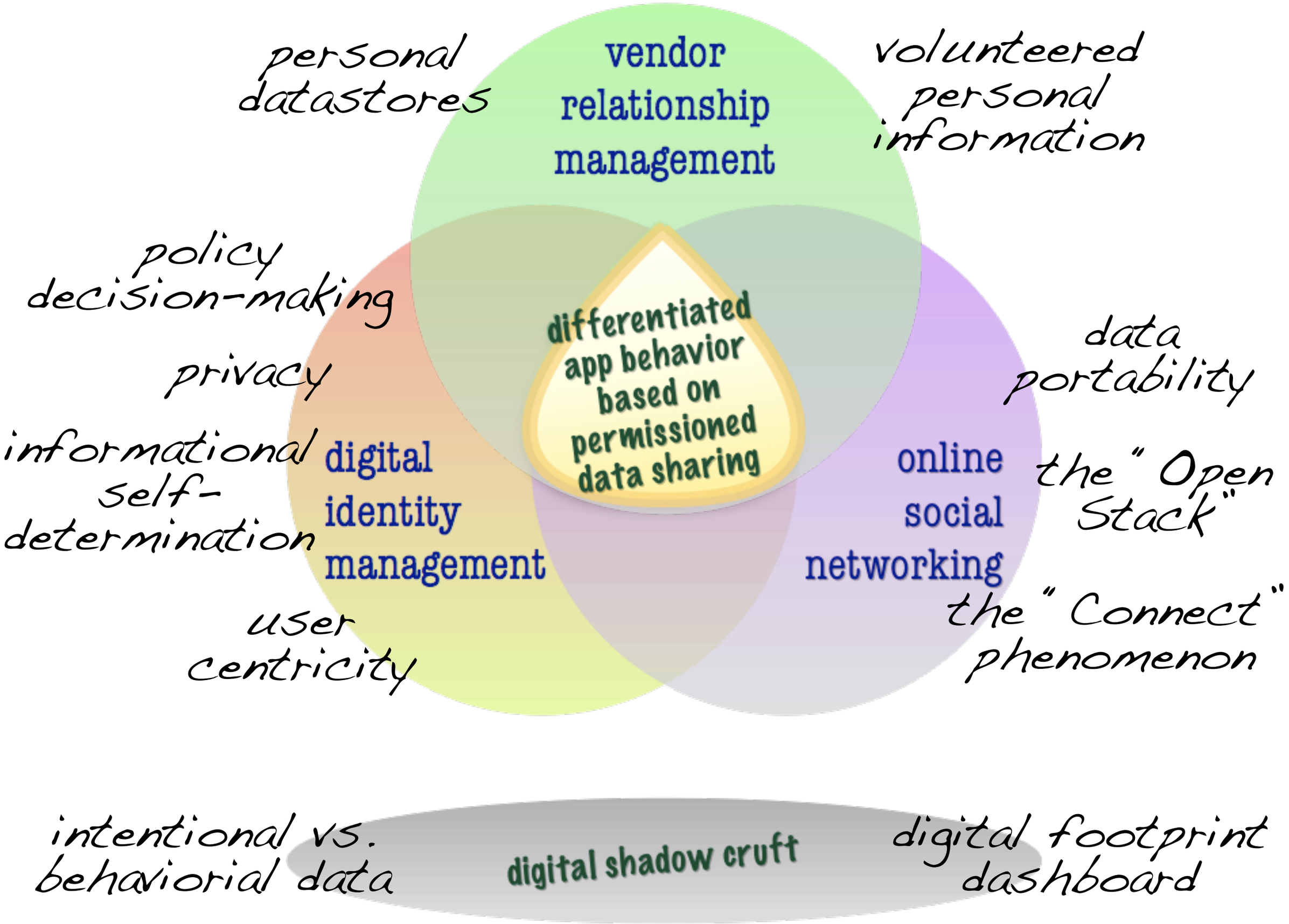
UMA Update

Eve Maler, Maciej Machulak, Łukasz Moreń

UMA Work Group

IIWX / May 2010

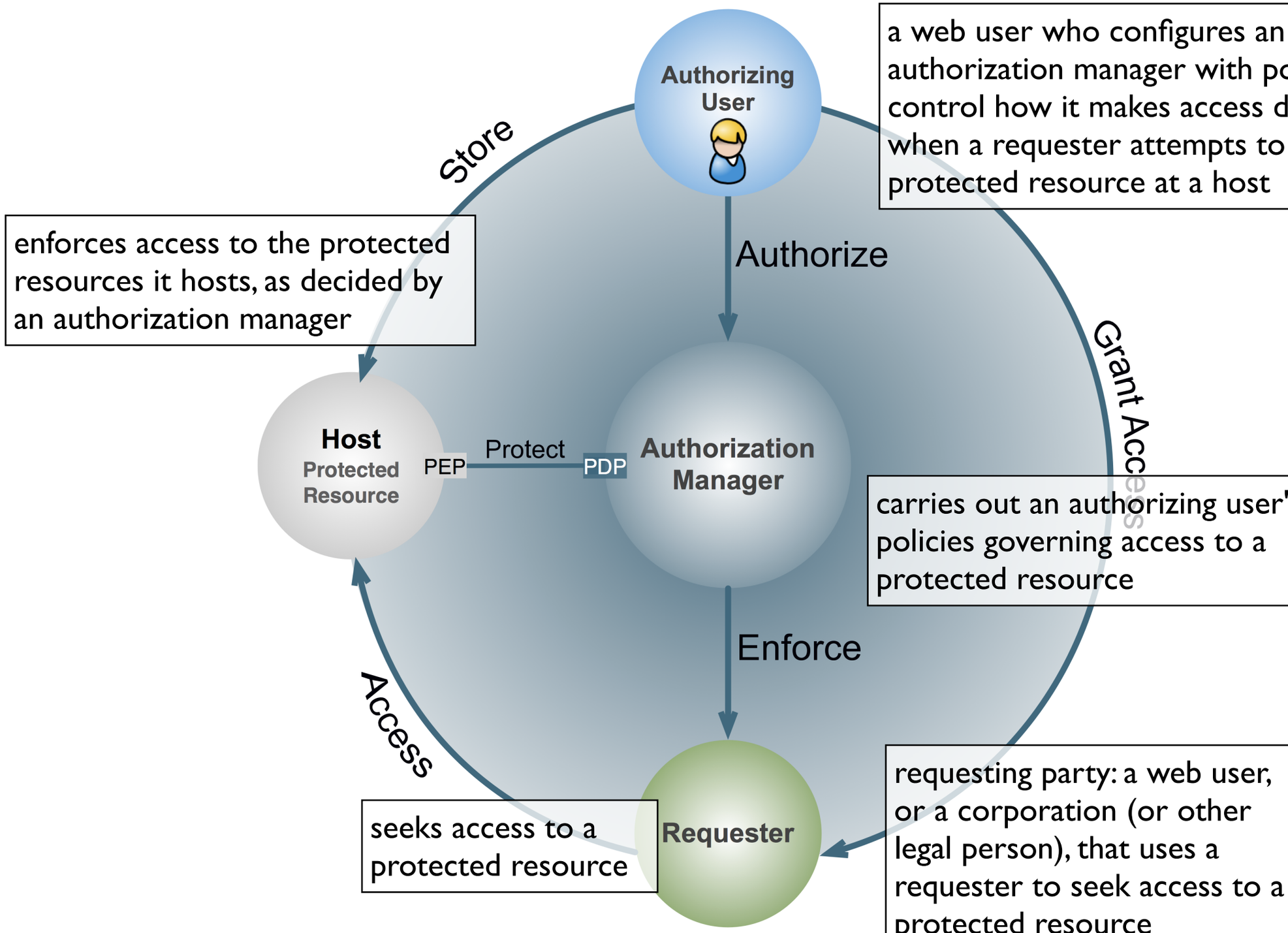

personal datastores
vendor relationship management
volunteered personal information
policy decision-making
privacy
informational self-determination
digital identity management
differentiated app behavior based on permissioned data sharing
data portability
online social networking
the "Open Stack"
user centricity
the "Connect" phenomenon
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
- Heading towards multiple implementation efforts
- Going to be contributed to the IETF
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly

The players

(definitions come from core protocol spec)



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

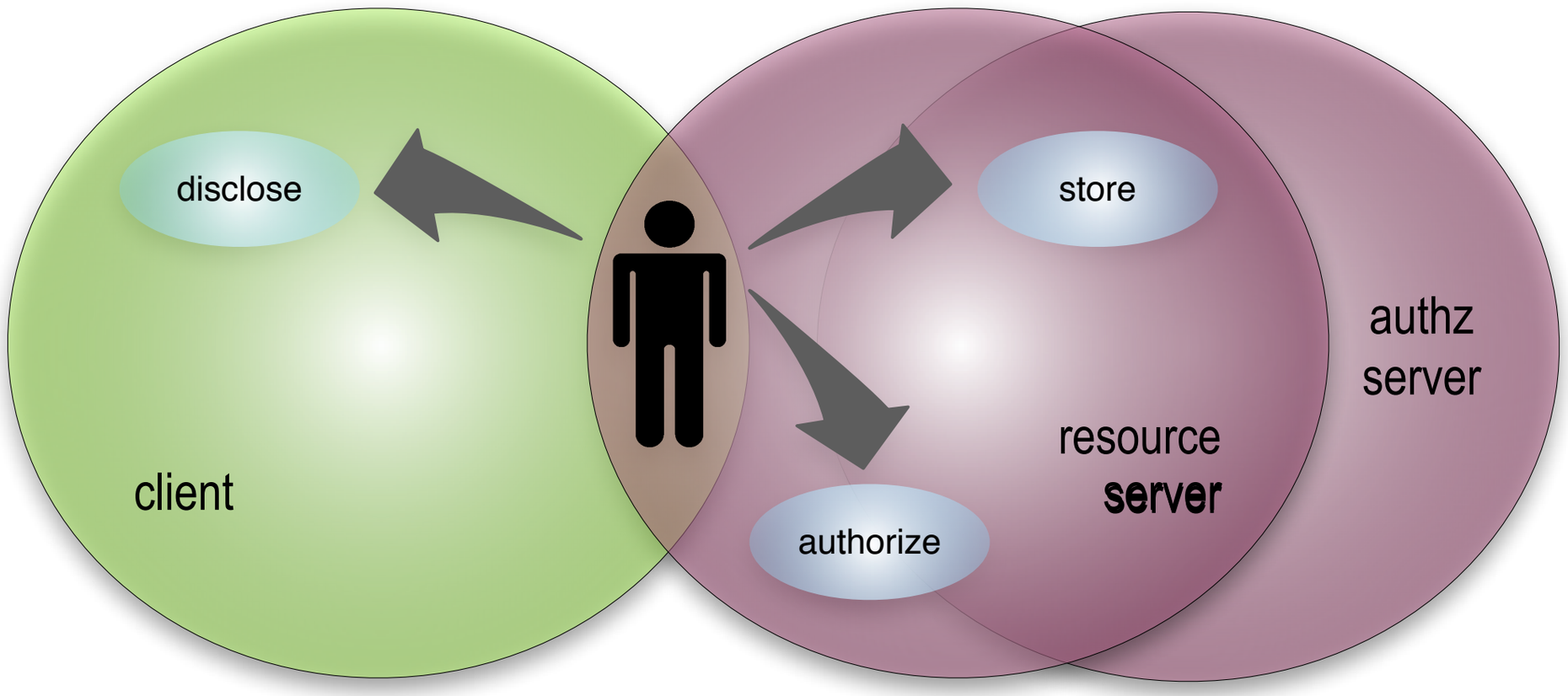
carries out an authorizing user's policies governing access to a protected resource

seeks access to a protected resource

requesting party: a web user, or a corporation (or other legal person), that uses a requester to seek access to a protected resource

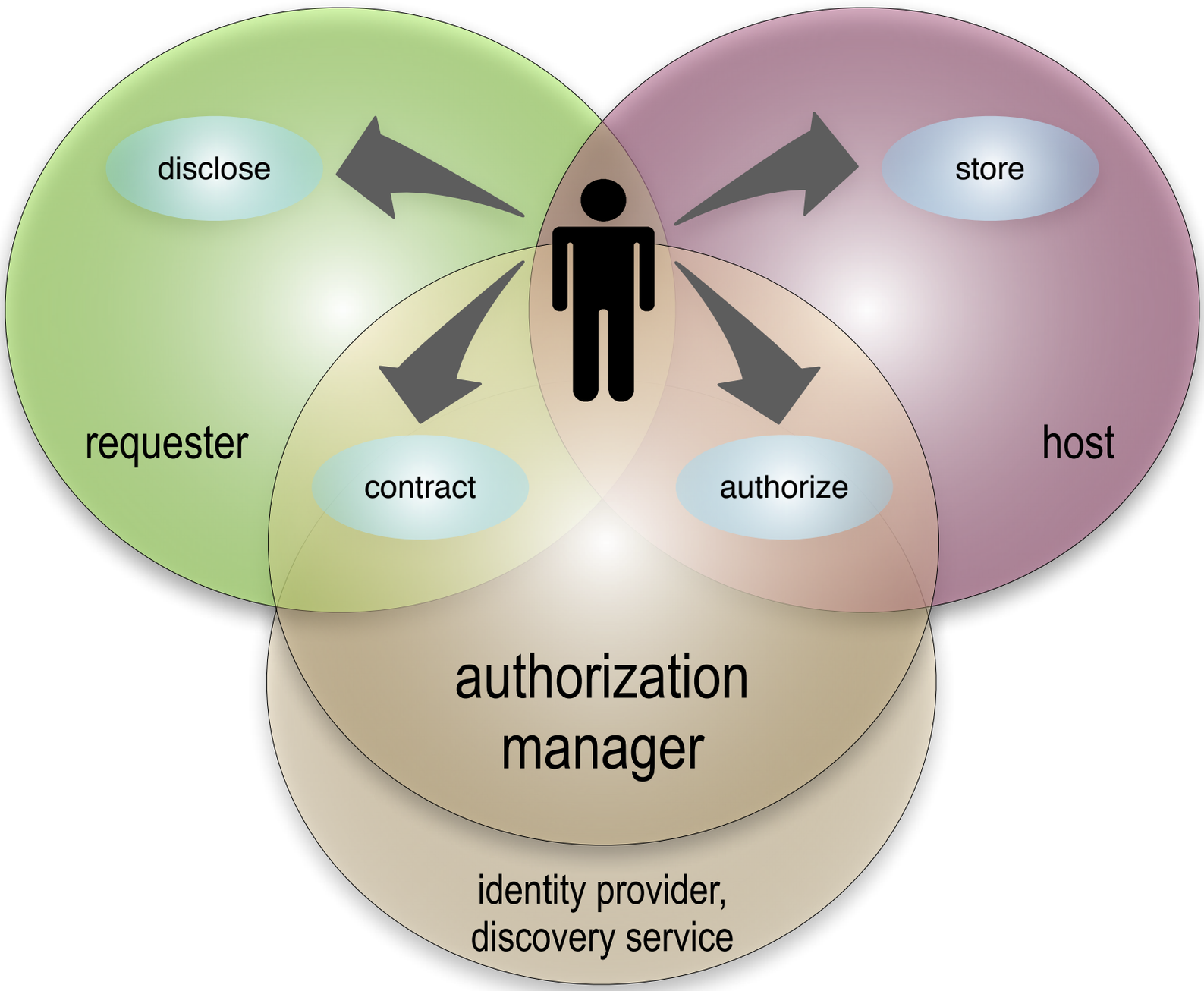
Comparing models

OAuth2 model



Comparing models

UMA model



Comparing OAuth2 and UMA: terms

• resource owner	➡ authorizing user
• resource server	➡ host
• authorization server	➡ authorization manager
• client	➡ requester

Comparing OAuth2 and UMA: concepts

- There is one resource owner in the picture, on "both sides"
- The resource server respects access tokens from "its" authz server
- The authz server issues access tokens based on the client's ability to authenticate

➡ The authorizing user may be granting access to a truly autonomous party

➡ The host outsources authz jobs to an authz manager chosen by the user

➡ The authz manager issues tokens based on user policy and "claims" conveyed by the requester

Comparing OAuth2 and UMA: dynamic trust

- The client and server sides must meet outside the resource-owner context ahead of time

➡ A requester can walk up to a protected resource and attempt to get access without registering first

- The resource server meets its authz server ahead of time and is tightly coupled with it

➡ The authz user can mediate the introduction of each of his hosts to the authz manager he wants it to use

- The resource server validates tokens in an unspecified manner, assumed locally

➡ The host has the option of asking the authz manager to validate tokens in real time

Comparing OAuth2 and UMA: protocol

- Two major steps: token-getting (with multiple flow options) and token-using

➡ Three major steps: host/authz manager introduction (trust), token-getting, and token-using

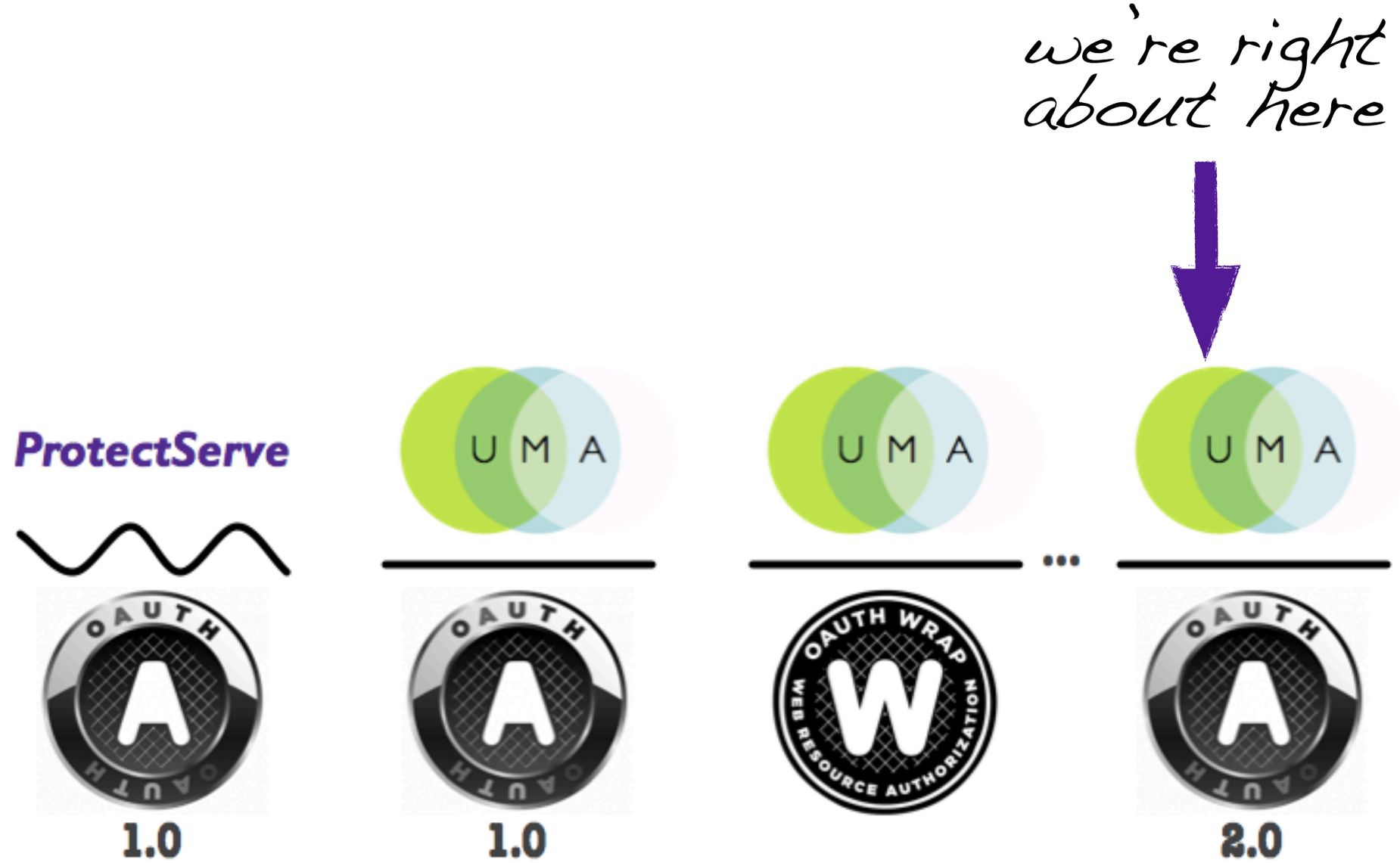
- User delegation flows and autonomous client flows

➡ Profiles (TBD) of OAuth flows that add requests for claims and claim responses

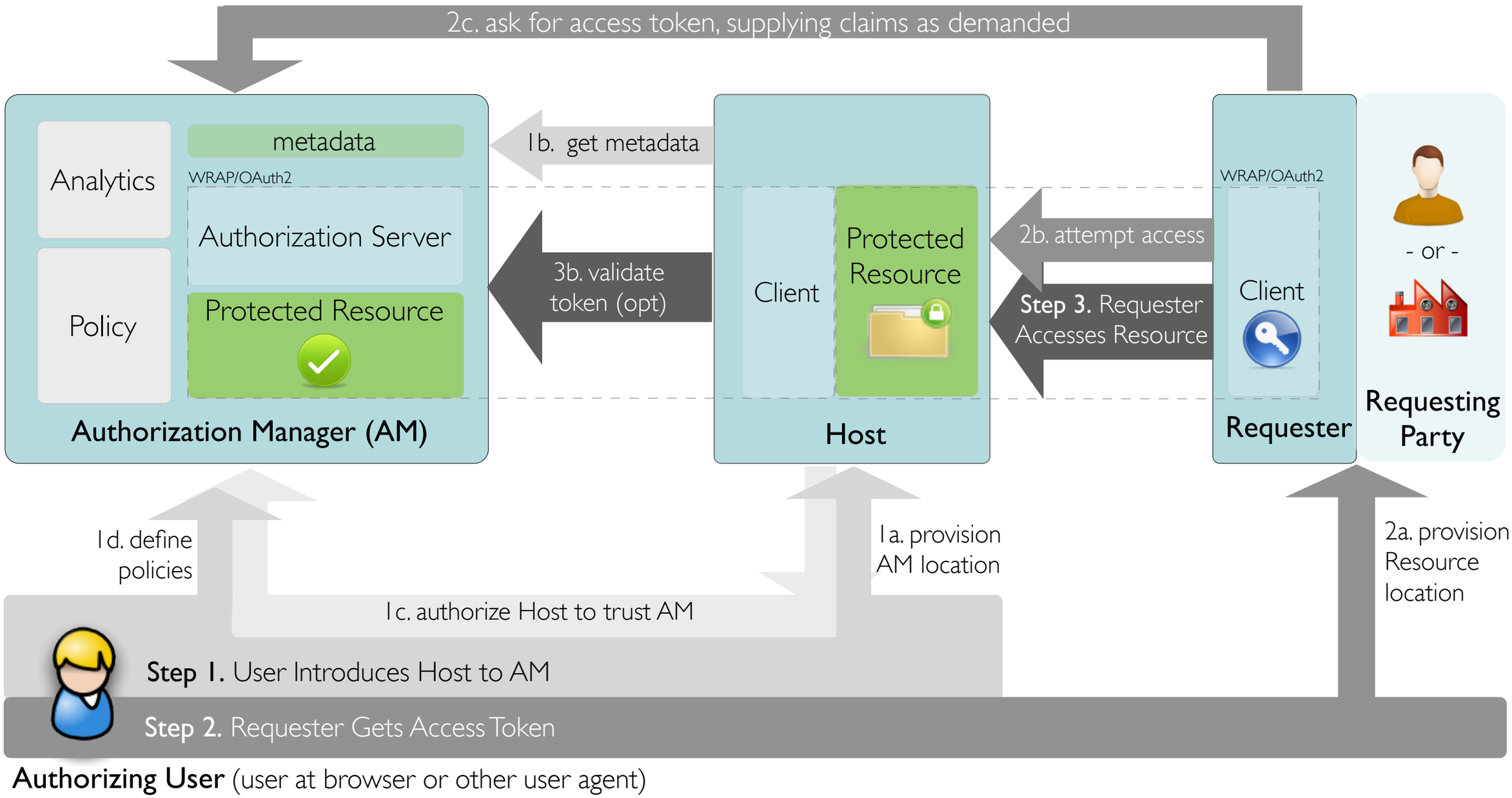
- Resource and authz servers are generally not expected to communicate directly vs. through the token

➡ Authz manager gives host its own access token; host uses it to supply resource details and request token validation

UMA's history with OAuth



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



Policies can be unilateral or can require claims

- Unilateral:
  - "Allow access for a week"
- Claims-requiring:
  - "Allow access to anyone who agrees to my licensing terms" (*promissory* statement)
  - "Allow access to someone who can prove themselves to be bob@gmail.com" (*affirmative* statement)
  - "Allow access to anyone who says they're 18 or older" (*affirmative* statement)

About Kantara Initiative

http://kantarainitiative.org

- **Participation:** Open global identity, web, and developer community of individuals and organizations, such as:
  - Deployers, operators, Web 2.0 service providers, eGovernment agencies, IT vendors, consumer electronics vendors
  - Developers and members of the open source, legal, and privacy communities
- **Goal:** Harmonize identity community activities to help ensure secure, identity-based, online interactions
  - While preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments.
- **Work:** 18 Work Groups and Discussion Groups (including UMA) and two certification oversight bodies (Assurance and Interop)

How to participate

- It's absolutely free to participate in any group
  - You can also support the overall goals of the Initiative with an individual or organizational Membership
- Today is a public workshop
  - You are invited to become an UMA WG participant ("UMAnitarian"!) to contribute actively to our work
  - To become a participant right now, visit **kantarainitiative.org**, select the User-Managed Access Group, and click on Join This Group
    - We operate under reciprocal royalty-free rules