Exploring a Simple Trusted Claims approach

Kantara UMA WG
Agenda

• Goal
• Approach
• Trust Requirements
• Conceptual Model of Trust
• Propagation of Trust
• Considerations
Goal

• Provide a simple approach to create a trust path for third party Claim issuing.
UMA Subject

• An UMA subject is an entity that refer to either Authorizing User, or Requesting Party that can perform actions on the AM respectively to authorize data sharing or to provide claims.
UMA Subject’s Data

- Subject
  - Authorizing User
  - Requesting Party

- Data
  - Sharable user data
  - Claims
Claims Host

- Claims Host refers to a TTP Identity Provider who provides certified user claims (i.e. Personal Identifiable Information - PII)
- Claims Host can be protected by a AM’s Requesting Party.
Approach

• The Requesting Party refers to an Identity Provider which acts as **Host/Claim Issuer**.

• The Requesting Party protects the **Host/Claim Issuer** using an Authorization Manager (**AM2**).

• The Authorization Manager’s (**AMI**) Authorizing User acts as **Requester** for the claims.
Trust Requirements

- Authorization Managers (AMs) are well-known Service Provider certified by an Trusted Authority (TA).

- Claim Issuer (CI) is a Trusted Third Party.
Conceptual Model of Trust

Default policy for claims request: Allow only for trusted AM, Online consent requested

(resource protected)

Authorizing User

Host

AM1
Claims Requester

AM2

Requester

Requesting Party

IdP1

restful identity service

IdP2
Claims host

PKI-based trust relationship

Online consent requested

untrusted

Allo
ownly for trusted AM,
Propagation of Trust

1. AM1 Claims Requester requests claims [untrusted] from Requester.

2. AM1 Claims Requester discovers IdP2 Claims Host and requests claims [trusted, not Authorized] from TTP.

3. AM1 Claims Requester gets Token [trusted] from AM2.

4. AM1 Claims Requester requests claims [trusted, Authorized] from IdP2 Claims Host with Signed Claim.
Wireframe claims at AM2
Wireframe claims at AM2

CopMonkey protects your data
an UMA sample AM

Hello Bob,
login information, user settings

Claims Providers

Professional claims
May 4th, 2010

May 4th, 2010

Privately Identifiable Information (PII) (empty)

Profile Attributes (Complete)

- Job Title
- Employer
- Employment date
- Role

Your information around the World

Click to enlarge view

© copyright 2009 CMInc. All rights reserved.
Considerations

- Leverage UMA protocol to propagate trust
- Requesting Party does not need to manage keys
- All the connections are HTTPS