Federated Identity Management Breakout

SEARCH Membership Group Meeting
January 24, 2013
Portland, Oregon

David Steingraber
Member At-Large

Scott Came
Executive Director
Introduction and Background

Speakers’ background

Goals for the session

- Real-world problems solved by Fed IdM
- How does it work?
- Federation options: join or build?
- OJBC support
- Leadership opportunities for SEARCH?

What would you like to get out of the session?
Common Information Sharing Problems

- Inconvenience/expense for users
- Expense for information owners
- False sense of security and control
- Difficulty applying policies across jurisdictions: the MOU proliferation problem
What is different about Fed IdM?

- Users authenticate once (home agency)
- Authentication is shared when needed
- Trust but verify!
- “Federated policy” approach
- Federation Management - models
How it Works: Web SSO

1. User requests web page
2. Browser sends request to web server
3. No user session – SP requests auth from IdP
4. IdP authenticates user and sends assertion to SP
5. Web server receives assertion from SP
6. Web server responds to request

SAML + GFIPM
Key Features of Fed IdM

- There is no single policy for information exchanges – each resource owner gets to set (and enforce) its own policy
- Agreement between the participants focuses on establishing trust (in the legal and technical sense) not codifying the requirements of each exchange
- No centralized user directory to manage – each participant manages its own users
- Interoperability (scalability and flexibility)
Global Federated ID and Privilege Management (GFIPM) Initiative

Partner initiative to the Global JRA

Provides implementers with a head start on governance, technology standards
Before establishing your own federation, consider joining an existing one, such as:

http://www.connectconsortium.org

http://nief.gfipm.net
SEARCH Members leading OJBC-enabled federations in:

- Hawaii
- Vermont

Other jurisdictions that have established federations:

- South Dakota
- Pennsylvania
- Texas
- Los Angeles County, CA
- Others?
Other National Initiatives

National Strategy for Trusted Identities in Cyberspace

IDManagement.GOV

State Identity Credential and Access Management (SICAM) Guidance and Roadmap
Leadership Opportunities

Does SEARCH Membership wish to play a role in evolving Fed IdM nationally?

Ideas:

- Dialogue with FBI on implications for our national information sharing infrastructure
- Guidelines for assertion attributes necessary to authorize CHRI access
- Model service policies
- Federated policy strategy for interstate information sharing
Thank You!

Scott Came  
Executive Director, SEARCH  
scott.came@search.org  
916-212-5978

David Steingraber  
Senior Policy Adviser  
dsteingraber@ncja.org  
202-448-1716