

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.

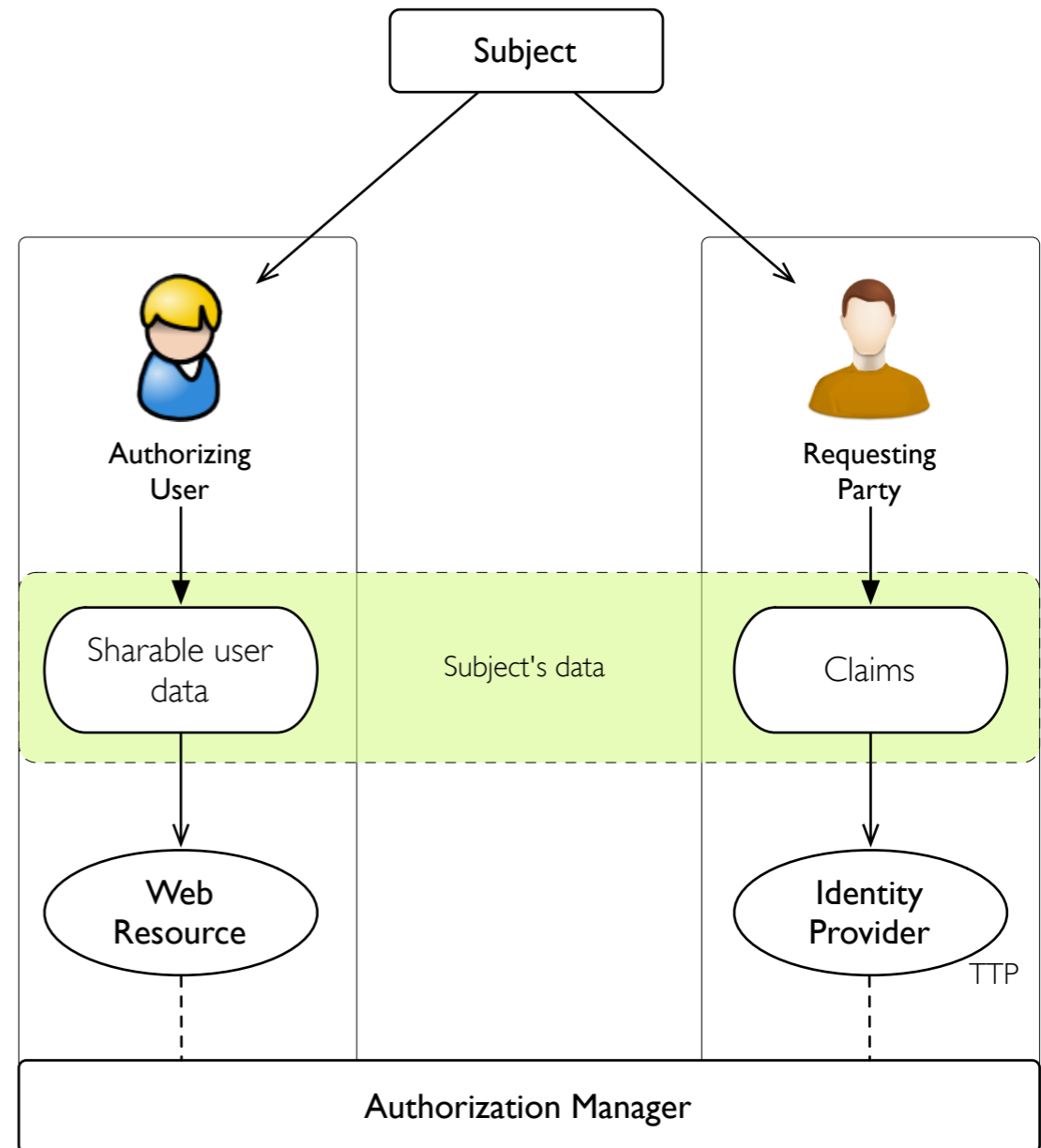
UMA Subject

- 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.

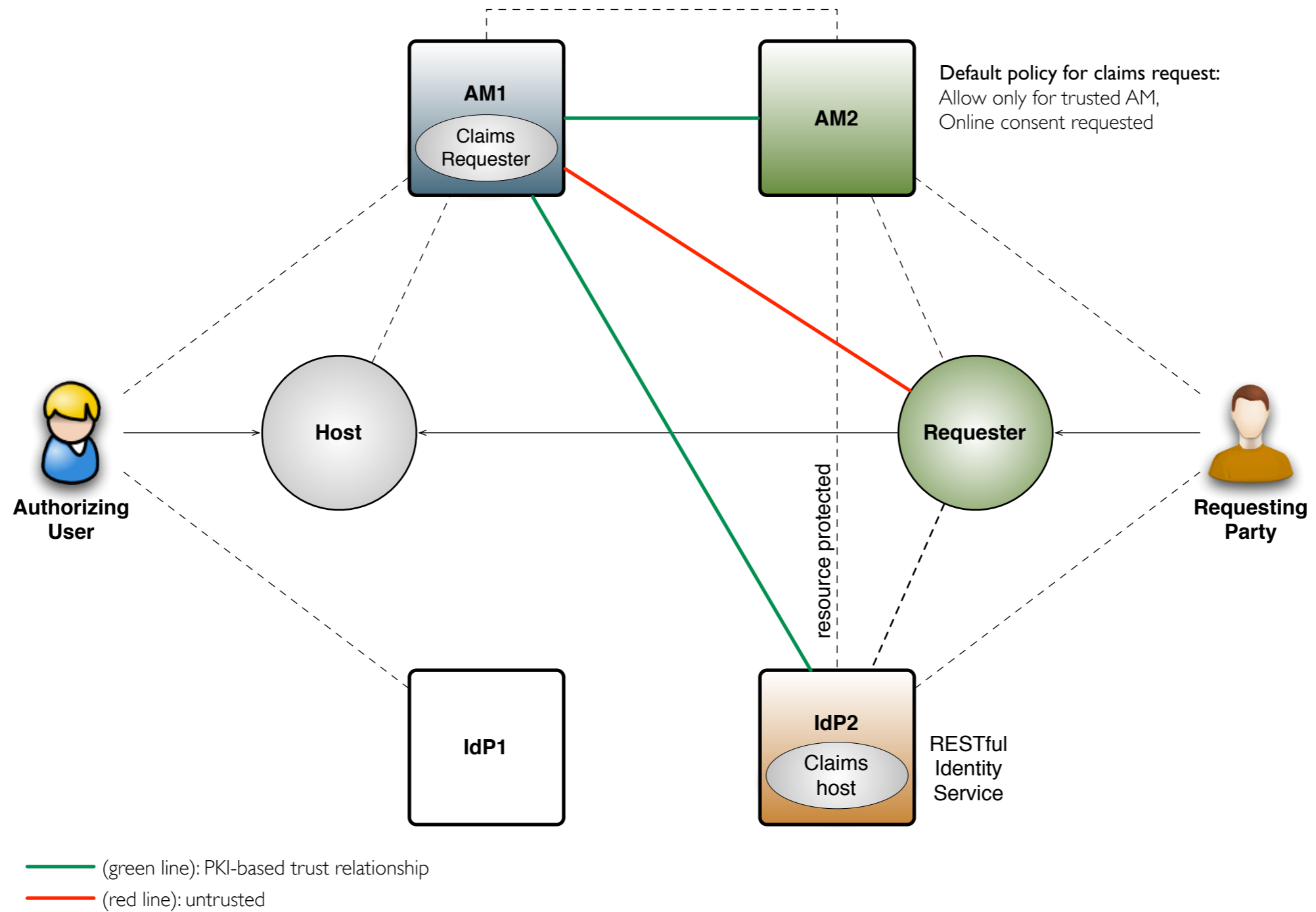
Approach

- 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.

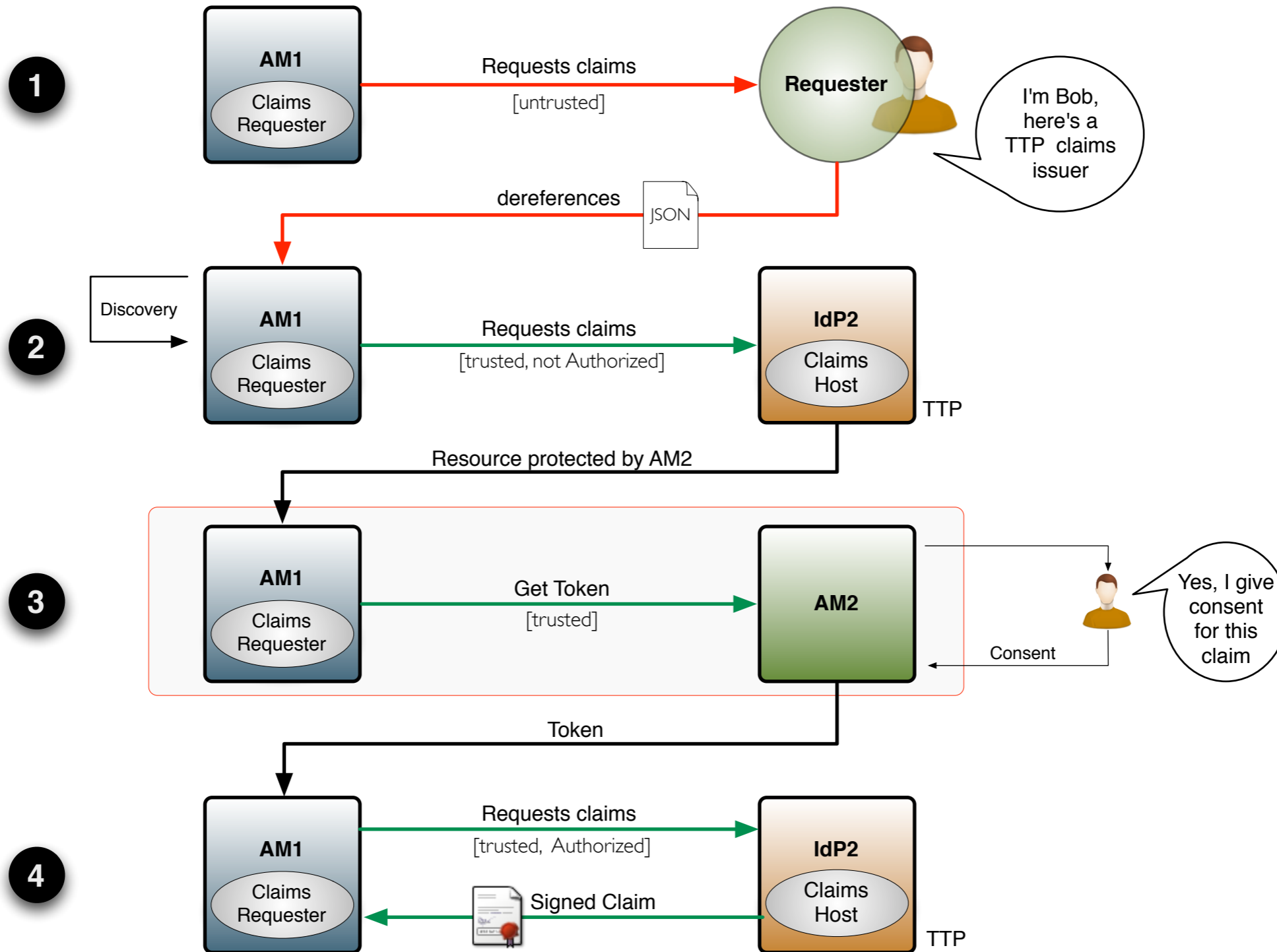
Trust Requirements

- 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



Propagation of Trust



Wireframe claims at AM2

The screenshot shows a web browser window titled "Top Sites" displaying the CopMonkey interface. The page is titled "CopMonkey protects your data an UMA sample AM". The navigation bar includes "Home", "User Profile", "Protected Resource", "Claims", and "Grant Access". The "Claims" tab is selected, indicated by a red arrow. The main content area is divided into several sections:

- Hello Bob, login information, user settings**
- Claims Providers**: A list of providers, including "Professional claims at Global Broker IdP Active" dated "May 4th, 2010". A red arrow points to this entry.
- Trusted AM**: A section with a "Search AM" button and a flag icon.
- Privacy Exposure**: A gauge showing levels of exposure: Moderate, High, Very High, and Extreme.
- Your information around the World**: A world map with flags indicating data locations. A "Click to enlarge view" link is present.
- Personally Identifiable Information (PII) (empty)** and **Profile Attributes (Complete)**: Two rows with "Edit" links. Red arrows point to these rows.

At the bottom, there are links for "Contact", "Jobs", and "Site Map", and a copyright notice: "© copyright 2009 CMInc. All rights reserved." A logo with the letters "UMA" is visible in the bottom right corner.

Wireframe claims at AM2

Top Sites

Go to this address

URL Shortener Cuil Apple (79) Identity Manager Amazon eBay Yahoo! Notizie (393) Safari eBooks Babel Fish

Top Sites

CopMonkey protects your data
an UMA sample AM

Home User Profile Protected Resource **Claims** Grant Access

Hello Bob,
login information, user settings

Claims Providers

Professional claims May 4th, 2010
at Global Broker IdP
Active

Personally Identifiable Information (PII) (empty) [Edit](#)

Profile Attributes (Complete) [Edit](#)

- Job Title
- Employer
- Employment date
- Role

Trusted AM

[Search AM](#)

Privacy Exposure

Your information around the World

Click to enlarge view

[Contact](#) | [Jobs](#) | [Site Map](#)

© copyright 2009 CMI Inc. All rights reserved.



Considerations

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

