

UMA Claims 2.0 and OpenID Connect An integration scenario

Kantara UMA WG



Agenda

- **UMA Claims 2.0**
- **Requirements**
- **OpenID Connect**
- **Conceptual model**
- **User Experience**

UMA Claims 2.0

- The primary driver for Claims 2.0 is the process of negotiation for access authorization defined by the User-Managed Access (UMA) core protocol, in which an authorization manager can require a requester to convey claims on behalf of a requesting party, in order to satisfy the policies of an authorizing user.

Requirements Analysis

- Authorizing User needs a claims-based access control to restrict access to own protected resource.
- UMA Authorization Manager can require a requester to convey claims.
- Requesting Party must provide specific Claims to access to protected resource under claim-based access control.

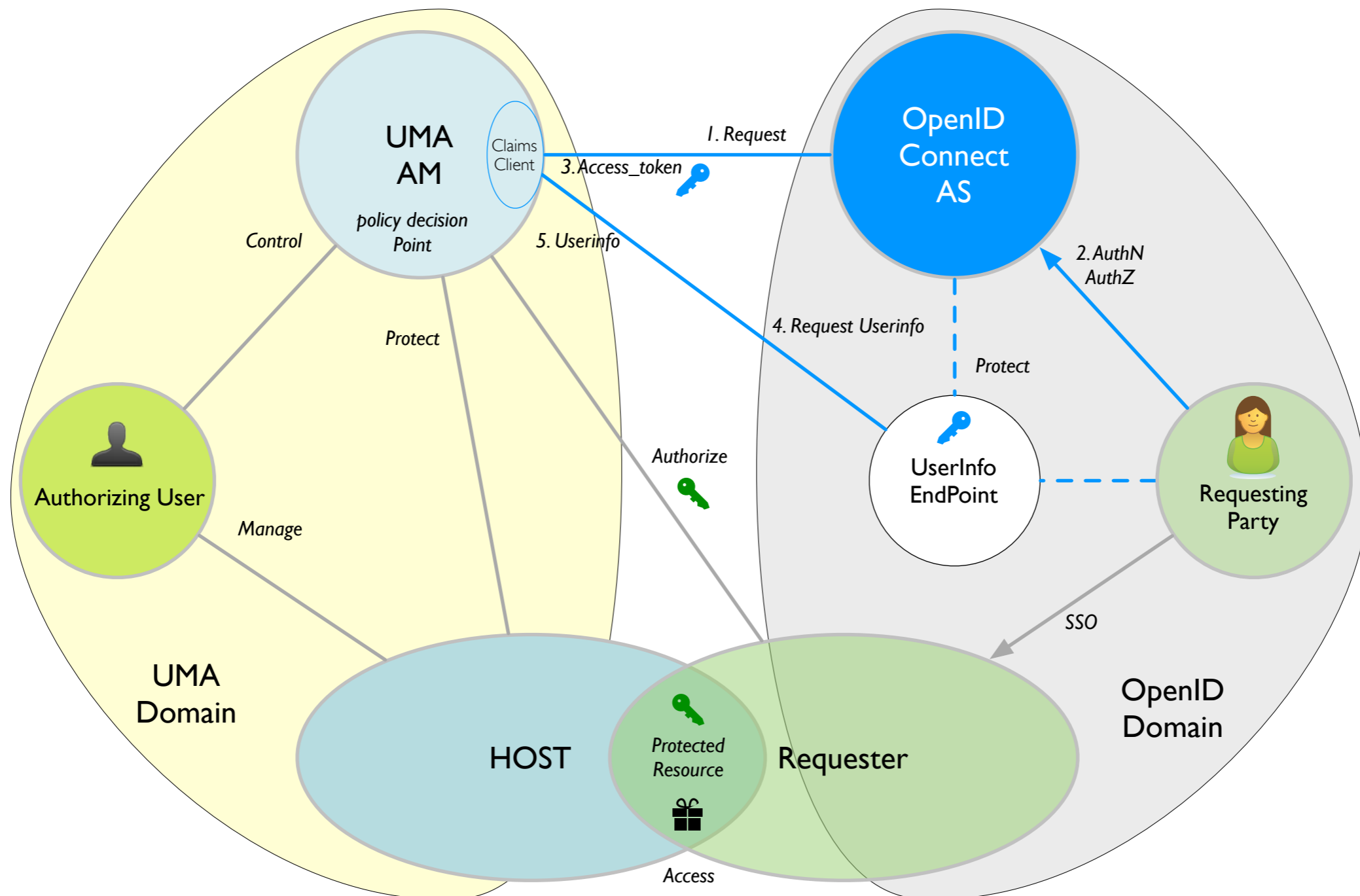
OpenID Connect

- OpenID Connect provides authentication, authorization, and attribute transmission capability. It allows third party attested claims from distributed sources.
- This specification is largely compliant with OAuth 2.0 draft 15.

OpenID Connect protocol overview

- **OpenID Connect protocol in abstract follows the following steps:**
 1. The Client sends a request to the Server's End-User Authorization Endpoint.
 2. The Server authenticates the user and obtains appropriate authorization.
 3. The Server responds with `access_token` and a few other variables.
 4. The Client sends a request with `access_token` to the Userinfo Endpoint.
 5. Userinfo Endpoint returns the additional user supported by the Server.

UMA-OpenID Connect Integration Conceptual Model



User eXperience

Scenarios

- UMA Host In-App Fast AuthZ settings.
- Requesting Party requests direct access to Protected Resource.
- OpenID Connect interaction.

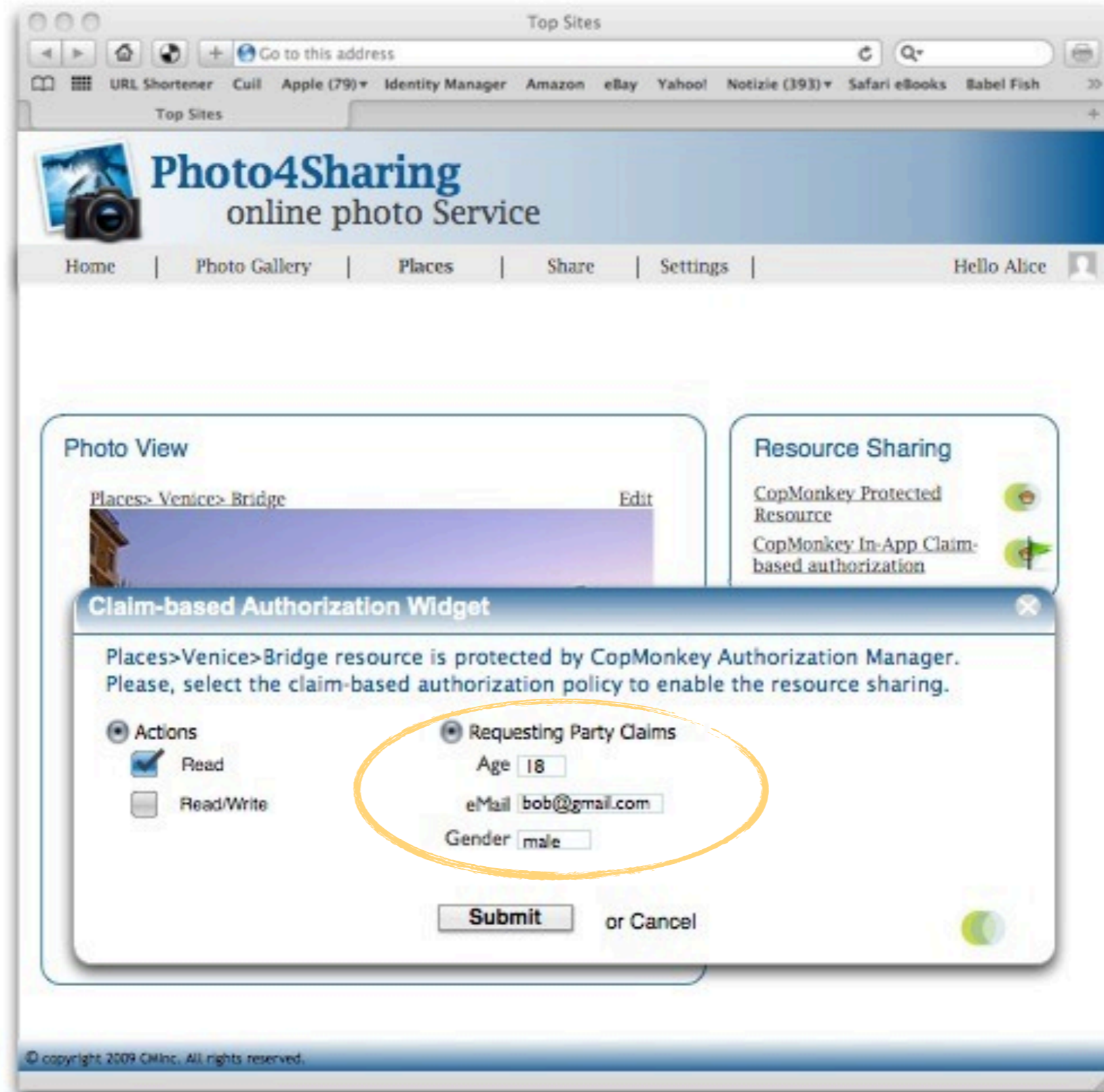
Alice at
Host Site

Protected
Resource by
CopMonkey
AM



in-App Fast
AuthZ Settings for
sharing

Alice defines claims-based authorization policy, using In-App widget



Protected Resource is ready for sharing under authZ policy



Alice shares the Protected resource through twitter

The screenshot shows a web browser window with the address bar containing "Go to this address" and a search icon. The browser's top sites list includes "URL Shortener", "Cuil", "Apple (79)", "Identity Manager", "Amazon", "eBay", "Yahoo!", "Notizie (393)", "Safari eBooks", and "Babel Fish". The main content area displays the "Photo4Sharing" website, which is an "online photo Service". The navigation menu includes "Home", "Photo Gallery", "Places", "Share", "Settings", and "Hello Alice".

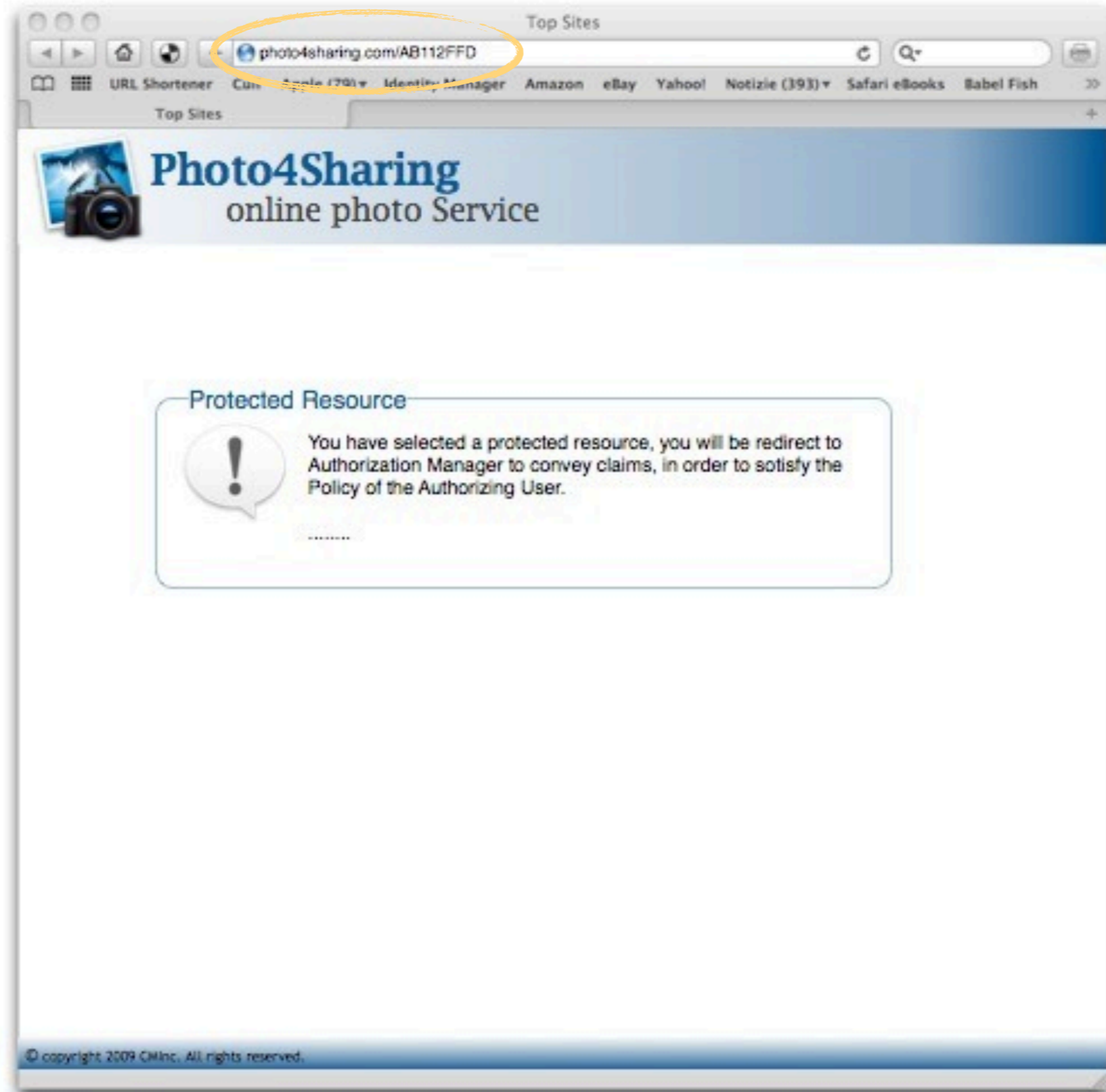
Overlaid on the website is a Twitter sharing interface for a user named "Alice". The interface includes a "Photo View" section with a photo of a bridge in Venice and the text "Places> Venice> Bridge". The main text area contains a tweet that has been partially filled out: "Photo4Sharing: Places:Venice:Bridge at <http://photo4sharing.com/AB112FFD>". A red arrow points to this URL. Below the main text are several placeholder tweets, each starting with "22 hours ago reply" and followed by a truncated tweet text and a link to "http://bit.ly/ds5c6z". The Twitter logo is visible at the bottom of the sharing interface.

© copyright 2009 CMInc. All rights reserved.

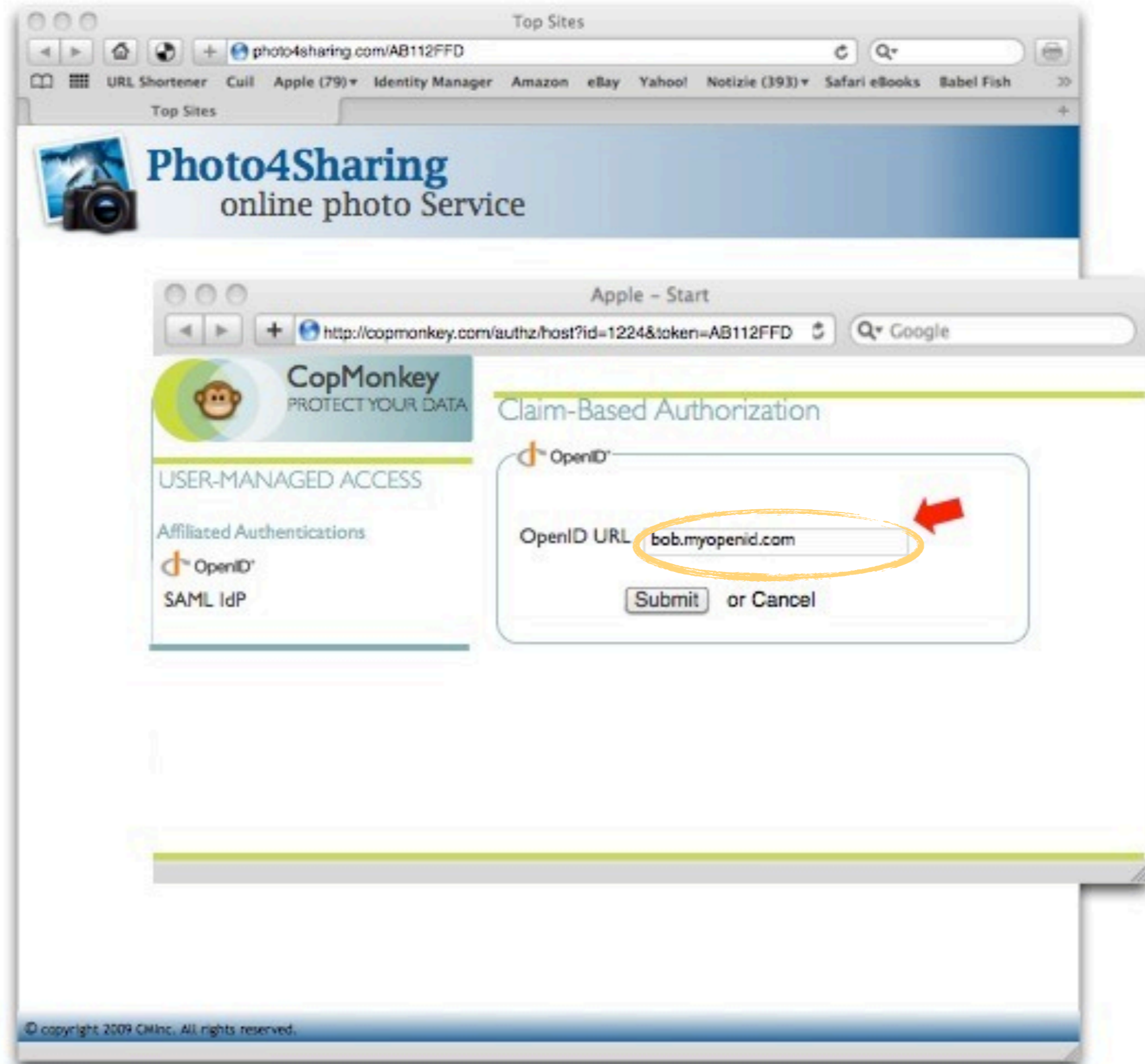


Bob attempts to access to protected resource.

Bob is redirect to AM to convey claims



CopMonkey authenticates Bob through OpenID, in order to initialize OpenID Connect protocol



Bob is redirect to IdP's authorization service to grant claims.

The image shows a browser window with two overlapping pages. The top page is 'Photo4Sharing online photo Service' with the URL 'photo4sharing.com/AB112FFD'. The bottom page is 'MyOpenID Digital Identification' with the URL 'http://idp.myopenid.com/connect/authorization?userid=bob24'. The MyOpenID page displays an 'Authorization Service' dialog box. The dialog box contains the following text: 'Remote Service (CopMonkey.com) is requesting the following claims in order to grant access to protected resource.' Below this text is a table with four columns: Claims, Type, Provider, and Privacy Impact. The table contains three rows of data. At the bottom of the dialog box are two buttons: 'Deny' and 'Allow'. The footer of the browser window shows '© copyright 2009 CMInc. All rights reserved.'

Claims	Type	Provider	Privacy Impact
Birthday	Public	Google.com	Low
eMail	Public	Google.com	Low
Gender	Public	Google.com	Medium

Bob gets access to the protected resource



Thanks