InCommon Silver

InCommon Silver: Identity Assurance Profile Discussion

2008 Internet2 Spring Member Meeting
April 21, 2008

David Wasley, a member of the InCommon Technical Advisory Committee, provided an overview of the proposed InCommon Silver level of assurance.

InCommon Silver is based on the Federal eAuth level of assurance program, which will include four levels of trust. Silver is roughly equivalent to the eAuth level 2, while the original InCommon profile, now called Bronze, is equivalent to eAuth level 1. Silver provides an additional level of trust for Identity Providers that require this enhancement.

Assurance profiles provide a structured set of requirements for the management of access to general classes of resources. The draft of the Silver profile is available for review and feedback on the InC-Collaborate wiki here.

The InCommon Silver Profile assesses these policies and operations of an IdP:

Business, Policy and Operational Factors

- Established legal entity
- Designated authority for IdMS & IdP
- General disclosures to identity subjects
- Documentation of policies & practices
- Appropriate staffing
- Subcontracts
- Helpdesk
- Audit of IdMS operations
- Risk Management plan
- Logging of operation events

Registration and Identity Proofing

- Identity Verification Process disclosure
- Retain records of Id documents
- And one or more of:
    - Existing relationship with the IdP organization
    - In-person proofing
    - Remote proofing

There was some discussion in the area of identity proofing. Universities many times provide credential to students and faculty before they arrive on campus. One suggestion for that scenario is to assign those individuals a bronze or undefined level, then do more substantial identity proofing in person and reassign them to Silver, as appropriate. Another option is to implement a remote proofing process.

In terms of either in-person or remote proofing, the InCommon Silver proposal includes is a list of required information and is aligned with NIST 800-63-1 and eAuth. A Registering Authority is required to verify two forms of identification presented by an individual. This could include government-issued IDs, a credit card or proof of utility service.

The InCommon TAC's intention is to make the identity proofing requirements consistent with an institution's employment activities. For example, the hiring process must comply with federal and state requirements and would typically include checking the identification of someone being hired. The intent is to make the identity proofing similar and not create additional burdens. Many universities already do this, but may not document the process, which InCommon Silver requires.

It is possible that some individuals may be proofed at the Silver level (most employees, for example) and some at the Bronze level (prospective students, for example). In addition, some applications may not require Silver, so why put people through that process unnecessarily? A student may be Bronze, for example, until the FAFSA moves to Level 2, at which time, Silver will be required.

Digital Electronic Credential Technology

- Unique credential identifier (User ID)
- Subject modifiable shared secret
- Strong resistance to guessing shared secret
- Stronger credentials are acceptable too

Regarding a "strong resistance to guessing shared secret," a NIST document provides a metric concerning how complicated a password must be to be prevented from being guessed. NIST provides an Excel spreadsheet that, after input of credential requirements (i.e. upper and lower case, numbers and letters, etc.), provides a numerical rating for the strength of the password.

Credential Issuance and Management

- Unique Subject identifier
- Credential status management
- Confirmation of delivery
- Credential verification at time of use
- Suspected credential compromise
- Credential revocation

In the case of suspected credential compromise, NIST locks out accounts. Universities typically do not want to do this, so some discussion in this area is required.

Security and Management of Authentication Events

- End-to-end secure communications
- Proof that Subject has control of credential
- Session token authentication
- Secure stored secrets
- Restricted use of secrets
- Mitigate risk of sharing credentials
- Threat protection
- Authentication protocols

Identity Information Management

- Identity status management (if something about an individual changes, the information must be updated in a timely way.

Identity Assertion and Content

- InCommon recommended attributes (eduPerson attributes)
- Identity Assertion Qualifier
- Cryptographic security

Technical Environment

- Configuration Management
- Network Security
- Physical Security
- Continuity of Operations plan

Implementation - Qualifying for Silver

1. Notify InCommon of your intention to qualify
2. Have an assessment conducted by independent (internal) audit
    a. Auditor writes summary letter for InCommon (submitting the entire audit report is not necessary)
3. Execute participation agreement addendum
4. InCommon adds ID Assurance designator(s) to IdP directory data
5. IdP then may include Identity Assurance Qualifiers (IAQ) in assertions
    a. IdP is responsible to ensure they are appropriate
    b. Technical implementation yet to be determined

Use of Incommon IAQs

- IAQ represents a profile, not a "level."

- A given IdP can support multiple profiles
- IdP may assert InCommon IAQ(s) only if assigned to it by InCommon
- Identity assertion may contain multiple IAQs
    - E.g., "Bronze" or both "Silver" and "Bronze"

-
    - Avoids implying hierarchy and allows for additions with minimal disruption
- Relying Party looks for IAQ(s) it will accept

PKI and Federation

- Similar trust models

- trusted authority
- registration authority
- assurance included in cert or assertion
- credential compromise is dealt with
- Linking federations is like PKI bridging

PKI plus federation

- Best of both worlds
- PKI provides strong local authentication
- Federation provides rich, flexible identity
    - Protects Subject privacy
    - Also solves the TA problem
- PKI also supports S/MIME, signatures, data integrity, etc.

NIH Discussion

Debbie Bucci from the National Institutes for Health was at the session. She said that NIH is working to roll out applications that they are looking to federate. For example, a Sharepoint service for public information officers is expected to go live in May. The grant community is looking to federate with NIH and there are a number of Level 2 applications being developed.

The NIH is exploring ways for faculty and other campus-based individuals who have NIH-assigned accounts to begin federating with their campus IDs. NIH is developing a way for these individuals to map their NIH accounts to their federated accounts.

Gap Analysis

The InCommon TAC encourages institutions to perform a self-assessment, based on the Silver profile. Penn State, for example, did a gap analysis, reviewing the Silver document and listing what would need to be accomplished to meet the requirements.