Exploring a Simple Trusted Claims approach

Kantara UMA WG

Agenda

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

Goal

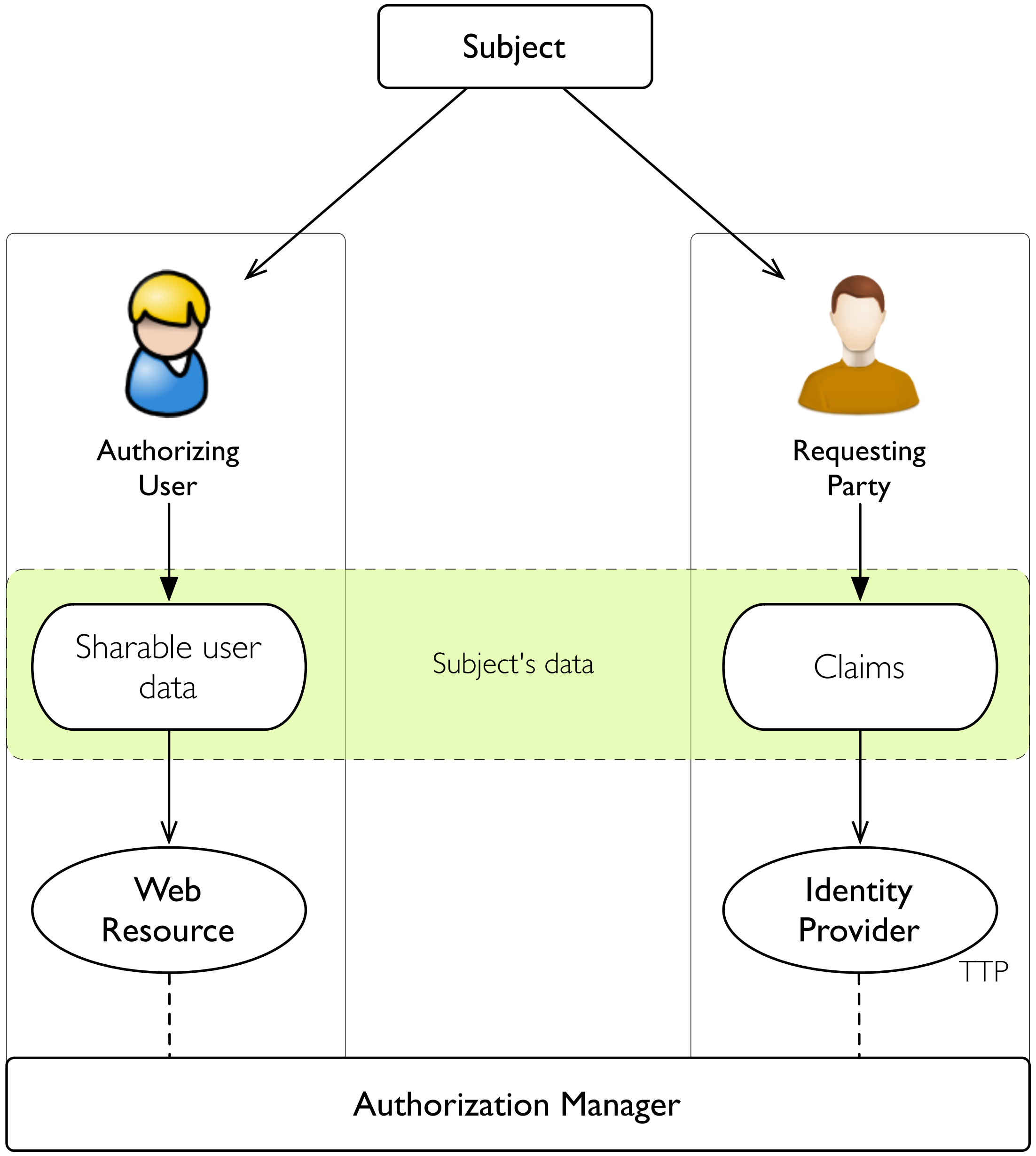
- Provide a simple approach to create a trust path for third party Claim issuing.

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.

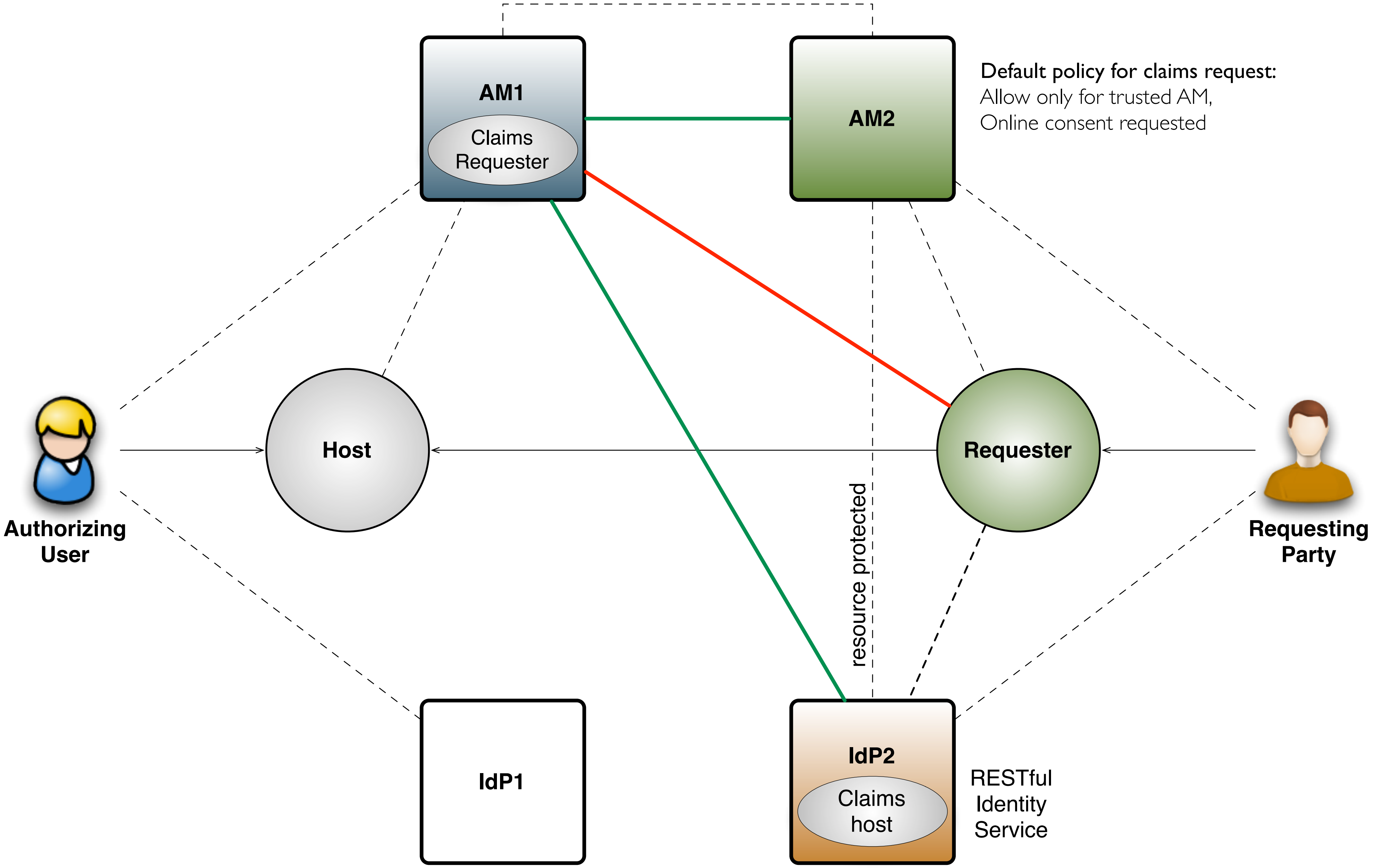
Approach

- 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 (**AM1**) 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



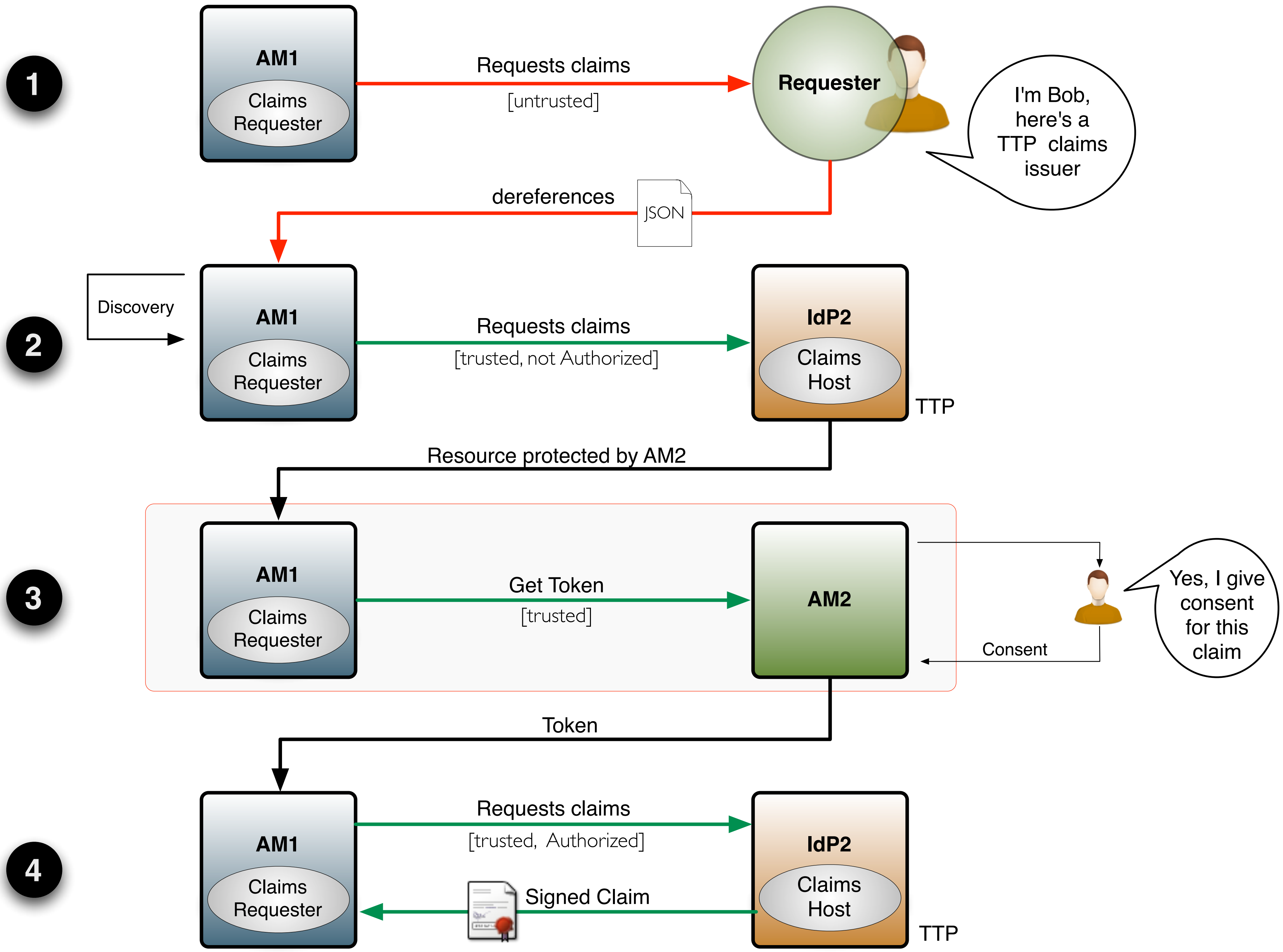
Default policy for claims request:
Allow only for trusted AM,
Online consent requested

RESTful
Identity
Service

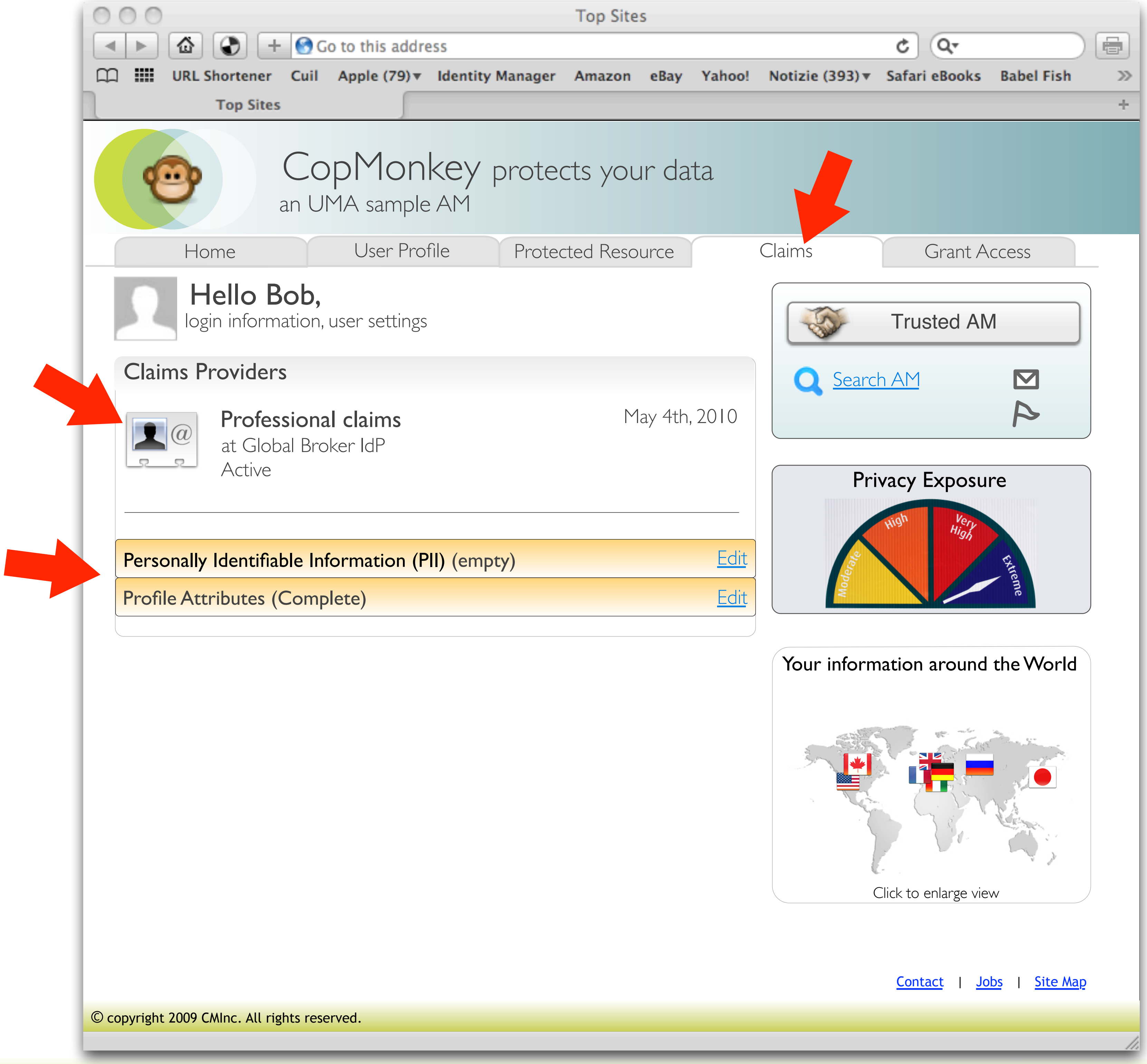
(green line): PKI-based trust relationship

(red line): untrusted

Propagation of Trust



Wireframe claims at AM2



CopMonkey protects your data
an UMA sample AM

Hello Bob,
login information, user settings

Claims Providers

Professional claims
at Global Broker IdP
Active

May 4th, 2010

Personally Identifiable Information (PII) (empty) Edit

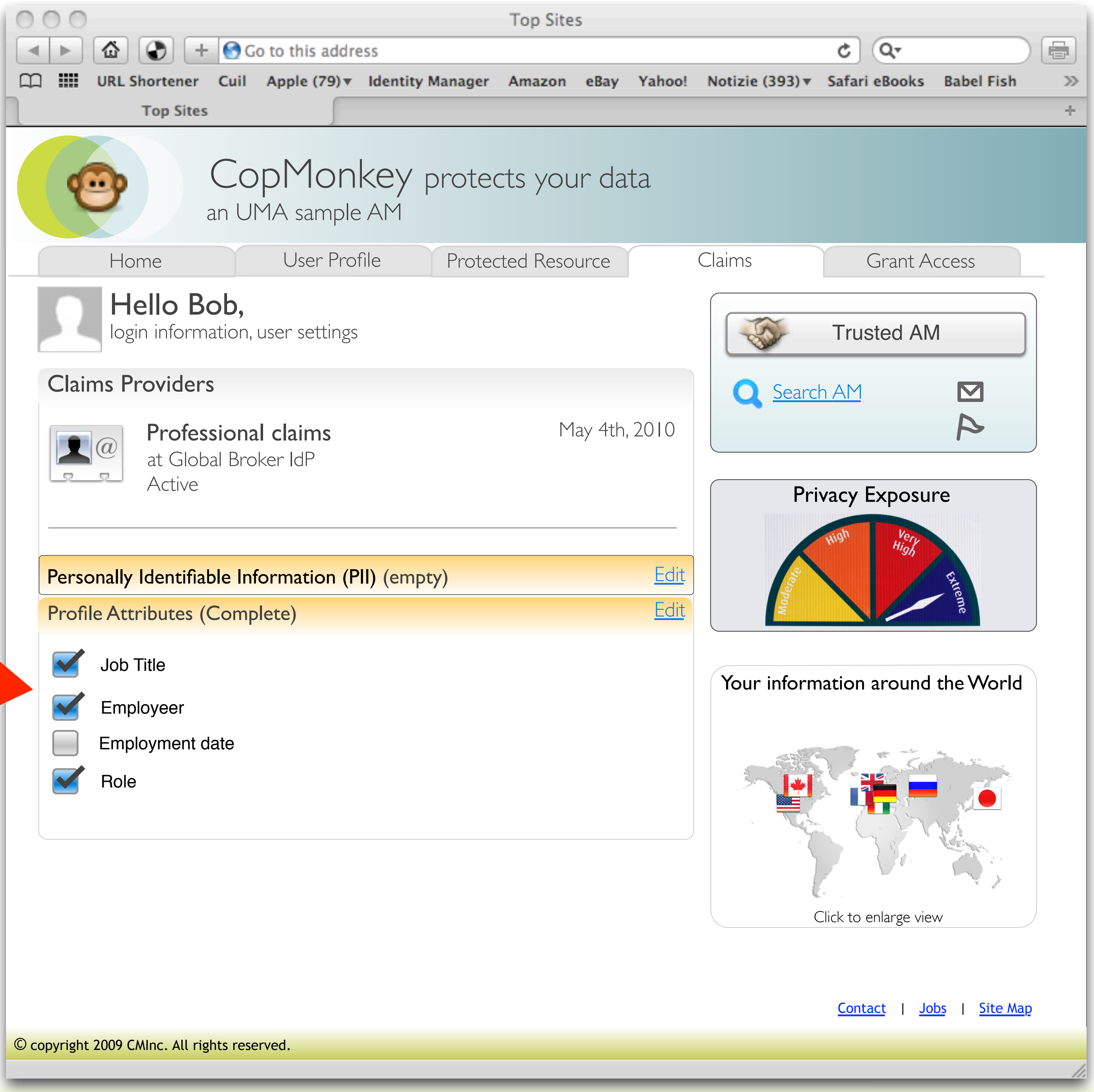
Profile Attributes (Complete) Edit

Your information around the World

Click to enlarge view

© copyright 2009 CMInc. All rights reserved.

Wireframe claims at AM2



CopMonkey protects your data
an UMA sample AM

Hello Bob,
login information, user settings

Claims Providers

Professional claims
at Global Broker IdP
Active

May 4th, 2010

Personally Identifiable Information (PII) (empty) Edit

Profile Attributes (Complete) Edit

☑ Job Title

☑ Employeer

☐ Employment date

☑ Role

© 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