User-Managed Access Control for Web 2.0 Applications

Aad van Moorsel, Maciej Machulak, Lukasz Moren

Newcastle University
Centre for Cybercrime and Computer Security
aad.vanmoorsel@ncl.ac.uk
cccs.ncl.ac.uk

IFIP 10.4 Taiwan, July 3, 2011

UMA is…

- A **web protocol** that let you control authorization of data sharing and service access made on your behalf
- A **Work Group** of the Kantara Initative 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

SMART Project

- The **SMART** (Student-Managed Access to Online Resources) project will:
  - Define HE scenario for UMA
  - Develop UMA
  - Deploy UMA
  - Evaluate UMA
  - **Actively** participate in the UMA WG

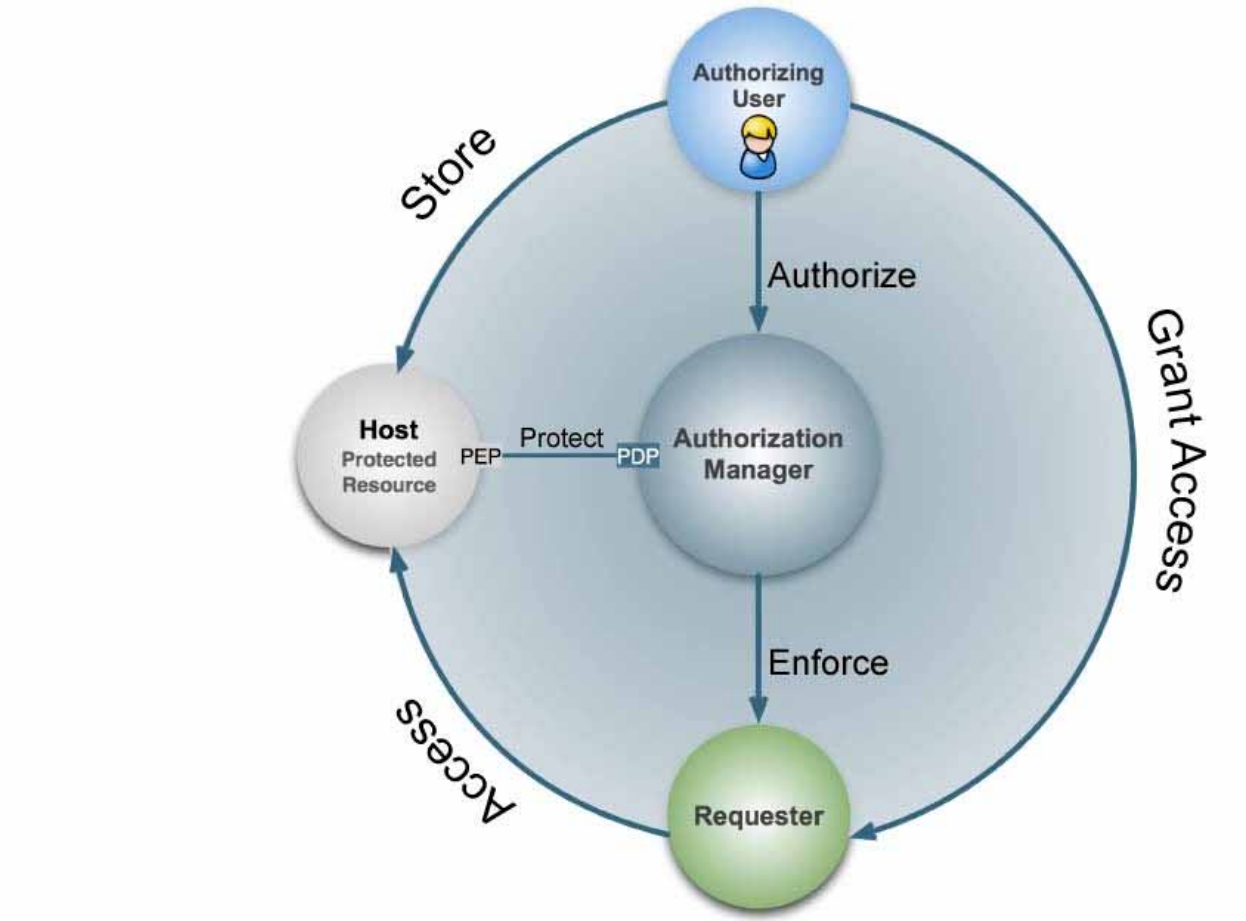
SMART Project

- The **SMART** (Student-Managed Access to Online Resources) project will:
  - Define HE scenario for UMA (accepted)
  - Develop UMA (prototype implemented)
  - Deploy UMA
  - Evaluate UMA
  - **Actively** participate in the UMA WG (ongoing)

Project Team

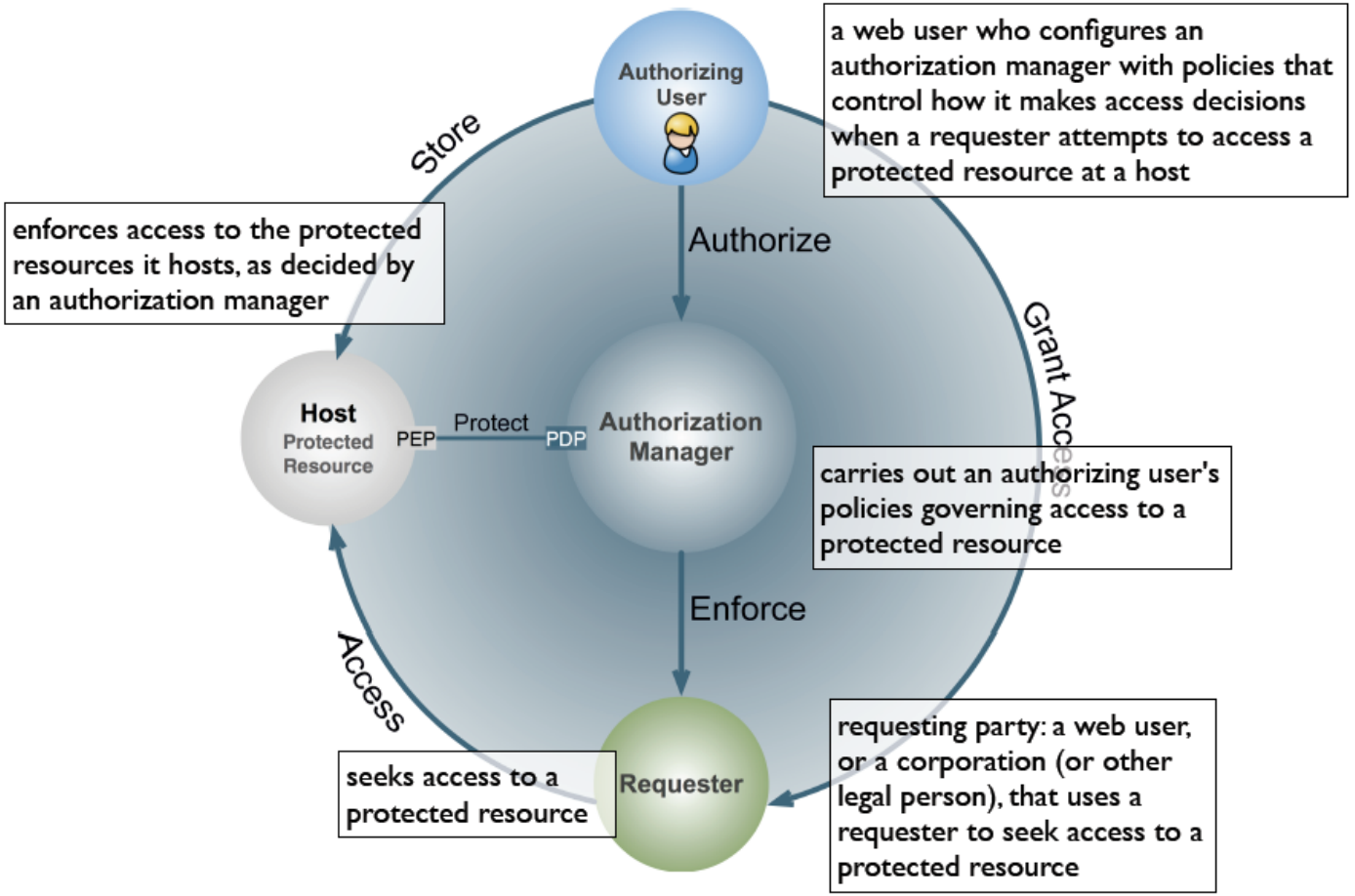
- Project Team at Newcastle University:
  - Maciej Machulak, project lead and management, vice-chair UMA
  - Lukasz Moren, research and development
  - Maciej Wolniak, human computer interaction
  - Jacek Szymon, development
  - Domenico Catalano, Oracle, Italy (HCI, visiting during July)
  - Chris Franks (Information Systems and Services), HE case study
  - Aad van Moorsel

UMA – The Players



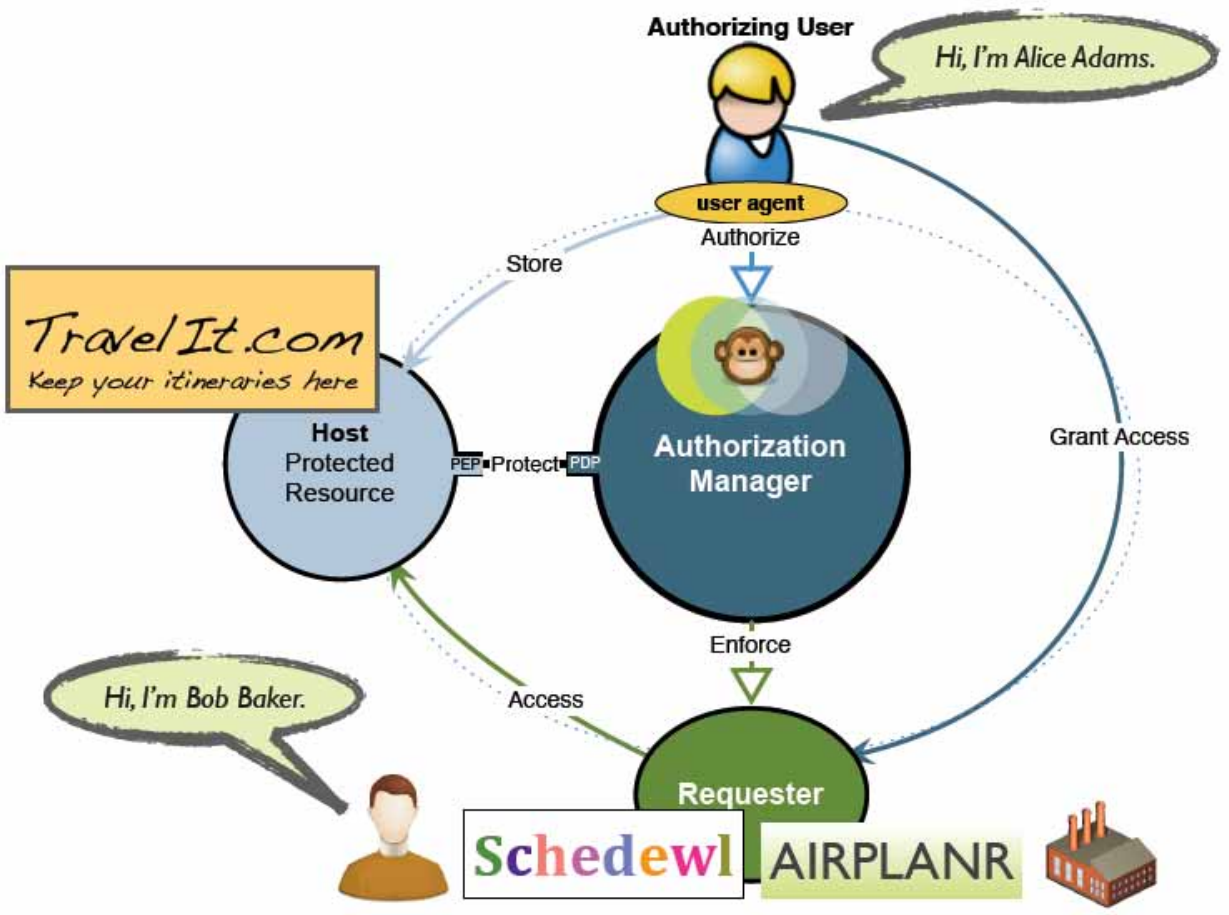
Author: Domenico Catalano, Sun Microsystems, Inc.

UMA – The Players



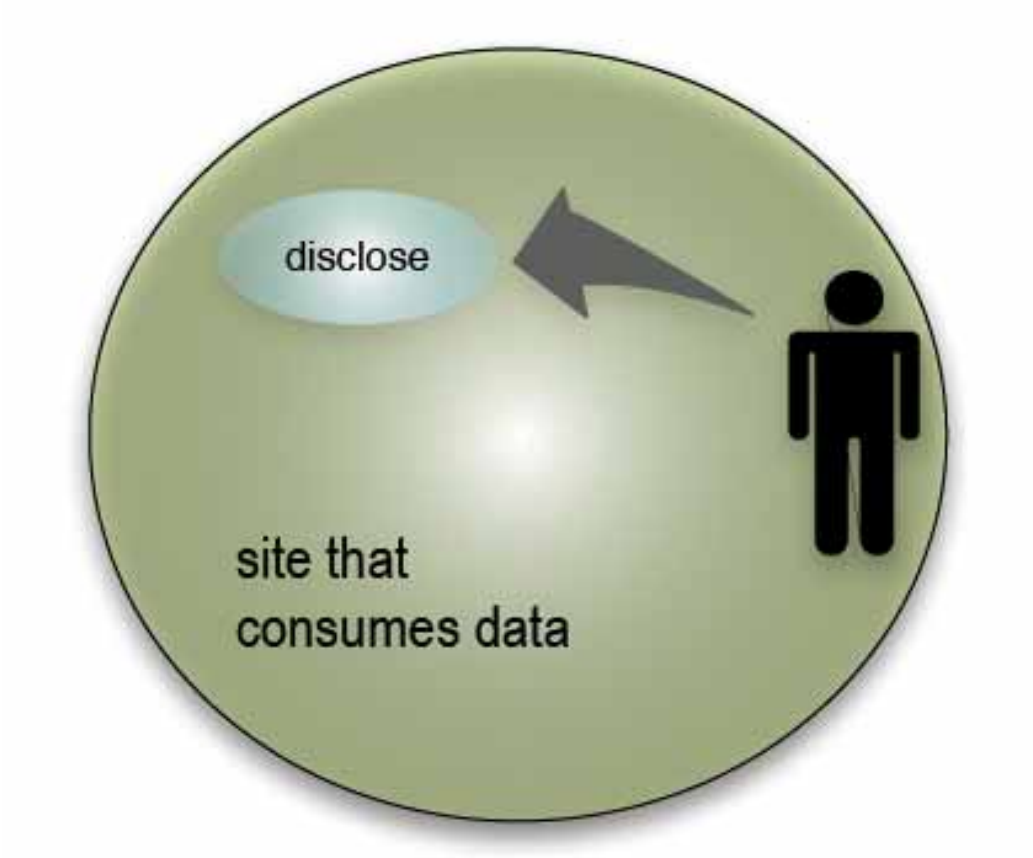
Author: Domenico Catalano, Sun Microsystems, Inc.

UMA – Simple Scenario



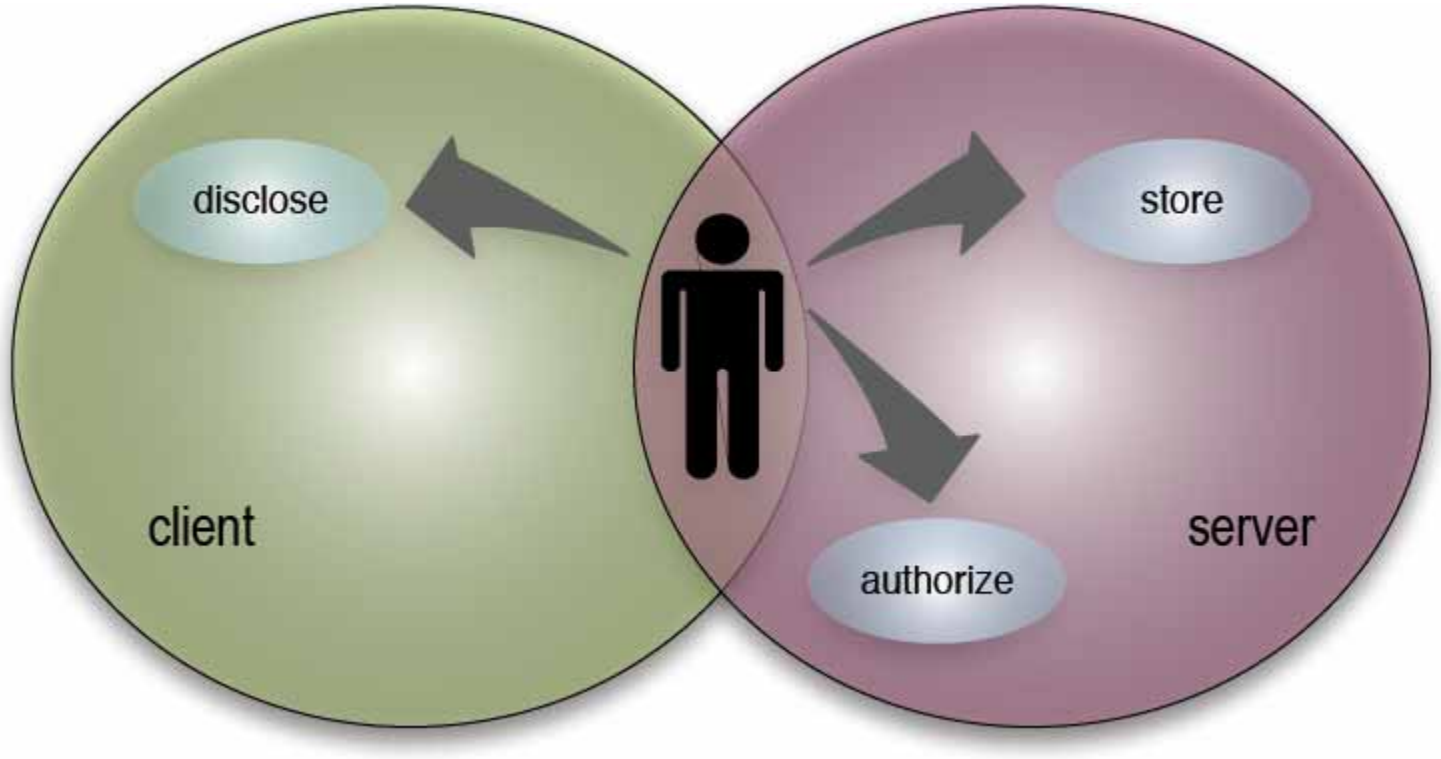
Author: Domenico Catalano, Sun Microsystems, Inc.

Classic Web model



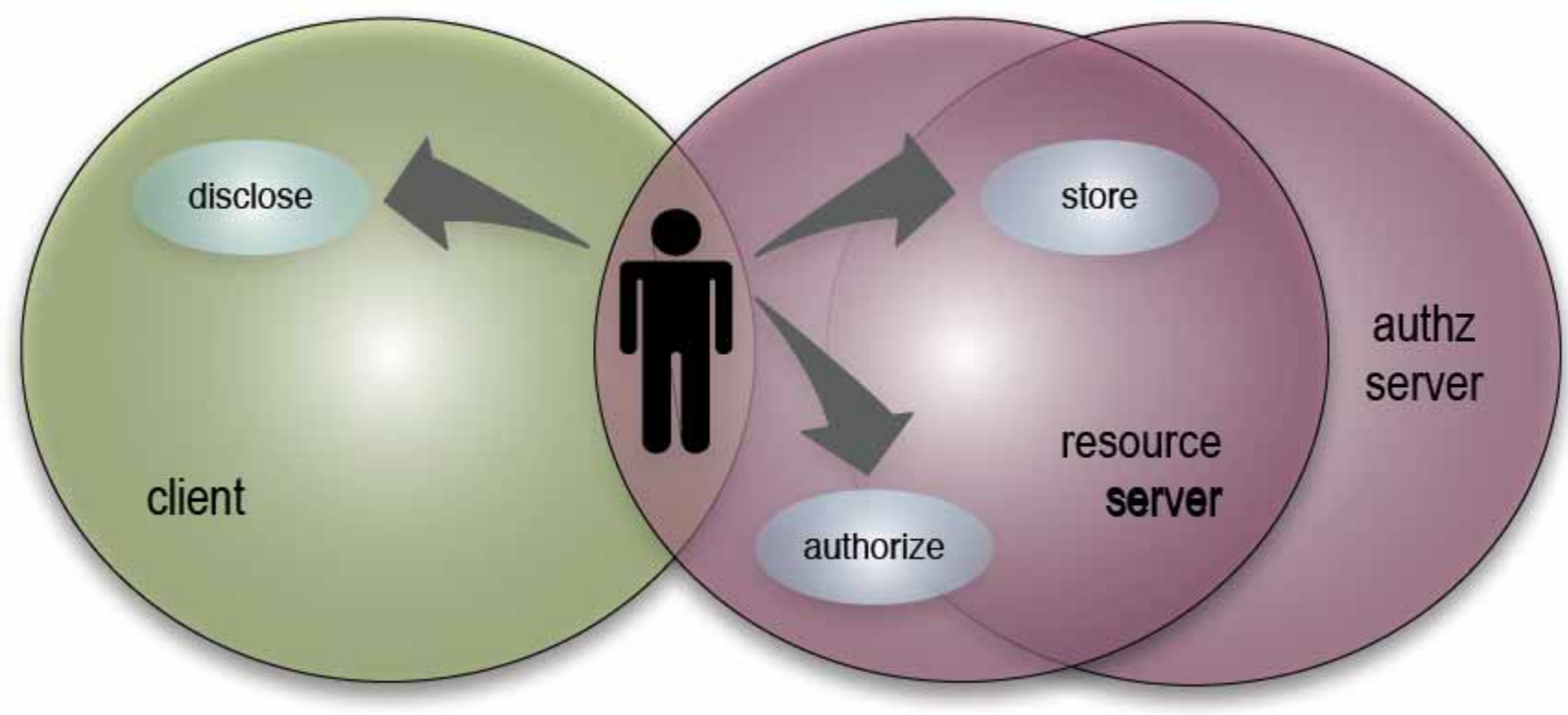
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

OAuth 1.0



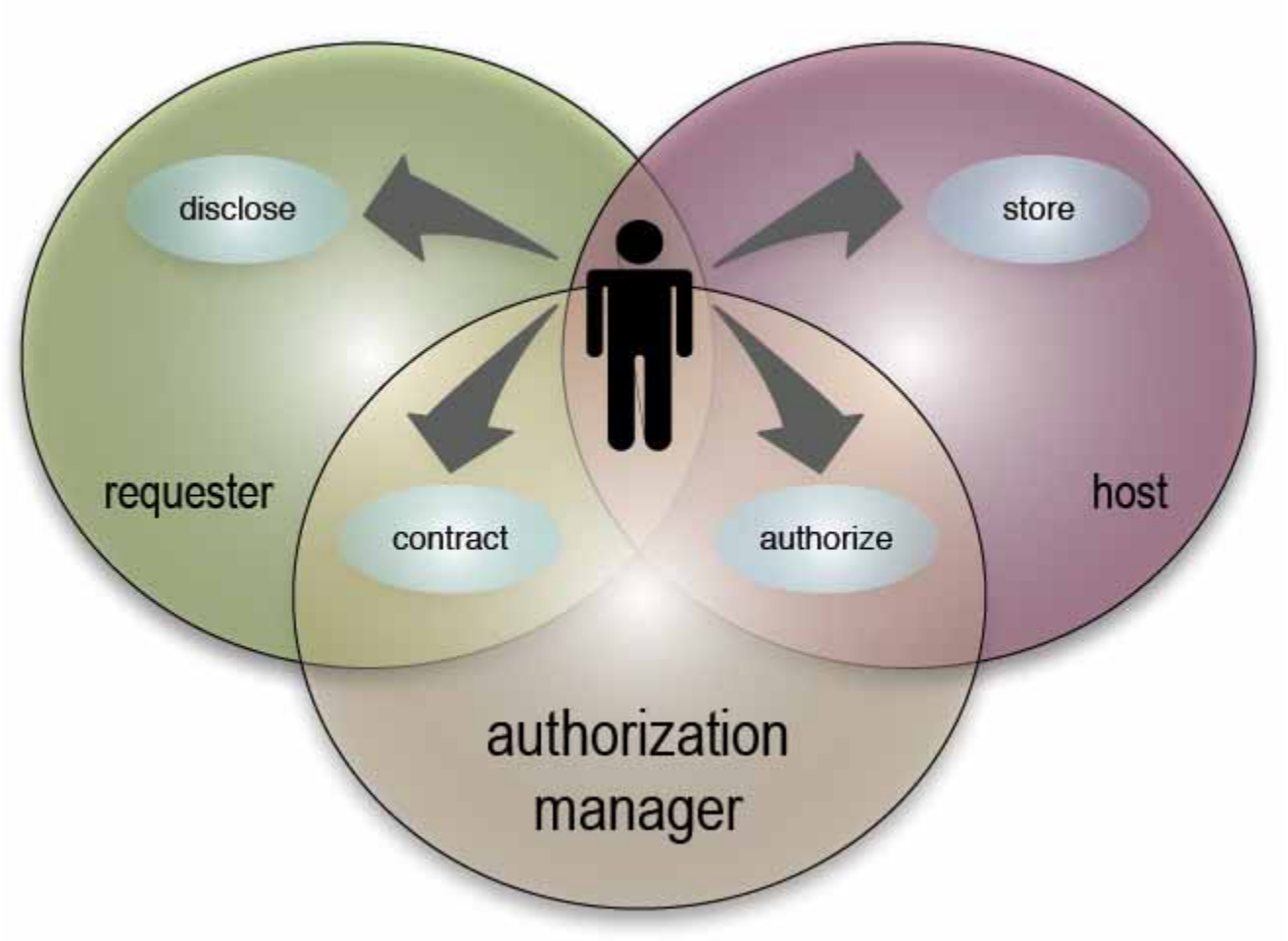
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

OAuth 2.0



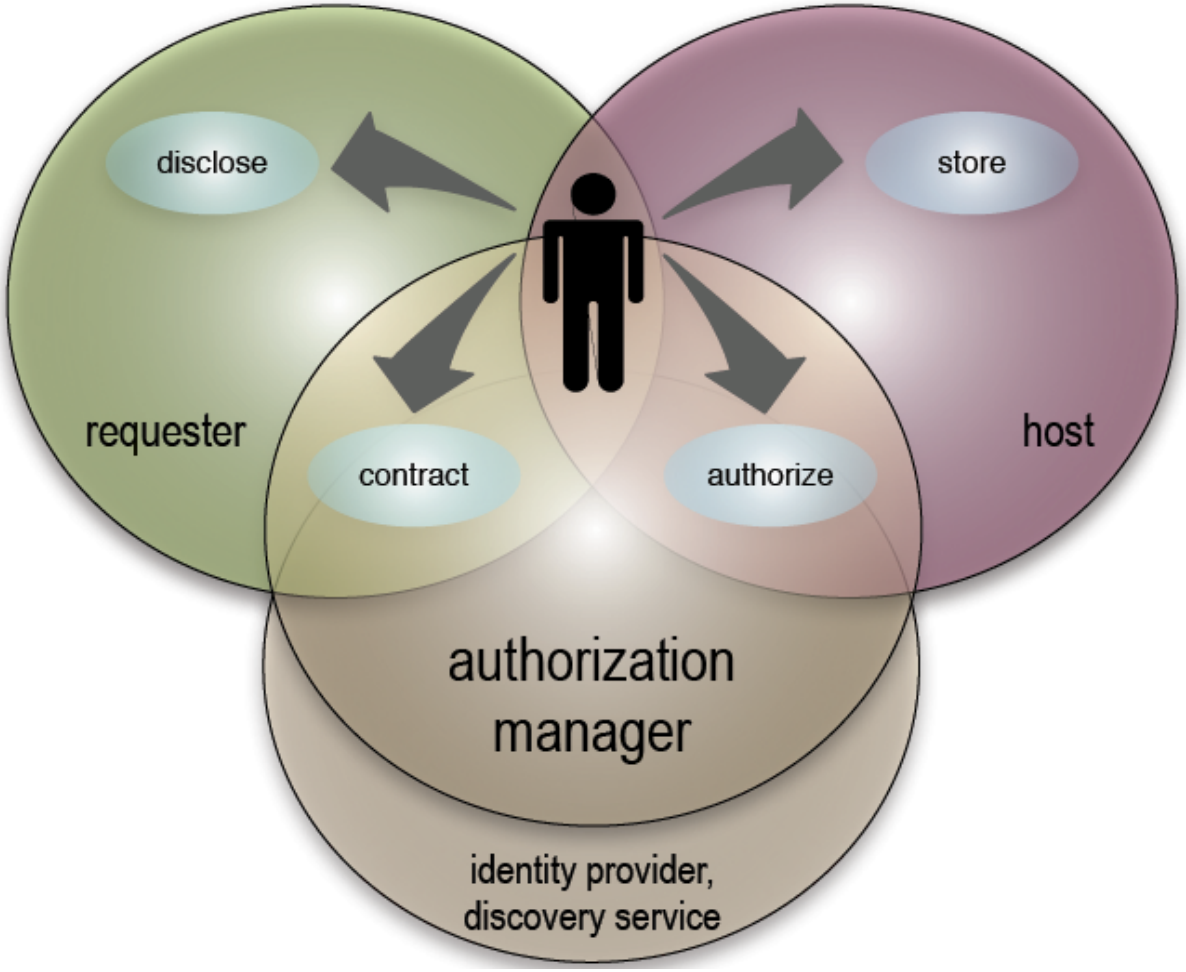
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

UMA



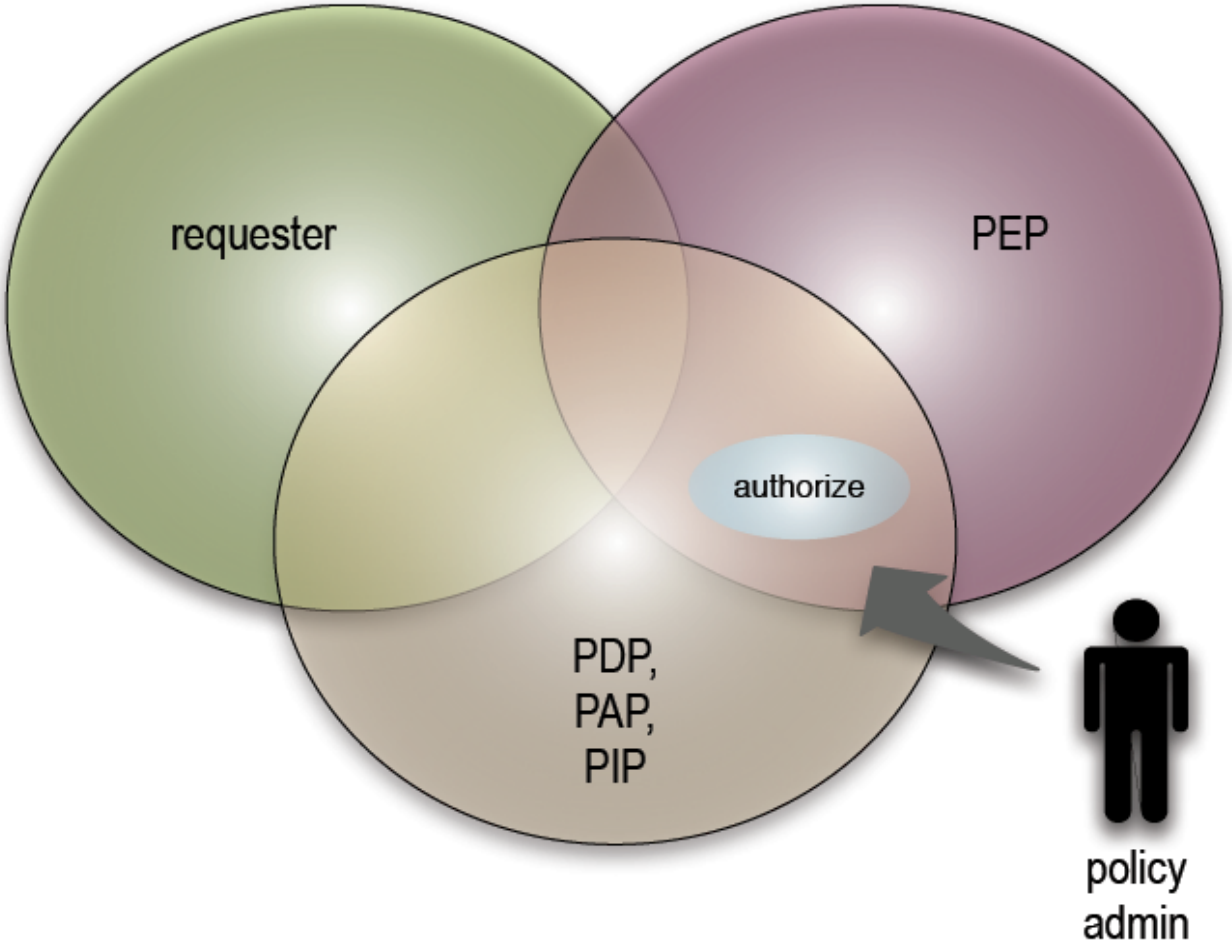
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

UMA



Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

Classic Access Management

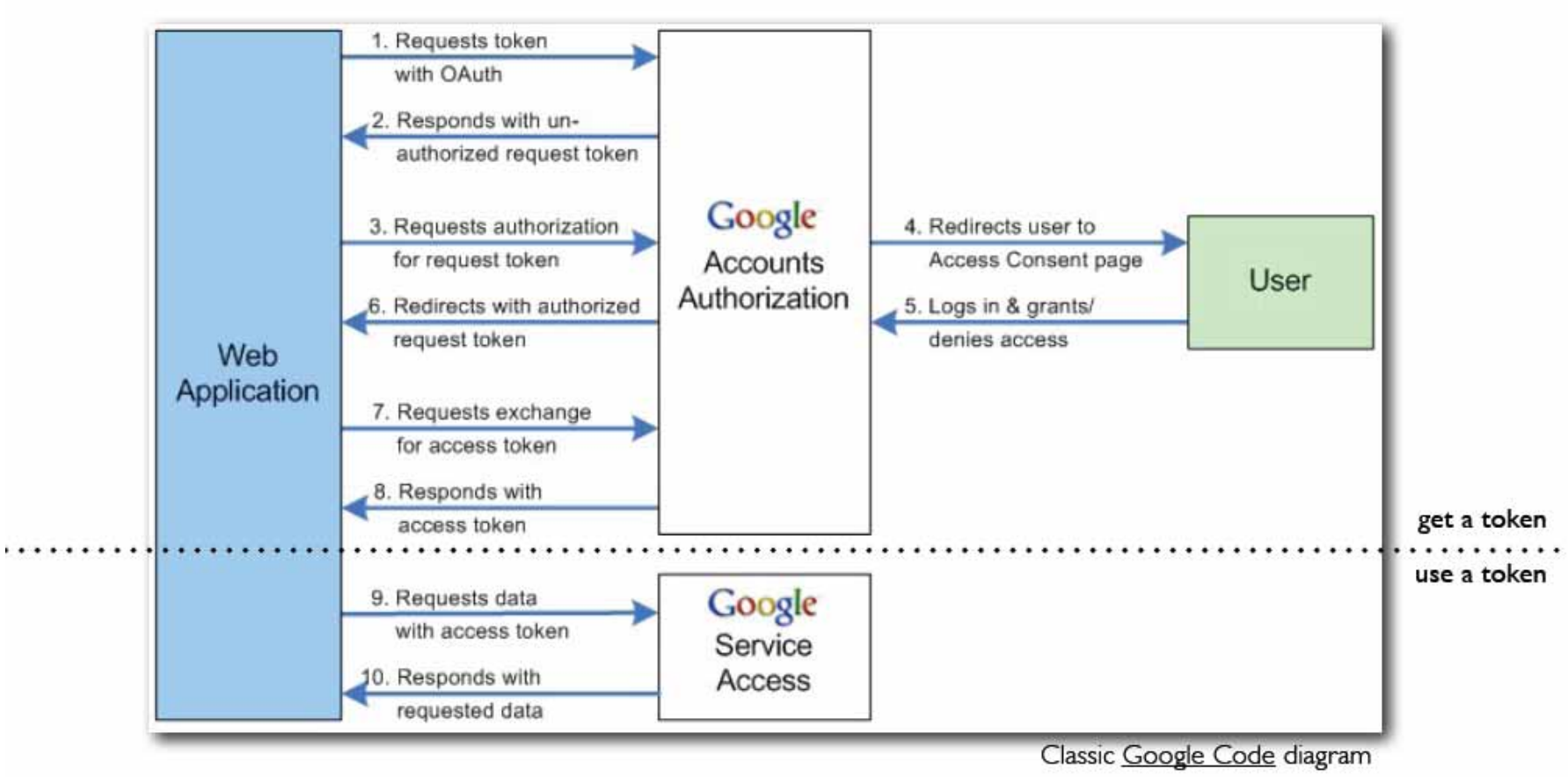


Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

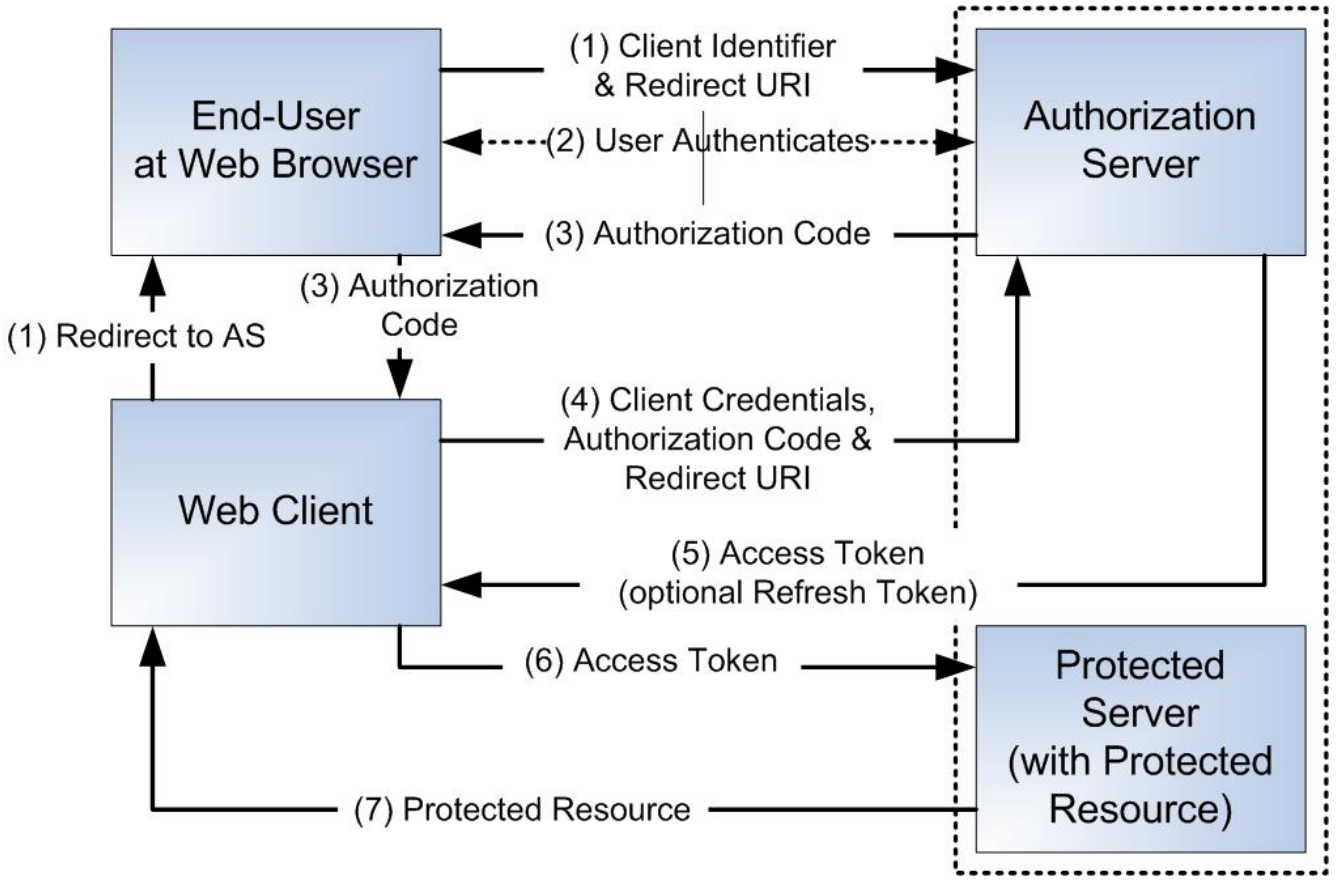
UMA Protocol

Technical Deep Dive

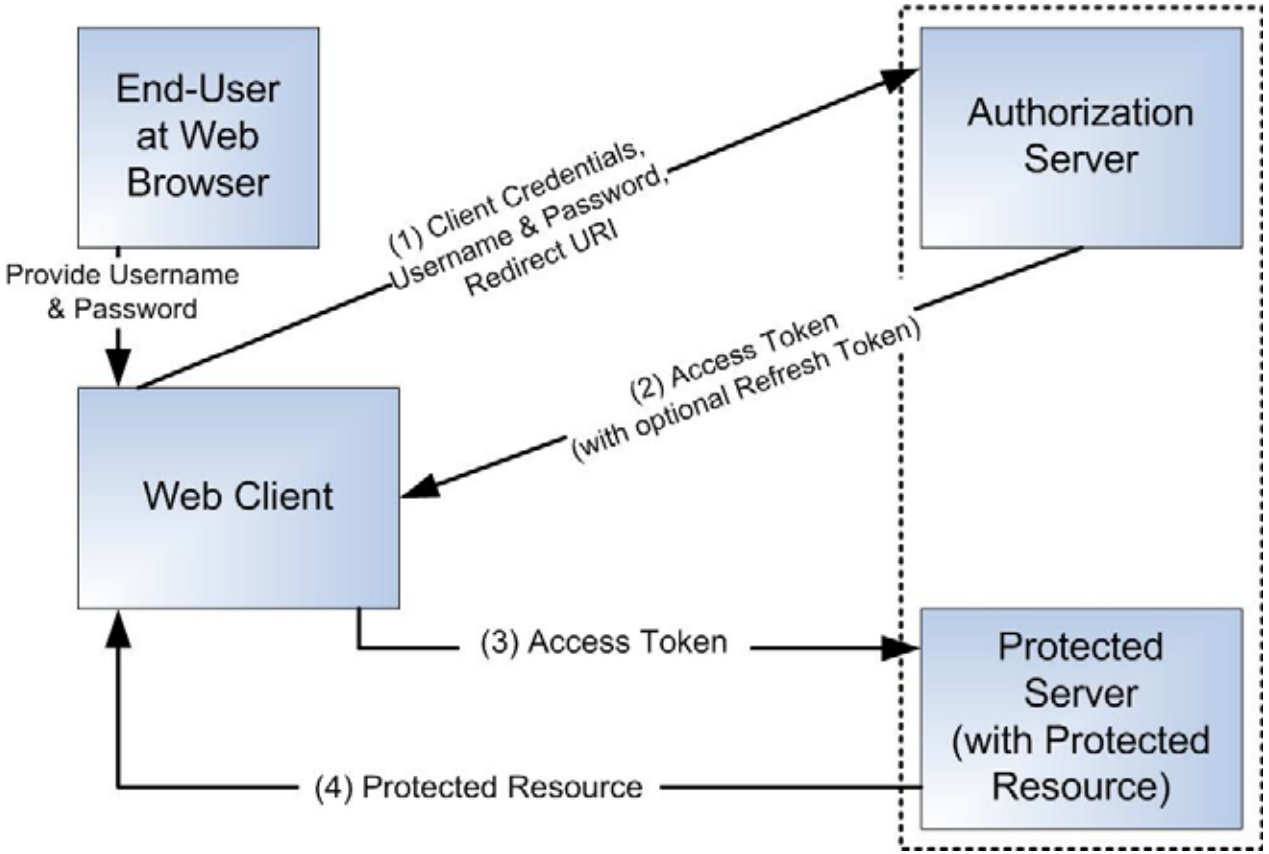
OAuth



OAuth 2.0 – Web Server Flow



OAuth 2.0 – Username/Password Flow



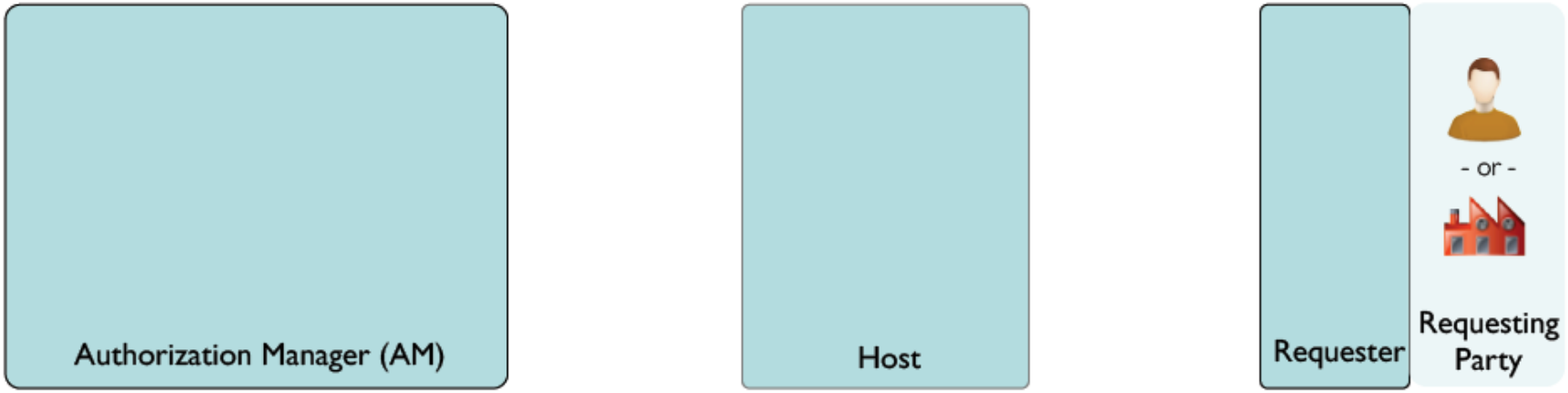
UMA

(1) Trust a Token

(2) Get a Token

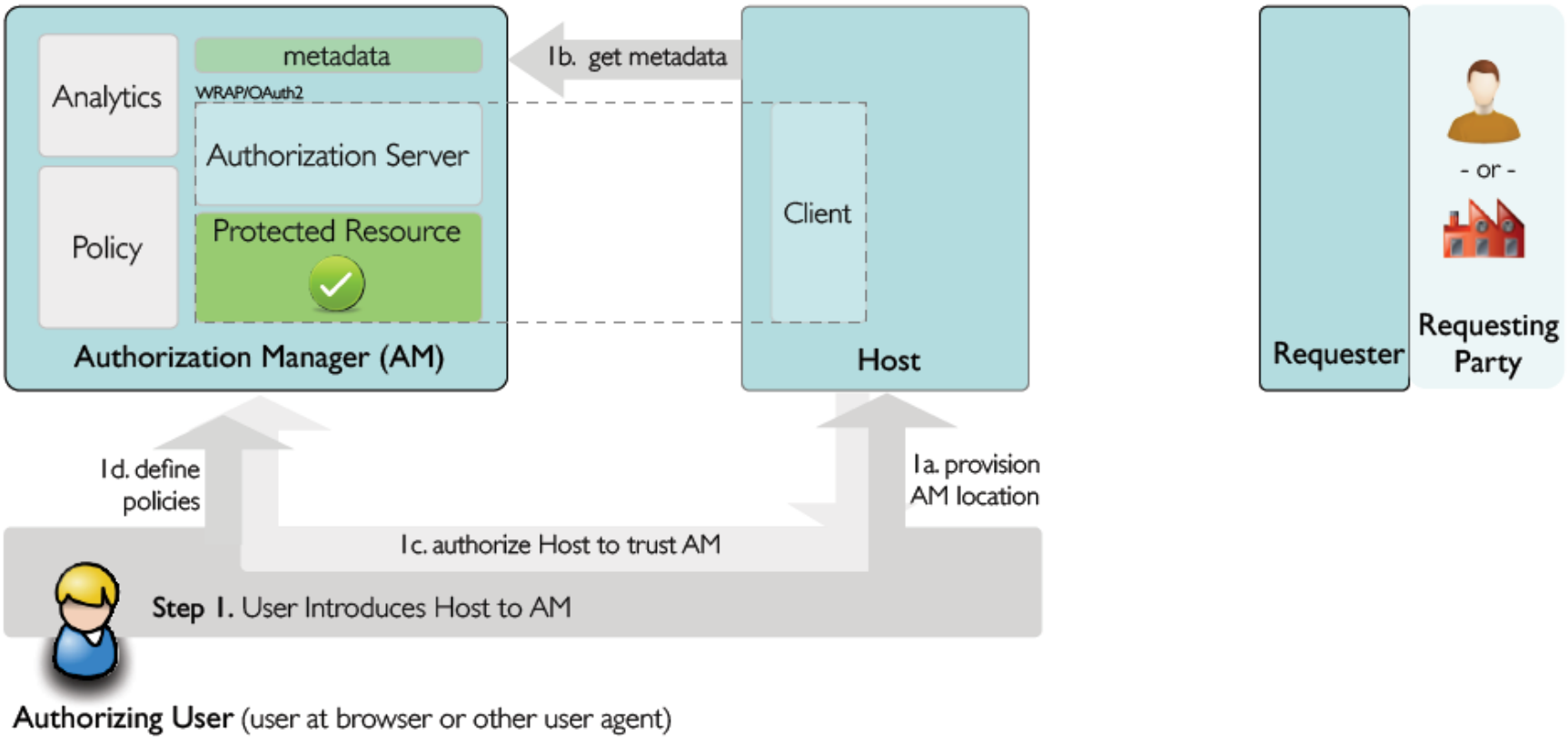
(3) Use a Token

UMA

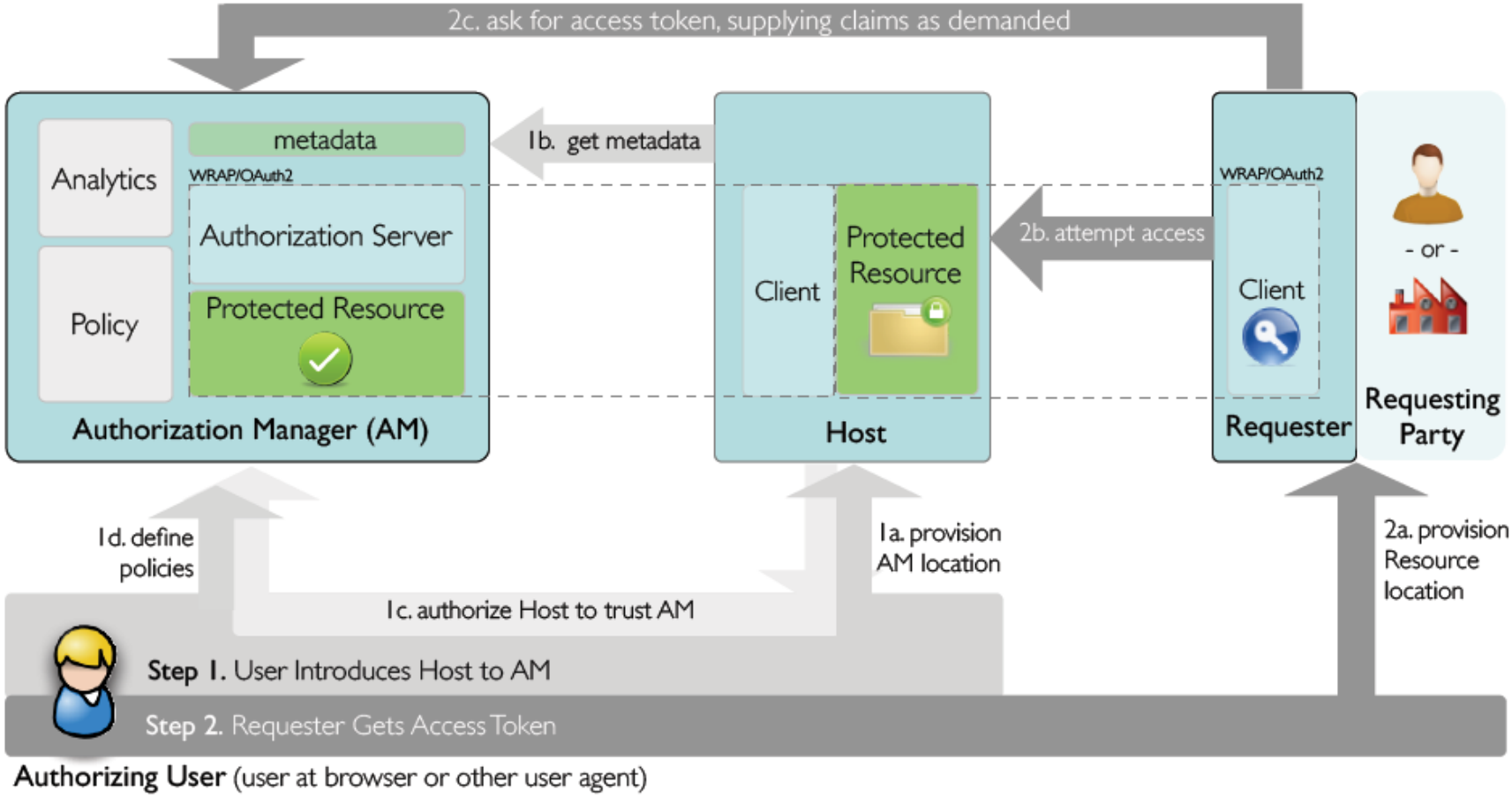


Authorizing User (user at browser or other user agent)

UMA

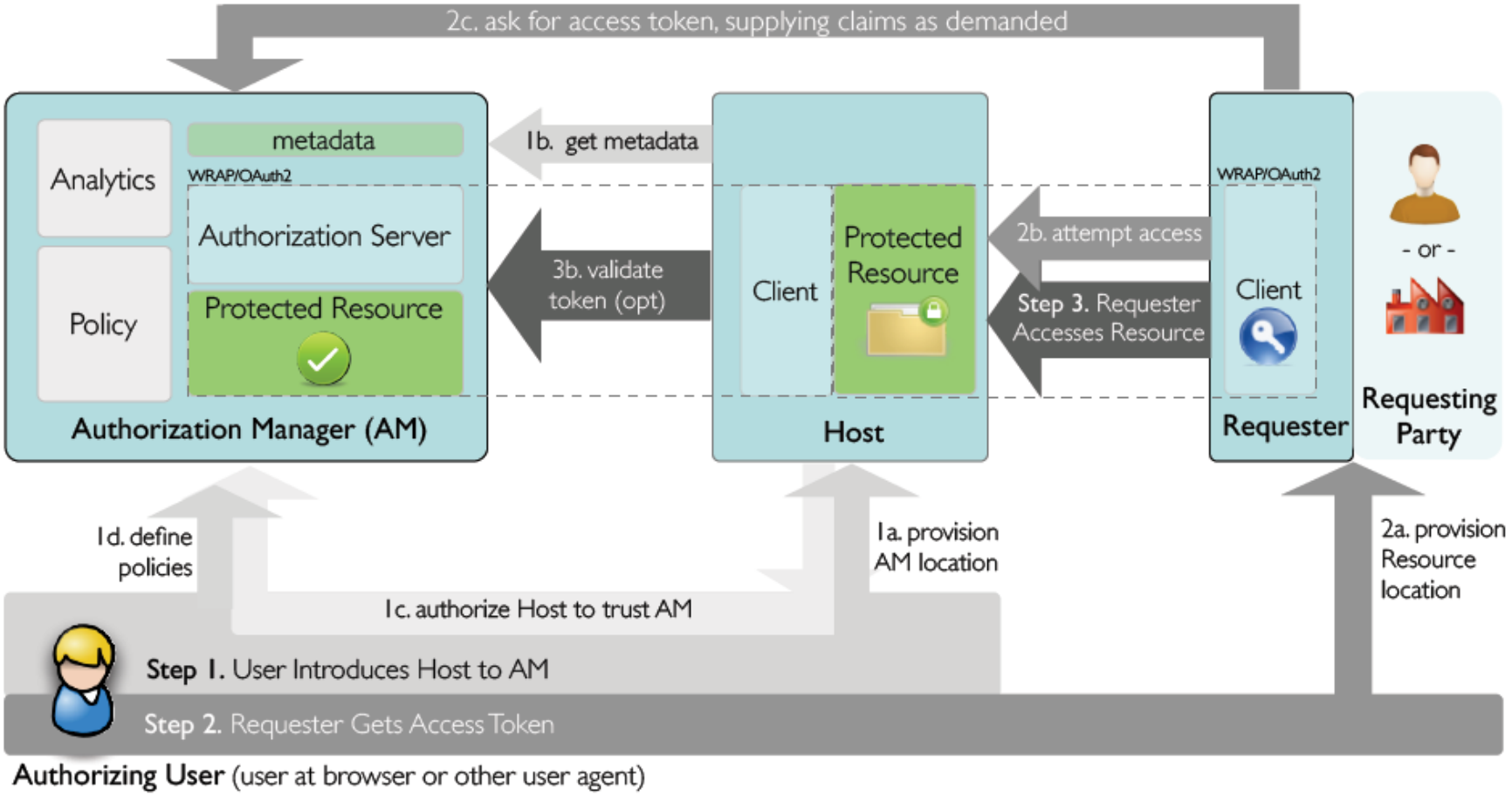


UMA



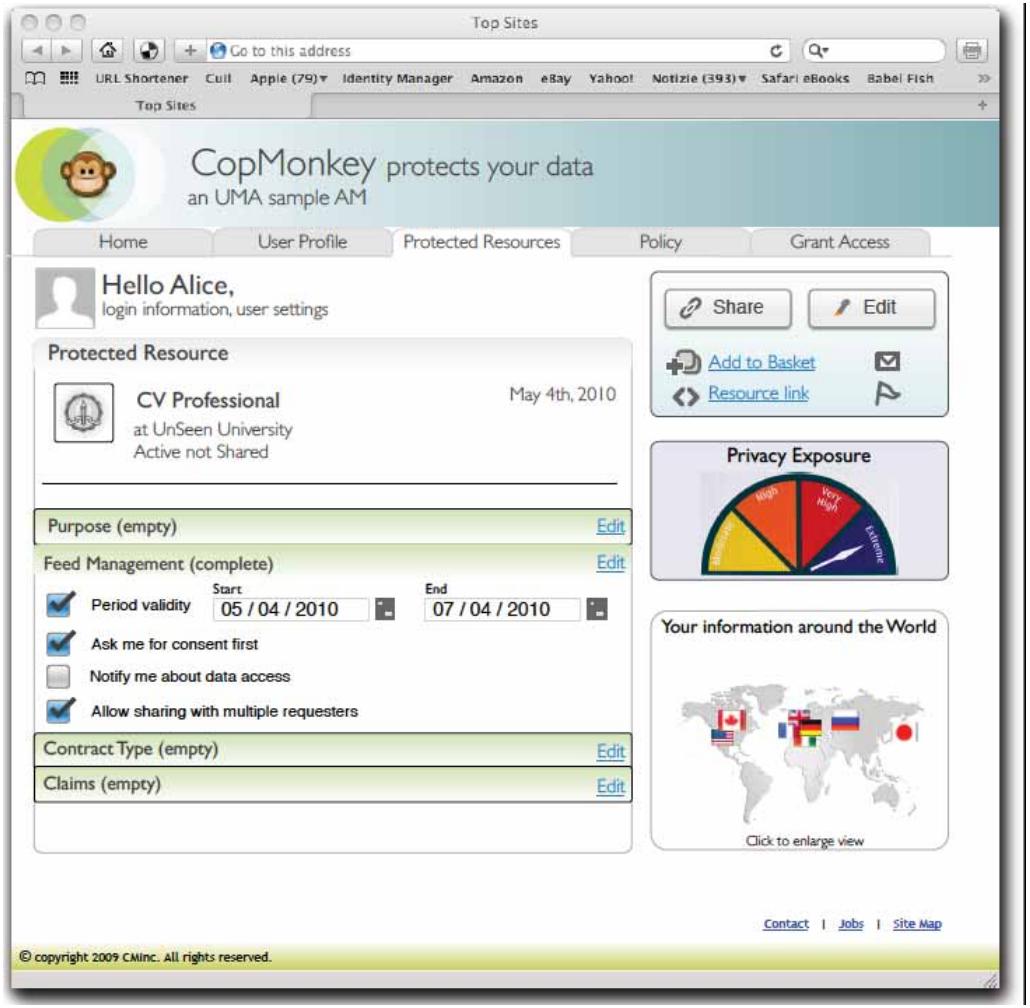
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

UMA



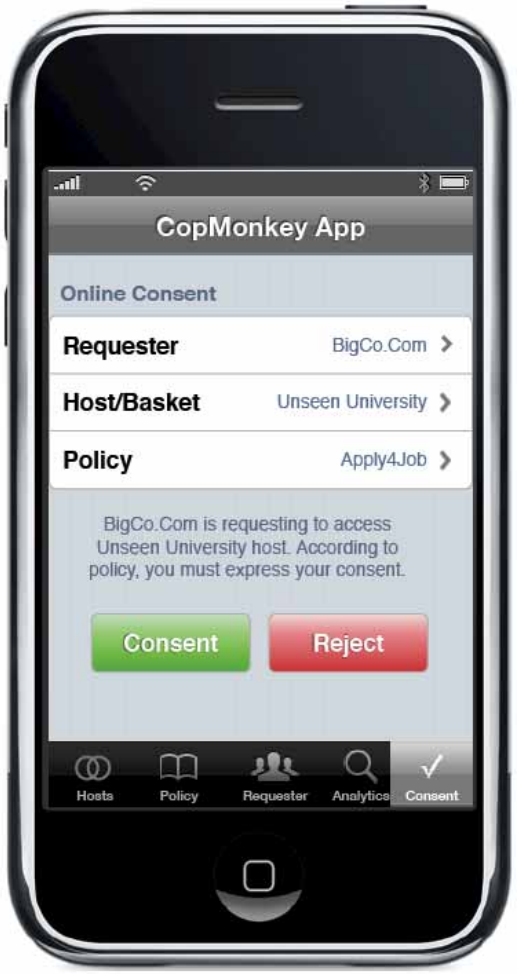
Author: Domenico Catalano, Sun Microsystems, Inc.; Eve L. Maler, PayPal, Inc.

UMA – Authorization Manager



Author: Domenico Catalano, Sun Microsystems, Inc.

UMA – Real-Time User Consent

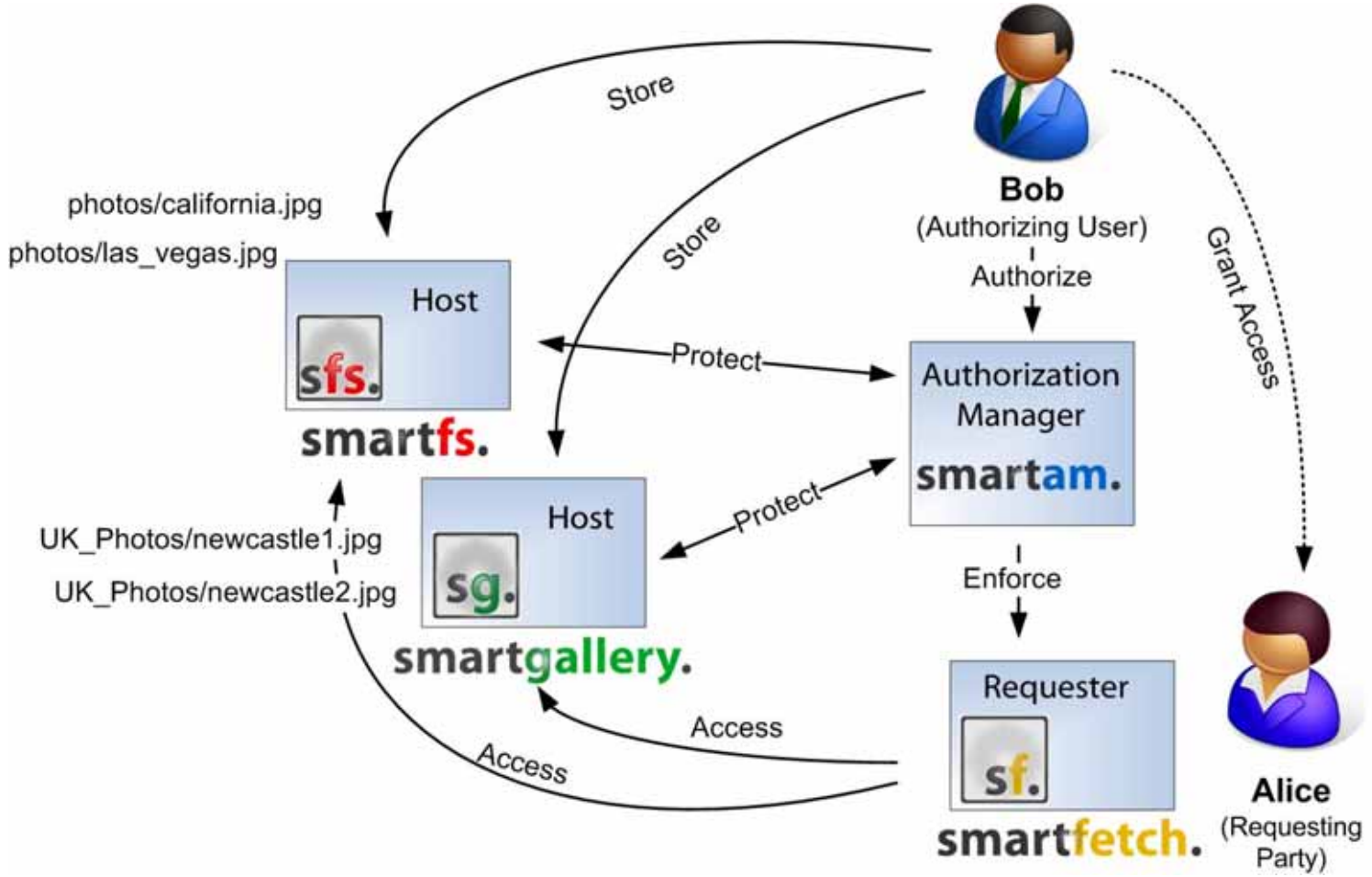


Author: Domenico Catalano, Sun Microsystems, Inc.

UMA - Policies

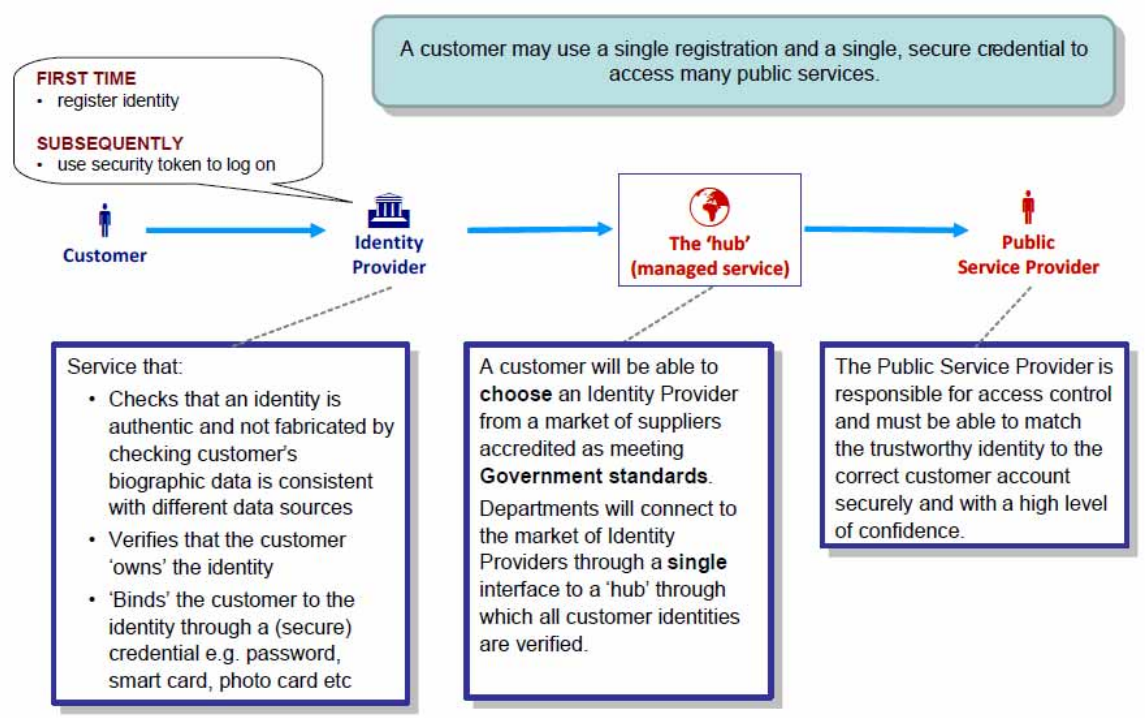
- Unilateral:
  - “Allow access for a week”
- Claims-requiring:
  - “Allow access to anyone who agrees to my licensing terms” (promissory statement)
  - “Allow access to someone who can prove themselves to be bob@gmail.com” (affirmative statement)
  - “Allow access to anyone who says they’re 18 orolder” (self-asserted affirmative statement)

Demo - Architecture



UK government

- identity assurance programme + mydata programme, both to finish in October
- to deal with UK sensitivities: this is not ID card through the back door



conclusion

- UMA emerging as a proposed standard for sharing data in Web 2.0 scenarios
- UMA takes the user perspective
- UMA is gaining a lot of attention, especially when government is involved in services
- at Newcastle: open source software available (currently leeloo OAuth2.0, soon UMA)
- commercial development