OVERVIEW:
IDENTITY ASSURANCE PROGRAM

Ann West
InCommon Assurance and Community Manager

InCommon’s Trust Services

- Federation Service
- Certificate Service
- **Assurance Service**

PROGRAM BACKGROUND

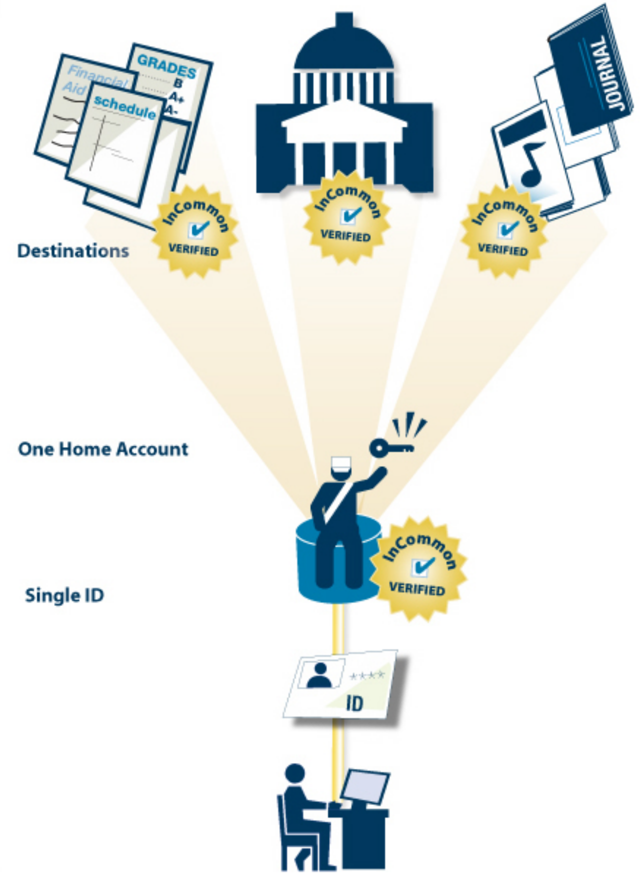
Federated Transactions

Services Relying on External Identities:

- I need to trust you to manage online identities for me?
- What are my risks?
- What are the odds and the degree of harm?

Parties need agreed-upon criteria for identity assurance

Trust. Measuring and balancing: cost, risk, adoption.



InCommon Assurance Program

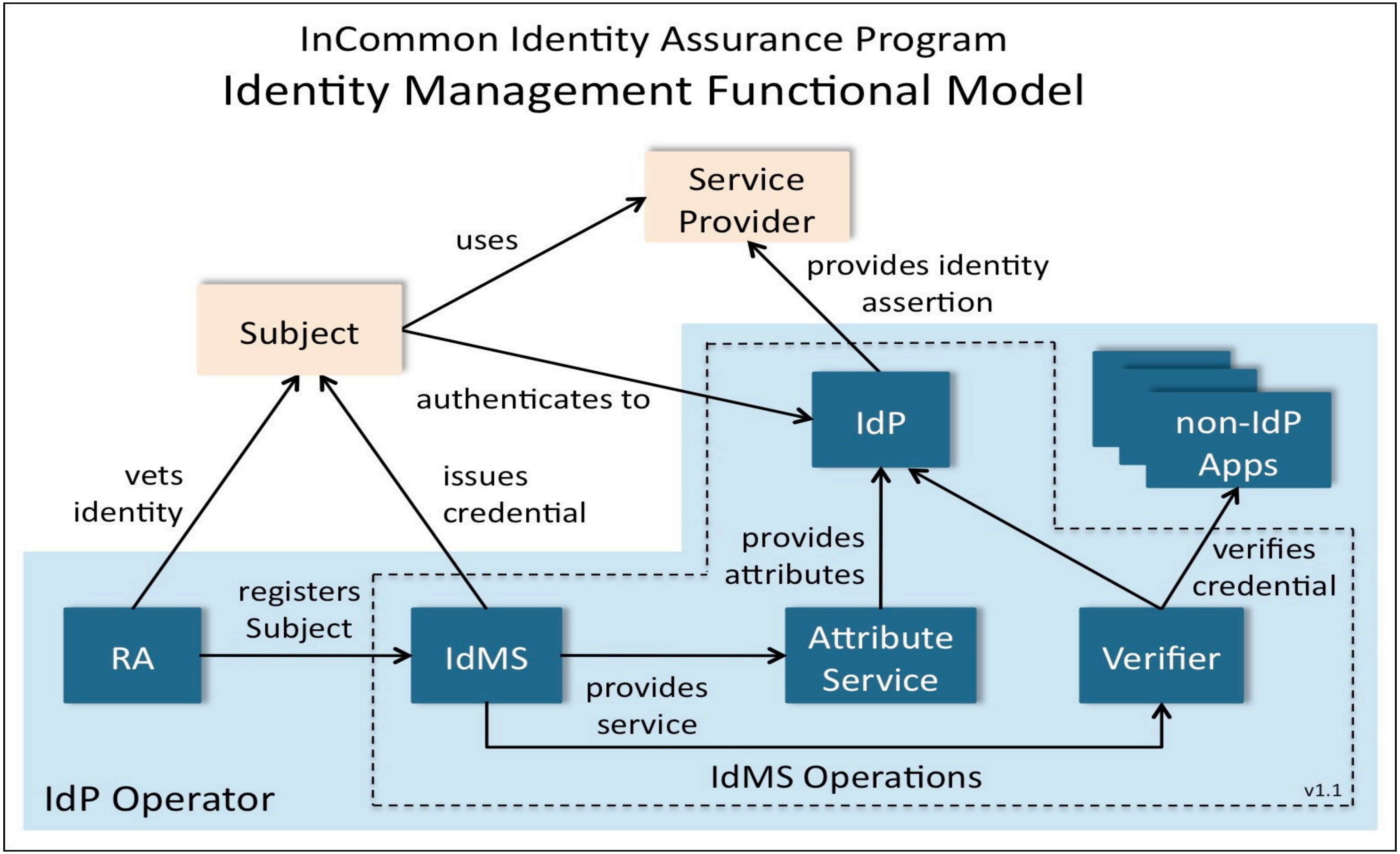
- 2004: USG defines 4 Levels of Assurance (NIST 800-63)
- 2009: USG Identity, Credential and Access Management (ICAM)
  - Establishes criteria for trust framework prov interaction with federal agencies
  - InCommon is an Approved Federal Trust Framework Provider

ICAM
Identity, Credential,
& Access Management

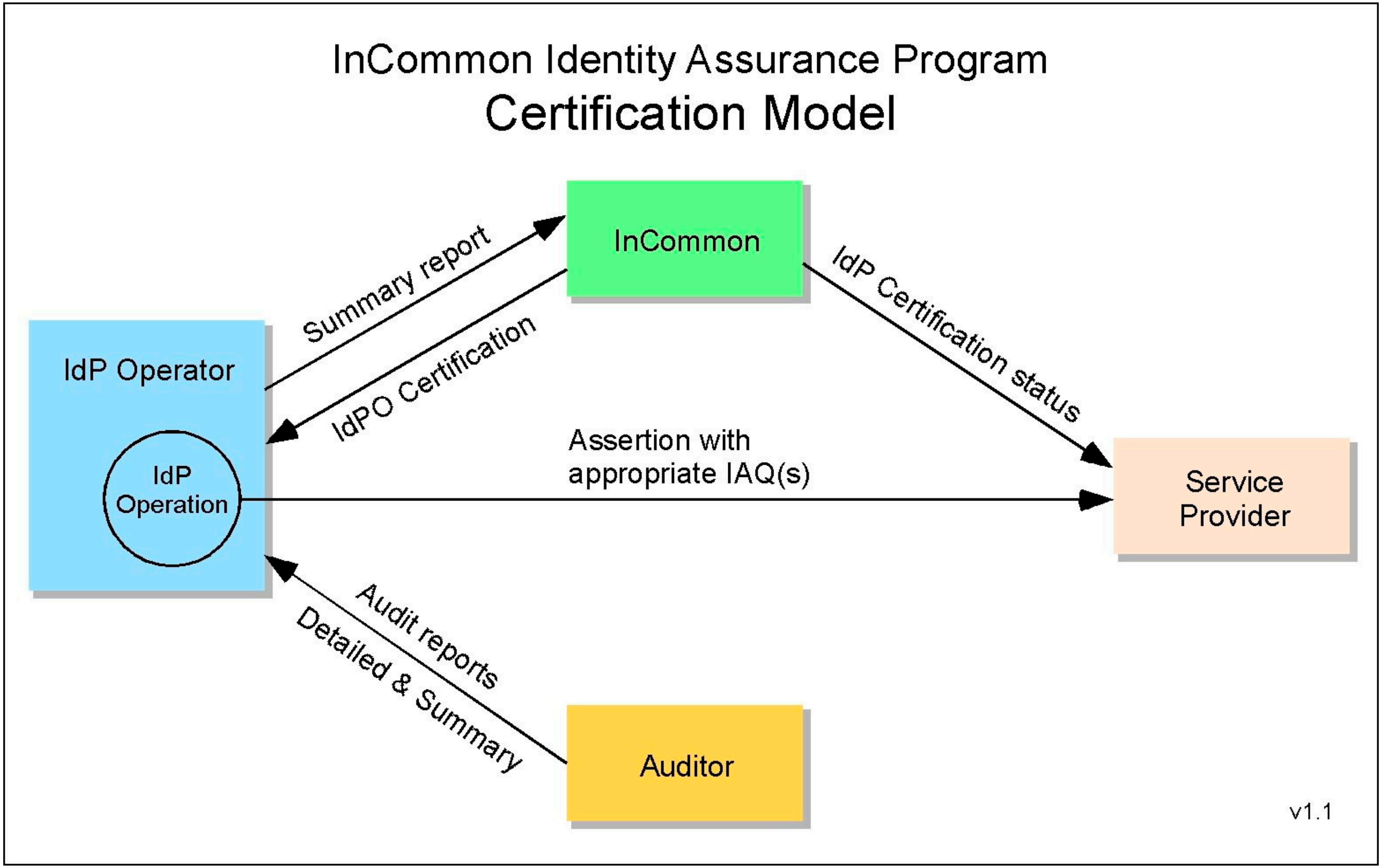
Program Basics: Definitive Documents

- Identity Assurance Assessment Framework (IAAF)
  - Trust and certification model
- Identity Assurance Profiles (IAP)
  - Specific requirements
    - Bronze (FICAM TFPAP Level 1)
    - Silver (FICAM TFPAP Level 2)
- Legal Addendum
  - Privacy criteria from FICAM's TFPAP

IAAF: Functional Model



IAAF: Assessment and Audit



InCommon IAP addresses…

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

PROGRAM DETAILS

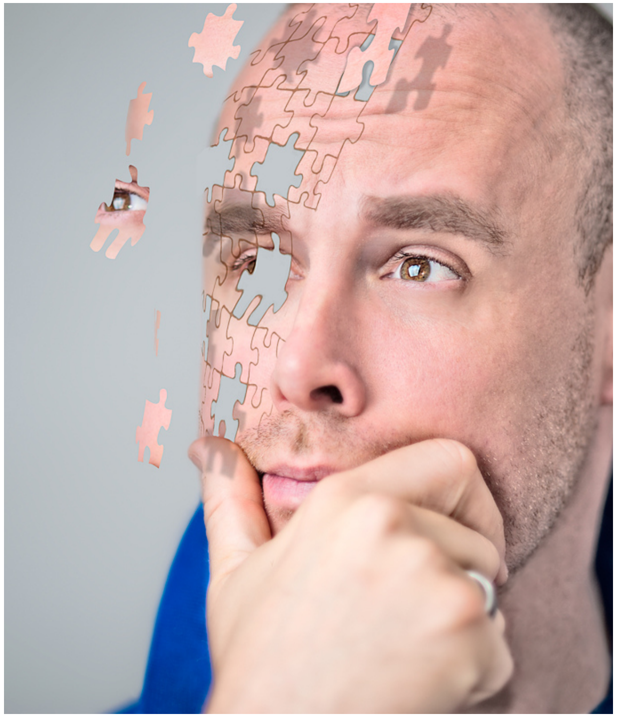
Eligibility

- InCommon Identity Provider Operators
  - Higher Education
  - Not-for-profit Research Organizations
  - Not-for-profit Sponsored Partners

Assurance Program Components

- Profiles/Framework
- Federation Operation Policies and Practices
- Legal Framework
- Certification Program
- InCommon Metadata
- Practice and Implementation Outreach
- Program Oversight: Assurance Advisory Committee

Identity Provider



- Support profile(s)
- Audit
- Apply
  - Audit Summary/Qualifications
  - Assurance Addendum
- Pay Fee
- Configure SAML software

Fees for Identity Provider Operators

Tier	2012	2013	2014	2015
1	$1,875	$1,875	$3,750	$7,500
2	$1,563	$1,563	$3,125	$6,250
3	$938	$938	$1,875	$3,750
4	$688	$688	$1,375	$2,750

Graduated to reflect

- Increasing value
- Early adopter contributions

New Simplified Bronze will be priced differently

Service Provider

- Determine which qualifier to request
  - OMB 04-04 E-Authentication Guidance for Federal Agencies
- Configure SAML Software to check metadata and request qualifier
- Notify InCommon of your intent to request
- No fee

Service Providers Requiring Identity Assurance Qualifiers

Early List for 2012

- National Student Clearinghouse/Meteor
  - Financial Aid Access
- CILogon (Open Science Grid)
- Selected LIGO Services
- Federal Services – Stay tuned

AuthnContext, Not Attributes

- Use SAML2 AuthnContext to express assurance
    - See: http://wiki.oasis-open.org/security/SAML2IDAssuranceProfile
- Once certified:
    - InCommon adds Identity Assurance Qualifier to metadata to authorize you to assert Silver/Bronze.
    - IdP/SP updates software to return/request IAQs
        - Shibboleth is the only known implementation that adequately supports AuthnContext
        - Custom login handler for IdPs
    - Identifiers for InCommon Silver/Bronze:

```
http://id.incommon.org/assurance/silver
http://id.incommon.org/assurance/bronze
```

Technical Documentation

Service Provider Behavior
https://spaces.internet2.edu/x/m4yVAQ

Identity Provider Behavior
https://spaces.internet2.edu/x/mYyVAQ

Shibboleth docs

- https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionInitiator

- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPUserAuthn

THE SIMPLIFIED BRONZE

The Simplified Bronze (LoA 1)

- Oct 2011: Federal CIO Memo
- 40+ Federal Apps at LoA1 in InCommon now
  - NIH – 42 including PubMed, CTSA wiki
  - NSF – research.gov/Fastlane grant submission
- ICAM encouraging broad Bronze deployment
- New Bronze available for review
    - Reduces requirements to simplify deployment
    - Removes profile audit requirement

The Simplified Bronze: How does this affect me?

- InCommon to submit docs to ICAM for review
  - Docs may change
  - Work with community on migration plan
- Still working with US Government, LIGO, CILogon, and National Student Clearinghouse on Silver
- Looking to move community forward under Bronze
  - Considering waiving Assurance fee for 2012-2013 for Bronze only
  - Possible implementation timeframe 6-9 months
  - Doable? What would you need?

New v1.2 of IAAF and IAP: How can I comment?

- Review site: spaces.internet2.edu/x/KYXNAQ
- Send comments to community list assurance@incommon.org
- Comment period open until May 7
- Interested in hearing:
  - Specific changes
  - Does the new Bronze enable you to implement the profile more quickly?
  - How long do you think it would take you to deploy? (Have we made it easy enough?)

Chickens and Eggs? Rocks and Hard Places….

- Service Provider requirements are evolving
- Identity Providers risk/work averse
- ICAM and Agencies
    - Pointing to our list of certified campuses
- HE Communtiy
    - Pointing to our list of SPs requiring assurance
- Remember InCommon Federation way back when
    - We have 394 members as of today
    - But with Assurance it's dejavu all over again….

What Resources are Available to Help?

- Your Peers on assurance@incommon.org
  - New resources are announced here too.
- Community Resources
  - AD Silver Cookbook
  - Multi-factor Authentication Guidance
- Webinars
  - IAM Online: Active Directory and Silver on March 14, 3 pm ET
- Monthly Calls (Next Call May 2nd at Noon ET)
- Meetings
- Toolkit (coming soon)