Implementation of User-Managed Access Framework for Web 2.0 Applications

Lukasz Moren, Maciej Machulak, Aad van Moorsel
Newcastle University

Outline

- Data Sharing on the Web
  - Current models
  - Shortcomings
- User-Managed Access
  - Architecture
  - Protocol
- UMA/j framework
  - Demo
  - Architecture
  - Existing technologies

Classic Web model

Name	
Street Address	
City	
State	Enter Text
Zip/Postal	
Province	
Country	Enter Text
Phone	
Email	
Preferred Communication	◯ Postal Mail ◯ Phone ◯ E-mail

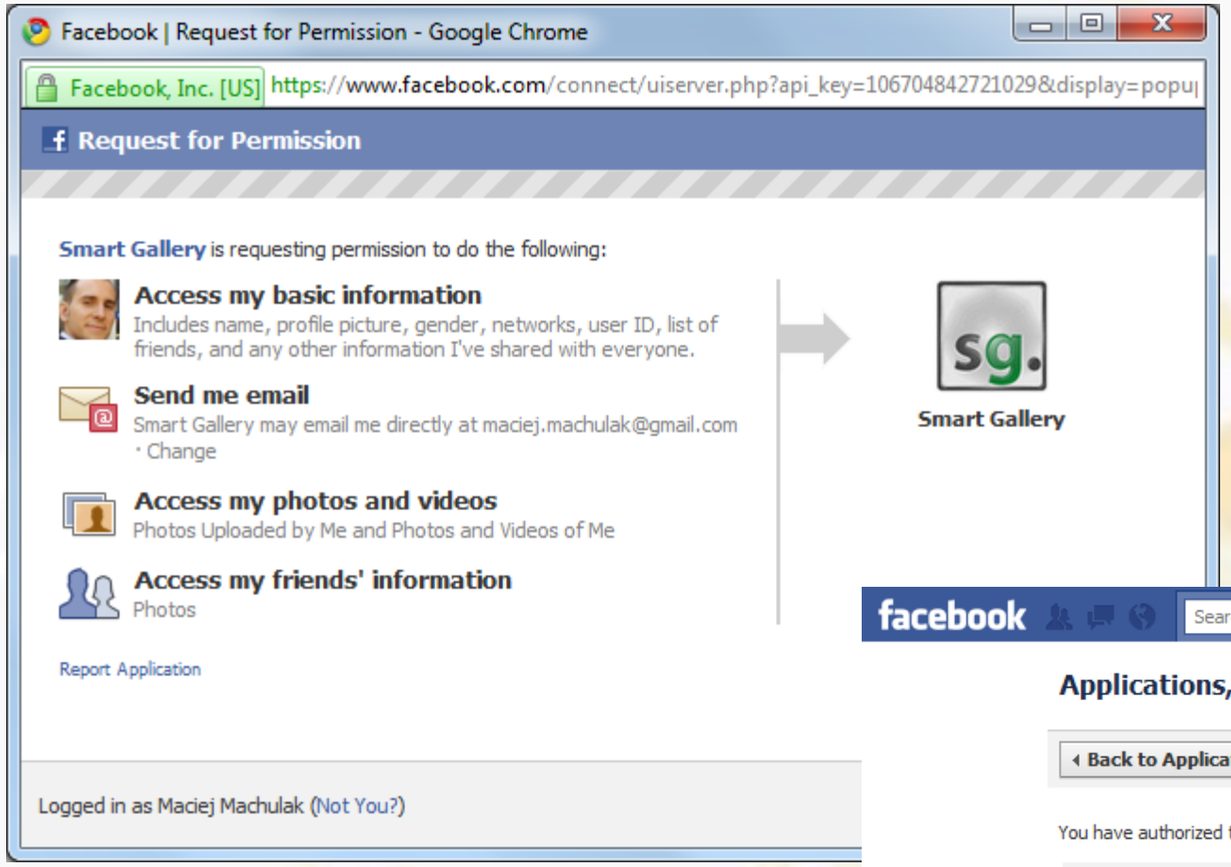
Upload Photos to: **New Photo Album**

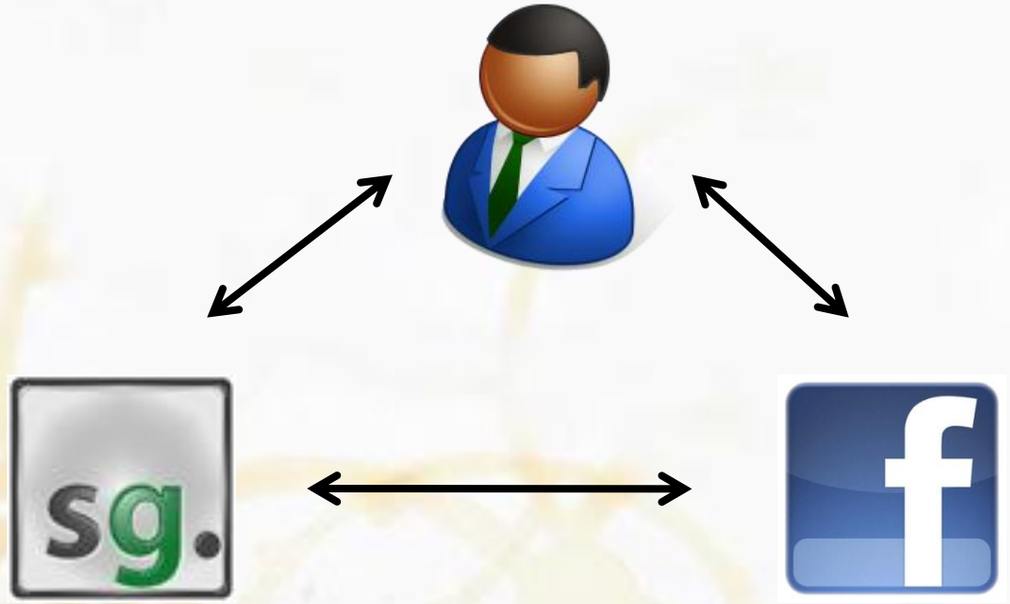
Select photos to upload — Clear All — Cancel

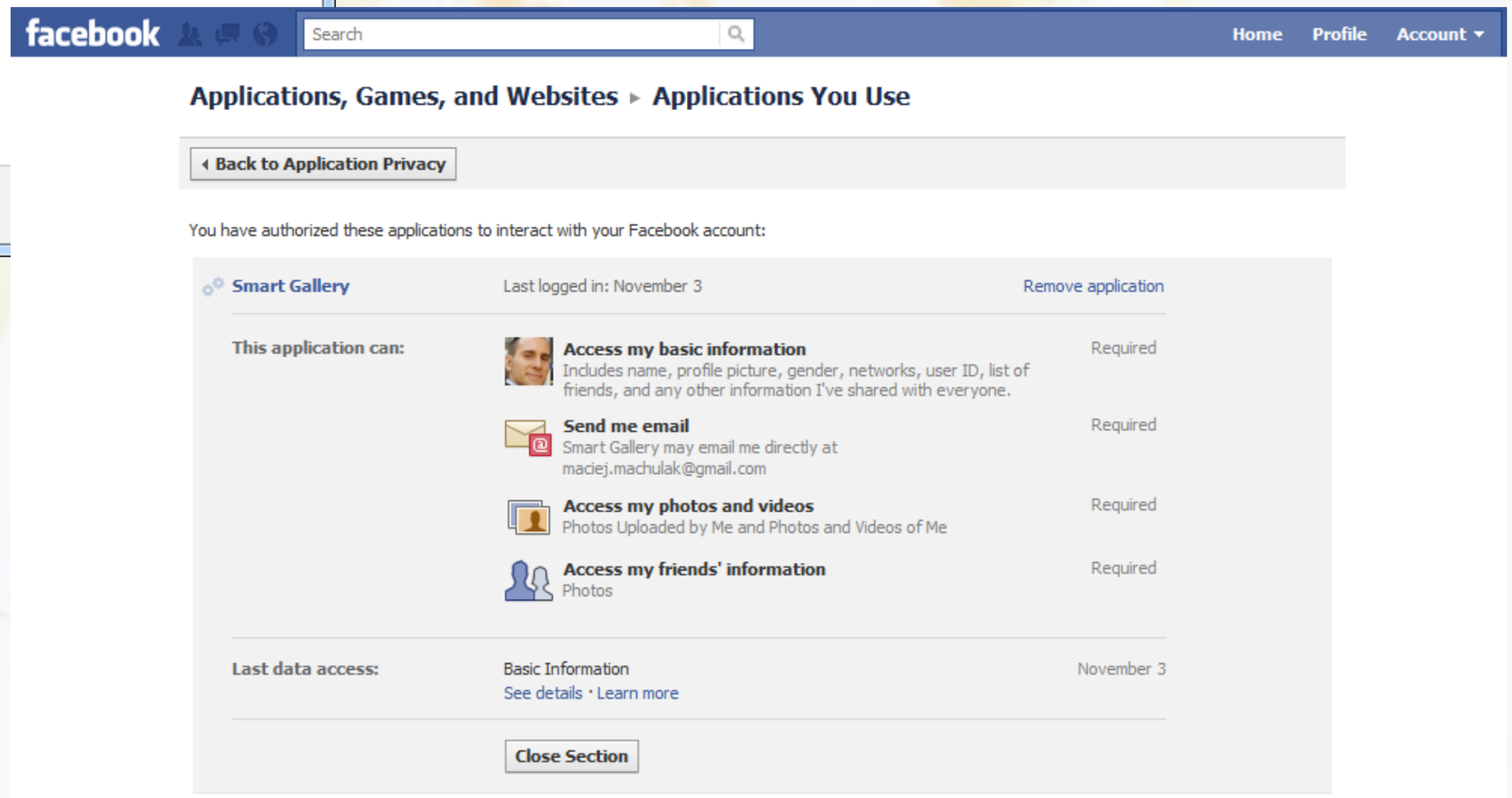
Choose File No file chosen
Choose File No file chosen
Choose File No file chosen
Choose File No file chosen
Choose File No file chosen

Start Upload

OAuth 2.0


Facebook | Request for Permission - Google Chrome
Facebook, Inc. [US] https://www.facebook.com/connect/uiserver.php?api_key=106704842721029&display=popu
Request for Permission
Smart Gallery is requesting permission to do the following:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.
Send me email
Smart Gallery may email me directly at maciej.machulak@gmail.com · Change
Access my photos and videos
Photos Uploaded by Me and Photos and Videos of Me
Access my friends' information
Photos
Smart Gallery
Report Application
Logged in as Maciej Machulak (Not You?)




facebook
Search
Home
Profile
Account
Applications, Games, and Websites ▸ Applications You Use
Back to Application Privacy
You have authorized these applications to interact with your Facebook account:
Smart Gallery
Last logged in: November 3
Remove application
This application can:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.
Required
Send me email
Smart Gallery may email me directly at maciej.machulak@gmail.com
Required
Access my photos and videos
Photos Uploaded by Me and Photos and Videos of Me
Required
Access my friends' information
Photos
Required
Last data access:
Basic Information
See details · Learn more
November 3
Close Section

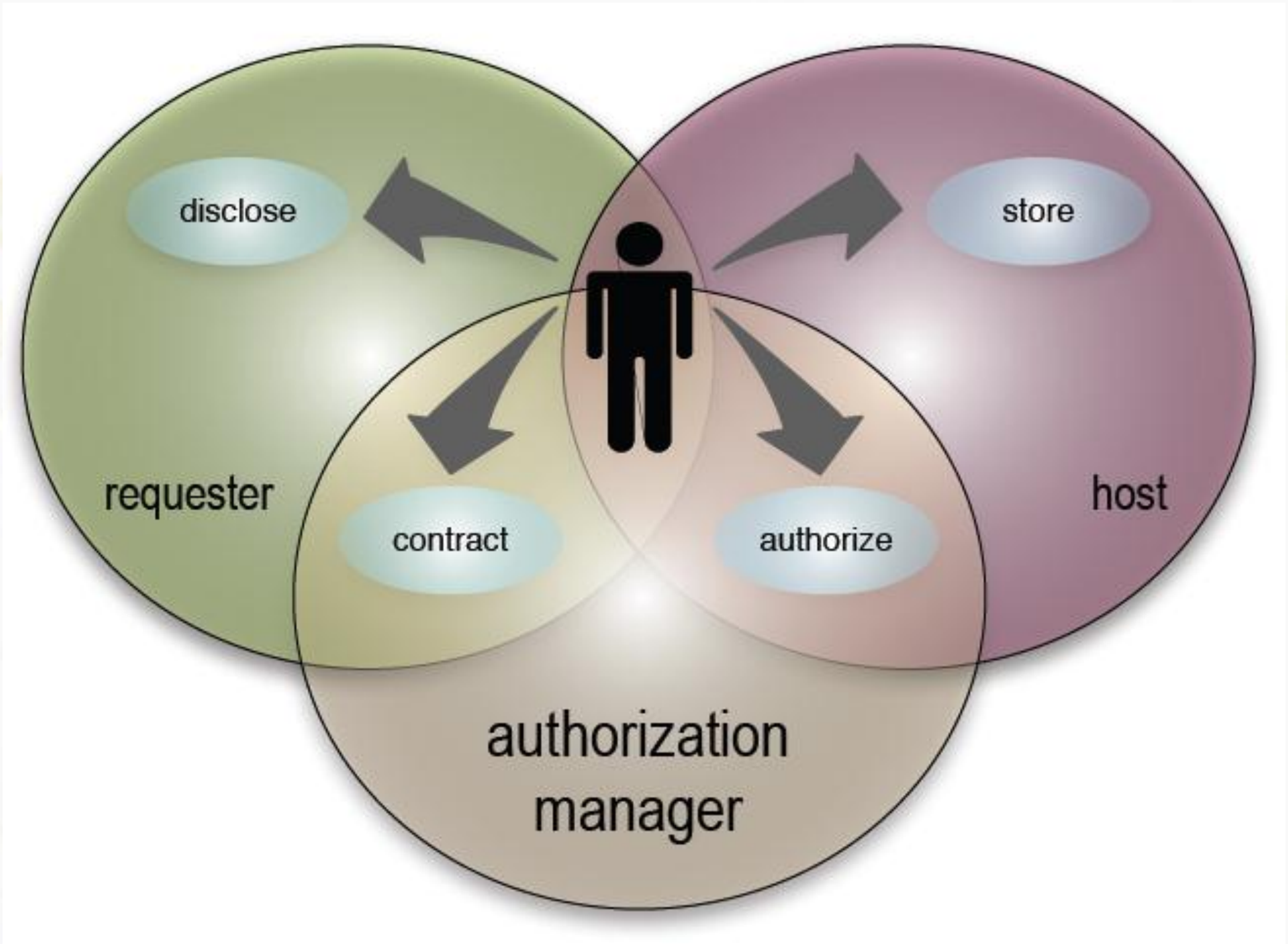

OAUTH
OAUTH

Shortcomings

- Access control **lacks sophistication** since it is a side issue for typical Web 2.0 applications.
- **Lack of central management** of access relationships between Web services hosting and accessing data.
- User needs to use many diverse and bespoke policy management tools with **diversified User Experience** (UX).
- Policies expressed in **diverse** and possibly **incompatible** policy **languages** cannot be reused for distributed Web resources.
- **Poor support for attribute-based policies** does not allow Web users to express their sharing settings in a flexible way.

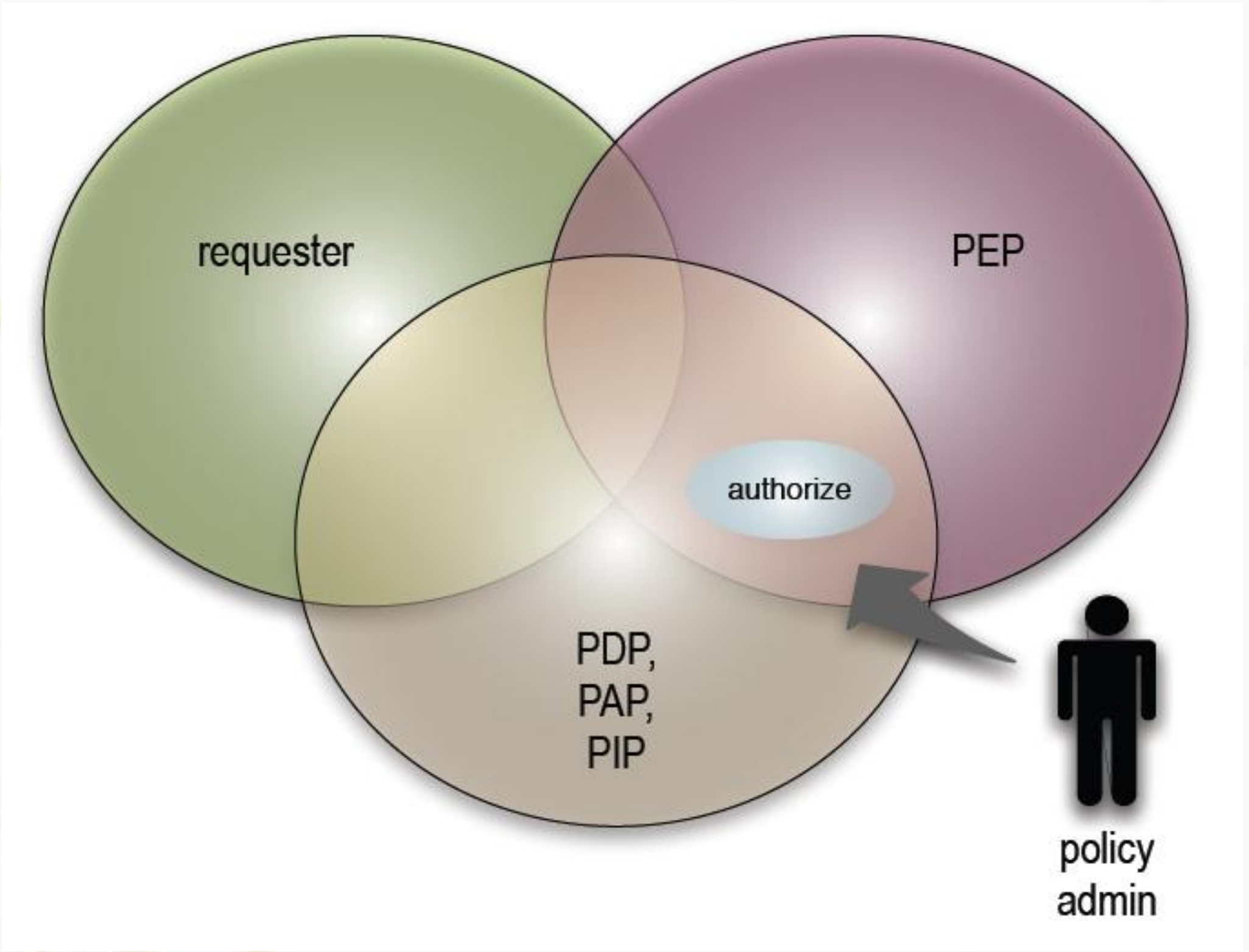
Introducing User Managed Access (UMA)

User-Managed Access (UMA)

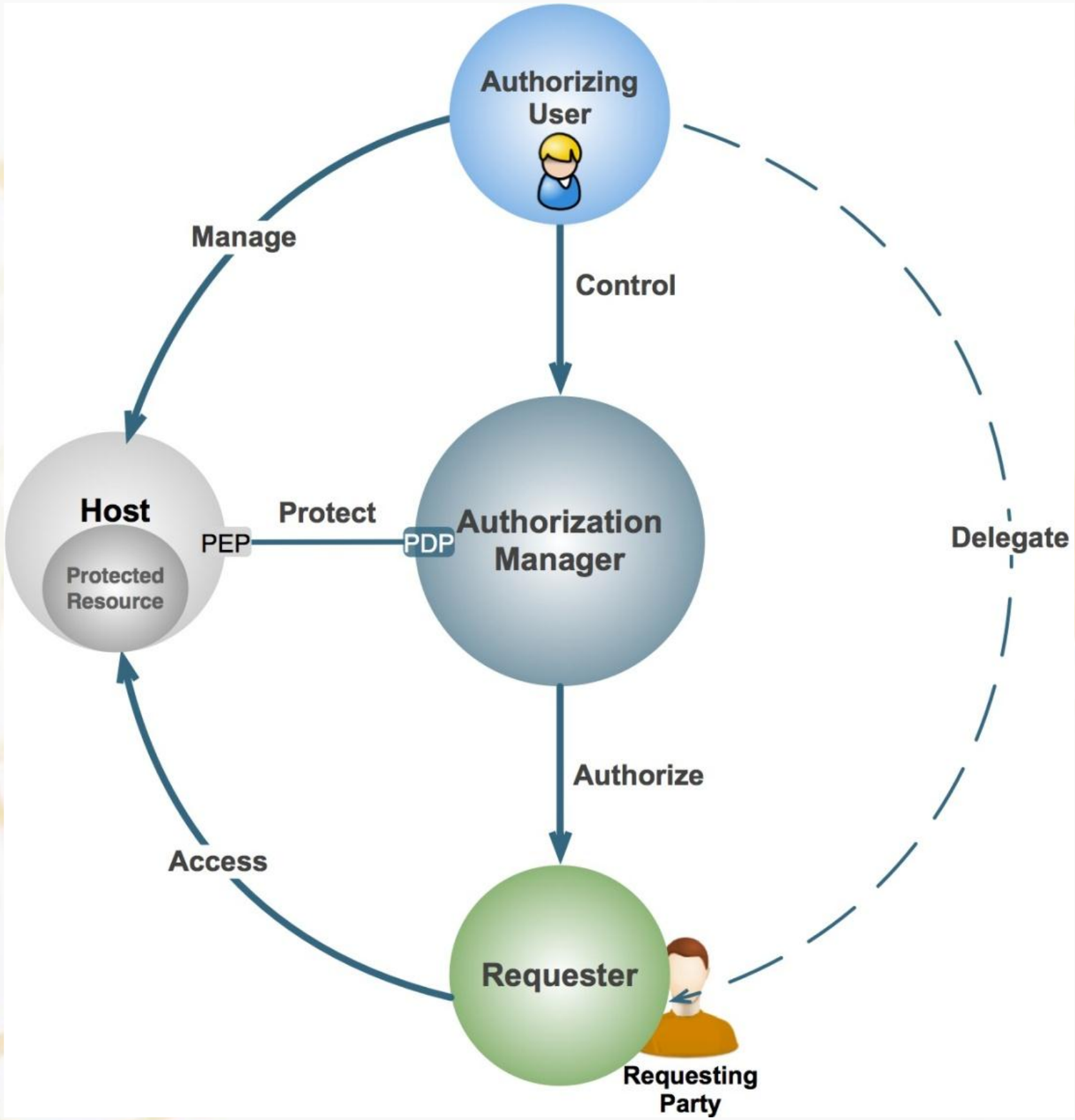


Domenico Catalano, Oracle Corp.

Classic Access Management



UMA – Players


Authorizing User
Manage
Control
Delegate
Host
Protected Resource
PEP
Protect
PDP
Authorization Manager
Authorize
Access
Requester
Requesting Party

UMA – Protocol

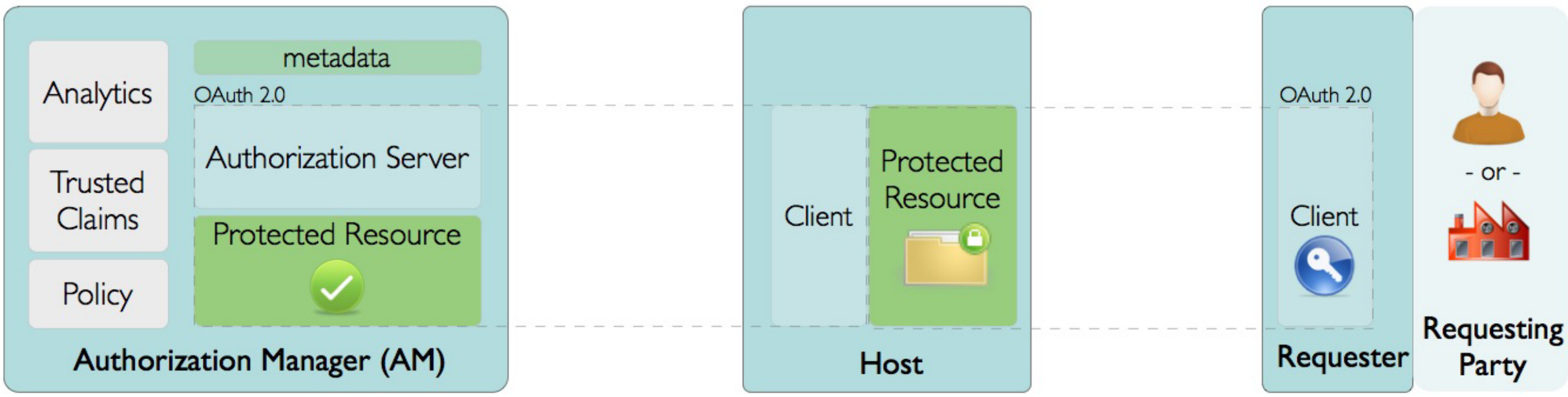
(1) Trust a Token

(2) Get a Token

(3) Use a Token

UMA – Protocol

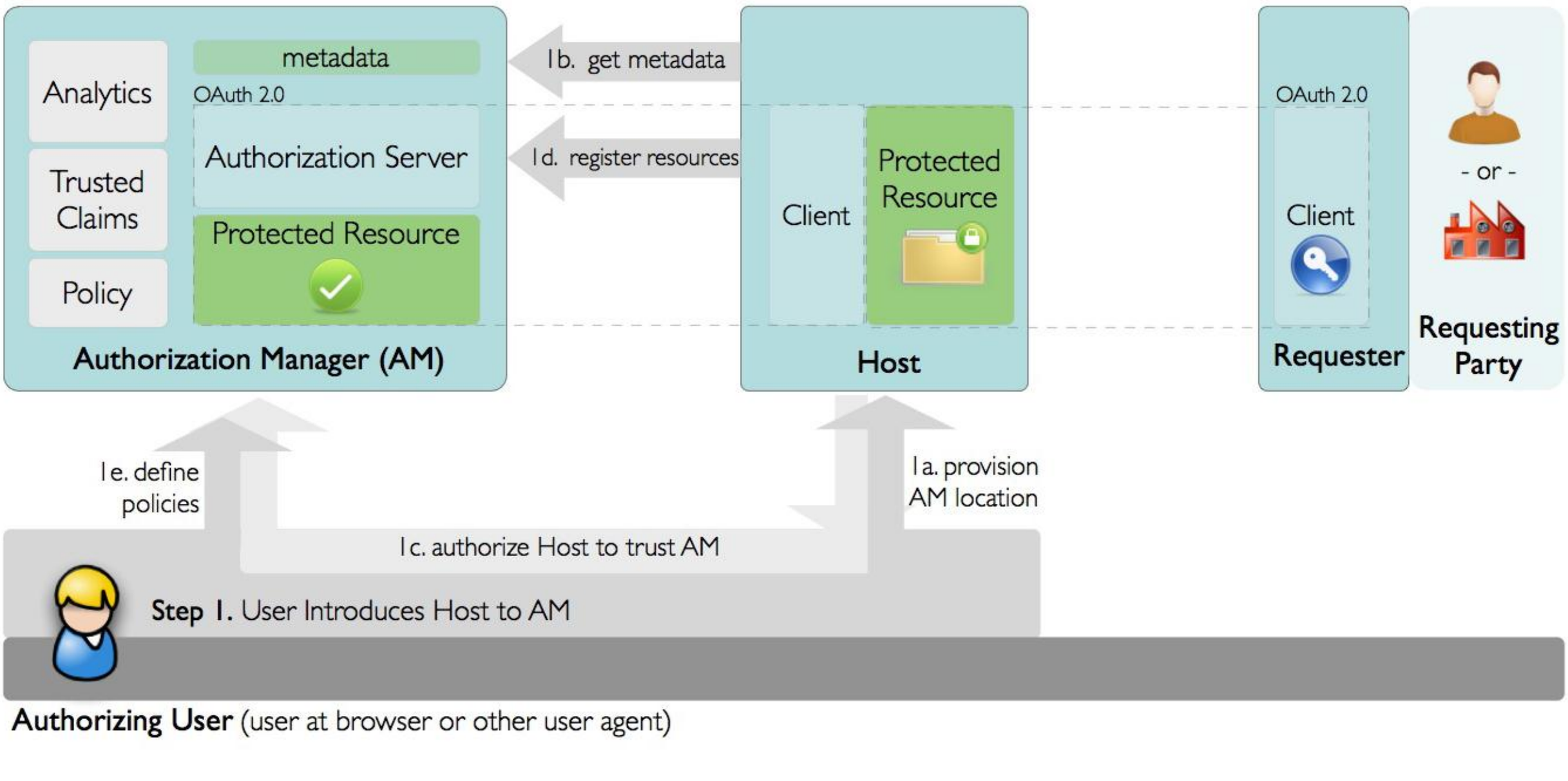
(1) Trust a Token



Authorizing User (user at browser or other user agent)

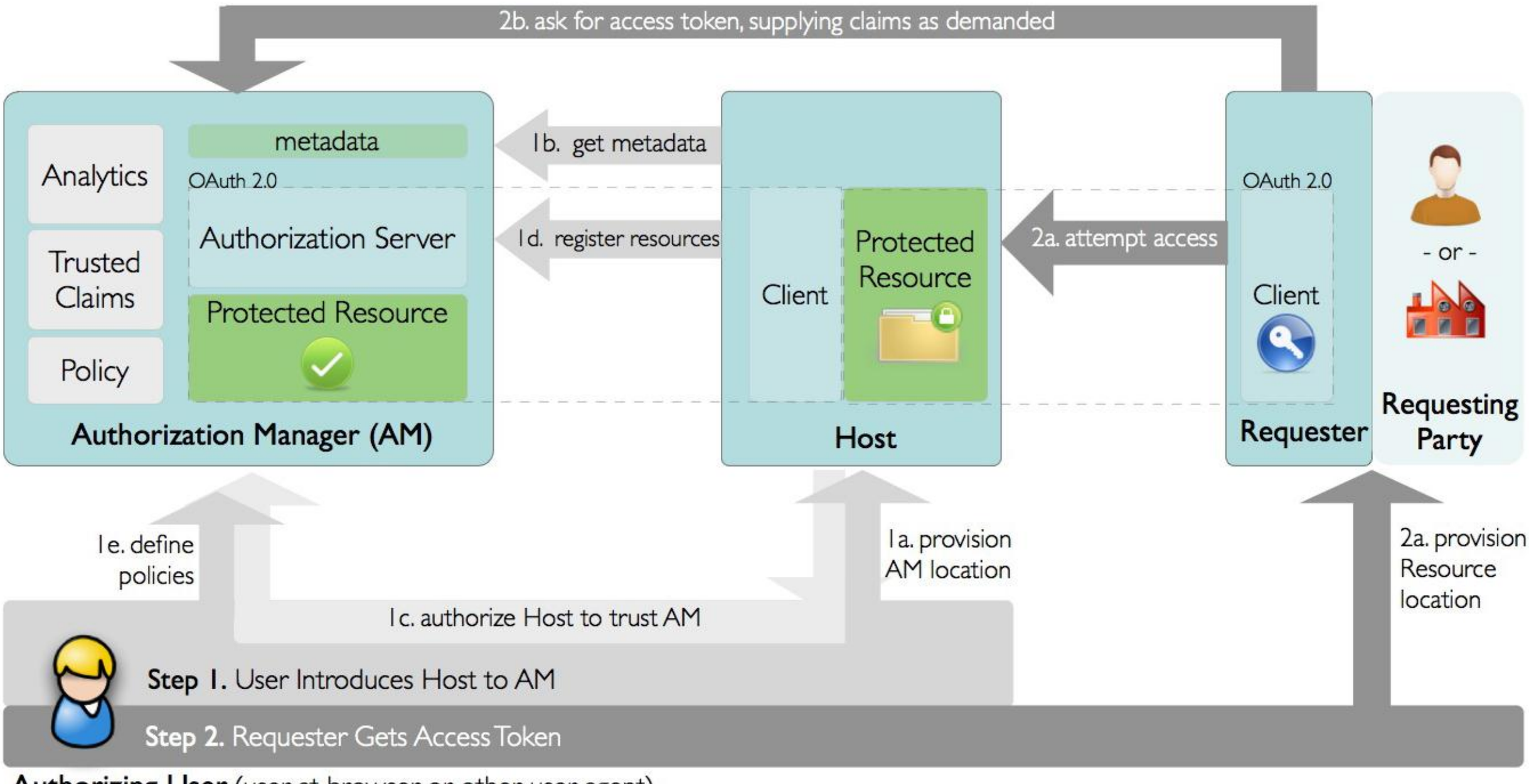
UMA – Protocol

(1) Trust a Token



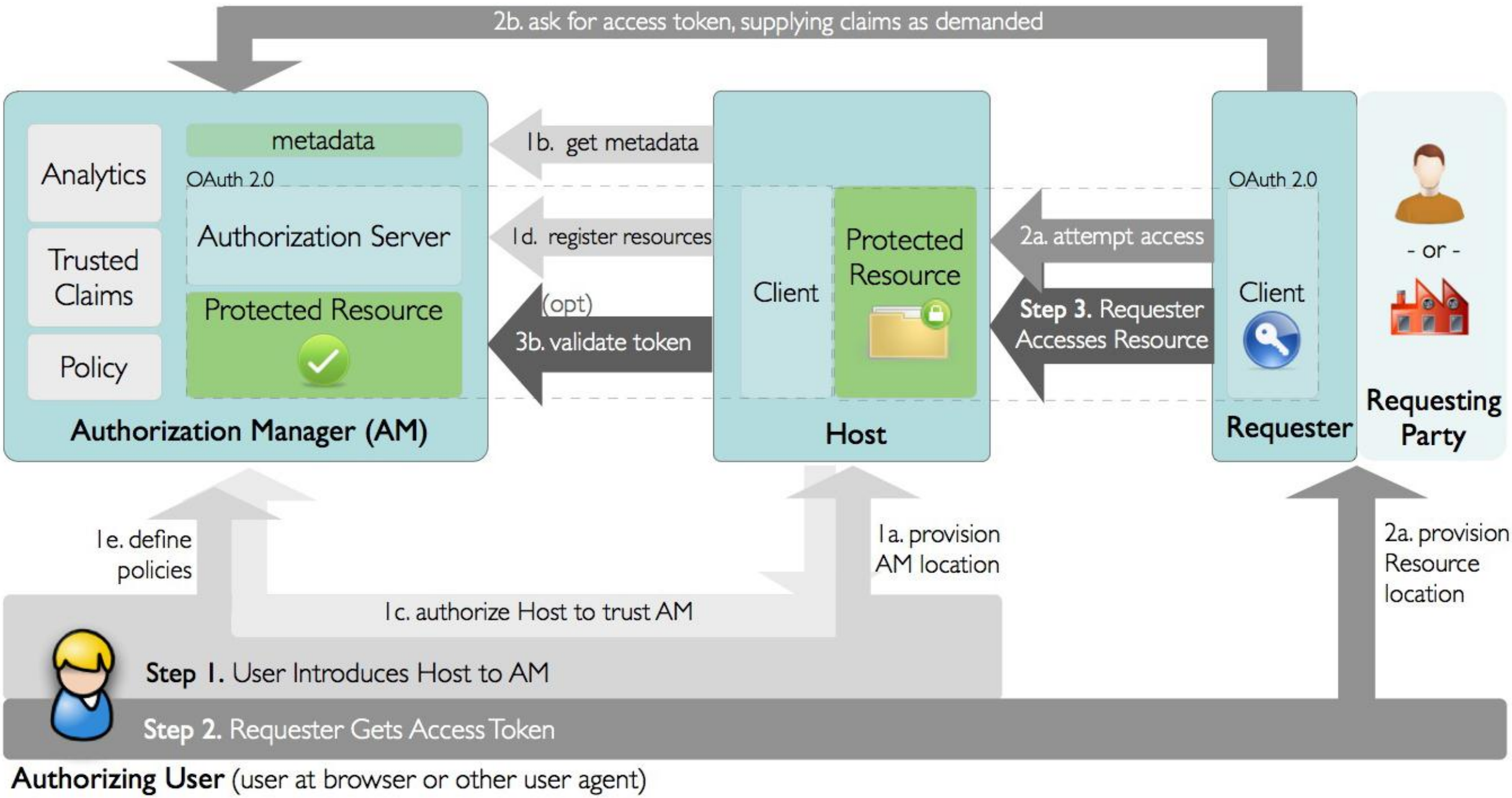
UMA – Protocol

(2) Get a Token



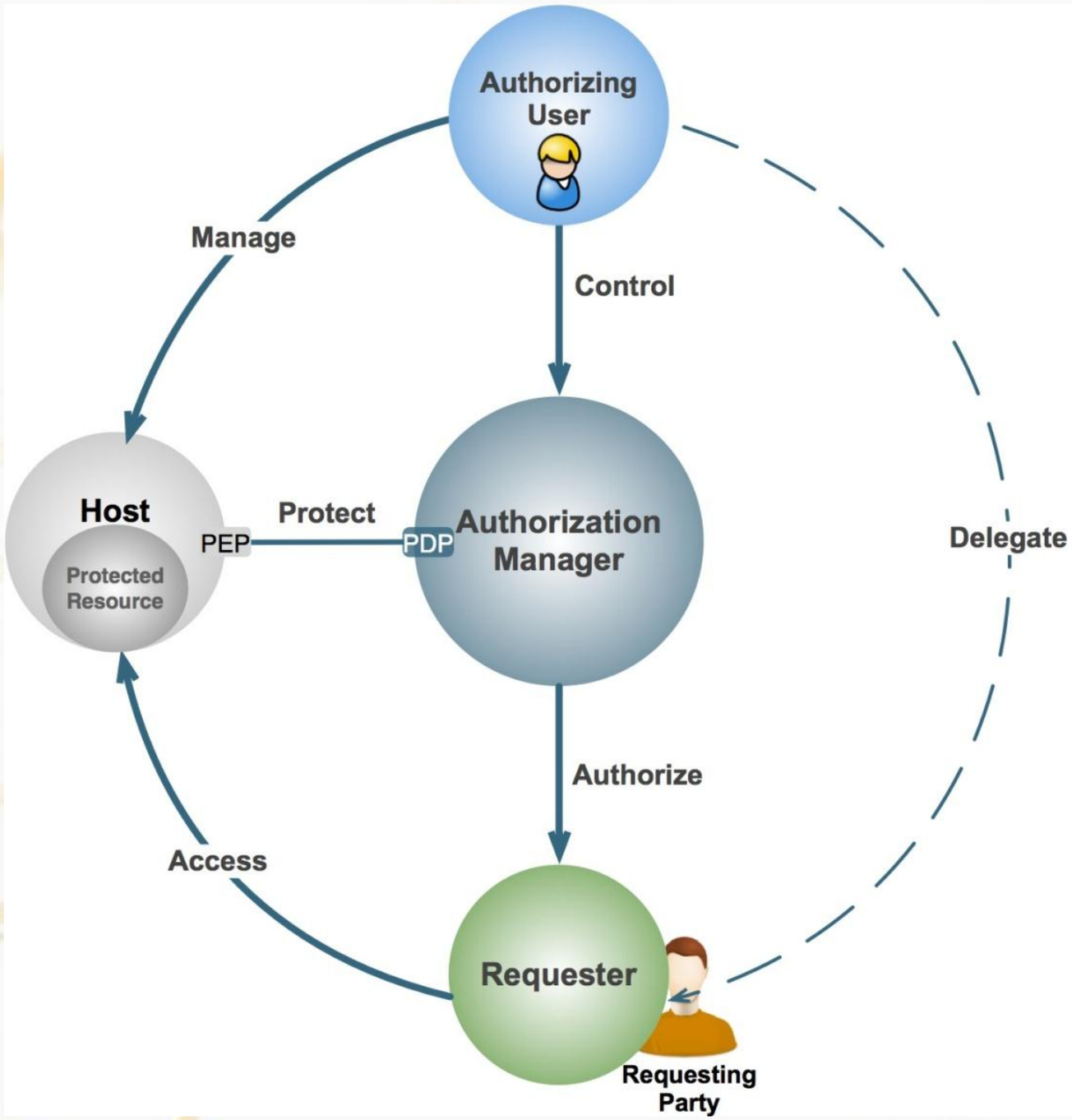
UMA – Protocol

(3) Use a Token

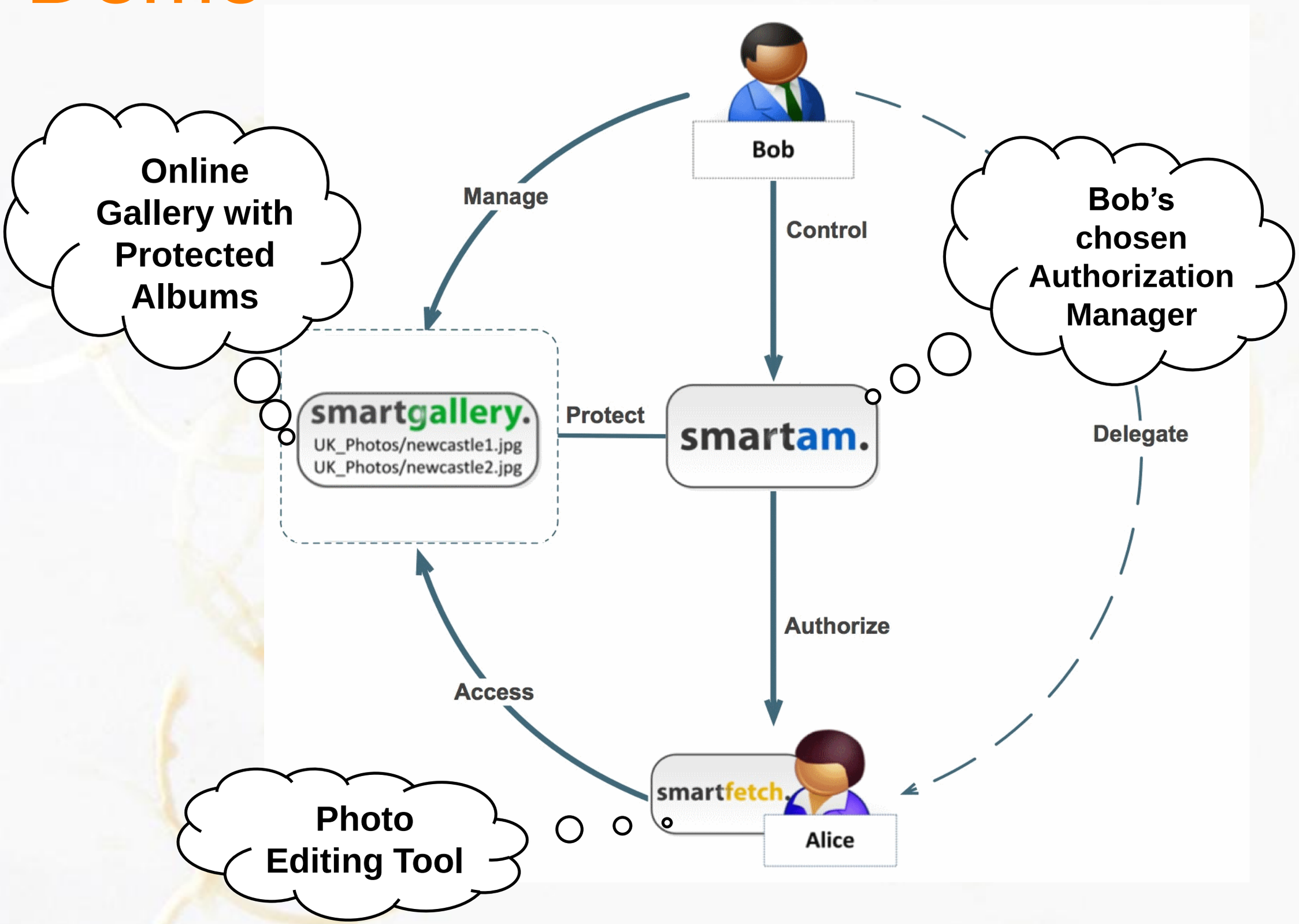


Demo

Demo


Authorizing User
Manage
Control
Host
Protected Resource
PEP
Protect
PDP
Authorization Manager
Delegate
Authorize
Access
Requester
Requesting Party

Demo


Online Gallery with Protected Albums
Bob
Manage
Control
Bob's chosen Authorization Manager
smartgallery.
UK_Photos/newcastle1.jpg
UK_Photos/newcastle2.jpg
Protect
smartam.
Delegate
Authorize
Access
smartfetch.
Alice
Photo Editing Tool

Acting as Bob

localhost:9002/app/bob/...

localhost:9002/app/bob/UK_Photos

smartgallery.

Hello, **bob@example.com.** (Sign Out)

/bob/ UK_Photos

Delete Clear thumbnail

Upload Choose File No file chosen

Newcastle University

UMA

localhost:9002/app/bob?...

localhost:9002/app/bob?uma

smartgallery.

Hello, **bob@example.com.** (Sign Out)

/bob

Choose your Authorization Manager:

smartam.

Newcastle University

UMA

smartam. - please log in

localhost:9000

smartam.

Log in

User bob

Password ••••••••••

Remember me? ☑

Log in

Newcastle University

smartam. - please confir...

localhost:9000/uma/host_user?type=web_server&client_id=K5AqWkPfr6ApnmjzQYtWG/r2fDKWW2JHCCrVTFeHENDdHkzHPYK/Bw%3D%3D8

smartam.

Confirm

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

Name: **Smart Gallery**
URL: **http://localhost:9002**
Description: **UMA-enabled Online Gallery**

Would you like to allow that?

Allow | Don't allow

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

People I want to share with

Manage people with whom you want to share your data

Alice @ smartFETCH

Add Update Remove

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

Advanced Permissions

Define restrictions for your sharing settings

You must acknowledge to be over 18 years old to be granted access to this item.
You must acknowledge to not provide information contained in these documents to any other party.

Add Update Remove

Restrictions Help

Restrictions allow you to define properties of people who use your data. For example, you can share your data with UK Citizens or people who are over 18 years old rather than with specific people that you know.

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

My Shared Items

California Picture

Las Vegas Picture

UK Photos

My Shared Item:

UK Photos (http://localhost:9002/app/bob/UK_Photos)

Located At: Smart Gallery

Share It!

Your current sharing settings

Details Remove

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

My Share

Select Sharing

Applied Set

None of the above

Create New Set

Sharing Settings

* Name: Share with Alice

Description: Share data with Alice @ smartFETCH

Share With

Share With		Available
Alice @ smartFETCH	->	
	<-	

Restrictions

Cancel | Save

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

My Share

Select Sharing

Applied Set

None of the above

Create New Set

Sharing Settings

* Name: Share with Alice

Description: Share data with Alice @ smartFETCH

Share With

Restrictions

Restrictions

You must acknowledge to be over 18
You must acknowledge to not provide

->

<-

Available

Cancel | Save

Newcastle University

SMART_AM_Protect_You...

localhost:9000/index.html

smartam.

Welcome Bob Logout | Help

My Applications | My Shared Items | People I want to share with | Advanced Permissions

My Shared Items

California Picture

Las Vegas Picture

UK Photos

My Shared Item:

UK Photos (http://localhost:9002/app/bob/UK_Photos)

Located At: Smart Gallery

Share It!

Your current sharing settings

Share with Alice - Share data with Alice @ smartFETCH

Details Remove

Newcastle University

localhost:9002/app/bob

localhost:9002/app/bob

smartgallery.

Hello, **bob@example.com.** (Sign Out)

/bob

UK_Photos UMA

New album NewAlbum

Newcastle University

UMA

Acting as Alice

UMA Sample Requester - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/protectedResourceRequester.jsf

Google

UMA Sample Requester

smartfetch.

Access 'california.jpg' Download

Access 'las_vegas.jpg' Download

Access 'newcastle1.jpg' Download

Access 'newcastle2.jpg' Download

Credentials page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/protectedResourceRequester.jsf;jsessionid=10s2qzi73hnaxp3jp3oa0uzxg

Google

Credentials page

smartfetch.

This resource is protected with the following Authorization Manager:

smartam. protected

Please provide your credentials at this AM:

Username:

alice

Password:

•••••

Get Authorization

Claims page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/credentials.jsf

Google

Claims page

- [ ] You must acknowledge to be over 18 years old to be granted access to this item.
- [ ] You must acknowledge to not provide information contained in these documents to any other party.

Confirm

Claims page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/credentials.jsf

Google

Claims page

smartfetch.

UMA Sample Requester - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/protectedResourceRequester.jsf

Google

UMA Sample Requester

smartfetch.

Access 'california.jpg' Download

Access 'las_vegas.jpg' Download

Access 'newcastle1.jpg' Download

Access 'newcastle2.jpg' Download

Claims page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:9003/credentials.jsf

Google

Claims page

smartfetch.

Introducing

UMA/j

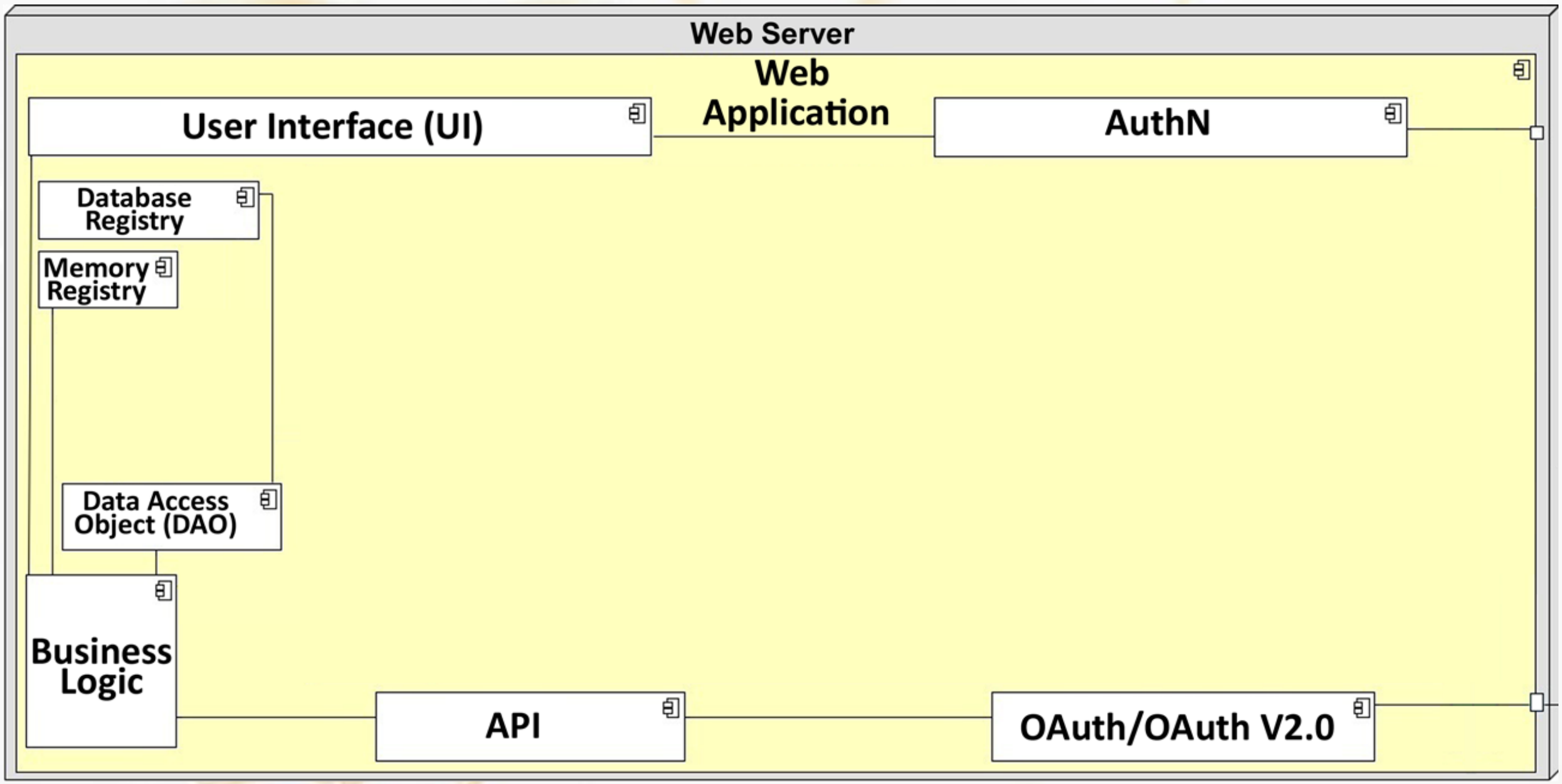
UMA/j Framework

- Java implementation of the UMA protocol
  - developed at Newcastle University (SMART)
- Allows Web 2.0 applications to delegate their access control functionality
  - *Separates policy enforcement and decision making*
  - *Dynamicly established relationships between UMA components*
  - *User is the king – chooses their preferred access control mechanisms*
  - *Selective sharing of data across walled-gardens*

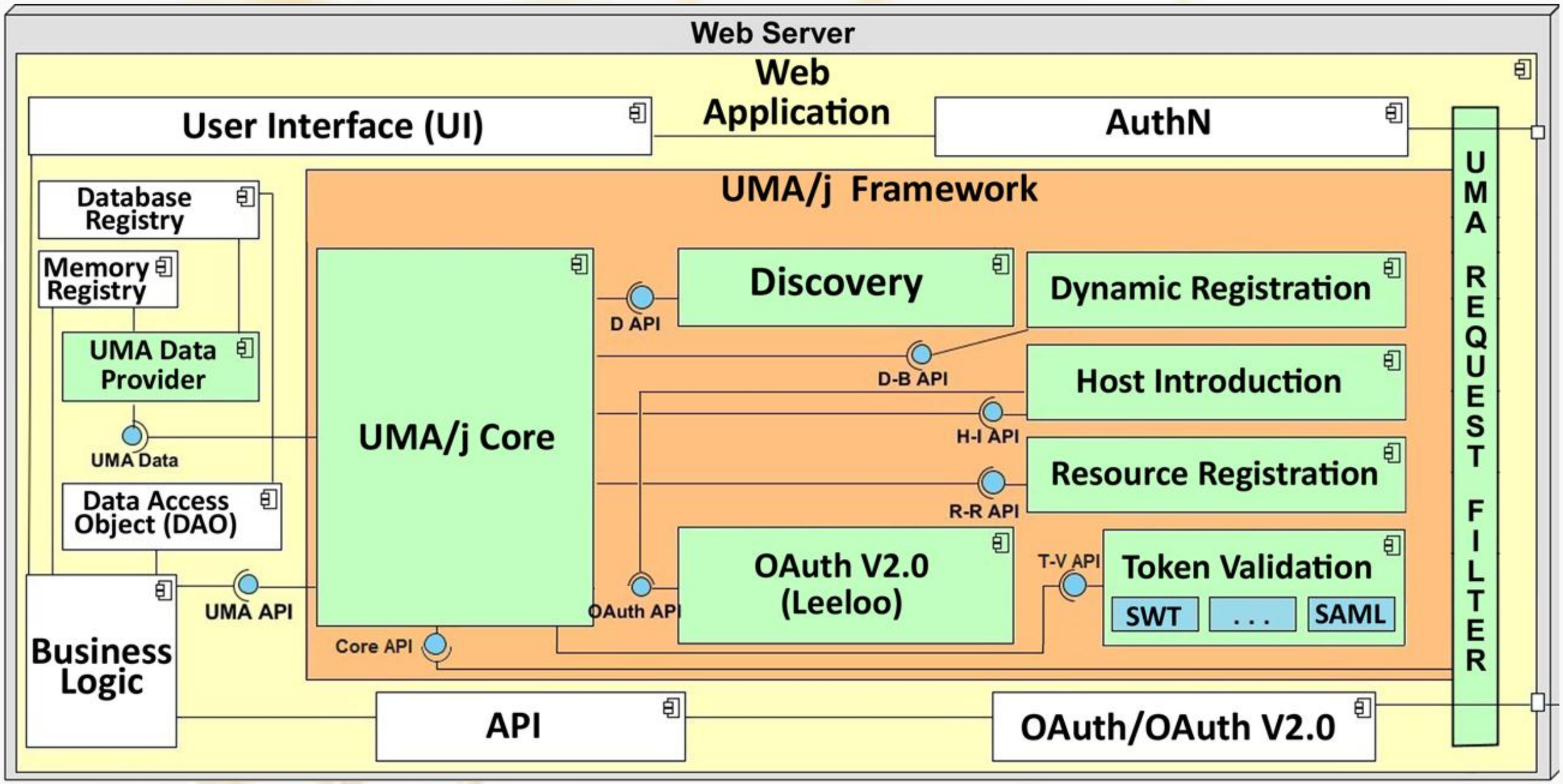
UMA/j Framework

- Web 2.0 and Internet standards
  - UMA Core Protocol 1.0 (UMA WG)
  - OAuth V2.0 (IETF I-D 10, July 2010)
  - Discovery – site-meta (RFC 5785), host-meta (IETF I-D, Jun 2010)
  - XRD V1.0 (OASIS Standard, Nov 2010)
  - OAuth Dynamic Client Registration (IETF I-D 00, Aug 2010)
  - Resource Registration (UMA WG)
  - Token Validation (UMA WG)
  - Claims 2.0 (UMA WG)

UMA/j Architecture



UMA/j Architecture



UMA/j and existing technologies

- UMA/j and OAuth
  - –Builds on top of OAuth 2.0
  - –Supports dynamic introductions between component
  - –Uses **OAuth leeloo**

- UMA/j and XACML
  - – XACML as a policy expression language
  - – RESTful authorization query/response protocol

UMA/j and existing technologies

- UMA/j and SAML
  - –SAML assertion complementary to SWT

- UMA/j can extend Spring Security
  - – Access control policies defined at runtime by end users
  - – Policies reusable across multiple Web applications
  - – Does not require developing custom UI
  - – Dynamic discovery of the end user’s chosen AM

UMA and UMA/j Summary

- Existing authorization solutions
  - Lack of central management of access relationships between online services
  - Diversified User Experience
  - Poor support for claimed-based policies
  - Not unified security policies language
- UMA and UMA/j addresses shortcomings:
  - Centralised access management
  - Unified UX
  - Consolidated view of applied access control rules
  - Single policy language for all Web resources

Acknowledgement

Eve L. Maler

Domenico Catalano

Thanks for your attention!

UMA/j

http://uma.smartam.net

UMA Work Group

http://tinyurl.com/umawg