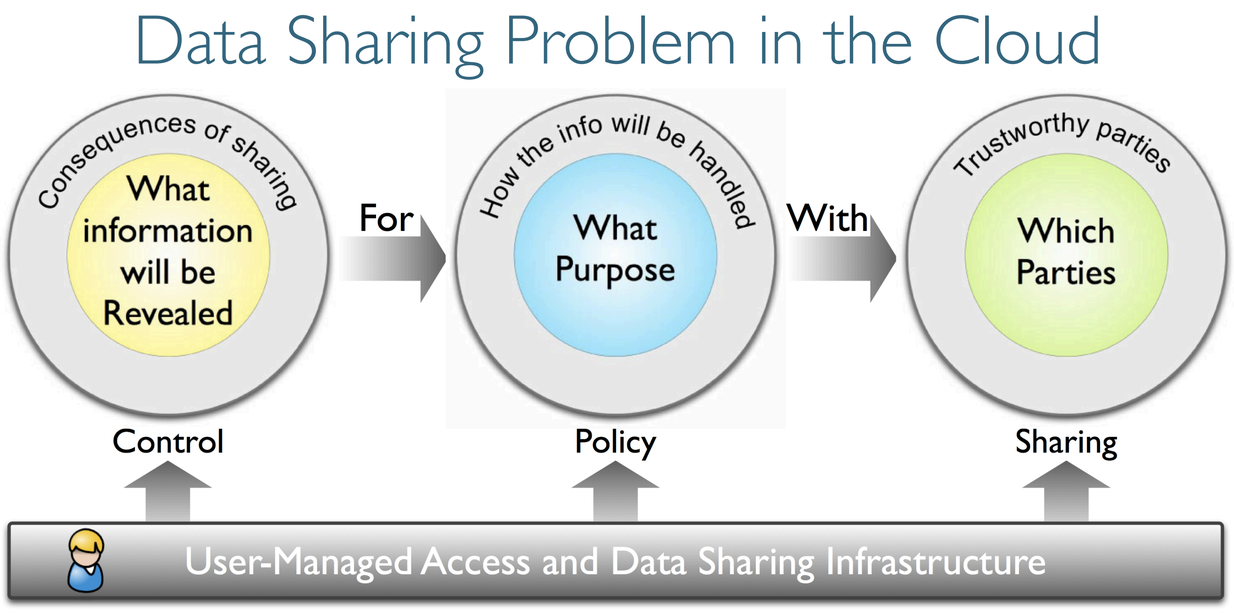
User-Managed Access to Web Resources

Maciej P. Machulak Newcastle University Newcastle upon Tyne, UK - m.p.machulak@ncl.ac.uk
Eve L. Maler PayPal, Inc. San Jose, CA, USA - eve.maler@paypal.com
Domenico Catalano Sun Microsystems Rome, Italy - domenico.catalano@sun.com
Aad van Moorsel Newcastle University Newcastle upon Tyne, UK - aad.vanmoorsel@ncl.ac.uk

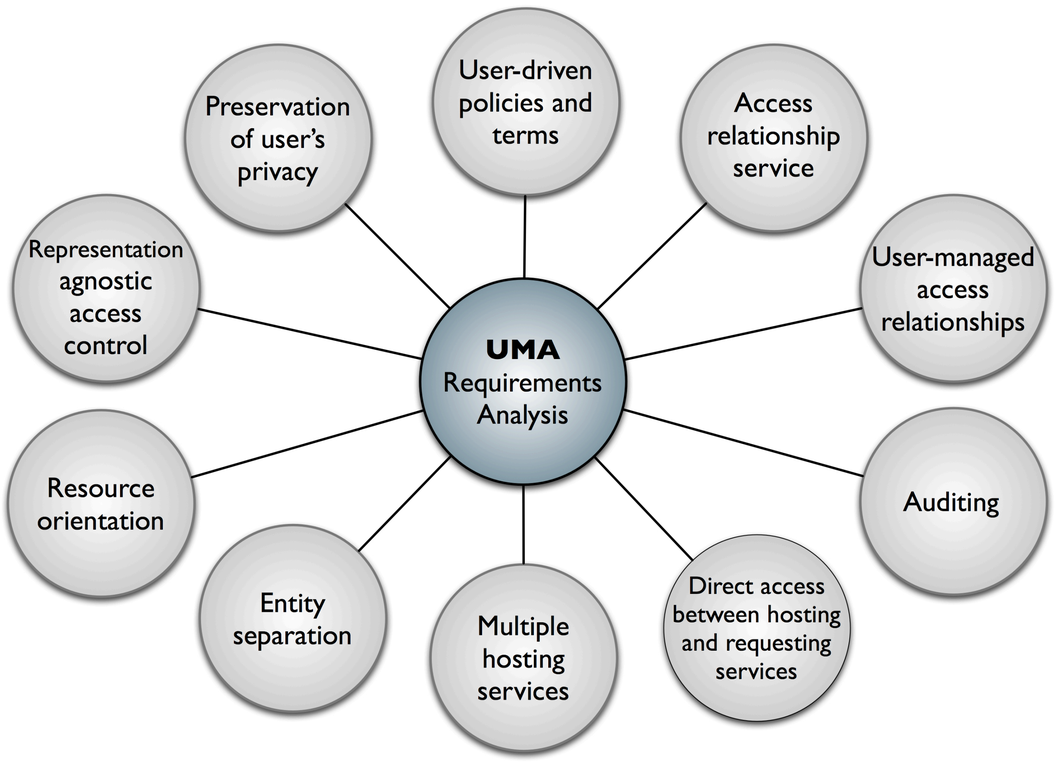
Introduction

Web 2.0 supports users in creating data and acting as content publishers. It allows them to disseminate this data and share it with other users and services on the Web. This requires access control to be put in place. Existing authorization solutions, however, are not well-suited to the user-driven Web environment. They are tightly bound to applications and have limited flexibility in terms of their configuration or adaptation to a particular user's security requirements. Following the highly collaborative Web 2.0 paradigm, there is a clear need for new approaches to access management which would include a user as a core part of their model.

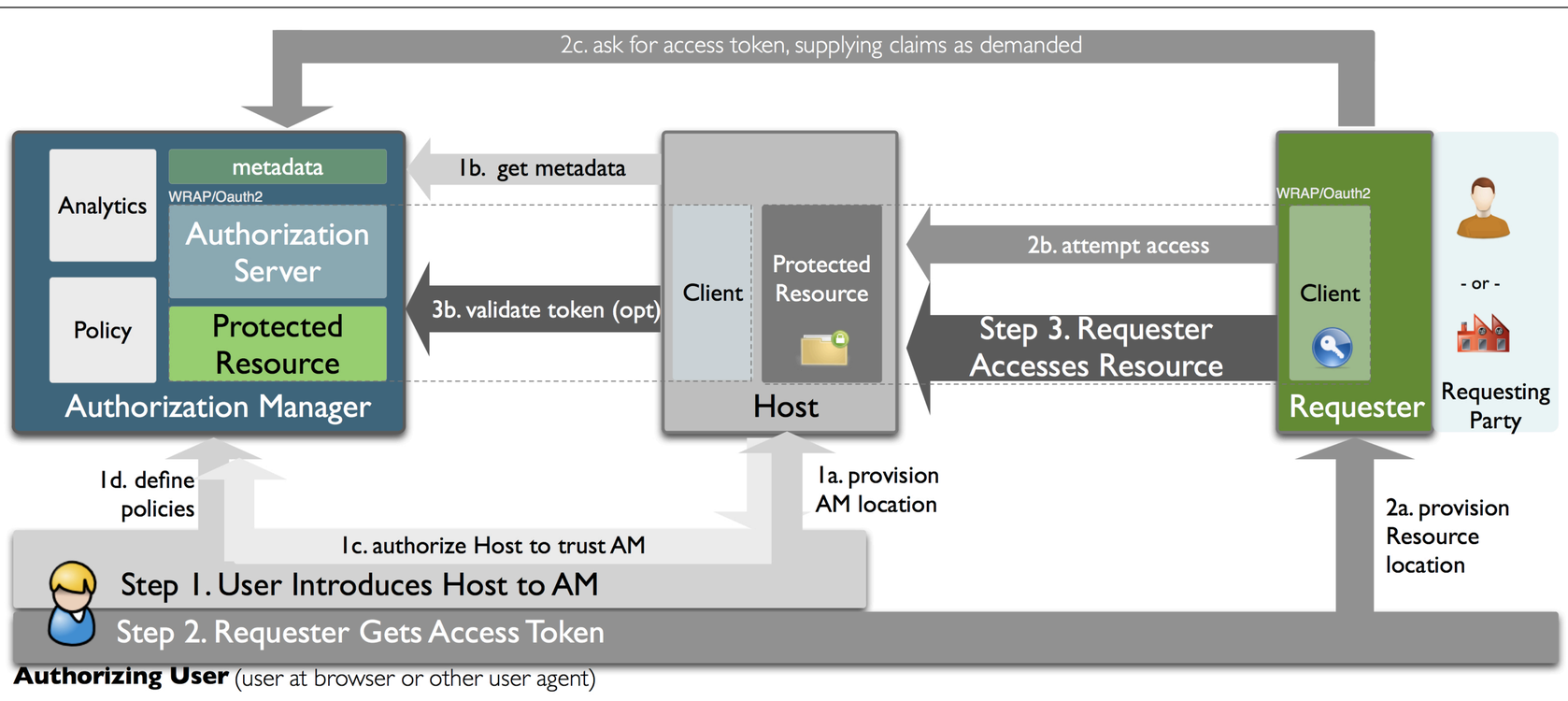


Requirements Analysis

Access management systems for the Web should allow a user to be in control of assigning access rights to their data irrespective of the location of this data. Moreover, they should allow a user to apply the necessary security and privacy controls while retaining all the benefits of social interactions and data sharing on the Web.



The UMA Protocol: Trust a Token, Get a Token, Use a Token



UMA Universe and Approach

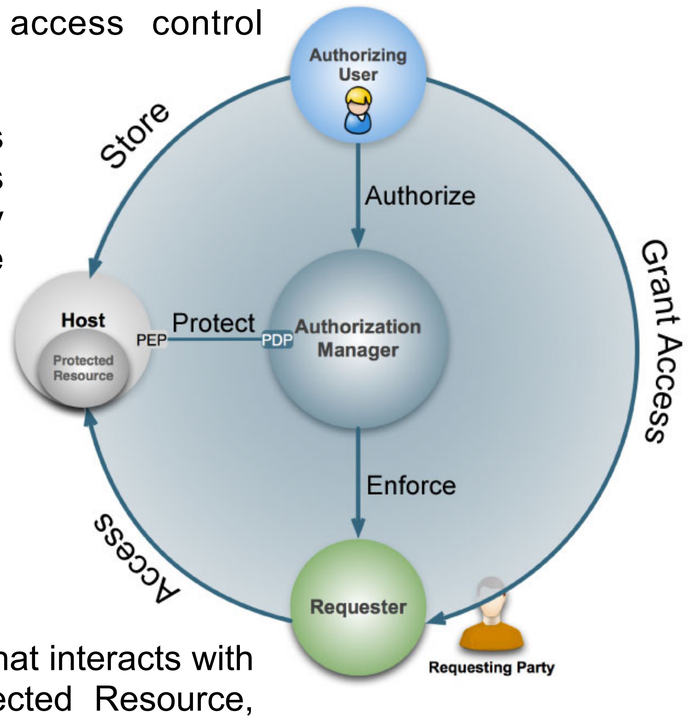
1. Authorizing User - delegates access control from their chosen set of Hosts to an Authorization Manager (AM) and composes access control policies at the AM.

2. Authorization Manager - acts on behalf of the user and evaluates access requests made by Requesters against applicable policies, issuing Access Tokens.

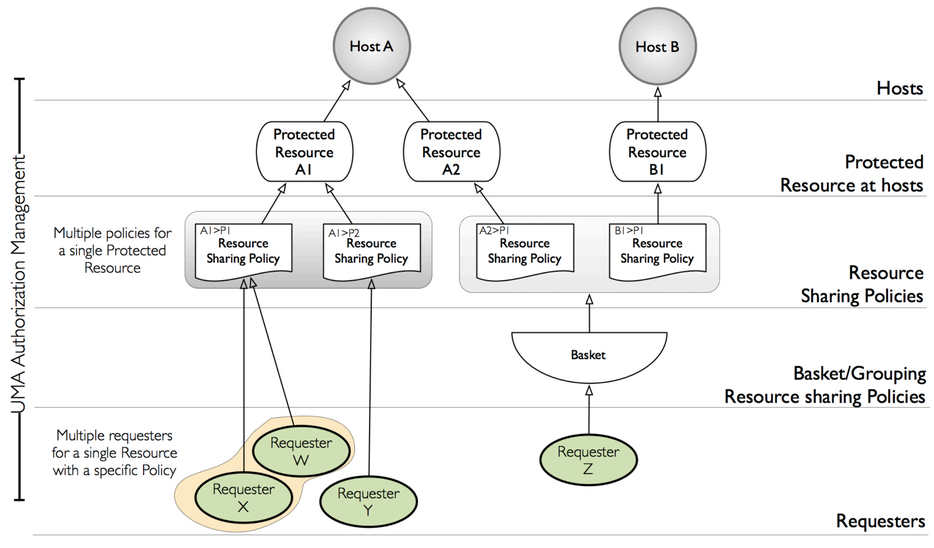
3. Host - a Web application that is used by an Authorizing User to store and manage Protected Resources. It delegates access control to an Authorization Manager.

4. Requester - a Web application that interacts with a Host to get access to a Protected Resource, which can be accomplished after it interacts with the AM to obtain an Access Token.

5. Requesting Party - a person or a company (or a legal person) that uses a Requester to seek protected resource access on their own behalf.



Authorization Manager Information Architecture



Conclusions

The User-Managed Access approach to authorization for Web resources allows a user to play a pivotal role in its model. It empowers a user to flexibly apply the necessary security and privacy controls to their data residing on any number of Hosts and to introduce those hosts dynamically to a user-chosen Authorization Manager. Moreover, UMA supports requesters in gaining authorized access to such data.

This work is partially funded by UK TSB ('Trust Economics') and UK JISC ('SMART').