

Approaches to InCommon Bronze From George Washington University and Harvard

March 4, 2015

Speakers

Asif Hafiz, Director, Identity and Access Management, George Washington University

Scott Bradner, Senior Technical Consultant, Harvard University

Moderator

Ann West, Associate Vice President for Trust and Identity, Internet2

Introduction and Overview

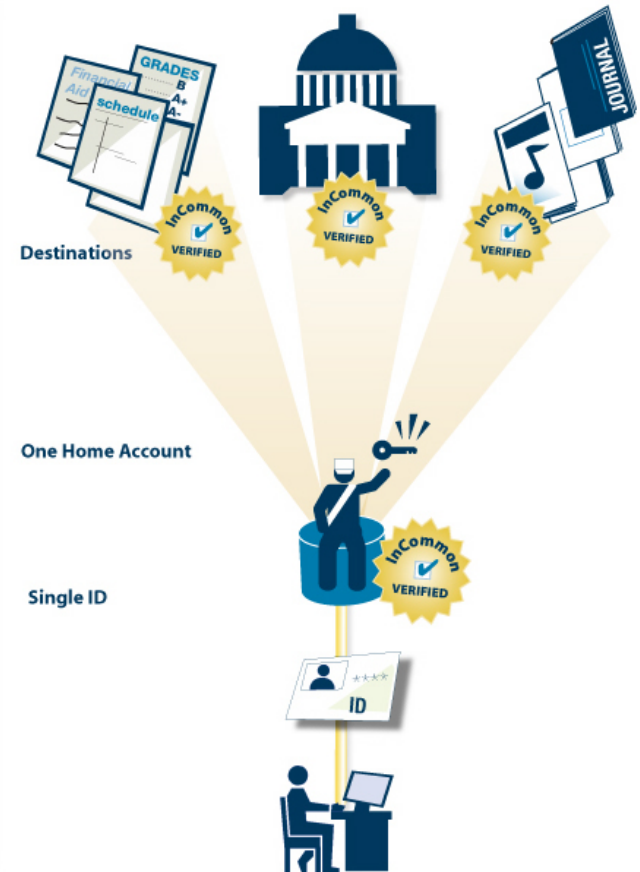
Federated Transactions

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.



We have MFA, Why Worry About Passwords?

- Do you use passwords to protect sensitive data?
- Not every risk is about phishing...

Strategy and choices

- Use stronger credentials where you can
- Improve passwords until you no longer need them



InCommon Identity Assurance Profiles

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

Provenance: InCommon Profiles

- US Government FICAM
 - Based on NIST 800-63
 - Assesses comparability
- Profiles
 - Developed for HE
 - Address FICAM requirements with HE flexibility



Due Diligence

- What standard do you use now?





InCommon Bronze Certification



Agenda



- **GWU facts**
- **IAM History**
- **IAM ecosystem**
- **IAM Governance**
- **Drivers for InCommon Bronze**
- **GW's response to InCommon Bronze requirements**
- **Questions?**



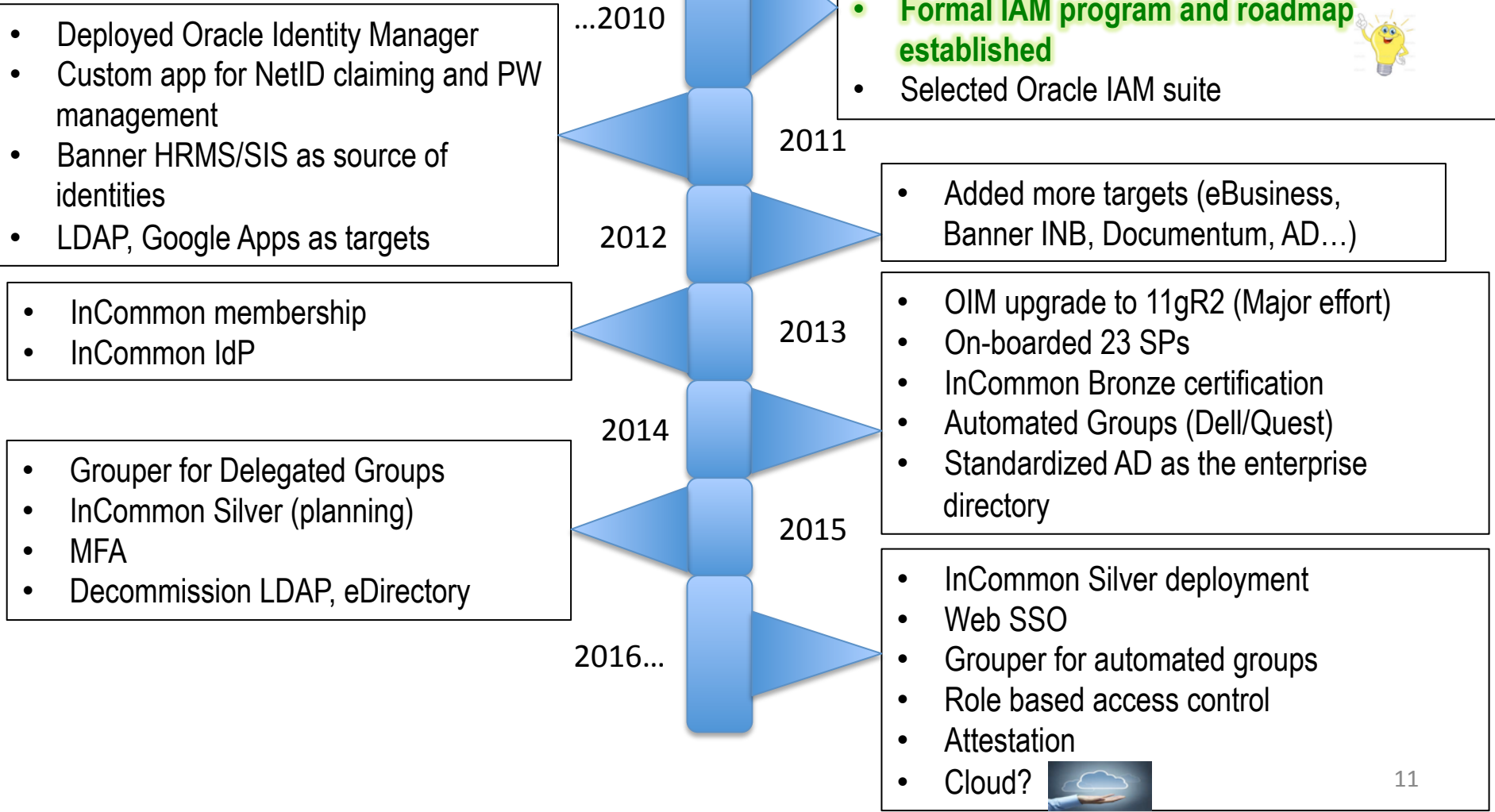
GWU Facts



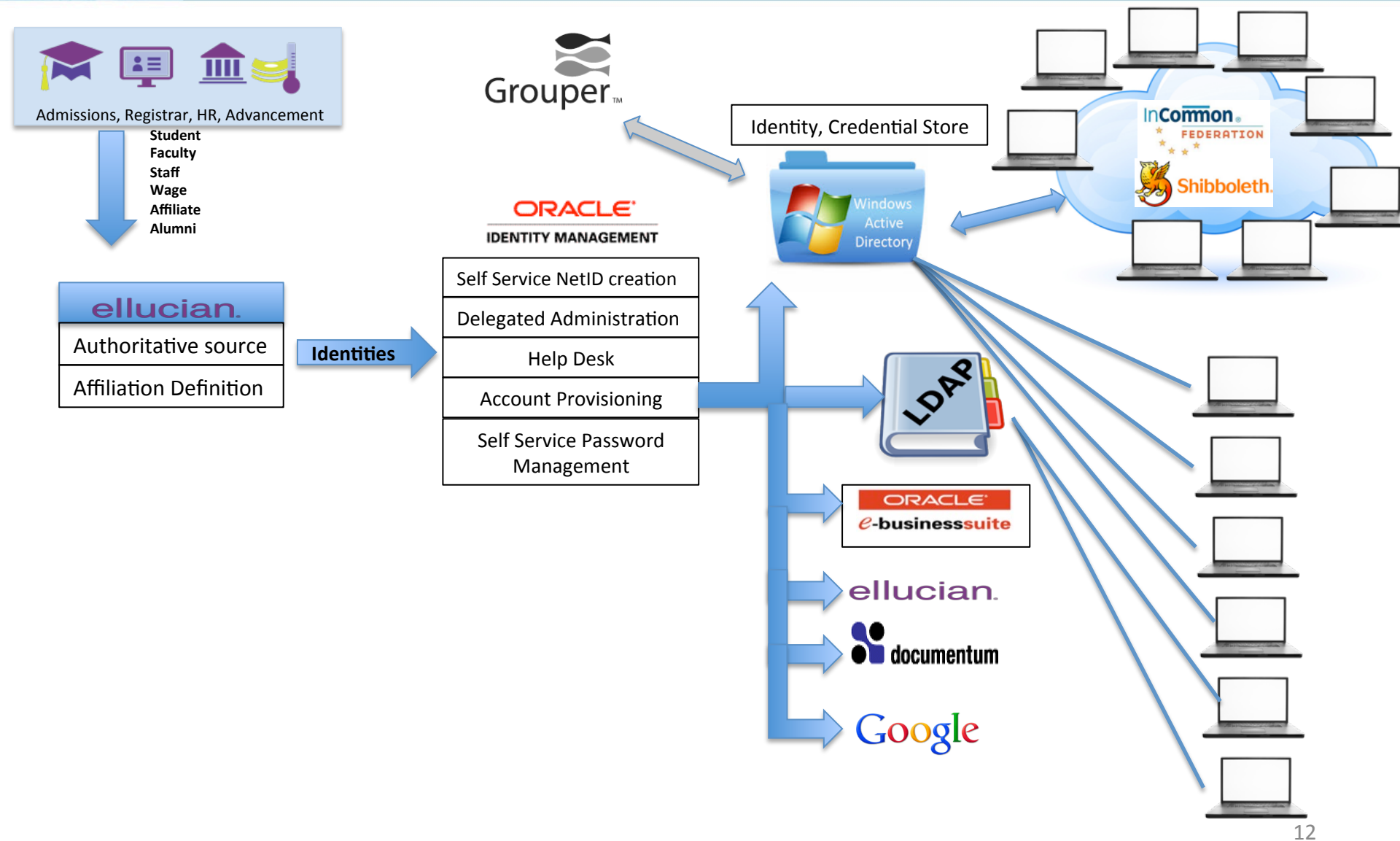
- The University was chartered in 1821 by an act of congress
- Main campus is 4 blocks from the white house and mere blocks from many major government and non-government agencies, making research, internship and career opportunities for students and faculty literally a short walk away
- 3 Campuses: Foggy Bottom and Mount Vernon in Washington DC and the Virginia Science and Technology Center in Ashburn, Virginia
- 10 Schools including a Law and a Medical School
- Largest Institution of higher education in Washington DC
- 25,000 students enrolled from all 50 states and more than 120 countries
- 270,000 alumni in more than 150 counties worldwide



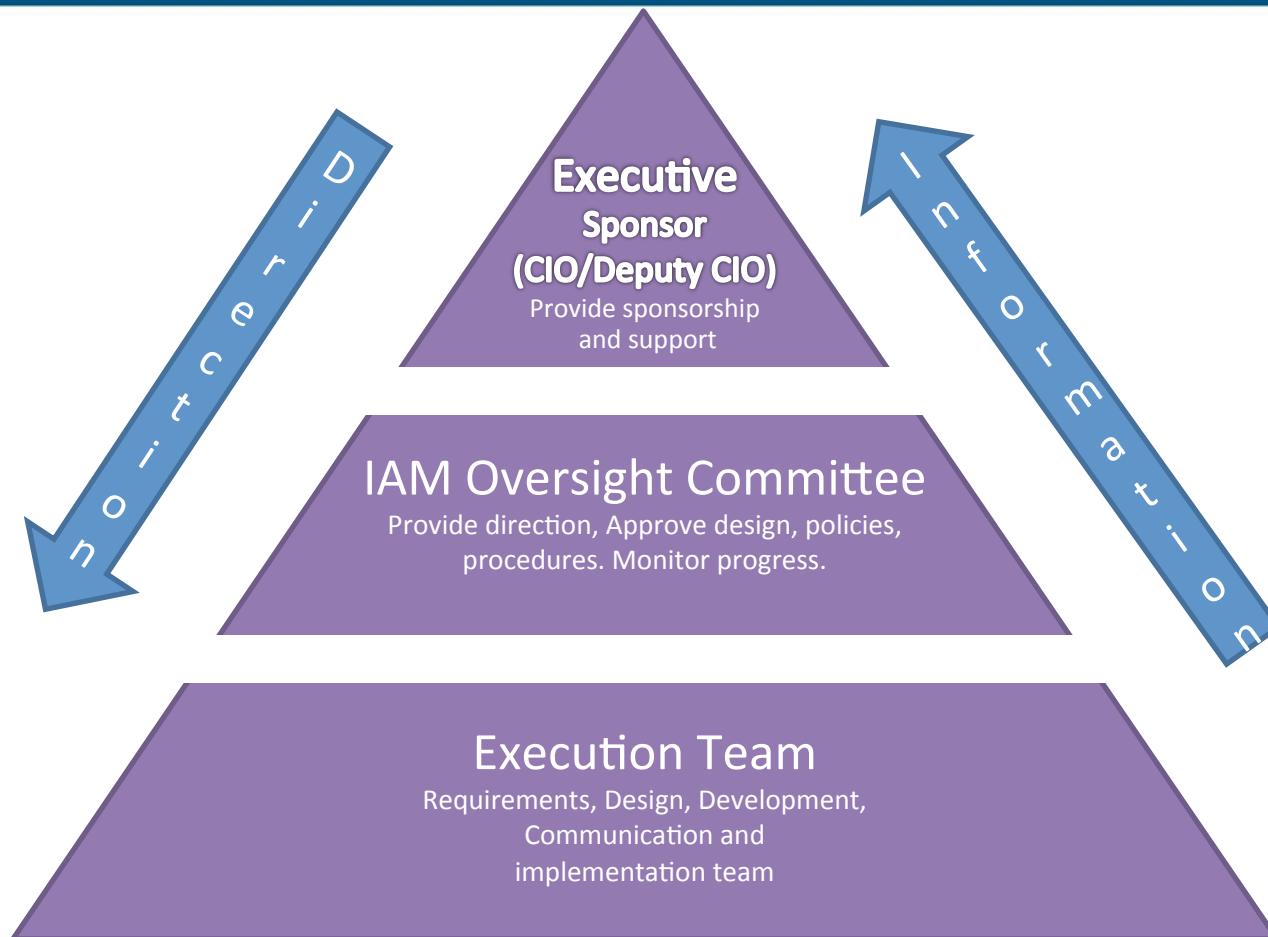
GWU IAM History



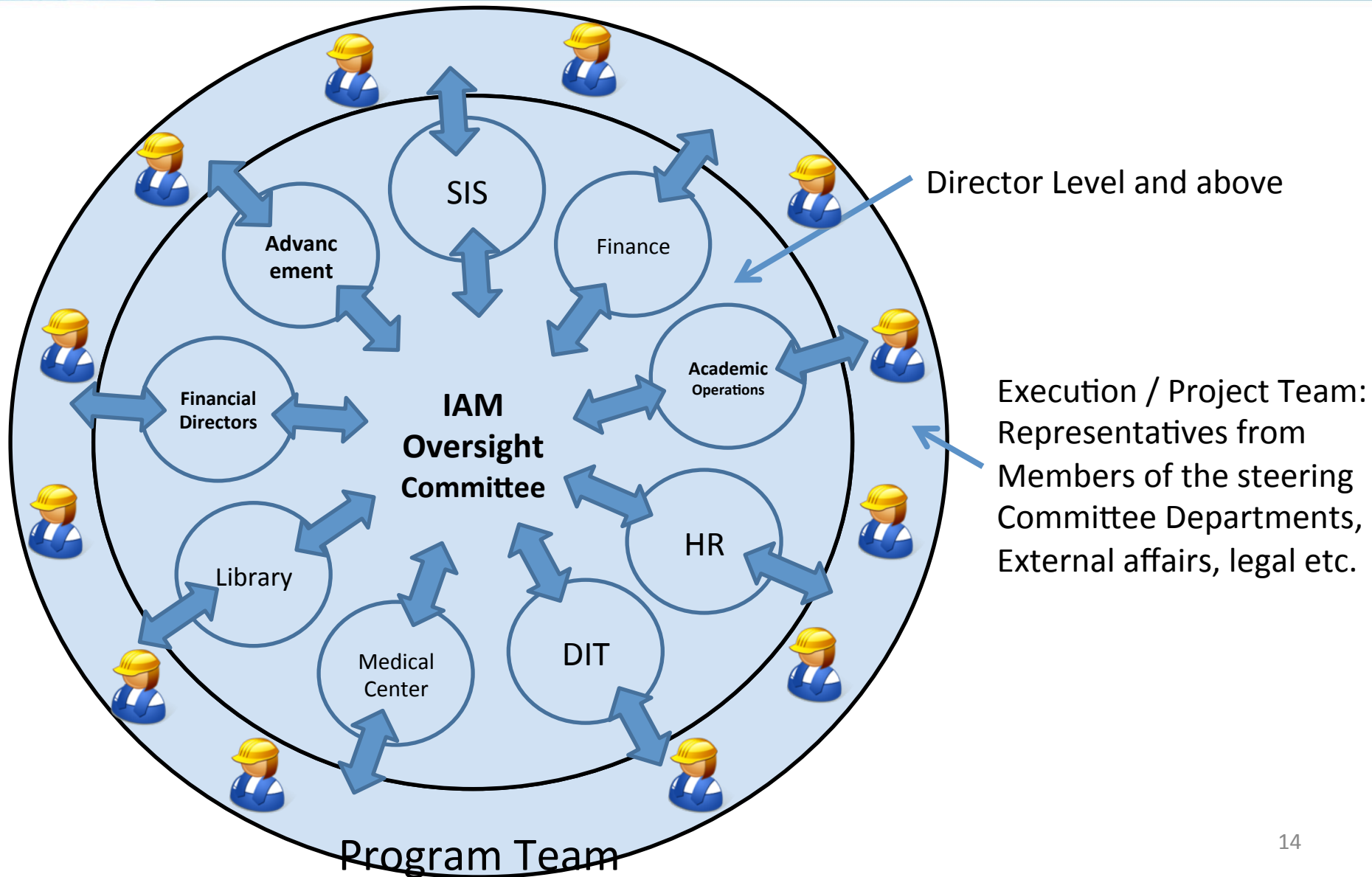
GWU IAM Ecosystem



IAM Governance



IAM Governance



Drivers for InCommon Bronze



- **Desire to meet federal standards and security guidelines**
- **Federal grants will have acceptance criteria tied to the security posture of an institution**
- **It is expected that the security controls and procedures already put in place meet or exceed Bronze certification requirements**
- **No external audit required, process is simple and bronze certification is free.**
- **Stepping stone to the next assurance level of Silver**



GW's response to InCommon Bronze requirements



- **Business, Policy, & Operational Criteria**

- ✓ • IdPO must be an InCommon Participant in good standing
- ✓ • IdPO must notify InCommon of any significant changes to its IAM operations that may affect its compliance to its Identity Assurance profile.
- ✓ • IdPO must declare to InCommon continued compliance with profiles under this IAP at least every 3 years
- ✓ • The IdPO must align with the organization's risk management objective by a periodic review process.



- **Protection of Personally Identifiable Information**

- ✓ • Any PII information collected during registration and/or Identity proofing must be protected from unauthorized disclosure

- **Credential Unique Identifier**

- ✓ • Each Credential issued by the IdPO shall include a unique identifier
- ✓ • A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.
- ✓ • The IdPO shall clearly associate the Credential unique identifier to the Subject's registration record in the IdMS, for use by the Verifier or other parties
- ✓ • The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 1 in 1,024 over the life of the Authentication Secret.



- **Credential Unique Identifier**

- ✓ • Authentication Secrets shall not be stored as plaintext
- ✓ • Plaintext passwords or Secrets shall not be transmitted across a network.

- **Credential Issuance / Revocation**

- ✓ • The Subject shall identify himself or herself in any new transaction with information known only to the Subject
- ✓ • The IdPO shall revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised.
- ✓ • A Subject must be authenticated for purpose of Credential renewal or re-issuance by any of the 3 methods provided.

- ✓ • The process or processes used by the IdPO while issuing credentials must enable the Subject to verify that the IdPO is the source of Credentials they receive.
- **Resist Replay and eavesdropper Attack**
- ✓ • The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.
- ✓ • The authentication protocol must resist an eavesdropper attack
- ✓ • Communication between Subject and IdP must use a Protected Channel.
- ✓ • The authentication process shall prove the Subject has possession of the Authentication Secret or Token

IAM Bronze Requirements



- ✓ • Session maintenance methods implemented by the IdP shall resist session hijacking
- ✓ • The IdPO must have policies, practices, or guidelines in place that prohibit Subjects from sharing their Credentials.
- ✓ • Annually faculty, staff and students must complete a mandatory Privacy and Information Security Training Program.
- **Identity Record qualification**
- ✓ • If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record.

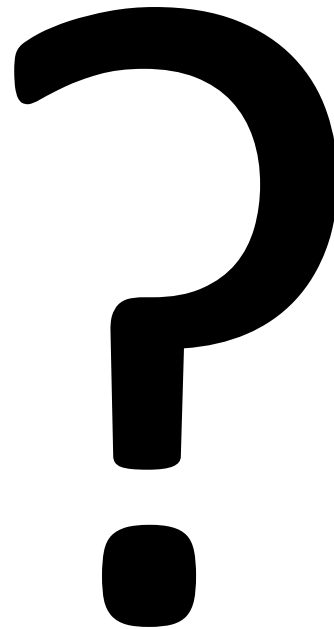


- **Identity Attributes**

- ✓ • The actual meaning of any attribute values identified as attributes used by InCommon Participants should be consistent with InCommon Attribute definitions
- ✓ • An IdPO may be certified by InCommon to be eligible to include one or more InCommon IAQs as part of Assertions. The IdP must not include an InCommon IAQ that it has not been certified by InCommon to assert.
- ✓ • Cryptographic operations are required between an IdP and any SP



Questions?

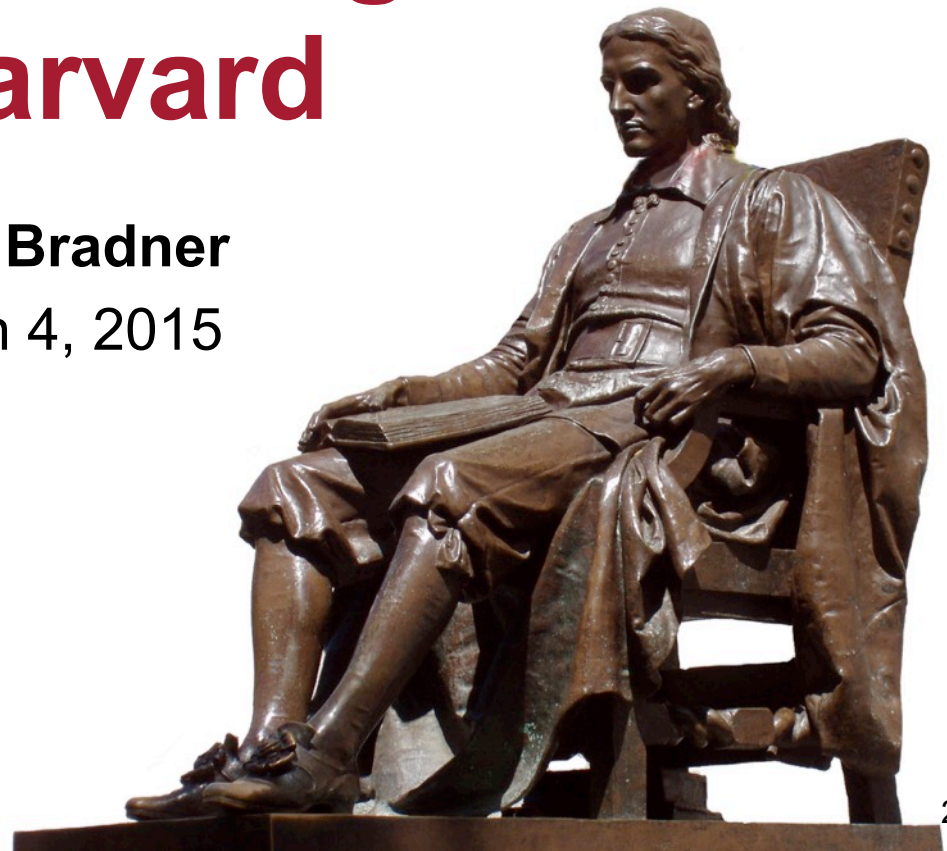




HARVARD UNIVERSITY
Information Technology

The Bronzing of Harvard

Scott Bradner
March 4, 2015



Agenda

- The Existing Environment
- Why InCommon Bronze?
- Coverage Decisions
- The Certification Process
- Dealing with Certification Issues
- Lessons Learned

The Existing Environment: Harvard University

- Harvard has been around for a while (since 1636!)
 - 47 Nobel Prizes
 - 32 heads of state
 - 48 Pulitzer Prizes
- 11 principal academic units
 - Significant IT distribution among academic units
- Scale
 - 2,400 faculty and 10,400 academic appointments
 - officially 6,700 undergraduate and 14,500 graduate students
 - database has 24,011 ☺
 - 58,800 employees (including student employees)
 - 323,000 living alumni

The Existing Environment: Harvard ID Numbers

- Non-sequential 8-digit ID number (HUID) assigned to Harvard staff, faculty, students, and others
 - “Others” include contractors, library borrowers, spouses, tenants, overseers, employees of the Smithsonian Astrophysical Observatory and Harvard Management Company, sponsored accounts ...
- “HUID for life”
 - Effort to ensure that any one person is assigned a maximum of one permanent HUID
- Not in Harvard’s FERPA directory list
 - Thus, must be kept confidential

The Existing Environment: Identity and Access Management

- Harvard started to develop a “single-sign-on” PIN System in late 1998
 - Based on then-existing ID card database ... the only database that included all active persons assigned Harvard ID numbers
 - First augmented with telephone directory info
 - Later augmented with other info, such as roles
 - Evolved into Harvard’s current core person identity registry (IdDB)
- The system now supports more than 600 applications
 - This includes vendor applications through a proxy

The Existing Environment: Microsoft Active Directory

- Large University Active Directory
- Most active HUID holders are in University AD
 - Major use: Office 365 for staff
- Harvard's new password management system will push the same passwords to both the PIN System and AD
- Thus, the status of AD needs to be taken into account when certifying for Bronze (or Silver)

The Existing Environment: IdDB

- IdDB gets regular feeds from many sources, including:
 - Human resources
 - Registrar systems (many)
 - Student Information System
 - Division of Continuing Education
- Now never forgets: 642,129 entries (as of 2/17/15)
- Fields include:
 - HUID number
 - Directory information
 - Role and status information
 - Miscellaneous information, including UUID and EPPN
(learn more: <http://iam.harvard.edu/resources/iam-database-information>)

The Existing Environment: LDAP

- Harvard currently has two LDAP server sets, which are being combined:
 - HU-LDAP (directory information)
 - AuthLDAP (credentials)
- Many IdDB fields are exported into the LDAPs

The Existing Environment: Authentication via PIN System

- Applications redirect users to the PIN System for authentication
 - User prompted for credentials
 - HUID & password
 - Credentials checked against AuthLDAP
 - User redirected back to app with a signed token in the URL
- PIN System supports some “one-way federation”
 - Users can select other servers for credential checking, such as Active Directory or the Harvard Medical School authentication engine

The screenshot shows the Harvard University PIN System login interface. At the top, the Harvard University logo and name are displayed. Below this is a dark red header with the text "PINSYSTEM" and navigation links for FAQ, HELP, PRIVACY, and LOGOUT. The main content area prompts the user to "Select a Login type: What is a login type?". Four radio buttons are listed: "Harvard University ID (HUID)" (selected), "eCommons Login", "FAS/Central Username", and "XID Login". Below this, there are two input fields: "Login ID:" and "PIN / Password:", each with a placeholder text "What is a login ID?" and "What is a PIN / Password?" respectively. A "Login" button is positioned below the PIN/Password field, along with a link "New user? Forgot your PIN / Password?". At the bottom, a footer contains the date "Tue Feb 17 09:48:56 EST 2015", copyright information "Copyright © 1999 - 2015 The President and Fellows of Harvard College", and a disclaimer about the use of the PIN System.

HARVARD UNIVERSITY

PINSYSTEM

FAQ | HELP | PRIVACY | LOGOUT

Select a **Login type**: What is a login type?

☒ Harvard University ID (HUID)

☐ eCommons Login

☐ FAS/Central Username

☐ XID Login

Login ID: What is a login ID?

PIN / Password: What is a PIN / Password?

[New user? Forgot your PIN / Password?](#)

Tue Feb 17 09:48:56 EST 2015
Copyright © 1999 - 2015 The President and Fellows of Harvard College

The Harvard University PIN System, and the systems, data, and other resources that require PIN authentication for access, are only for legitimate Harvard University users. Use may be monitored, and improper use of the PIN System or those resources may result in disciplinary action and civil and criminal charges.

The Existing Environment: Next-Generation Authentication System

- PIN System redone in 2013
 - From homebrew system to CAS-based solution (“PIN/CAS”)
 - Application interface and application configuration database maintained for compatibility
- PIN System will be rebranded in Summer 2015 as HarvardKey
 - Includes new login name based on email address
 - More robust self-service portal for users
 - Adding options for multifactor authentication

HARVARDKEY

The Existing Environment: Harvard IdP

- Harvard's Shibboleth IdP uses PIN/CAS for authentication
 - Gets attributes from LDAPs
 - *ScopedAffiliation* attribute calculated from role and status information
- Learn more: <http://iam.harvard.edu/resources/incommon>

Why InCommon Bronze?

- Theoretically useful by itself (in the future)
- An external set of technical and process standards also provides a good forcing function
 - “Certifying with InCommon verifies to the Harvard Community that University IAM efforts meet nationally recognized external standards”
- Reassures Harvard users that IAM is following good practices
 - Learn more: <http://iam.harvard.edu/news/incommon-bronze>

Coverage Decisions

- Basic decisions:
 - IdDB is for everyone, for all time
 - The Harvard IdP will only vouch to InCommon SPs for users we “know” and who are a current part of the Harvard Community
 - We do not vouch for others outside these criteria, even if they have valid Harvard credentials
- Specifically, we decided to not attempt to validate everyone in IdDB for Bronze

Coverage Decisions: How Do We Know You?

- The Harvard IdP will vouch to InCommon SPs for the following categories:
 - Active paid employees
 - ID proofed by employment process
 - Active Harvard Community members who have picked up ID cards
 - Government-issued photo ID checked during card pick-up process
- This includes faculty, staff, on-campus students and others
 - Does not currently cover distance learners
- Will also add an additional in-person verification mechanism
 - Not currently considering remote proofing

The Certification Process

- Imported Assurance Profile 1.2 into a spreadsheet outlining requirements for both Bronze and Silver
- Went through line-by-line describing current status
- Identified the few gaps in Harvard's systems:
 - Relevant to both Bronze and Silver:
 - Resistance to guessing authentication secret
 - SHA-1
 - Relevant to Silver only:
 - Securing authentication traffic
 - Stored authentication secrets
 - Strong protection of authentication secrets

Certification Issues: Resistance to Guessing

- The PIN/CAS system does not require people to change their passwords on a regular basis
- Harvard's password complexity requirements have recently been strengthened
- When verifying to a Bronze SP, the Harvard IdP will only verify users who have changed their passwords since the new rules went into effect *and* within the last 5 years (within the last year for Silver SPs)
 - If time requirement not met, user receives an error of “your password must be changed”
- Thus, impact only on those who want to use Bronze or Silver SPs

Certification Issues: SHA-1

- Took time to coordinate certainty that all SPs using the Harvard IdP could support SHA-2
- Reconfiguration put into production Jan. 6, 2015

Certification Issues: Stored Authentication Secrets

- Issue for Silver certification
- Credentials stored using hash — no seed
 - Implemented whole-disk encryption for PIN/CAS
 - The next PIN/CAS update will use seeded hash
 - Will implement whole-disk encryption for AD

Certification Issues: Securing Authentication Traffic

- AD-specific issue for Silver certification
- Must configure AD to not use LM or NTLMv1
 - NTLMv2 may also be an issue
- Learn more: <http://tinyurl.com/silver-ad-cookbook>

Certification Issues: A Surprise

- U.S. Federal ICAM Privacy Assurance addendum was a surprise
 - Not in IAP — only in agreement
- Had to publish information on attribute release, etc.
 - See section 9 in <http://iam.harvard.edu/resources/incommon-bronze>
- Will likely support user managed attribute release control (e.g., PrivacyLens) at some point

Lessons Learned

- Bronze certification wasn't difficult ... once we made a few simplifying decisions:
 - Use role and status to decide whom we vouch for
 - Force password changes only on users of Bronze (or Silver) SPs
 - Use employment status and card pick-up status for ID proofing
- Harvard is ready for Silver certification, except for AD
 - And documenting (& paying) for an audit

Thank you!

Questions? Email scott_bradner@harvard.edu



InCommon Assurance Website

<http://www.incommon.org/assurance/>

InCommon Assurance Wiki

<https://spaces.internet2.edu/display/InCAssurance/InCommon+Assurance+Program>

Please join for the next Assurance Call

Wednesday, April 1, 2015 at noon ET

Eric Goodman, University of California Office of the President,
will lead a discussion of password reset issues.