Managing Resource Protection in UMA

Eve Maler | eve@xmlgrrl.com | @xmlgrrl

V01
15 Dec 2010
Key UMA user story for selective sharing

• As an authorizing user...

• I want to set up selective sharing of one or a set of resources residing at any of my hosts on the web...

• so that I can ensure the resources are shared only with parties I choose, and only in ways I choose, allowing me to track sharing using a single "hub".
Desired abilities

I want to **share** this stuff **selectively**!

I want to **protect** this stuff from being seen by everyone!
Many ways to divide up host and AM responsibilities

**All host**
- Host makes authz decisions; “AM” is just informed of them for auditing reasons

**Balanced**
- Host is in charge of resources; AM is in charge of protection; work is divided for privacy, liability, “single hub” reasons

**All AM**
- AM knows everything about all resources being protected; host hands over all responsibility

**host manages resources; AM protects them**
OAuth 2.0 leaves unspecified how the two servers interact.
UMA has to make their communications interoperable
The AM protection dividing line

AM
host of protected resource
401
go to this AM

requester

halt!
prove you're worthy...
Edge case: host protects some resources itself

- Host allows user to introduce it to an AM, but chooses to protect some of the user’s resources itself
- These resources could be totally private, totally public, or selectively shared through host-specific mechanisms
Edge case: AM protects “totally public” resource

- User wants AM to make it “public but AM-tracked”
- Maps authorization constraints to it that are very loose

AM
host of protected resource

401

go to this AM

requester

halt!

sure, you’re in, I’m just writing this down...
Edge case: AM protects “totally private” resource

- User wants AM to “totally protect” it now, for potential later selective sharing
- Maps authorization constraints to it that are very tight

not no way, not no how!

halt!

401

host of protected resource

401

host of protected resource

go to this AM

requester

?
@@tbs: detail about abstract resource set/action dividing line...

Authorization Manager (AM)
- Analytics
- Trusted Claims
- Policy

metadata
- OAuth 2.0
- Authorization Server

Protected Resource

Client

Host

Requester
- OAuth 2.0

Requesting Party

Authorizing User (user at browser or other user agent)
Step 1 protocol flow

1a. Provision AM location

1b. Get metadata

1c. Authorize Host to trust AM

Ie. Define policies

Ia. Provision AM location

Authorizing User (user at browser or other user agent)
Step 2 protocol flow

**Step 1.** User Introduces Host to AM

1a. provision AM location

1b. get metadata

1c. authorize Host to trust AM

1d. register resources

1e. define policies

**Step 2.** Requester Gets Access Token

2a. attempt access

2b. ask for access token, supplying claims as demanded

**Authorizing User** (user at browser or other user agent)
Step 1. User Introduces Host to AM

Step 2. Requester Gets Access Token

Step 3 protocol flow

1a. provision AM location

1b. get metadata

1c. authorize Host to trust AM

2a. attempt access

2b. ask for access token, supplying claims as demanded

3b. validate token

I. e. define policies

I. a. provision AM location

Step 3. Requester Accesses Resource

Requesting Party

- or -

OAuth 2.0

Policy Analytics

Trusted Claims

Authorization Server

Protected Resource

Authorization Manager (AM)

metadata

OAuth 2.0

Requester

Client

Host

Client

Protected Resource

Step 2. Requester Gets Access Token

Authorizing User (user at browser or other user agent)