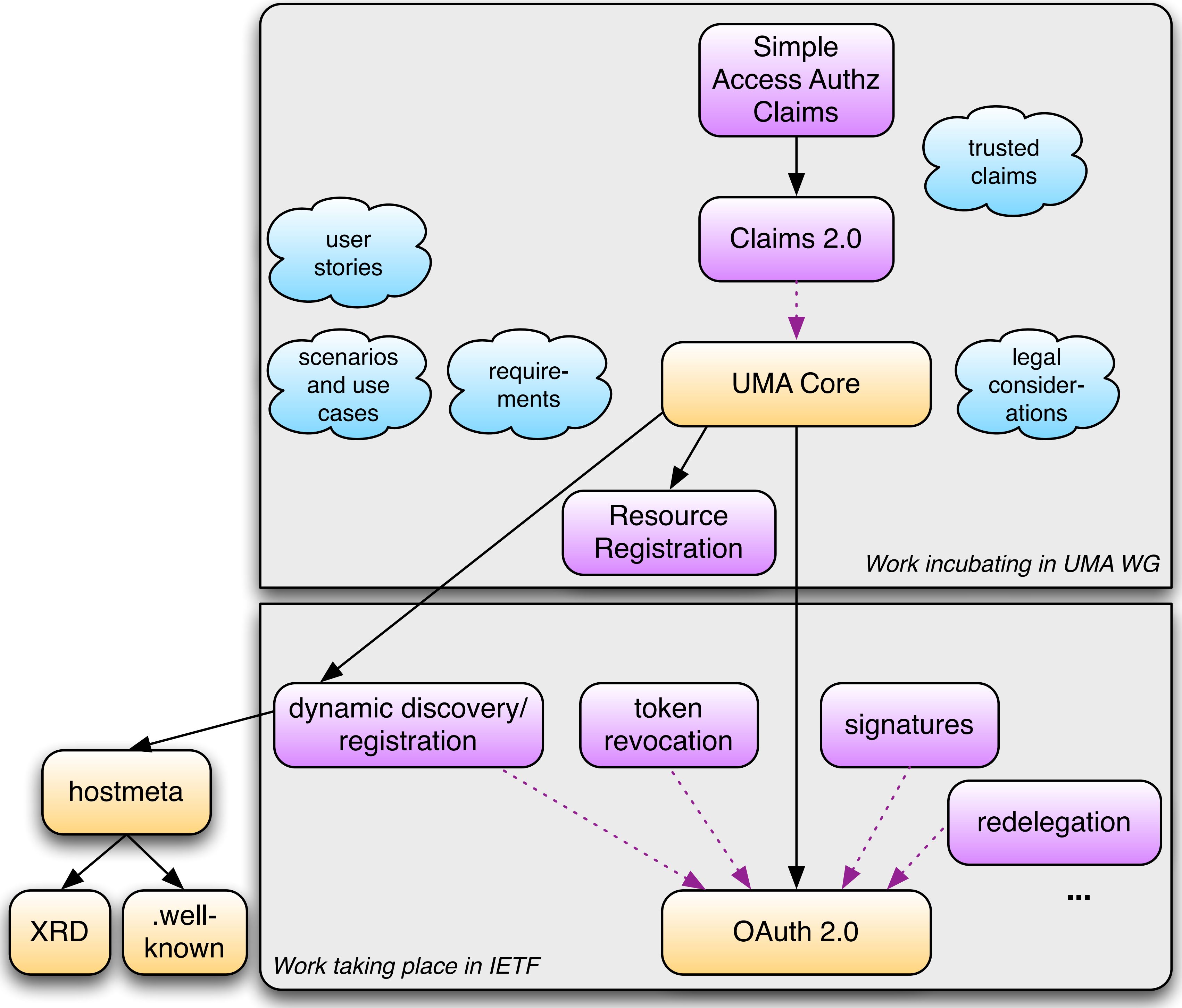
# A potential claims trust model: make them UMA-protected resources



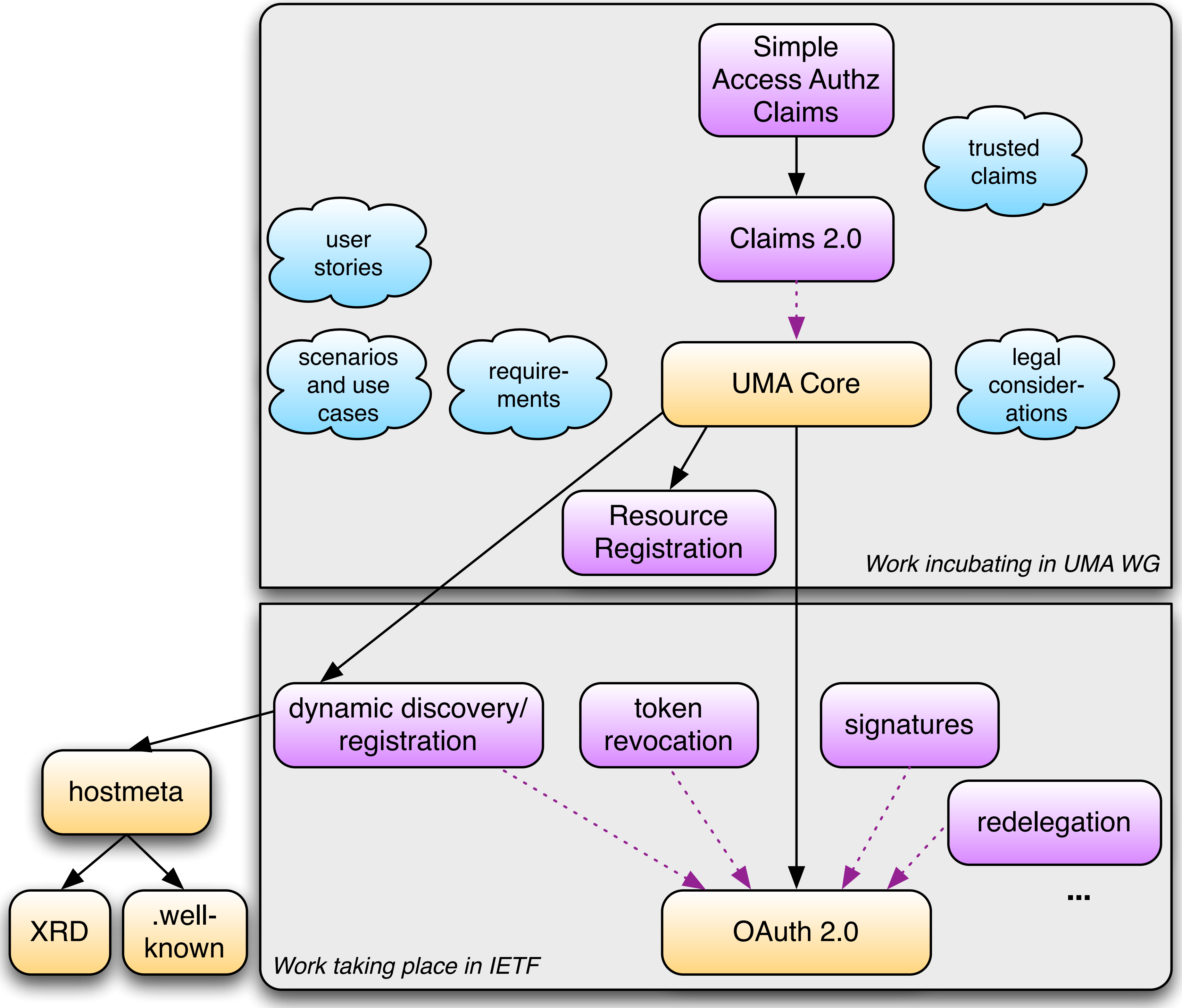
– – – (green dashed line): PKI-based trust relationship

– – – (red dashed line): untrusted

# Status of UMA development



# Status of UMA development



Newcastle University

OAUTH leeloo

kantara INITIATIVE

UMA Validator Bounty Program

# Thanks! Questions? Comments?

http://tinyurl.com/umawg