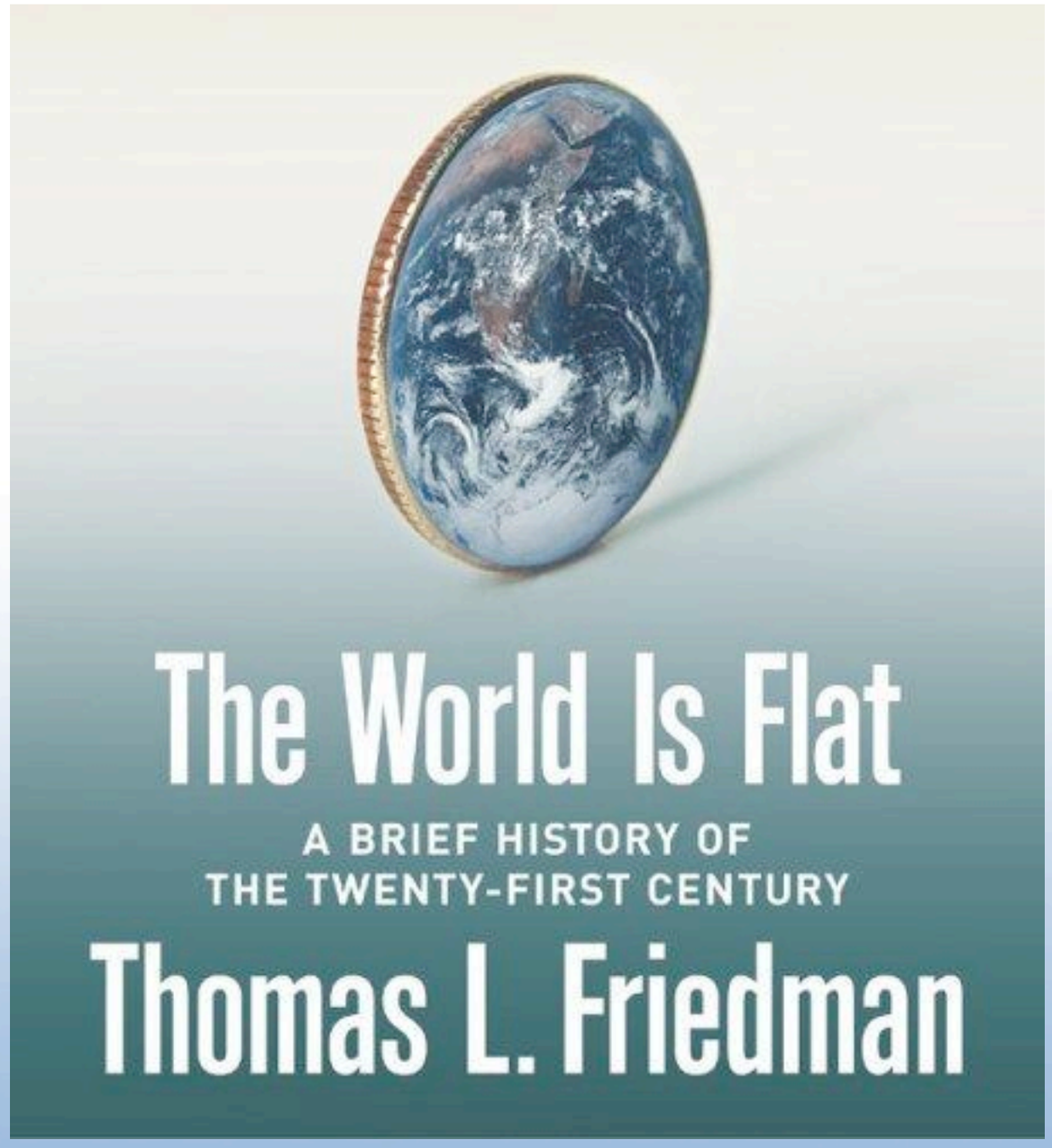
Bronze and Silver Identity Assurance Profiles For Managers

CAMP – In Production: Management
Tues, 22-June-2010, Raleigh, NC
Keith Hazelton, UW-Madison
Renee Shuey, Penn State

Problem Statement



InCommon®

Federated Identity as Flattener?

- Challenge is providing users with vappropriately controlledv access to online resources
- Federation: User has one org that makes assertions about their digital identity, and another org that delivers online resources and services
- The rub: How to establish Service Provider trust in the assertions about the user made by the Identity Provider

InCommon®

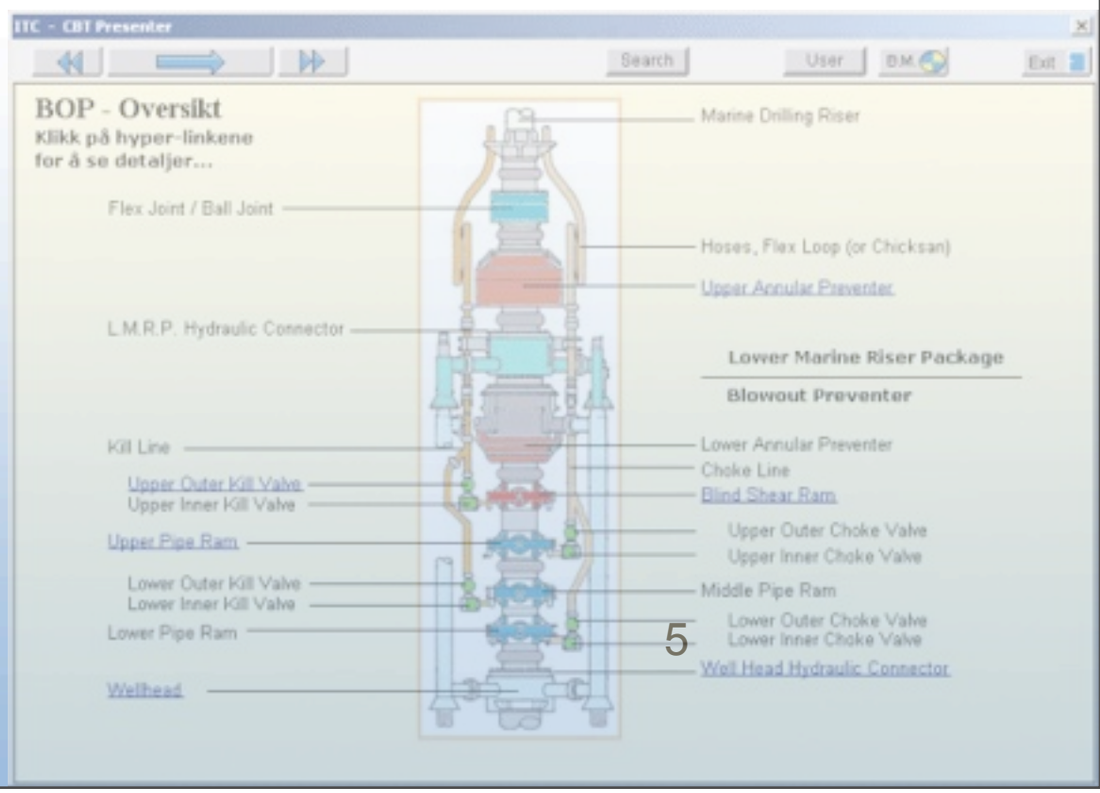
Problem Statement

The Rub: Establish SP trust in IdP

- Why might the SP mistrust?
- The IdP may be lying
- The IdP may not be the "real" IdP
- The IdP may not have done a good-enough job in
  - Establishing the user's true identity
  - Binding the user to their login credential
  - Picking the method by which user logs in
- SP’s acceptable risk goes down as value of service goes up

A shared language for communicating risk factors

- Identity Assurance Profiles (IAP)
- If Identity Provider claims to support a specific documented IAP, the Service Provider has the information they need to determine whether the IdP's assertions about a user fall within the range of acceptable risk for a given service/resource.



InCommon IAPs: Bronze and Silver

- http://www.incommonfederation.org/assurance/
- Bronze: Identity Provider support at least basic userID/ password credentials with reasonably hard to guess passwords
- Silver:
  - credentials with (at least) very hard to guess passwords
  - better credential management
  - reasonably verified personal information about each Subject
  - unique Subject identifiers that are never reassigned
  - and secure business and operational processes

InCommon IAPs: Bronze and Silver

- Crafted to match the US standards in this space
- Key document is NIST SP 800-63, defining four levels of assurance
  - "1," "2," "3," "4"
  - Bronze ≅ 1
  - Silver ≅ 2
- *Some* hope of providing a common assurance regime.

University of Chicago
University of Illinois
Indiana University
University of Iowa
University of Michigan
Michigan State University
University of Minnesota
Northwestern University
Ohio State University
Pennsylvania State University
Purdue University
University of Wisconsin-Madison

About the CIC

C·I·C
COMMITTEE ON INSTITUTIONAL COOPERATION
www.cic.net

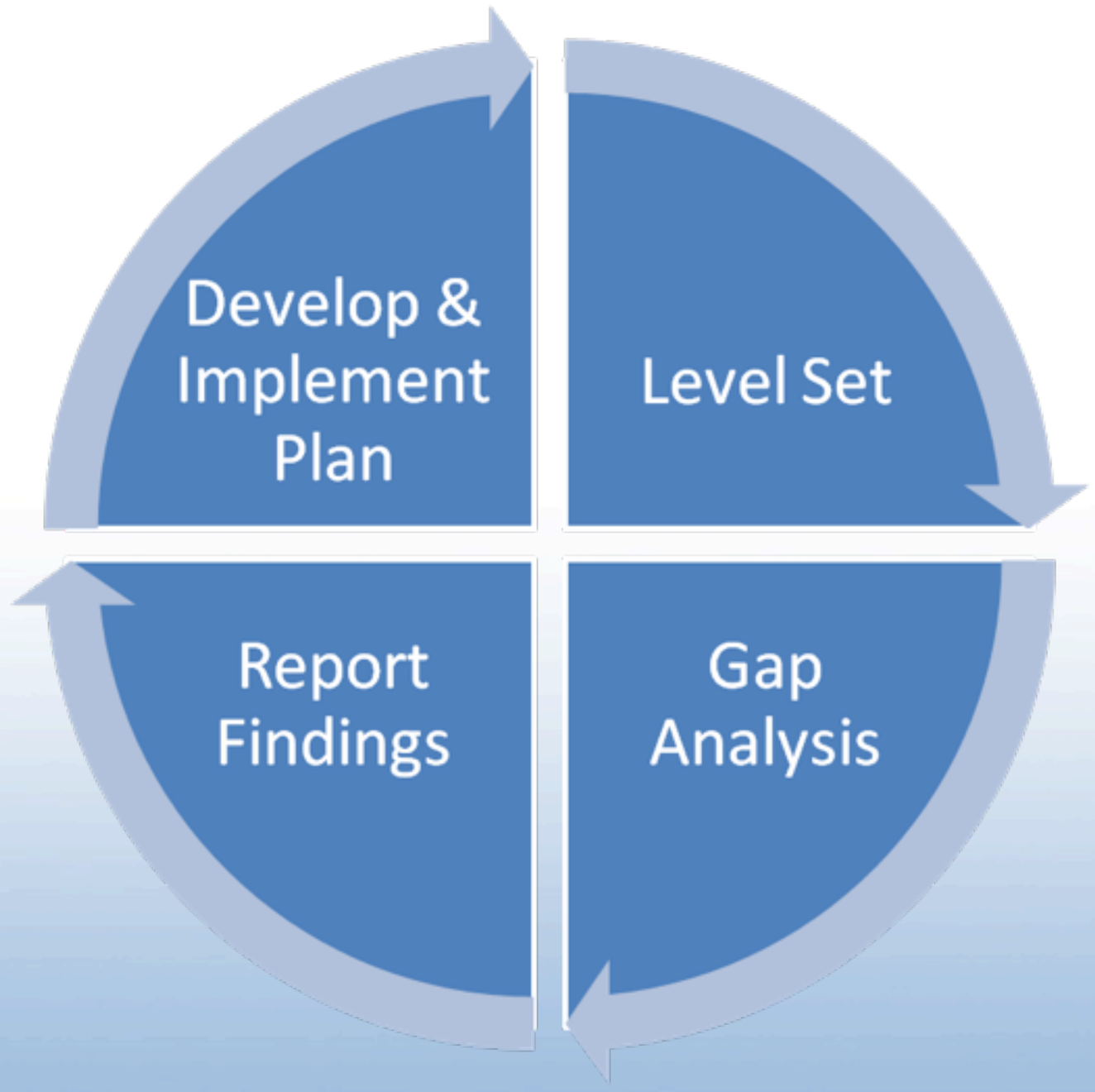
CIC Silver Project
Three Phase Approach

- Phase I - Documentation of policies and procedures and standard operating practices

- Phase II - Strength of authentication and shared secrets

- Phase III - Registering identity subjects and issuing credentials to them

CIC Silver Project Phase



Defining Scope

- One of the first decisions
- Systems included in Silver Certification
- Communities included in Silver Certification

Finding and Engaging Key Stakeholders

- Auditor
- Registrar
- World Campus
- Outreach
- Law School
- Medical School
- Undergrad Admissions
- Grad School
- Security
- Privacy & Risk

Key Stakeholders - Really?

- Access to Protected Library Resources
- Library Staff Access to Integrated Library System
- Access to Library Public Workstations
- HMC Affiliate
- Access to Library Resources
- Access to Alumni Library Resources
- Access to Electronic Theses and Dissertations Web Site
- Graduate School Exit Survey Federating to blogging hosted Services
- Prospective students applying for financial aid
- Employee Confidentiality
- Provisioning of an employee's digital Identity
- Student early access to residence hall requests and immunization
- Continuing Education and Adult Students
- New Students Applying for Admissions and Oncampus Housing
- Prospective Students Visiting Penn State New Kensington
- New Faculty and Access to ANGEL and Other Class Resources
- Adjunct Faculty Activating Access Account
- New Faculty & Staff Selecting Benefits
- Terminated Faculty Member Maintains Access
- Physicians at the Hershey Medical Center and Access to Library Resources
- Patients, Family Members, and Visitors at the Penn State Hershey Medical Center
- Alumni Donors
- Local Community Member and Short Term Access Accounts
- Registrar Relationships
- Student Lifecycle
- New Students Applying for Undergraduate Admissions
- Provision of Access to Course Work For Students at a Distance
- Library Resources
- ITS Computer Store Access
- CIC CourseShare
- Deprovision User content after graduation or resignation
- Google Cache Updates
- Access to user content after graduation and or resignation
- Access to directory data
- Emergency Rehire
- Updating ISIS Security Profile
- Multiple Security Realms, Same Userids but Different Passwords
- ROTC Instructor Affiliation
- Instructor with Independent Contractor Status
- Name change switching in the directory
- Special Affiliates (for example Religious Affiliates)
- Father and son who is a JR
- Cloning ISIS Security Profiles
- New PSUid assigned for new PSU affiliation
- Student Football Tickets
- Department Identity
- DSL Use Case Interview
- Police Services Use Case Interview
- Police Services Use Case

Registration Processes

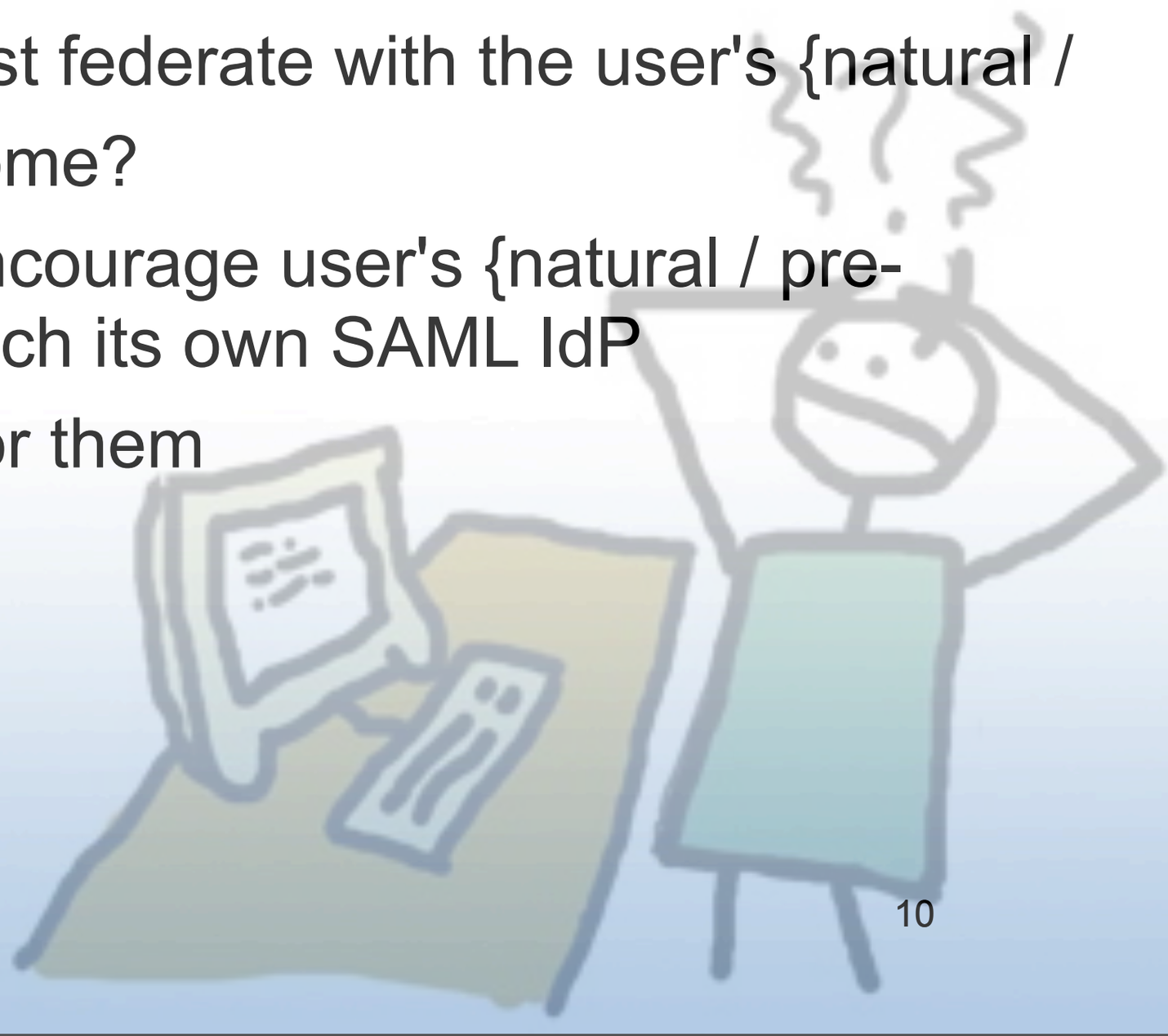
- Undergrad Admissions
- Medical Center
  - HR System
  - Student
- World Campus
- Outreach
- Human Resource
- Grad
- School of Law
- Registrar

Registration Processes: UW

- PhotoID operations on each campus do identity proofing and vetting for our nascent “Wisconsin Federation”
- Employees of Spun-off Hospital: Parking application
- Alumni:
  - From hazelton@wisc.edu
  - To hazelton@alum.wisconsin.edu
- Prospective Students/Applicants/Admitted/Matriculated
- Summer Research Opportunity Programs
- Need to support LOWER levels of assurance, too

Registration Process Conundrums: UW

- For which populations should the U "home" people?
- When should the U just federate with the user's {natural / pre-existing} identity home?
- When should the U encourage user's {natural / pre-existing} home to launch its own SAML IdP
- …or offer to host it for them



Friday, June 18, 2010

Bronze Registration Process

Vetting

Proofing

Issue Credentials

Digital Identity

BRONZE

User completes a PennState web based account profile. User enters: • Full name • Email • Phone	• N/A	• Account activated • PSU ID created	• User receives an access account and password • Digtal Identity complete

Friday, June 18, 2010

Silver Registration Process

Vetting

Proofing

Issue Credentials

Digital Identity

SILVER

User completes a PennState web based account profile. User enters:

- Gov't photo ID #
- Full name
- DOB
- Address
- Email
- PSU ID (If available)

- User visits Registration Authority.
- Registration Authority verifies identification **matches** user and account profile.

ID Match?

YES

- Account activated
- User receives official notice at address of record.

NO

- User receives credentials at their official address.
- User activates account.

- User receives an access account and password
- Digtal Identity complete

External Business Drivers

- National Institutes of Health
  - CAGT
  - PICS - PGRN Information & Communication Site
  - CTSA – Clinical Translational Science Awards
- CIC CourseShare
- TIAA CREF
- National Science Foundation
- ICAM – Refeds
- LIGO Community

External / Internal (?) Business Drivers

- UW Common Systems
- HR
- Learning Management System(s)
- Library
- Portal
- Help Desk

Internal Business Drivers

- Financial Aid
- Extending digital life-cycles to meet today's service requirements
- Globalization
- Distance Education
- Increasing numbers and types of affiliates

4.2.8 Technical Environment
Management Decisions

- 4.2.8.1 Configuration Management
- 4.2.8.2 Network security
- 4.2.8.3 Physical security
- 4.2.8.4 Continuity of Operations

InCommon®

Approaches to Reaching Higher Identity Assurance

InCommon®

Approaches to Reaching Higher Identity Assurance

Penn State IAM Strategic Recommendations

1. Create Central IAM Policy and Governance

- Develop plan for formal Risk Assessment
- Create a Single Central Person Registry
- Add Level of Assurance Component to Credentials
- Promote Single Sign-on, Federated Identity, and control of University digital identity
- Streamline Vetting, Proofing, and Issuance of Digital Credentials
- Streamline and Automate Provisioning/De-provisioning of Services
- Promote Awareness and Education of IAM

Penn State IAM Strategic Recommendations

1. Create Central IAM Policy and Governance

- Develop plan for formal Risk Assessment
- Create a Single Central Person Registry
- Add Level of Assurance Component to Credentials
- Promote Single Sign-on, Federated Identity, and control of University digital identity
- Streamline Vetting, Proofing, and Issuance of Digital Credentials
- Streamline and Automate Provisioning/De-provisioning of Services
- Promote Awareness and Education of IAM

UW-Madison: Amen!!

IAM Governance

Penn State IAM Governance Council

Co Sponsored by:

Rob Pangborn
VP and Dean of
Undergrad Admissions

Kevin Morooney
Vice Provost of
Information Technology

- VP for Student Affairs, Director
- University Police Services
- CIO Hershey Medical Center
- Sr., VP Research & Dean Grad. School
- Assoc.VP of Auxiliary and Business Services
- Assoc.VP for Human Resources

- Vice President of Outreach
- Assoc. Dean of Tech - Dickinson School of Law
- VP of Commonwealth Campuses
- Dean of University Libraries & Scholarly Communications

University of Wisconsin IAM Governance

- http://registrar.wisc.edu/imlg/ Five + years

- UW System:
  - Identity, Authentication and Authorization (IAA) Governance Committee
  - System CIOs
  - Identity and Access Management (IAM) Steering Committee

Resources

- InCommon Federation
  - http://www.incommonfederation.org/assurance/
- Penn State Identity Access Management
  - https://iam.psu.edu/
- Univ. of Wisconsin Identity Access Mgmt. Project
  - https://wiki.doit.wisc.edu/confluence/display/IAMP/IAM+Stakeholders
- Identity, Credential and Access Management
  - http://www.idmanagement.gov/drilldown.cfm?action=icam