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 polices 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 Core 1.0 - draft 04

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.

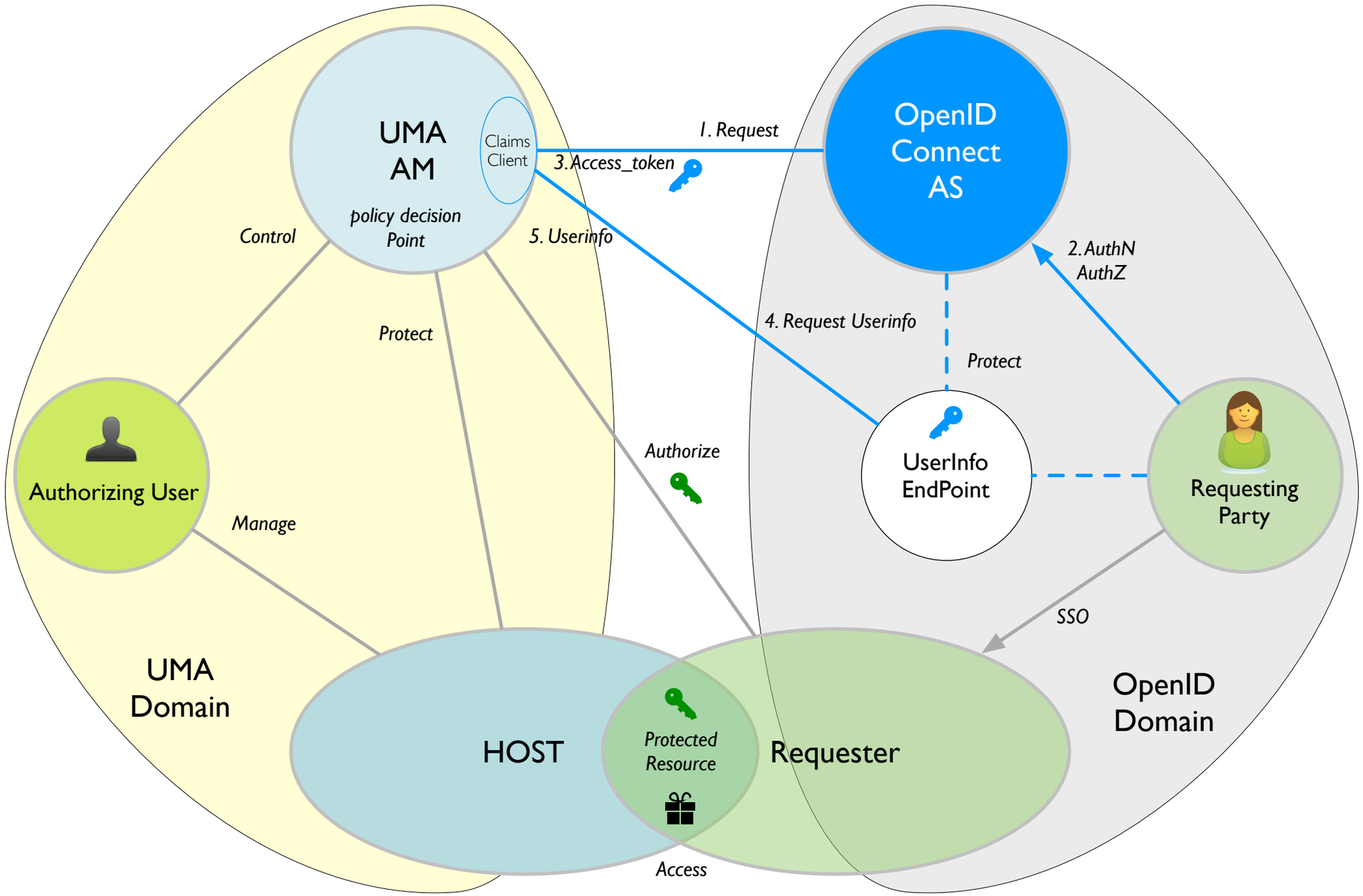
2. The Server authenticates the user and obtains appropriate authorization.

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

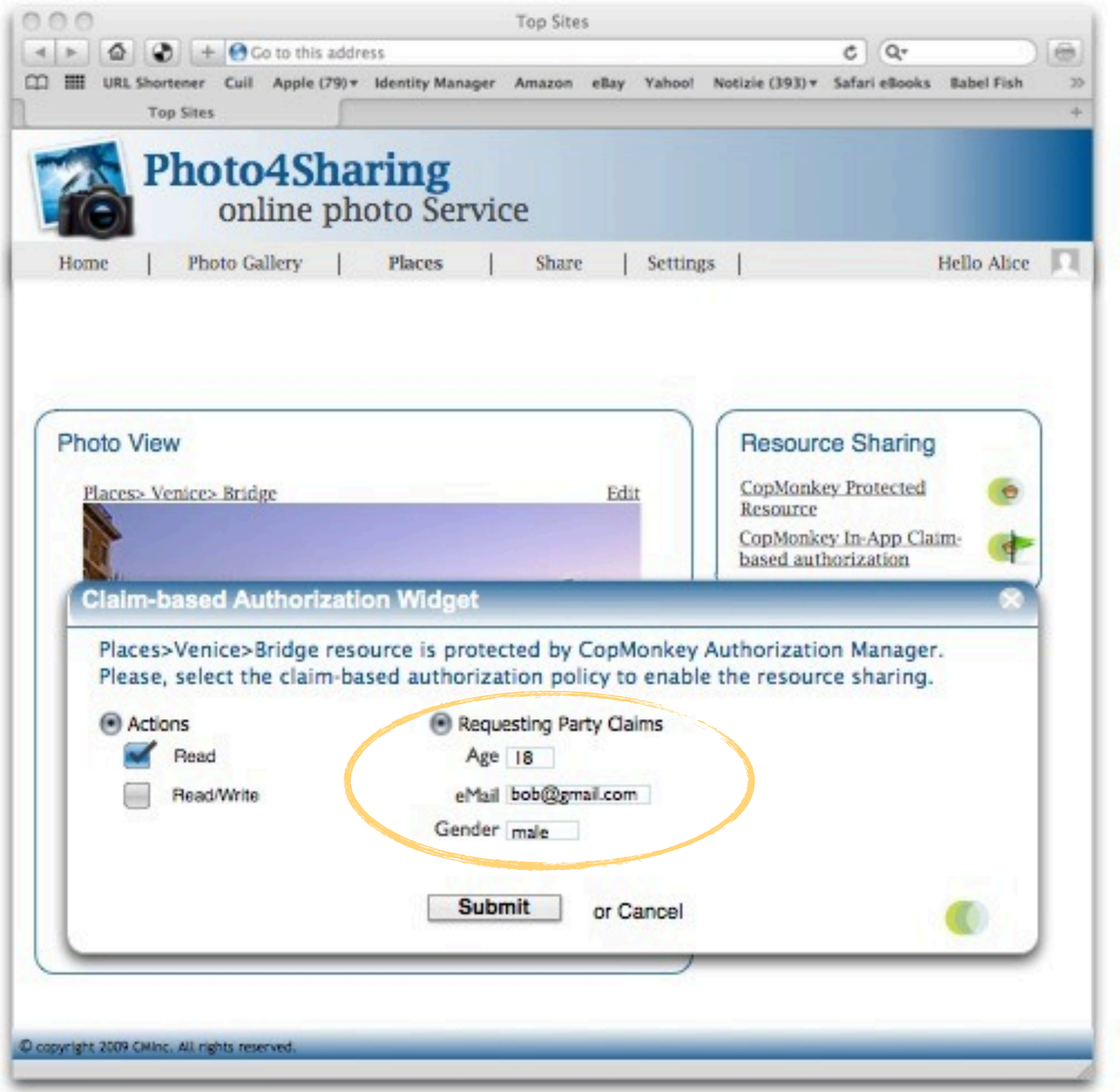
- UMA Host In-App Fast AuthZ settings.
- Requesting Party requests direct access to Protected Resource.
- OpenID Connect interaction.

Alice at Host Site

Protected Resource by CopMonkey AM

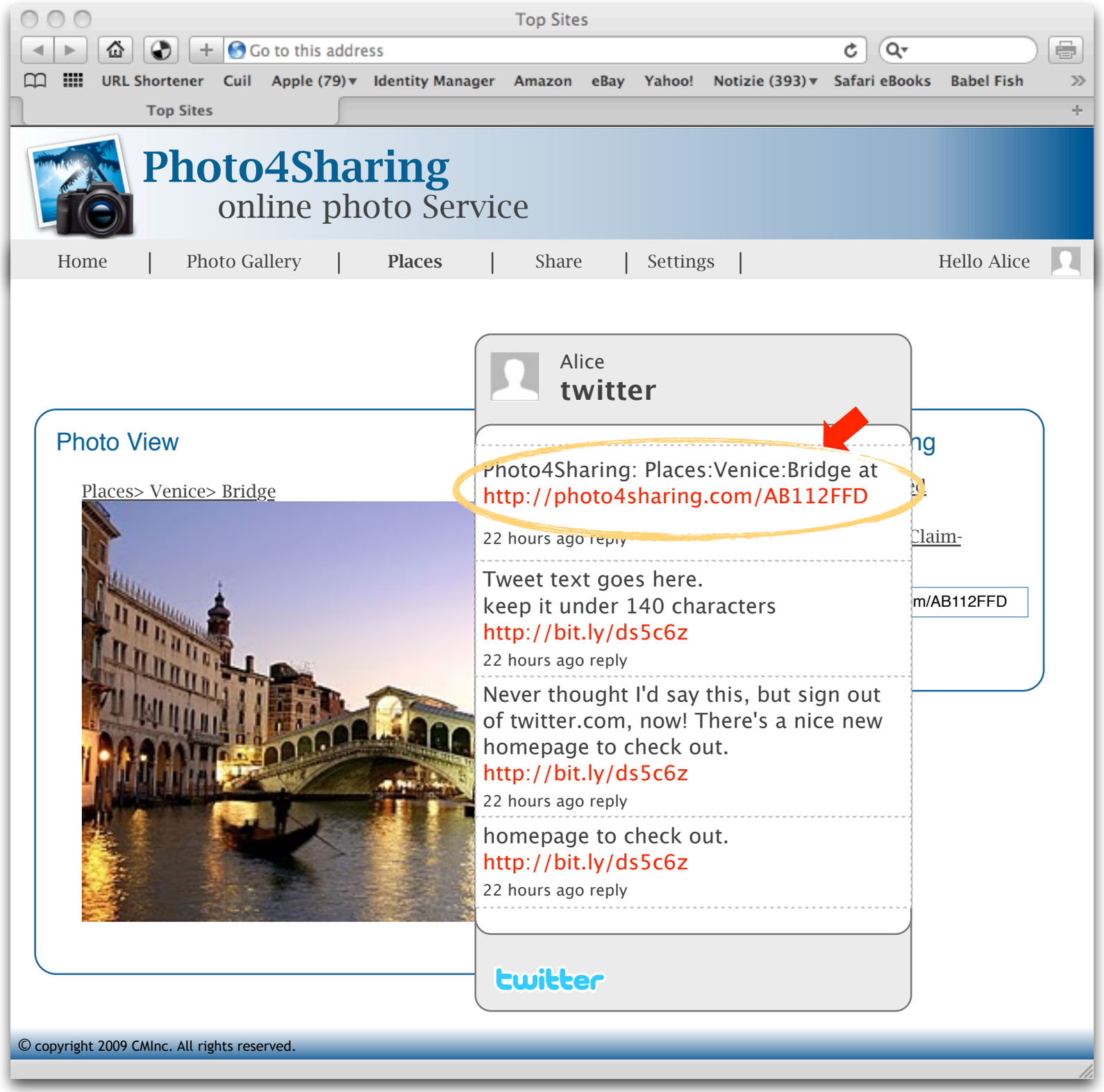
in-App Fast AuthZ Settings for sharing

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



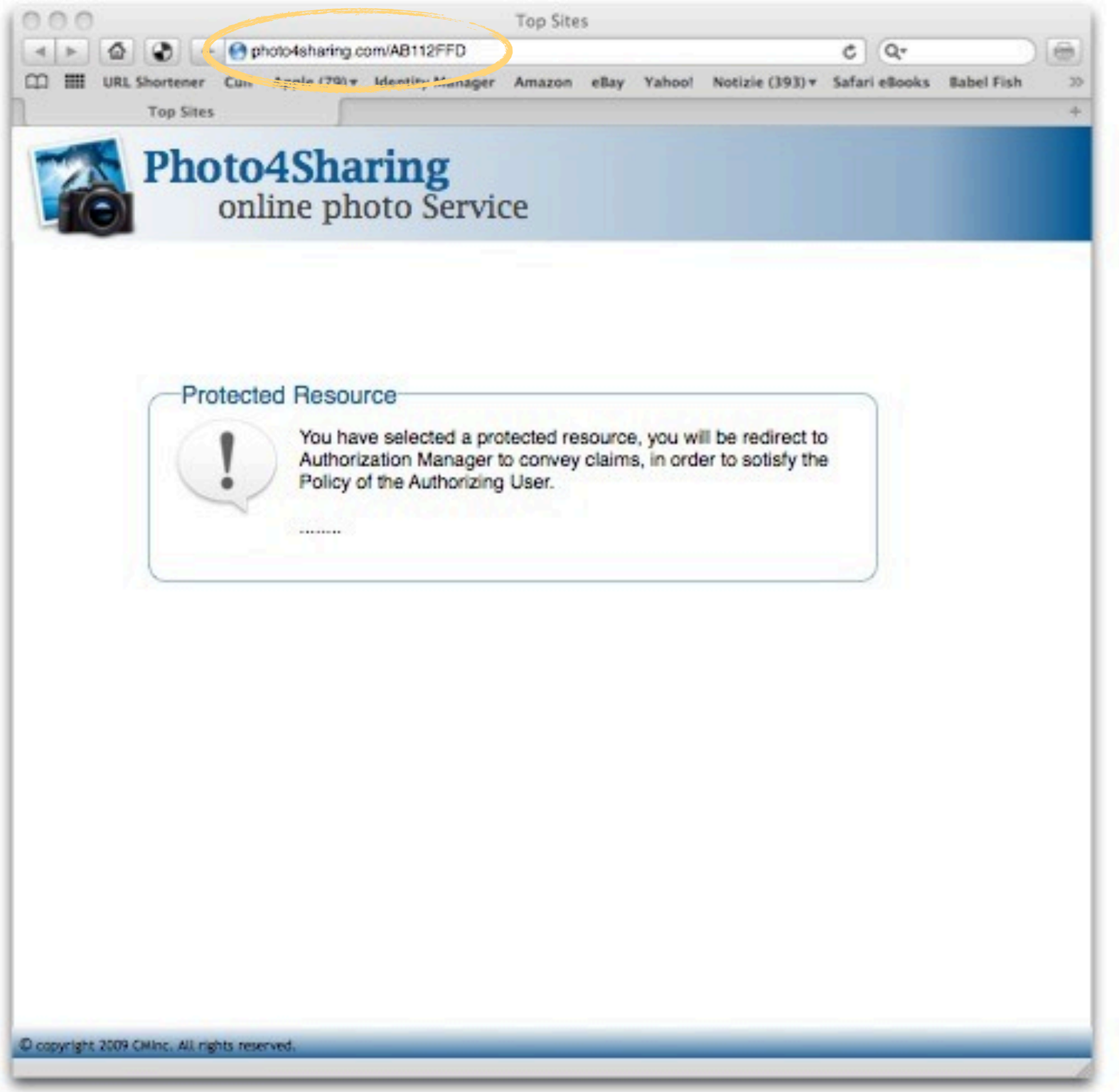
Protected Resource is ready for sharing under authZ policy

Alice shares the Protected resource through twitter

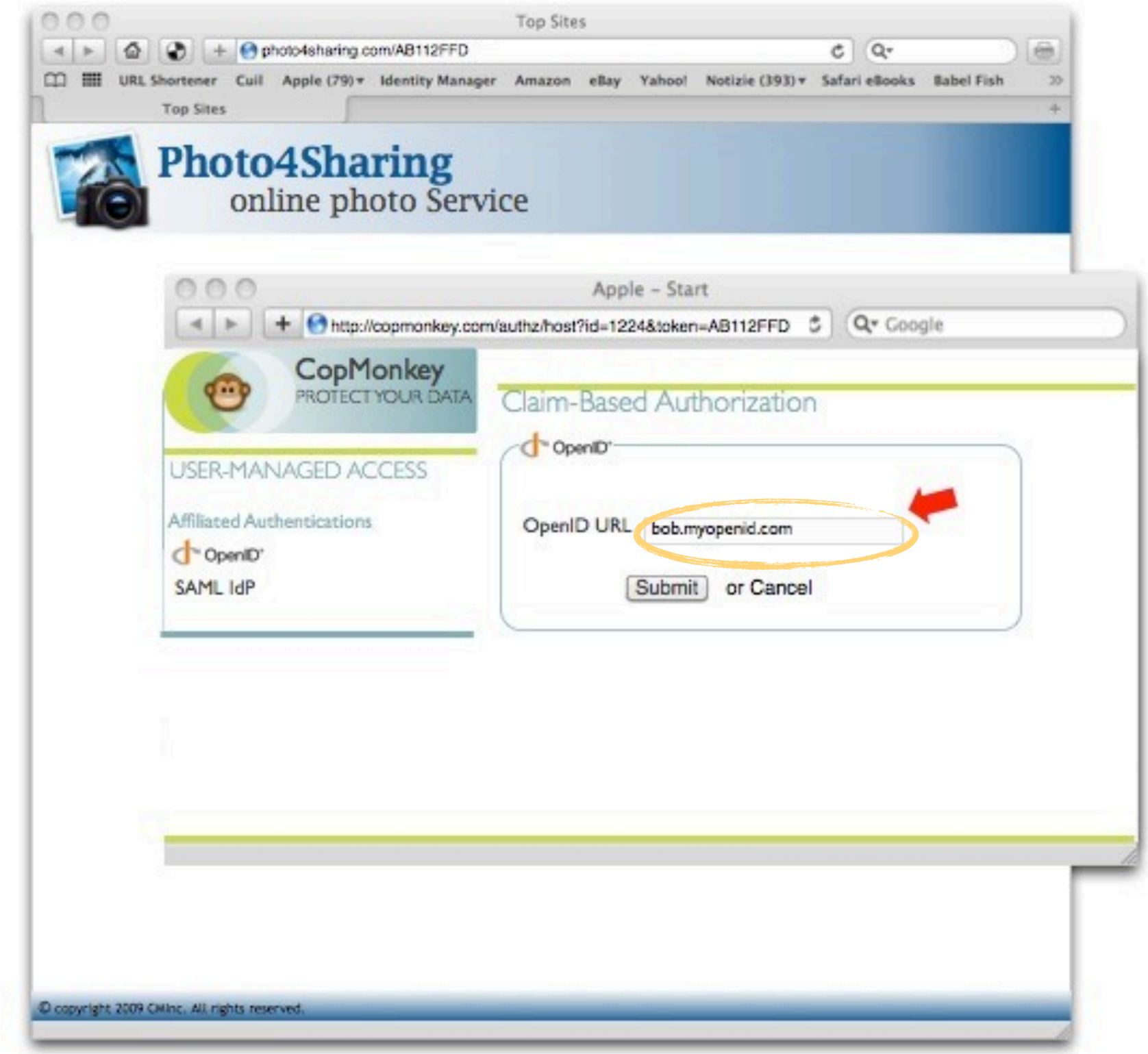


Bob attempts to access to protected resource.

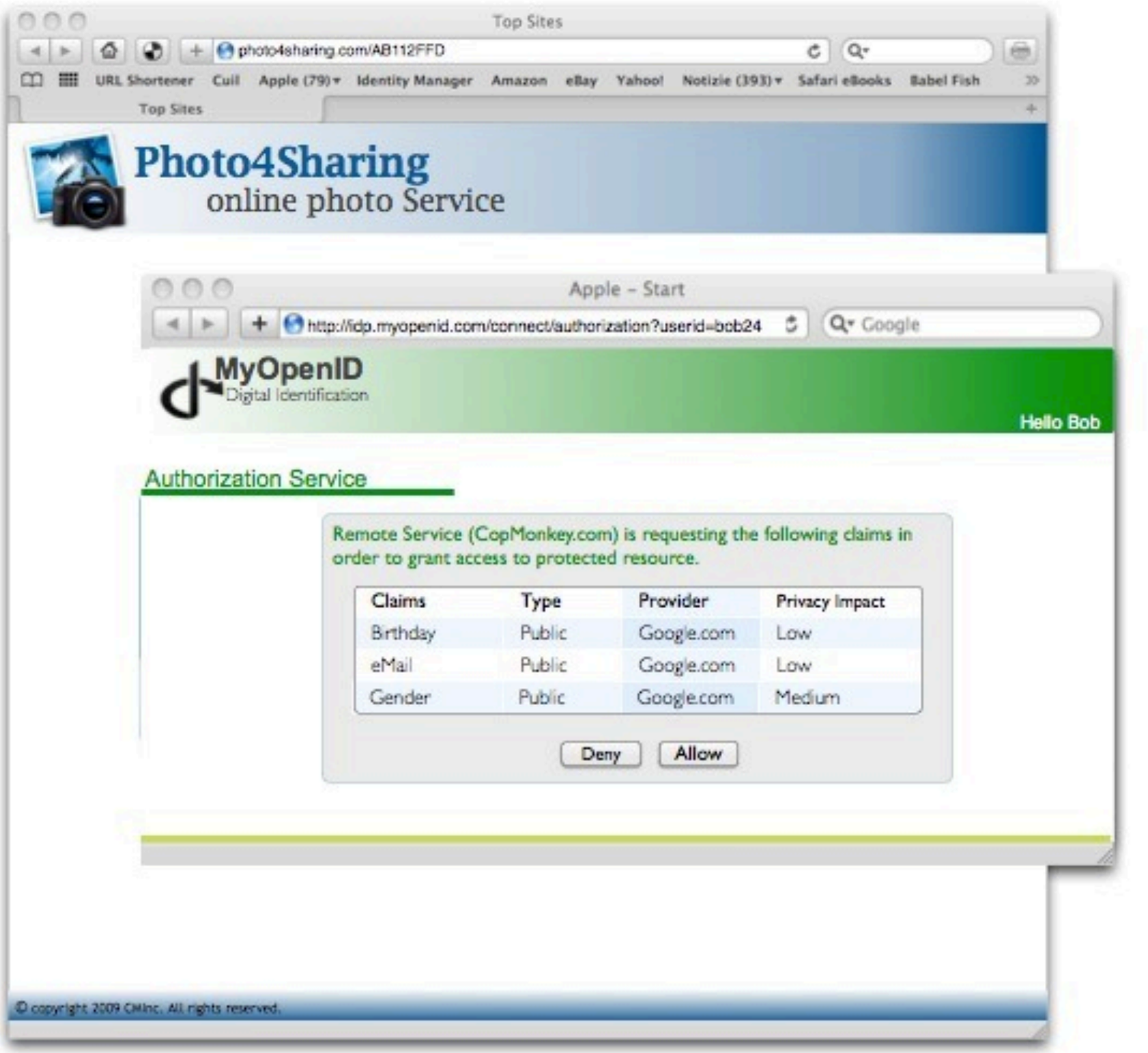
Bob is redirect to AM to convey claims



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



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



Bob gets access to the protected resource

Thanks