Federating Your Identity Management System

Jacob Farmer

Indiana University

INDIANA UNIVERSITY

UNIVERSITY INFORMATION TECHNOLOGY SERVICES

Agenda

Introduction
Work through POP
Wrap-up

One rule: Participate!

Acronym Soup

IdP – Identity Provider

SP – Service Provider

RP – Relying Party

Lexical Gumbo

Electronic Identity – Collection of information about a person

Etymological Bisque

Attribute vs. Assertion

Jargon Consommé

Maybe I should stop there…

What is POP?

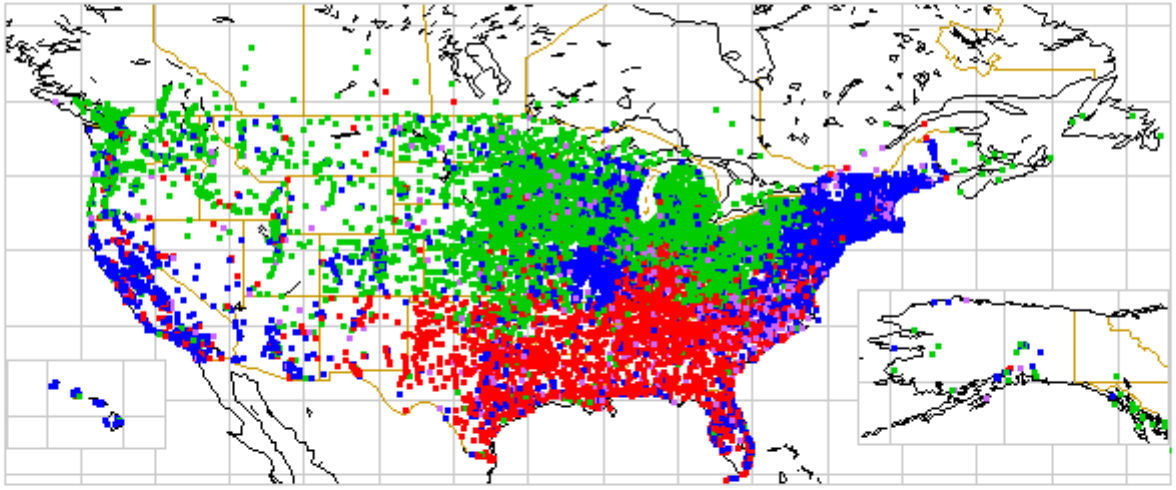
The Pop vs. Soda Page - Mozilla Firefox

http://popvssoda.com/

Google

The Pop vs. Soda Page

The Great Pop vs. Soda Controversy



Pop vs. Soda data as of October 3, 2002

"Pop" "Soda" "Coke" Other

show all | pop | soda | coke | other

Done

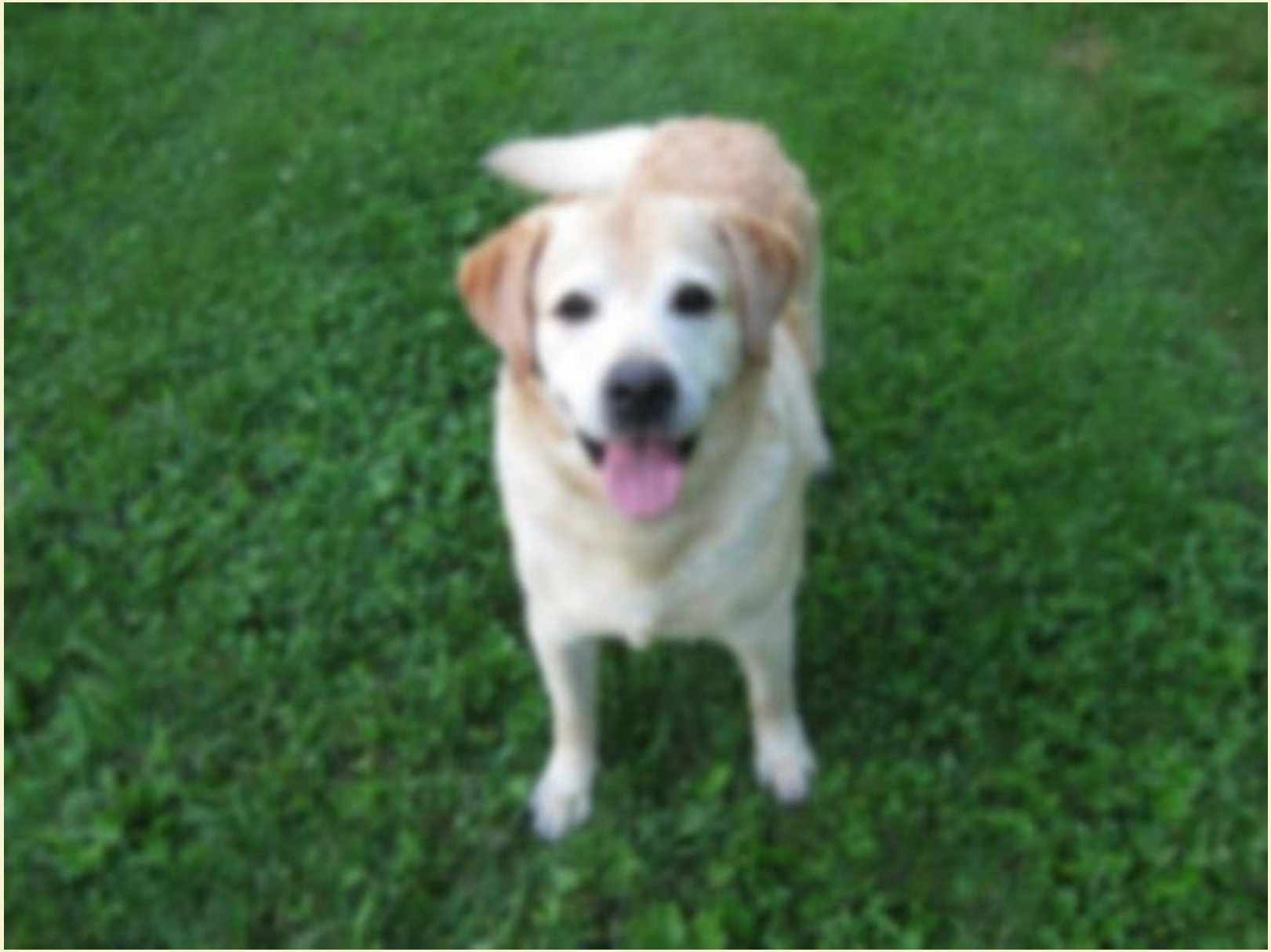
Fiddler: Disabled

Participant Operating Practices

More Simply: How do you do IdM?

Why do I care about your IdM system?

Federation == Trust



Do we really need this level of assurance for everyone?

Levels of assurance to the rescue!*

*(this is a dramatic oversimplification)


Basic
Bronze
Silver
Gold

The POP helps us understand how we reach basic

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

2.2 “Member of Community” is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is “current student, faculty, or staff.”

What subset of persons registered in your identity management system would you identify as a “Member of Community” in Shibboleth identity assertions to other InCommon Participants?

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose. For example, “Registrar’s Office for students; HR for faculty and staff.”

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (i.e., “clear text passwords” are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

2.6 If you support a “single sign-on” (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with “public access sites” is protected.

2.7 Are your primary electronic identifiers for people, such as “net ID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

2.8 How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

2.9 What information in this database is considered “public information” and would be provided to any interested party?

2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

2.11Would you consider your attribute assertions to be reliable enough to:

[ ] control access to on-line information databases licensed to your organization?

[ ] be used to purchase goods or services for your organization?

[ ] enable access to personal information such as student loan status?

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

4.1 Technical Standards, Versions and Interoperability

Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

4.2 Other Considerations

Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

Wrap-up