

IAM Online

Joining InCommon: The POP is Your Friend

Wednesday, March 9, 2011 – 3 p.m. ET

Jacob Farmer, Indiana University

Please note: you will not hear any audio until the session begins

Joining InCommon: The POP is Your Friend

Jacob Farmer
Indiana University

jpfarmer@indiana.edu



INDIANA UNIVERSITY

UNIVERSITY INFORMATION TECHNOLOGY SERVICES

One request: Participate!

Steps to Join InCommon

You are
here!

1. Identify your business case
2. Review your campus IdM system
3. Post your Participant Operating Practices
4. Install/Configure a SAML2 Identity provider
5. Support the eduPerson schema
6. Sign/Pay InCommon Agreement and Fee

Aligning Vocabulary

IdP – Identity Provider

SP – Service Provider

RP – Relying Party

Electronic Identity – Collection of information about a person

Attribute vs. Assertion

Pause for Questions

What is a POP?

Participant Operating Practices

**More Simply: How do you
do IdM?**

Why do I care about your
IdM system?

Federation == Trust

Pause for Questions

Do we really need the same
level of confidence in
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

Pause for Questions

Two parts: one for IdPs and
one for SPs

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?

2.4 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?

2.7 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?

2.9 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.

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

Pause for Questions

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.?

3.4 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?

Pause for
Questions

Joining InCommon: The POP is Your Friend

Jacob Farmer
Indiana University

jpfarmer@indiana.edu



INDIANA UNIVERSITY

UNIVERSITY INFORMATION TECHNOLOGY SERVICES

Upcoming Education and Outreach Events

Day CAMP: Getting Started with the InCommon Federation

www.incommon.org/camp

April 21, 2011 – Arlington, Virginia (after Internet2 Member Meeting)

Internet2 Spring Member Meeting

Federation track, Middleware track

April 18-20, 2011 – Arlington, Virginia

<http://events.internet2.edu/2011/spring-mm/>

Advance CAMP: Identity Services Summit III

May 25-27, 2011 – Westminster, Colorado

www.incommon.org/camp

Survey

Please complete the survey about today's IAM Online:

www.surveymonkey.com/s/iamonline_mar_2011

Next IAM Online www.incommon.org/iamonline

Wednesday, April 13, 2011 – 3 p.m. EST

Hot Topics in Identity Management

New! IAM Online Announcement List

Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.



*Brought to you by InCommon, in cooperation with Internet2
and the EDUCAUSE Identity and Access Management Working Group*