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 Claim issuing.
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 (**AM1**) Authorizing User acts as **Requester** for the claims.
Trust Requirements

• Authorization Managers (AMs) are well-known Service Provider certified by a 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

Authorizing User
Host
IdP1
IdP2
Requester
Requesting Party

AM1
Claims Requester

AM2

(resource protected)

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

(green line): PKI-based trust relationship
(red line): untrusted
Propagating Trust

1. **Requests claims**
   - AM1 Claims Requester
   - Requester
   - I'm Bob, here's a TTP claims issuer

2. **Discovery**
   - AM1 Claims Requester
   - Requests claims [trusted, not Authorized]
   - IdP2 Claims Host
   - TTP
   - Resource protected by AM2

3. **Get Token**
   - AM1 Claims Requester
   - AM2
   - Consent
   - Yes, I give consent for this claim

4. **Requests claims**
   - AM1 Claims Requester
   - Signed Claim
   - IdP2 Claims Host
   - TTP
   - [trusted, Authorized]
Considerations

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