InCommon®

The InCommon Assurance Program: Bronze and Silver

Wednesday, June 22, 2011

John Krienke, InCommon, Internet2
Renee Shuey, Penn State
Jacob Farmer, Indiana University

InCommon®

What we're going to talk about

- The need for identity Assurance
- The basics of Assurance: The 'Framework'
- The details: The 'Profiles'
- What's Next for the Assurance Program

InCommon®

Why IAPs

- 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

InCommon®

“...useful Concept Even Without Federation”

- 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
- We already do this today
- On Campus:
  - University Loan Program
  - Student Organizations
  - Registration
  - W-2s
  - Non Credit Courses

InCommon®

Assurance for Federating

- NIH - 70+ Apps at LoA 1 today, but It's not about the number of apps, it's about the number of users
- Providing access to 250,000 users today expecting 4x within 2 years
- If you still need the app....
  - Electronic Research Administration (eRA) - Gateway for many LoA 2 applications

InCommon®

Assurance for Federating

- National Science Foundation research.gov
- TIAA CREF
- National Student Clearinghouse Meteor
- CIC - Access to transcripts
- Other government agencies will follow...

InCommon®

Human Transactions

Risk: Odds of Harm, Degree of harm

Leads to: Protection & need for Trust

"Trust involves a chance outcome under the control of another party."

- Bohnet & Zeckhauser, Journal of Economic Behavior & Organization

The Internet: Relationships & Consequences at a distance

Measuring Risk, Measuring Assurance

Risk Leads to Assurance

- Starting point: Risk as determined by application/service
  - Example: OMB M-04-04

Table 1 – Maximum Potential Impacts for Each Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

InCommon®

US Government Engagement

- ICAM of GSA/DOD created a TFPAP program
  - Identity Assurance + Privacy
- Assurance 1.0.x documents: InCommon now Provisionally Approved as Trust Framework Provider
  - Level 1 and 2 of TFPAP map to InCommon Bronze & Silver
  - along with Kantara Initiative, Open Identity Exchange; useful collaboration with industry partners via these orgs

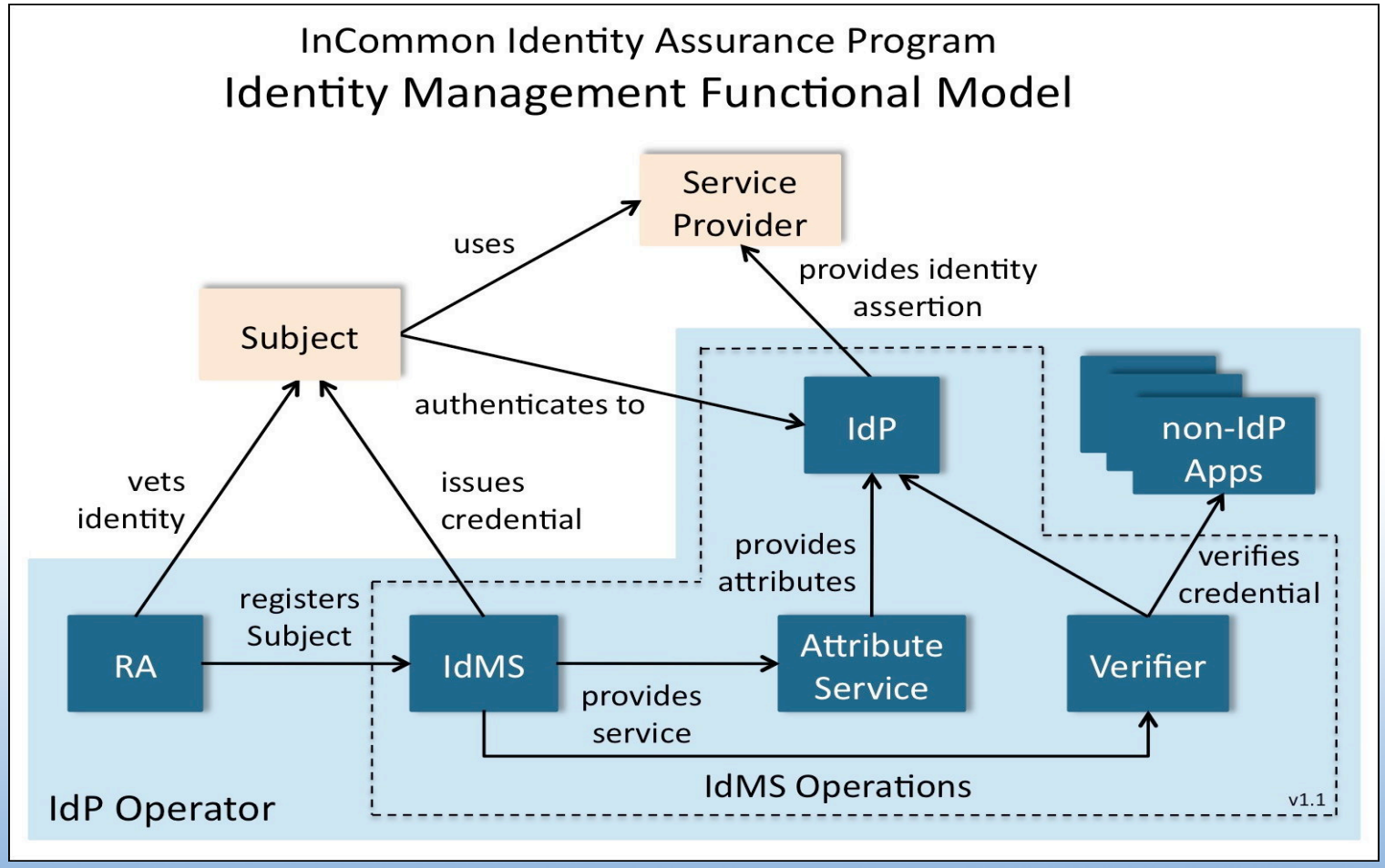
InCommon®

Assurance Documents

1. Identity Assurance Assessment Framework (IAAF)
    1. Functional Model
    2. The structure of the profiles: criteria and levels
    3. Assessment and Audit Process
2. Identity Assurance Profiles: Bronze and Silver (IAP)
    1. Business, Policy and Operational Criteria
    2. Registration and Identity Proofing
    3. Credential Technology
    4. Credential Issuance and Management
    5. Authentication Process
    6. Identity Information Management
    7. Assertion Content
    8. Technical Environment
3. Legal Addendum: Privacy stipulations

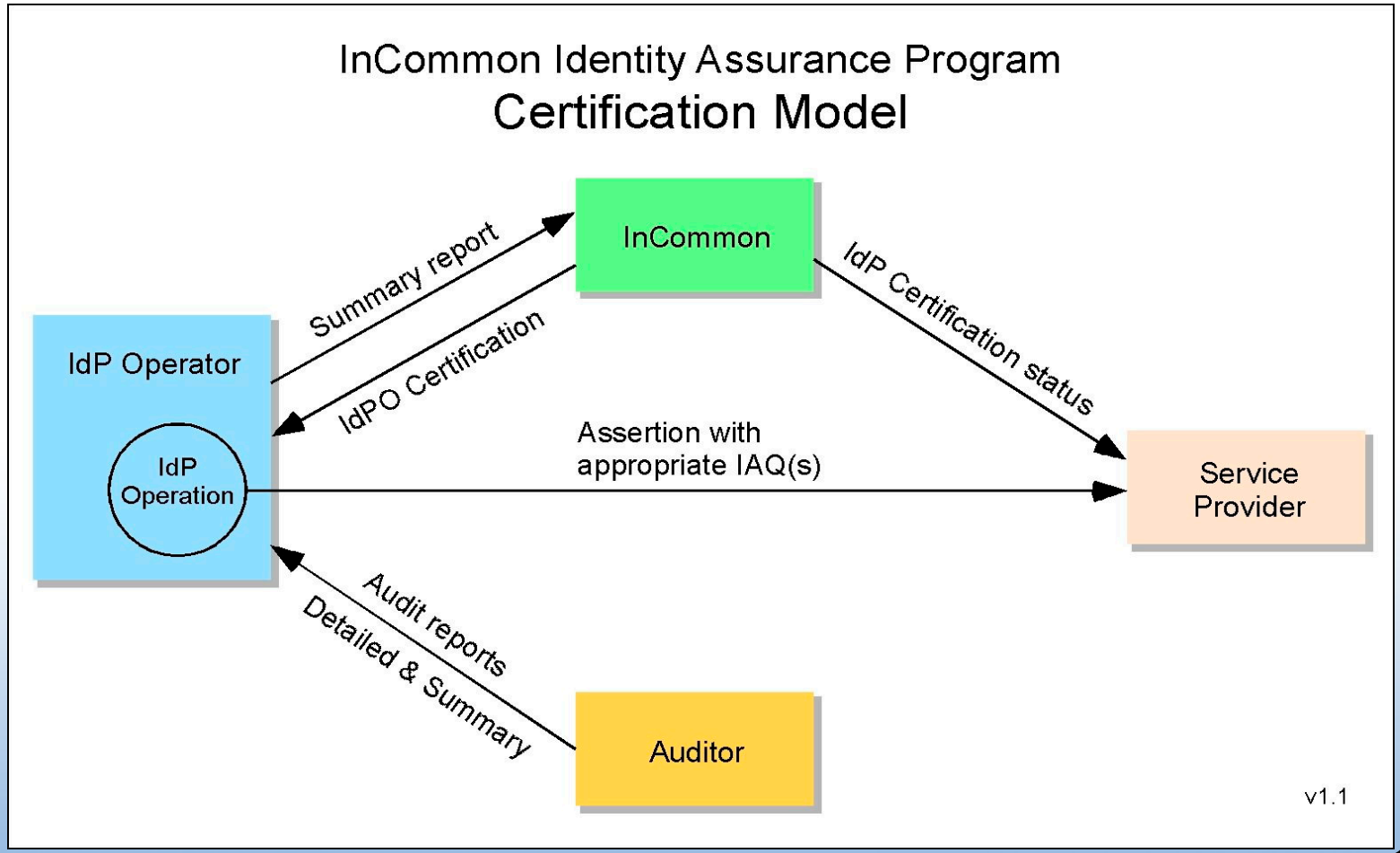
InCommon®

IAAF: Functional Model



InCommon®

IAAF: Assessment and Audit



InCommon®

IAP

1. Business, Policy and Operational Criteria
2. Registration and Identity Proofing
3. Credential Technology
4. Credential Issuance and Management
5. Authentication Process
6. Identity Information Management
7. Assertion Content
8. Technical Environment

InCommon®

Privacy affirmation

- Notice
  - written, prior, purpose
- Subject Participation
  - IdP participation is incorporated into Subject's role with campus
- IdP Description:
  - overview, scope of collected PII, management, problem resolution
- Information provided
  - Prior agreement
  - Least required
  - Abstract identifier whenever possible
- Protection of PII
  - Storage and transmission
  - Transaction data not shared with 3rd parties

InCommon®

FAQ: Assurance Program

Required: Participation at the basic level (POP)

Optional: Participation at defined Levels of Assurance

InCommon®

FAQ: Assurance Program

Assurance need not be for ALL people affiliated with a campus. Levels can be limited to a set of Subjects, for example:

- Principal investigators for grant administration
- Staff who access retirement funds
- Students with financial aid

InCommon®

4.2.1 BUSINESS, POLICY AND OPERATIONAL CRITERIA

IdP Operators must have the organizational structures and processes to come into and remain in compliance with the provisions of this IAP.

- 4.2.1.1 INCOMMON PARTICIPANT
- 4.2.1.2 NOTIFICATION TO INCOMMON
- 4.2.1.3 CONTINUING COMPLIANCE

InCommon®

4.2.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing in this IAP is based on government-issued ID or public records. Verified information is used to create a record for the Subject in the IdPO's IdMS.

- 4.2.2.1 RA AUTHENTICATION
- 4.2.2.2 IDENTITY VERIFICATION PROCESS
- 4.2.2.3 REGISTRATION RECORDS
- 4.2.2.4 IDENTITY PROOFING
- 4.2.2.5 ADDRESS OF RECORD CONFIRMATION

InCommon®

4.2.3 CREDENTIAL TECHNOLOGY

These InCommon IAPs 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.

- 4.2.3.1 CREDENTIAL UNIQUE IDENTIFIER
- 4.2.3.2 RESISTANCE TO GUESSING AUTHENTICATION SECRET
- 4.2.3.3 STRONG RESISTANCE TO GUESSING AUTHENTICATION SECRET
- 4.2.3.4 STORED AUTHENTICATION SECRETS
- 4.2.3.5 PROTECTED AUTHENTICATION SECRETS

InCommon®

4.2.4 CREDENTIAL ISSUANCE AND MANAGEMENT

The authentication Credential must be bound to the physical Subject and to the IdMS record pertaining to that Subject as described in this section.

- 4.2.4.1 CREDENTIAL ISSUANCE
- 4.2.4.2 CREDENTIAL REVOCATION OR EXPIRATION
- 4.2.4.3 CREDENTIAL RENEWAL OR RE-ISSUANCE
- 4.2.4.4 CREDENTIAL ISSUANCE RECORDS RETENTION

InCommon®

4.2.5 AUTHENTICATION PROCESS

The Subject interacts with the IdP to prove that he or she is the holder of a Credential, enabling the subsequent issuance of Assertions.

- 4.2.5.1 RESIST REPLAY ATTACK
- 4.2.5.2 RESIST EAVESDROPPER ATTACK
- 4.2.5.3 SECURE COMMUNICATION
- 4.2.5.4 PROOF OF POSSESSION
- 4.2.5.5 SESSION AUTHENTICATION
- 4.2.5.6 MITIGATE RISK OF SHARING CREDENTIALS

4.2.6 IDENTITY INFORMATION MANAGEMENT

Subject records in the IdPO's IdMS must be managed appropriately so that Assertions issued by the IdPO's IdP are valid.

- 4.2.6.1 IDENTITY RECORD QUALIFICATION

InCommon®

4.2.7 ASSERTION CONTENT

The IdPO must have processes in place to ensure that information about a Subject's identity conveyed in an Assertion of identity to an SP is from an authoritative source.

- 4.2.7.1 IDENTITY ATTRIBUTES
- 4.2.7.2 IDENTITY ASSERTION QUALIFIER (IAQ)
- 4.2.7.3 CRYPTOGRAPHIC SECURITY

InCommon®

4.2.8 TECHNICAL ENVIRONMENT

IdMS Operations shall use up-to-date supported software.

- 4.2.8.1 SOFTWARE MAINTENANCE
- 4.2.8.2 NETWORK SECURITY
- 4.2.8.3 PHYSICAL SECURITY
- 4.2.8.4 RELIABLE OPERATIONS

InCommon®

Questions Arising

- 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?

InCommon®

Next Steps

- Email discussion list: assurance@incommon.org
  - Send email to sympa@incommon.org “sub assurance” FirstName LastName
- InCommon will resubmit new 1.1 docs to ICAM TFPAP program
- Continuing negotiations on privacy-protection provisions in TFPAP program
- Establish Review Panel (Summer)
- Finalize Legal & Business structures (Summer)
  - Addendum: privacy, rights, responsibilities
  - Fees: balancing risk and work between InCommon and Campuses
- Finalize technical model & implementation for Federation, for IdPs/SPs, Working with NIH on technical interop, and planning for first Level2 apps
- Engage Other Service who may need higher LoA
- Engage University IT & Audit communities
- Open for Certifications (Fall)