Supporting High-Value, High-Risk Cloud Services with Federated Identity Management

Mary Dunker, Steve Devoti
Security Professionals Conference 2013
Agenda

• The problem/value proposition
• “Assurance”
• What’s new
• Examples/Experience
Value Proposition
The problem/value proposition

- High value services
  - What are they?
  - Why are they important?
  - How can we secure them?
    - Identity Management
    - Credential Assurance
  - SP Confidence
Assurance

- InCommon Assurance
- Increase Confidence, Reduces Risk
- A standard, community-based approach
- Economies of scale
- Better user experience
Cloud Services Introduce Risks
Who has access?
Why InCommon Assurance?

- NIST 800-63 – Federal government
- InCommon – Higher Ed
  - Identity Assurance Assessment Framework
  - Identity Assurance Profiles
- FICAM has approved IAAF and IAP 1.2
- SP interest
  - CI Logon
  - National Student Clearing House
  - NIH
Assurance Context

InCommon Identity Assurance Program
Identity Management Functional Model

- **Subject**
  - vets identity
  - authenticates to

- **RA**
  - registers Subject

- **IdMS**
  - provides service

- **IdP**
  - issues credential
  - provides attributes
  - provides identity assertion

- **Service Provider**

- **Verifier**
  - verifies credential

- **non-IdP Apps**

IdP Operator

IdMS Operations

Educause
Starting the Conversation

- Engaging Resources
  - InCommon
- Our Stories
- The Future
How do I get certified?
Assurance Process

- Join InCommon
- Set up SAML2 compliant Identity Provider – Shibboleth
- Identity Assurance Assessment Framework
- Identity Assurance Profiles (IAP) Bronze and Silver
Identity Assurance Profile (1.2)

4.2.1 Business, Policy and Operational Criteria
4.2.2 Registration and Identity Proofing (Silver)
4.2.3 Credential Technology
4.2.4 Credential Issuance and Management
4.2.5 Authentication Process
4.2.6 Identity Information Management
4.2.7 Assertion Content
4.2.8 Technical Environment (Silver)
Assurance Process

- IdP submits audit and/or RoC
- Assurance Advisory Committee (AAC) reviews
- AAC recommends to InCommon Steering
- InCommon adds Assurance level to metadata
What’s New
Representation of Conformance

- Simplified for Bronze
- Part of Legal Addendum
Alternative Means

Comparable or superior methods of complying with profiles

- Community contribution
- IdPO proposal prior to application
- IdPO proposal at time of application
“Approved algorithm” replaces “industry standard”

Any implementation of an algorithm or technique

- specified in a FIPS standard or NIST recommendation or
- conforming to an alternative means identified by InCommon as approved for specified IAPs
Federation

- InCommon Member
- Hundreds of internally exposed SPs
- System wide access via federation to common systems
- Shibboleth for WAM and federation
- ECP
Our Assurance Journey – The Good

- We’ve been at this a while – The CAF
- The WiscCard
- No enterprise Active Directory
- We chose not to develop a separate system
Our Assurance Journey – The Bad

- Management commitment has fluctuated
  - The chicken and egg business case
- Not able to engage auditors early
- No one can make anyone do anything
  - Credential management
- Now we have an enterprise Active Directory
- Our documentation is pretty bad
Our Assurance Journey – The different

- We chose not to develop a separate system
- Use monitoring to address credential entropy
Service Description:
Name of Service: InCommon Silver
Service Category: Identity and Access Management (IAM)
Description:
For users: The InCommon Silver Service allows users to access restricted, sensitive and/or high-value resources using their home institution credentials (e.g. NetID and password). These resources may be hosted at UW-Madison or elsewhere including other universities, virtual organizations, government institutions (e.g. NIH, NSF) or at private companies.
For Service Providers (SPs): Provides Service Providers (SPs), with a high level of assurance that:
- An individual identified as “InCommon Silver” who accesses a protected resource has been identity proofed such that there is high confidence that the individual is in fact who they claim to be and that any attributes associated with the individual and asserted by the identity provider (IdP) are correct.
- That the provisioning, proofing, credential store, authentication and authorization systems used to manage the user’s identity are secure and compliant with InCommon’s Silver Identity Assurance Profile (IAP).
[http://www.incommon.org/docs/assurance/IAP_V1.1.pdf ]
URL: [TBD on Middleware Services Team page]
Service offered to:
Any faculty/staff, student or affiliate of the University of Wisconsin-Madison who wish to access resources that require an assurance level of “InCommon Silver”. An individual can obtain the InCommon Silver classification by presenting the required identity documents to the Wiscard Office.
Any SP who wishes to restrict access to a resource to individual’s classified as “InCommon Silver”.
Middleware:
The following functions/processes are supported:
IdP/User Access:
The InCommon Silver Level of Assurance (LOA) is assigned after an individual presents documentation to the Wiscard Office sufficient to proof their identity to a high level of confidence. The Wiscard Office stores the LOA in their ViaNet system. An integration allows the identity management system to receive changes to a user’s LOA.
The LOA value is stored in the user attribute “eduPersonAssurance” in the University Directory.
The web access control infrastructure asserts LOA to SPs that have requested it.
The InCommon Silver Service process owner (e.g. DoIT Security, CAS, OCIS, MST, Wiscard Office) manages (e.g. lowers or raises) LOA. For example, in the event we believe a user’s credentials have been compromised, LOA would be lowered. Once the credentials are changed, LOA would be raised.
• **SP Support:**
  A service provider web link can be protected such that the web access control system only allows users classified as “InCommon Silver” to view content and/or access the application.
  A web service allows authorized SPs to query the identity management system and receive a user’s LOA.
  Best practices documents, sample code and other developer tools are available that allow SPs to modify their systems to use asserted LOA values. For example to allow users not classified as “InCommon Silver” to access parts of an application but not others.

• **Compliance:**
  The Technical Controls and Processes included in the InCommon IAP have been implemented and Documentation has been produced.
  An Audit has described by the InCommon Silver IAP has been performed, resulting in an audit opinion that the University of Wisconsin IAM systems and processes are compliant with the InCommon Silver IAP.

• **Identity Proofing:**
  Wiscard Office processes ensure that “InCommon Silver” classified individuals have been proofed such that there is high confidence that they are in fact who they claim to be and that any attributes associated with them and asserted by the identity provider (IdP) are correct.
University of Wisconsin-Madison Employee Identity Proofing Process - Part 1
University of Wisconsin-Madison Employee Identity Proofing Process - Part 2
Recommended Assurance Process

- Create a project
- Scope the project
- Gain high level sponsor and engage auditors early
- Gap analysis
- Collaborate with other schools
- Management Assertions
- Audit and/or Representation of Conformance (RoC)
- Submit to InCommon
Virginia Tech Certification

- Certified for Bronze and Silver July 2012 under 1.1
- Full audit
- Multi factor “alternative means” with x.509 certificates on SafeNet eToken
- Integrated with Central Authentication System (CAS) for Single Sign-on
Next Steps for Virginia Tech

- Recertify under 1.2
- Multi factor alternative means
- Approved algorithms
- Updated audit may be required
Use Cases

- Government/research cloud service
  - CILogon, gives researchers access to Open Science Grid
- Campus service from a cloud provider
  - People Admin
Resources
www.incommonfederation.org/assurance
Discussion
Mary Dunker – dunker@vt.edu
Steve Devoti – devoti@wisc.edu