InCommon Defined Identity Assurance Program

• A Basis for Trusted Identity Assertions

David L. Wasley

Internet2 Spring Members Meeting
April 2008
Outline

- Why InCommon is offering this
- Identity Assurance generally
- InCommon support for Identity Assurance
- InCommon Identity Assurance Profiles
Why Identity Assurance

- The intent is to give Relying Parties confidence in information they receive about a Subject.
- Federal agencies were early to see this.
- Higher Ed interacts with many of them.
- Not all Relying Parties want or need the same degree of confidence.
Identity Assurance generally

- Trust is based on many factors
  - Relying Parties must do risk analysis
  - Profiles can be created for classes of RPs
  - No trust is perfect

- Build on existing conventions
- Mechanism must be practical
  - Excessive complexity won’t be accepted

- Not required for every Subject or RP
PKI Levels of Assurance

• Based on Federal PKI model
  – One CP
  – 4 levels of trust (plus “test”)
  – CP OIDs used to convey level
  – Allowed for mapping between PKI domains

• Copied by other PKIs
  – Pharma, aerospace, HEBCA, …
Identity Federation and LoA

• Federated IT environments separate identity and access management
  – Credential binds identifier to physical person
  – Necessary information about that person is given to access management separately

• IdP issues credentials & stores attributes
  – Id proofing attempts to ensure uniqueness
  – Id attributes come from authoritative sources

• Assurance doesn’t have to be hierarchical
  – Different “profiles” for different use cases
Identity Model

• Identity is the set of information relevant to a person

• Three parties involved
  – Identity Subject is who wants to claim an ID
  – Relying Party, e.g. Service Provider, receives identity information from an Identity Provider
  – Identity Provider supports identity Subjects by maintaining a database of reliable ID data

• Each party must trust the others
  – InCommon Silver addresses only IdPs
Identity Assurance projects

- NIST 800-63-1
  - Federal eAuthentication
  - See also M0404, HSPD-12 and NIST FIPS 201
- Liberty Alliance Identity Assurance Framework
- RealID “Final Rule”
- FBI Biometrics Database
- InCommon Identity Assurance Profiles
  - “Bronze”, “Silver”, ...
Compliance is optional!

Now in DRAFT for review and feedback

Structured sets of requirements intended to satisfy management of access to general classes of resources

Additional profiles may be needed
  - Hopefully limited in number(!)

First 2 defined to be comparable to eAuth
  - “Bronze” >= eAuth level 1
  - “Silver” >= eAuth level 2
Identity Assurance Framework

- Business, Policy and Operational Factors
- Registration and Identity Proofing
- Digital Electronic Credential Technology
- Credential Issuance and Management
- Security and Management of Authentication Events
- Identity Information Management
- Identity Assertion and Content
- Technical Environment
InCommon “Silver” Profile

• 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
InCommon “Silver” (cont.)

• 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

• Digital Electronic Credential Technology
  – Unique credential identifier •
  – Subject modifiable shared secret •
  – Strong resistance to guessing shared secret *
  – Stronger credentials are acceptable too
InCommon “Silver” (cont.)

• Credential Issuance and Management
  – Unique Subject identifier •
  – Credential status management •
  – Confirmation of delivery
  – Credential verification at time of use
  – Suspected credential compromise (†)
  – Credential revocation

† indicates an InCommon variant from the NIST recommendations
InCommon “Silver” (cont.)

• 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 *
InCommon “Silver” (cont.)

• Identity Information Management
  – Identity status management

• Identity Assertion and Content
  – InCommon recommended attributes • (†)
  – Identity Assertion Qualifier • (†)
  – Cryptographic security •

• Technical Environment
  – Configuration Management
  – Network Security
  – Physical Security
  – Continuity of Operations plan (†)
Implementation

- Notify InCommon of intention to qualify
- Assessment by independent (internal) audit
  - Auditor writes summary letter for InCommon
- Execute Participation Agreement Addendum
- InCommon adds Identity Assurance Designator(s) to IdP directory data
- IdP then may include IAQ(s) in assertions
  - Is responsible to ensure they are appropriate
  - 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 & Federation

• Similar trust models
  – Trusted authority vets adherence to profiles
  – Registration authority vets Subject identity
  – Assurance included in cert or assertion
  – Credential compromise is dealt with
    • Threats are mitigated
  – Linking federations is like PKI bridging
PKI plus Federation

• The 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.
IAP is new & evolving

• How many profiles are needed?
• Should attributes have separate IAP?
  – Must all attrs have the same assurance?
• Can we inter-federate and map IAQs?
• Use of SAML “authN Context”
• Etc. etc. etc…
Further Information

• InCommon Identity Assurance Profiles
  • https://spaces.internet2.edu/display/InCCollaborate/InCommon+Identity+Assurance

• NIST 800-63
  • http://csrc.nist.gov/publications/PubsSPs.html

• Liberty Alliance Identity Assurance Framework
  • http://www.projectliberty.org/liberty/strategic_initiatives/identity_assurance

• RealID
  • http://www.dhs.gov/xprevprot/programs/gc_1200062053842.sht

• FBI biometrics database
  • http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html