UMA Trusted Claims

Kantara UMA WG
Bootstrapping Trust

- Subject Registration
- Claims Host Registration
- UMA Introduction
- Subject
- IdP
- UMA AM
- IdP List
- Protected Resource
- TFP
- Notification (AM as RP)
- LoA Certification (AM as IdP)
- LoA Certification
- IdP
- Claims Host
- Affiliate Authentication
- Affiliate SSO
- LoA Certification
- Certifier
- UMA
- Claim Registration
If you would like to register a new account, select the preferred registration mechanism from list below and follow the instructions provided.

**Self-Service Registration (untrusted)**

**Trusted Registration (CopMonkey IdP - LOA:2)**

**Affiliate Registration**

- OpenID®
- SAML IdP
Hello Alice,

login information, user settings

Trusted Claims Providers

Google.com

Internet Identity Attributes
Affiliate Registration: LOA-1

Add Provider

Options

Trusted Claims Providers Feed
- Certified a new IDP
- Create a Claims Host
- Trusted Framework Provider
- Attributes Service at Telco

Privacy Exposure

Your information around the World

Click to enlarge view

Pre-registered Claims Host through Affiliate Registration
Add a Trusted Claims Host
Managing Trusted Claims
Add a new Claims Host

Hello Bob,
login information, user settings

Trusted Claims Providers

- **Google.com**
  - Internet Identity Attributes
  - LOA-1
  - May 4th, 2010
  - Options ▼

- **MyCompany.Com**
  - Professional Identity Attributes
  - LOA-2
  - May 4th, 2010
  - Options ▼

Trusted Claims Providers Feed
- Certified a new IDP
- Create a Claims Host
- Trusted Framework Provider
- Attributes Service at Telco

Privacy Exposure

Your information around the World

Click to enlarge view
Managing Trusted Claims
Select a preferred Claims Host
Managing Trusted Claims
Register the Claims Host
Managing Trusted Claims

Hello Bob,
login information, user settings

Trusted Claims Providers

Google.com
Internet Identity Attributes
LOA-1
Oct 4th, 2010
Options ▼

MyCompany.Com
Professional Identity Attributes
LOA-2
Oct 5th, 2010
Options ▼

Global Trust Bank
Account Identity Attributes
LOA-3
Oct 8th, 2010
Options ▼

Certified a new IDP
Create a Claims Host
Trusted Framework Provider
Identity Attribute at Telco

Privacy Exposure

Your information around the World

Click to enlarge view
Managing Trusted Claims
View attributes
Managing Trusted Claims
Attributes settings

Hello Bob,
login information, user settings

Claims Providers
Google.com
Internet Identity Attributes
LOA-1

Oct, 4th, 2010

Basic Attributes (6)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Consent</th>
<th>Notify</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fullname</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DataOfBirth</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timezone</td>
<td>Public</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Profile Attributes (empty)

Certified a new IDP
Create a Claims Host
Trusted Framework Provider
Identity Attribute at Telco

Privacy Exposure

Your information around the World

Click to enlarge view

© copyright 2009 CMInc. All rights reserved.
Managing Trusted Claims
Managing Trusted Claims
Add a new Claims

Hello Bob,
login information, user settings

Claims

Proof of Age
Nov 18th, 2010

Managing Trusted Claims
View available Claims
Create a new Claims
Update Claims

Privacy Exposure

Your information around the World

Click to enlarge view
Hello Bob,
login information, user settings

Create New Trusted Claims

Assign Resources sharing policy to Basket

<table>
<thead>
<tr>
<th>Claims Host Provider</th>
<th>Attribute</th>
<th>in the Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google.Com</td>
<td>FullName</td>
<td>Google.Com&gt; Email</td>
</tr>
<tr>
<td>MyEmployer.COm</td>
<td>Gender</td>
<td>&lt;</td>
</tr>
<tr>
<td>Global Trust Bank</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>eCommerce</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Done or Cancel
AM2|Authorization Manager

Hello Bob,
login information, user settings

Claims

- Proof of Age
  - Nov 18th, 2010
- Proof Email Account
  - Nov 18th, 2010

Managing Trusted Claims
- View available Claims
- Create a new Claims
- Update Claims

Privacy Exposure

Your information around the World

Managing Trusted Claims
View Trusted Claims available
Bob attempts to access to the Protected Resource
UMA
Trusted Claims
Sequence Diagram

Source diagram at http://is.gd/g0gJH
STEP 1
Subject Authentication
STEP. 1
Authentication
STEP 2. Provisioning Protected Resource Link
STEP 2.
Provisioning Protected Resource Link
STEP 3.
AM1 applies policy
STEP 3.
AMI applies policy

Validating request...

The protected resource requires trusted claims...

In few seconds you will be redirected to Trusted Claims Provider...
STEP 4.
AM2 - Subject Authentication
STEP 4.
AM2 - Subject Authentication
STEP 5.
Subject Consent
STEP 5.
Subject Consent

MyPhoto.Com
Shared Photo

Hello Bob,

Enter login information, user settings

Shared Photos

New Gallery

Insert the link to get access to the shared photos

https://photo4friend.com/share?d=f2bc56dd45

AM2|Authorization Manager

CopMonkey.Com, on behalf of Photo4Friend's Authorizing User, is trying to get the following claims:

Proof Email Account

Nov 18th, 2010

Deny  Allow
STEP 6
Bob gets access to the resource