Using UMA tClaims model to restrict and personalize access to online service
An Enterprise Class scenario

Kantara UMA WG
Agenda

- Scenario
- Requirements Analysis
- Conceptual Model
- Example Deployment model
- tClaims Flow
- User Interaction
- Trust Model
Accessing Personal Loan special program

Enterprise Class Scenario

- Bank online service provides an User-Managed tClaims access control to restrict and personalize access to special program/service (i.e. personal loan with low interest rate) to users which have determinate employment (i.e. government employee), and have an high credit score.
Requirements Analysis

- Authorizing User (Resource Owner) needs a claims-based access control to restrict access to own resources based on Identity attributes of Requesting Party.

- Identity attributes must issued by a Trusted Third Party (TTP) and verifiable by a Claims Requester.

- Claims may be logically aggregated to provide a collection of attributes from different Attribute Providers (Claims Host).
UMA tClaims Requirements

Personal loan with low interest rate

- User-Managed Automated Registration (opt)
  - Basic attributes (tClaims)
- Access Control to special program/service
  - Job role attribute (tClaims)
  - Credit score attribute (tClaims)
Example Deployment Model

Browser

Web Application

Enterprise Access Management (EAM)

UMA Authorization Manager

Claims Host

Requesting Party

Web Application

UMA Authorization Manager

Claims Host

Authorizing User

Admin

Fed

UMA Requester
UMA tClaims high level flow
UMA tClaims Access Token Request

- A tClaims Access Token Request must be done from a tClaim Requester in order to obtain a valid Access Token to request a tClaims Document from a Claims Host.
UMA tClaims Catalog

- **tClaims Catalog** is an UMA Authorization Manager’s function which maintains the list of tClaims referrals from registered Claims Hosts and provides the rules to match requested tClaims from a Requester.

- **tClaims Catalog** provides a single point-of contact for UMA AM tClaims Requester.
UMA tClaims Access Token

- **tClaims Access Token** is issued by UMA Authorization Manager after the Subject (Requesting Party) grants access to the tClaims requested from the Requester (Client).

- **OpenID AB** provides specification for constructing “**Positive Assertion**” that may be used as UMA tClaims profile for Claims Hosts which are OpenID Provider.
UMA tClaims Document

• **tClaims Document** is issued by Claims Host (an UMA protected Resource) after receiving a valid tClaims Access Token from the Requester and it contains Subject’s identity attributes.

• Claims Hosts being a registered resource at AM can optionally verify the tClaims Access Token with the AM (back-channel), before to release the tClaims Document.
User Interaction
Alice at Authorization Manager Site

AM Menu

Protected Claims Host

tClaims already used
Alice at Bank site for Authentication
Alice at Bank site for requesting access to a restricted service. An UMA protected resource.
Alice at CopMonkey site for Authentication
Alice at CopMonkey site for granting access to requested tClaims
Welcome to special loyalty program for US Government Employee.
Based on your Credit score you can have access to following personal loan amounts and conditions:

- $10,000 at 2.0%
- $20,000 at 2.5%

Select your preferred condition and click on continue to proceed with loan request, or Cancel to return online banking services.
Bootstrapping Trust

Subject Registration

Claims Host Registration

UMA Introduction

Protected Resource

IdP List

LoA Certification

TPF

Notification (AM as RP)

LoA Certification (AM as IdP)

Certifier

TFP

LoA Certification

IdP

Claims Host

UMA

AM

Subject

Affiliate Authentication

IdP

Affiliate SSO

Uma
Thanks