IAM Online

Grabbing the Bronze and Silver Ring: The InCommon Assurance Program

Wednesday, June 15, 2011 – 3 p.m. ET

Tom Barton, University of Chicago
R.L. “Bob” Morgan, University of Washington
Renee Shuey, Penn State

Please note: you will not hear any audio until the session begins
Identity Assurance and Federation: Three Perspectives

<table>
<thead>
<tr>
<th>Identity Provider</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider</td>
<td>Tom Barton</td>
</tr>
<tr>
<td>InCommon Federation</td>
<td>Bob Morgan</td>
</tr>
<tr>
<td>Campus Identity Provider</td>
<td>Renee Shuey</td>
</tr>
</tbody>
</table>
Service Provider Perspective

I get that federations provide a way for inter-organizational online transactions to happen at scale, but my SP provides access to sensitive data or export-controlled computing power.

How can I manage my risk when users are vetted and authenticated by campuses?

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Student Clearinghouse</td>
<td>student transcripts</td>
</tr>
<tr>
<td>TeraGrid/OSG/CILogon</td>
<td>ssh access to HPC, sensitive data</td>
</tr>
<tr>
<td>NSF &amp; NIH Virtual Orgs</td>
<td>sensitive data and equipment</td>
</tr>
<tr>
<td>Funding Agency</td>
<td>grant and report submission</td>
</tr>
<tr>
<td>ADP</td>
<td>employee payroll information</td>
</tr>
<tr>
<td>TIAA-CREF</td>
<td>employee retirement accounts</td>
</tr>
<tr>
<td>DoE Labs</td>
<td>classified programs</td>
</tr>
</tbody>
</table>
How can I manage my risk when users are vetted and authenticated by campuses?

A. I’ll still vet users and give them SP-specific credentials, but bootstrap the process using campus Identity Providers.

B. I’ll require campuses to accept terms and conditions of my own devise that specify standards and best practices for their IT operation. No cost to me, and solves the problem.

C. I might use InCommon alone, but

– Campuses seem to have varying practices and aren’t always willing or able to tell me what they are, so how do I gauge my risk?

– Would I need to compare my requirements with those of other SPs? How?

– Does this approach share the risk between my SP, a campus, and the InCommon Federation itself in a satisfactory way?
Identity Assurance Basics

- Helping the community deal with complex federated identity risk issues is one part of simplifying and promoting federation (along with protocols, attributes, metadata, etc).

- Starting point is risks to applications/services
  - applications seek to manage risks cost-effectively
  - identity risks are only one class of risks ...

- What is "identity"?
  - from app point of view, it is anything about a requesting party on which access decisions can be made
  - maybe just a userid, maybe lots of other info: name, group, role, authentication method, usage history, location, etc
One Size Doesn't Fit All

• Apps have many kinds of resources to protect, different budgets to do so
  – Low-security practices may create too much risk, or not
  – High-security practices are costly to operate, intrusive to users (showing identity docs, coming to help desk, two-factor, etc; so even if affordable, users will revolt) but may be necessary

• Hence, in practice there is a range of useful identity management practices, balancing costs and risks
  – need agreements between identity management systems and apps on what the options are
  – this is "identity assurance"; a useful concept even without federation
Interesting IdM Characteristics (1)

• Registration and identity proofing
  – creation of record in IdM system for a person, records management
  – external validation of personal information
  – obtaining/verifying contact information

• Credential assignment
  – e.g., username and password establishment so authentication acts can be tied to registered person
  – also includes re-establishment as needed (aka password reset)

• Authentication services/technology
  – technology by which users establish authenticated sessions with applications; strength of crypto/passwords
Interesting IdM Characteristics (2)

• Operational/technical
  – change-management and host/network security practices
  – password/secret protection

• Organizational maturity
  – organizational existence
  – ability to sign contract, notify about changes/exceptions

• User information management
  – various kinds of identifiers
  – roles, groups, privileges, etc.
Assurance "Levels"

- US government proposed 4 levels of risk (low, medium, high, very high), hence 4 levels of IdM practice
  - roughly: Internet; regular business; two-factor; military
- NIST SP 800-63 specifies well-known model
  - specifically for use in USG federation context, but widely adopted
- InCommon adapts these materials for HE environment
  - Assurance Framework and two (not 4) Assurance Profiles (Bronze and Silver)
  - version 1.0 documents released Nov 2008
  - version 1.1 documents released May 2011
InCommon IA Framework

- Background, models, terminology, elements
- IdM functional model: elements of typical enterprise IdM
- Profile structure
  - processes about which criteria are established
- Assessment, audit and certification processes
  - auditor qualifications
  - report, including proposed alternative methods
  - InCommon review and approval
  - re-certification, continuing compliance
InCommon Identity Assurance Program
Certification Model

IdP Operator

IdP Operation

Summary report
IdPO Certification

Assertion with appropriate IAQ(s)

Audit reports
Detailed & Summary

IdP Certification status

InCommon

Service Provider

Auditor

v1.1
InCommon IA Profiles: Bronze and Silver

• Bronze == USG LoA 1 == "low assurance"
  – must be InCommon participant organization
  – minimal password quality, but still password protection
  – no identity proofing
  – standard username/password web authentication
  – like typical "Internet account"
  – audit/assessment required
  – better than "no assurance"?
InCommon IA Profile: Silver

- Silver == USG LoA2 == "some assurance"
  - must be InCommon participant organization
  - modest password strength; passwords protected wherever they are, wherever they travel
  - typical "new hire" identity proofing and credentialing
  - standard username/password web authentication (or better)
  - non-onerous records retention
  - standard IdM operations security
  - audit/assessment required
  - adequate for most standard business purposes
InCommon IA "Refinement"

- 2010 feedback on 1.0 IA docs indicated need for change
  - all InCommon sites must be able to succeed with Assurance!

- Process:
  - address "pain points" from feedback, eg multiple audits
  - remove outdated requirements based on old USG programs
  - create IAM functional model to clarify elements, definitions
  - clarify role of auditors vs IT vs campus
  - remove "how-to", stick with "what-to-do"
  - reduce external references
  - many many fixes and cleanups
InCommon IA Program

• There's more to it than just the IA docs
  – technical bits: requesting and returning profile info; metadata
  – "review board": InCommon assessment/approval of submissions
  – participant agreement addendum
  – fees ...
  – participant support and collaboration
  – promoting IA use in the federation, helping IdPs and SPs understand the benefits ...
US Government Engagement

- InCommon now Approved as "Trust Framework Provider"
  - along with Kantara Initiative, Open Identity Exchange; useful collaboration with industry partners via these orgs
  - InC will resubmit for approval using new 1.1 docs, soon ...
  - working with NIH on technical interop, and planning for first Level2 apps
  - working with GSA on creating incentives around TFP program to help engagements with other agencies
  - continuing negotiations on privacy-protection provisions in TFP program
FAQs

• which IdP participant will be first to comply at Silver?
• will campus internal auditors be effective assessors?
• how will SPs (government and non-) begin to integrate Bronze/Silver into their operations?
• how will campuses organize to achieve Silver compliance?
• when should InCommon start work on Gold (== Level3)
• Will the 2 (or 3, or 4) profiles be enough for SPs?
• Will campus IdM need re-tooling to support Assurance?
  Will MS AD work OK?
Coming Next for InCommon Assurance

- Hire Program Manager (May 2011 – DONE)
- Develop collaboration resources for adopters (Summer – Ongoing)
- Establish Review Board (Summer)
- Finalize Legal & Business structures (Summer)
- Finalize technical model & implementation for Federation, for IdPs/SPs (Summer)
- Engage Services Providers (Ongoing)
- Engage University IT & Audit communities (Ongoing)
- Open for Certifications (Fall 2011)
IAM Online

Grab the Bronze and Silver Ring: Identity Assurance Progress - Penn State Case Study
What I’ll Be Talking About

• Strategic Business Decisions
• Who from the campus is involved
• Organizing the Conversation
• What’s in Scope for Silver
  • Infrastructure and Process
• Partnering with CIC Peers
PSU IAM Principles

• Federating Identity is an important part of Penn State’s IAM strategy

• University business is no longer conducted within four walls but must cross region, state, national and international boundaries with varying levels of risk for identity and services

• Identity Assurance Profiles are an important strategy for both internal and external business
Who is Involved?

- PSU Internal Auditors
- Registration Authorities
- Identity Assurance Authorities
- Risk, Security & Privacy
- IT IdM Infrastructure Group
### 4.2.1 Business Policy and Operational Factors

These are factors that indicate the identity service provider's readiness to support and operate a reliable operational service.

<table>
<thead>
<tr>
<th>Assessment Area</th>
<th>Factor</th>
<th>Requirement</th>
<th>Status*</th>
<th>Evidence of Compliance**</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1.1</td>
<td>InCommon Participant. <strong>Bronze/SILVER</strong></td>
<td>The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, &quot;good standing&quot; means not in arrears with respect to financial obligations to InCommon nor out of compliance with other contractual obligations to InCommon.</td>
<td>Complete</td>
<td></td>
</tr>
<tr>
<td>4.2.1.1</td>
<td>Notification to IdP</td>
<td>The IdP Operator must notify InCommon for any amicable or terminative dispute.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# 4.2.3 Digital Electronic Credential Technology

Section 4.2.3 Credential Technology.

These InCommon LAPS are based on use of "shared Authentication Secret" forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.

<table>
<thead>
<tr>
<th>Assessment Area</th>
<th>Factor</th>
<th>Requirement</th>
<th>Status</th>
<th>Evidence of Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.3.1</td>
<td>Credential unique identifier</td>
<td>Each Credential issued by the IdP shall contain a unique identifier (e.g. userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdP Operator.</td>
<td>Complete</td>
<td>Access Account Overview</td>
</tr>
<tr>
<td>BRONZE/SILVER</td>
<td>A Subject can have more than one Credential unique identifier, but a given Credential shall have a unique identifier.</td>
<td>Complete</td>
<td>Access Account Overview</td>
<td></td>
</tr>
</tbody>
</table>

**BRONZE/SILVER**
Scoping the Silver Effort

InCommon Identity Assurance Program
Identity Management Functional Model

- Subject
  - vets identity
  - authenticates to
  - issues credential

- Service Provider
  - uses
  - provides identity assertion

- IdP
  - provides attributes
  - verifies credential

- RA
  - registers Subject
  - IdP Operator

- IdMS
  - provides service
  - IdMS Operations

- Attribute Service

- non-IdP Apps

- Verifier
# Bronze: Identity Registration Process

The process for obtaining a digital identity that complies with the InCommon Bronze Identity Assurance Profile guidelines.

<table>
<thead>
<tr>
<th>Description</th>
<th>REGISTRATION</th>
<th>VETTING</th>
<th>PROOFING</th>
<th>CREDENTIAL ISSUANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process of collecting information from a user for the purpose of issuing digital identity.</td>
<td>The process of validating information collected from a user for the purpose of issuing digital credentials.</td>
<td>The act of binding someone's previously recorded data to the actual person.</td>
<td>The act of issuing a userid/password that will be used to establish the digital credential of someone.</td>
<td></td>
</tr>
</tbody>
</table>

**User Experience**

- User interacts with RA application.
- User directed to IAM.
- User provides basic biographical information and sets knowledge base questions.
- The web application displays the Access Account User ID.
- The user sets password.
- The user receives an email notification.

**Business Process**

- RA will request a digital identity to be created for the user.
- Approved Registration Authority.
- RA & third party validation of Name, Address, & Date of Birth.
- Data elements satisfied including answers to Knowledge Base questions.
- Affiliation provided by RA.
- IAP updated to InCommon BRONZE.
- An email is automatically generated and sent to user.

**Data**

- "Self-asserted": Full name, address, email, and date of birth (partial or full)
- SSN (if available)
- Knowledge Base answers
- Affiliation
- Registration Authority
- Full name, address, email and date of birth (partial or full)
- SSN (if available)
- Registration Authority
- Credential Issuance Date
- Registration Authority
- Event Type
- Event Date
<table>
<thead>
<tr>
<th>Description</th>
<th>REGISTRATION</th>
<th>VETTING</th>
<th>PROOFING</th>
<th>CREDENTIAL ISSUANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process of collecting information from a user for the purpose of issuing digital identity.</td>
<td>The process of validating information collected from a user for the purpose of issuing digital credentials.</td>
<td>The act of binding someone's previously recorded data to the actual person.</td>
<td>The act of issuing a userid/password that will be used to establish the digital credential of someone.</td>
<td></td>
</tr>
<tr>
<td>User interacts with Registration Authority (RA) application.</td>
<td>User visits authorized RA agent.</td>
<td>User presents valid government identification (Drivers License or passport) to agent.</td>
<td>The web application displays the Access Account User ID.</td>
<td></td>
</tr>
<tr>
<td>User directed to IAM.</td>
<td>The user sets password.</td>
<td>The user receives an email notification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User provides basic information &amp; sets Knowledge base questions.</td>
<td>RA will request a digital identity to be created for the user.</td>
<td>Approved RA.</td>
<td>IAP updated to InCommon SILVER.</td>
<td></td>
</tr>
<tr>
<td>Execute Match Process: Match biographical data with Central Person Registry data</td>
<td>RA &amp; third party (SAT scores, I-9, etc.) validation of Name, Address, &amp; Date of Birth</td>
<td>RA agent inspects government identification &amp; compares picture to user. RA agent records: Name</td>
<td>An email is automatically generated and sent to user.</td>
<td></td>
</tr>
<tr>
<td>Data elements satisfied including answers to KB questions</td>
<td>Affiliation provided by RA</td>
<td>** If available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>“Self-asserted”: Full name, address, email and date of birth (partial or full)</td>
<td>Full name, address, email and date of birth (partial or full)</td>
<td>Government Identification:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSN (if available)</td>
<td>SSN (if available)</td>
<td>Full name</td>
<td>Credential Issuance Date</td>
<td></td>
</tr>
<tr>
<td>Knowledge Base answers</td>
<td>Registration Authority</td>
<td>Address of Record</td>
<td>Registration Authority</td>
<td></td>
</tr>
<tr>
<td>Affiliation</td>
<td>** If available</td>
<td>Date of Birth (full)</td>
<td>Event type</td>
<td></td>
</tr>
<tr>
<td>Registration Authority</td>
<td></td>
<td>Document type</td>
<td>Event Date</td>
<td></td>
</tr>
</tbody>
</table>
Data and Event Triggers for IAPs

- RA & Third party vetting & verification – name, address, dob
- Matching Data elements
- Approved RA for IAP
- Password KB questions
- Event capture
Data and Event Triggers for IAPs

• As it appears on legal document:
  • Full name
  • Full address
  • Document issuer
  • Document type

• Approved RA Inspecting Document
Data and Event Triggers for IAPs

- Account compromise
- Security violation
- Expired or forgotten password with no Preset Knowledge Base Q&A
- Identity Lifecycle ends
Committee on Institutional Cooperation

- Partnering with Peers within the CIC & beyond
- CIC InCommon Silver Project - continue to reach for initial goal of InCommon Silver certification 2011
- Additional CIC IdM projects supporting Cyber-Infrastructure, User consent-UApprove adoption, Attribute Bundles
Additional Resources

• Committee on Institutional Cooperation - http://www.cic.net/Home/Projects/Technology/IdMgmt/Introduction.aspx

• Penn State IAM Community Website - https://iam.psu.edu/

• Penn State IAM Wikispace - https://wikispaces.psu.edu/display/IAM/Penn+State+Identity+and+Access+Management

• Penn State IAM Developers Site - https://iam.psu.edu/developer/

• InCommon - http://www.incommonfederation.org/

• IAM Technical Architect Group iam@psu.edu
Stay Tuned: More Info?

- Subscribe to assurance@incommon.org
- Look for announcements on incommon-announce@incommon.org
- Ann West
  awest@internet2.edu
Upcoming Events

**CAMP: Hot Topics in Identity and Federated Identity Management**
June 21-23, 2011 – Columbus, Ohio
[www.incommon.org/camp](http://www.incommon.org/camp)

**InCommon Certificate Service Overview (webinar)**
June 29, 2011 – 3 p.m. EDT
Registration (free) at [www.incommon.org/cert/why.html](http://www.incommon.org/cert/why.html)

**Shibboleth Workshop Series: Installation of IdP and SP**
July 21-22, 2011 – Milwaukee, Wisconsin
[www.incommon.org/educate/shibboleth](http://www.incommon.org/educate/shibboleth)
Evaluation
Please complete the evaluation of today’s IAM Online:
www.surveymonkey.com/s/VHKR5Q9

Next IAM Online
Wednesday, July 13, 2011 – 3 p.m. EDT
ECAR’s 2011 Study of Identity Management in Higher Education

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