Day CAMP: Getting Started with the InCommon Federation

Jacob Farmer, John O'Keefe, Ann West|

October 18, 2011

TOPICS FOR TODAY

- A story
- What is a trust federation?
- Why is this compelling?
- Interested? Here's how to get started…

A STORY

BIANCA SIGNS ON…

SHE GRADUATES…

SHE'S OUT INTO THE WIDE WORLD…

CRADLE TO PROBATE

LET'S PONDER THE STORY…

WHAT IS A TRUST FEDERATION?

THE GOAL

“ The National Strategy for Trusted Identities in Cyberspace describes a vision of the future—an Identity Ecosystem—where individuals, businesses, and other organizations enjoy greater trust and security as they conduct sensitive transactions online. The Identity Ecosystem is a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value. ”

National Strategy for Trust Identities in Cyberspace
http://www.nist.gov/nstic

TERMS

- Trust
  - assured reliance on the character, ability, strength, or truth of someone or something
  - one in which confidence is placed
- Assurance
  - satisfaction as to the certainty or truth of a matter

KEY ROLES

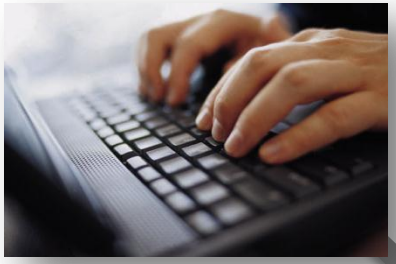
Three roles are involved in gaining access to a resource:

- **Subject** (i.e. user) – The person identified and the subject of assertions (or claims) about his or her identity.

- **Identity Provider** – The organization that maintains the identity system, identity-proofs the subject and issues a credential. Also provides assertions or claims to the service provider about a subject's identity.

- **Service Provider** (sometimes called the relying party) – Owner/provider of the protected resource to which the subject would like to access. Uses the assertions from the identity provider and makes an authorization decision.

FEDERATED AUTHENTICATION



Campus Identity Source

Campus End User

Service Provider

1

3

7

Authn

Enterprise Directory

Federation Schema

Federating Software

2 - Request Authn & Attributes

5 - Authn Verified. Sending Attributes

Federating Software

Services

4 – Authentication

6 - Authorization

InCommon

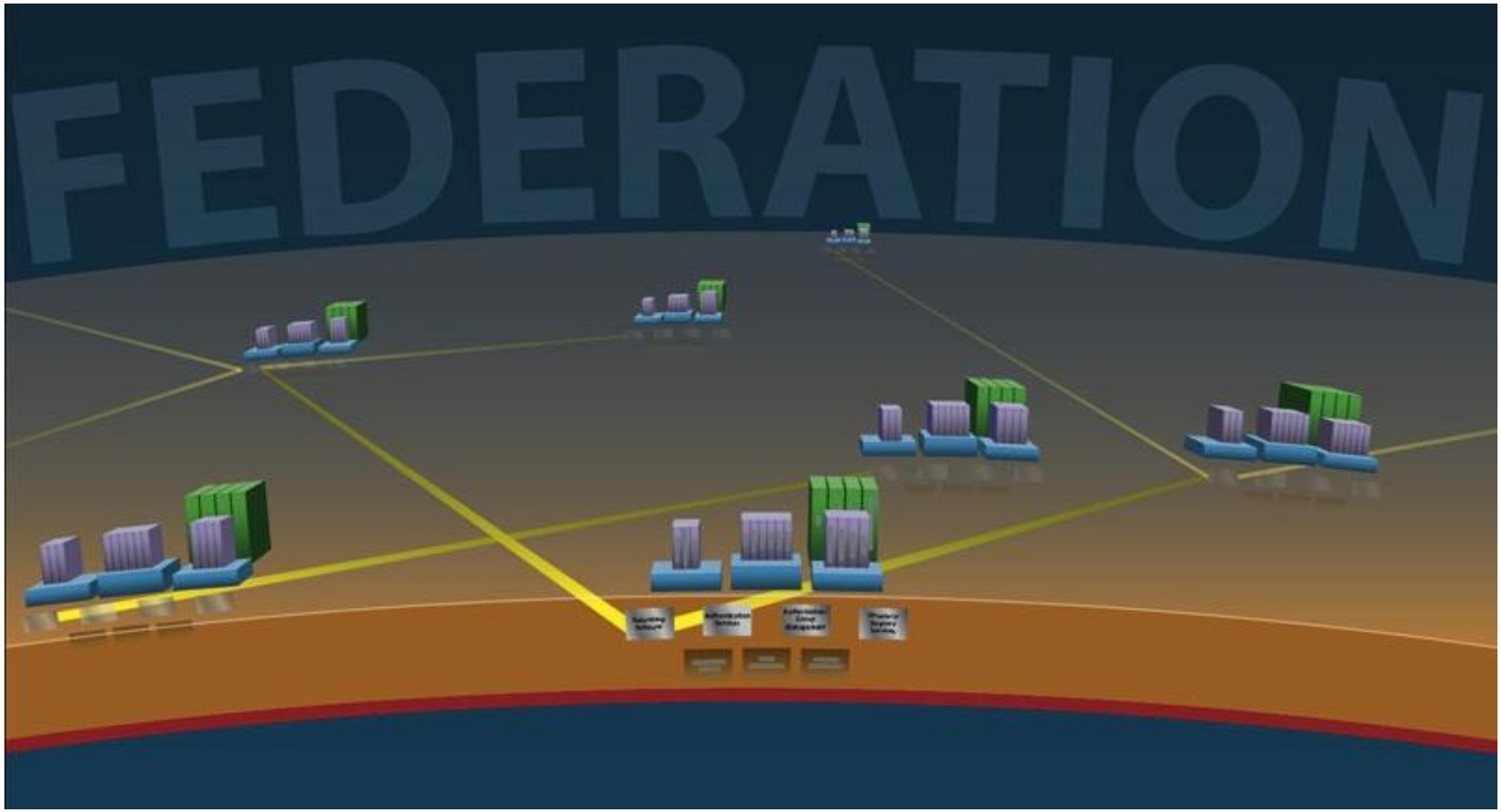
InCommon

COMPONENTS

- Technology (SAML, data schema, authentication context)
- Metadata (endpoints, contact names, attribute information)
- Processes (password management, identity vetting, institutional vetting)
- Policy (attribute usage)
- Legal (Indemnification)

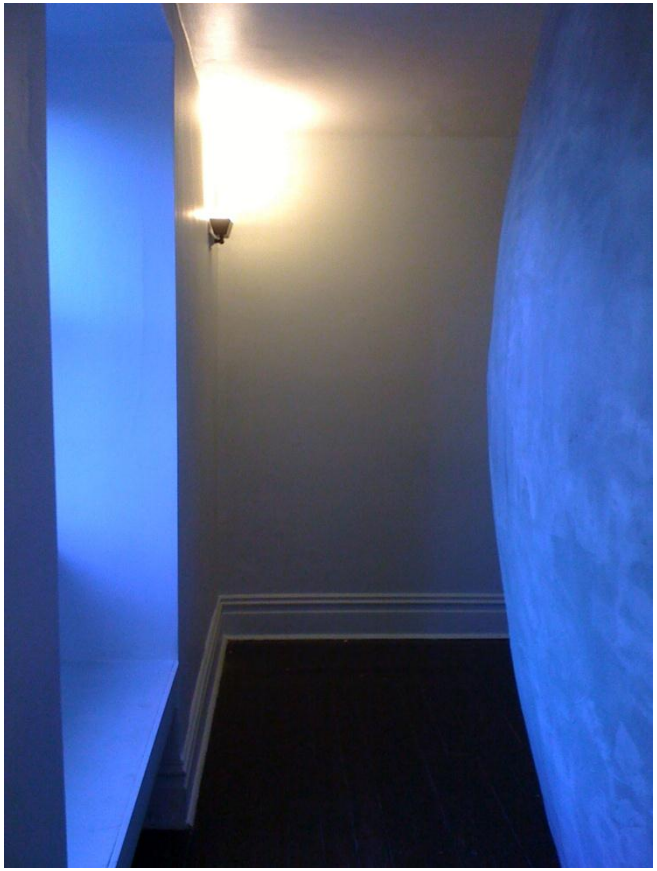
ATM EXAMPLE

NETWORK OF IDENTITY



NATIONAL STATS: INCOMMON

- 235 higher education institutions
- 14 national labs and research agencies
  - National Science Foundation
  - National Institutes of Health
- 87 corporate service partners
- Collaboration Groups
  - Libraries, Student Services, Research, International, Consortia, Assurance



WHY IS THIS COMPELLING?

LOOKING FOR ANY OF THESE?

- Business Functions
  - Benefits
  - Human Resources System
  - Career Services
  - Asset management
  - Talent management
  - Visas & INS compliance
  - Mobile alerts
  - Travel management
  - Energy management
  - Surveys and market analysis
  - Student loan eligibility verification
- Learning and Research
  - Journals (Lots of Content)
  - Databases and analytical tools
  - Multi-media access
  - Homework labs
  - Quiz tools
  - Plagiarism detection
  - Software downloading
  - Alcohol awareness education
  - Student travel discounts
  - Transportation and ride-share services.
  - Course sharing and video streaming
  - NSF/NIH Grant Submission

THE NEW IT

- IT is shifting from developing technical solutions to enabling efficient solutions through a mix of sourced technology services.
- How do we do that?
  - Embrace change
  - Streamline adoption
  - Provide integration
  - Facilitate reuse
- While protecting privacy, reducing institutional risk, ensuring continuity, meeting regulatory compliance and high availability requirements.

….And do it all for less $$$.

THOMSON REUTERS

ELSEVIER


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


CSO


outside
THE CLASSROOM
An EverFi Company


NATIONAL STUDENT CLEARINGHOUSE


qualtrics™


PeopleAdmin


symplicity


OUTSIDE THE CLASSROOM
AlcoholEdu®
for College

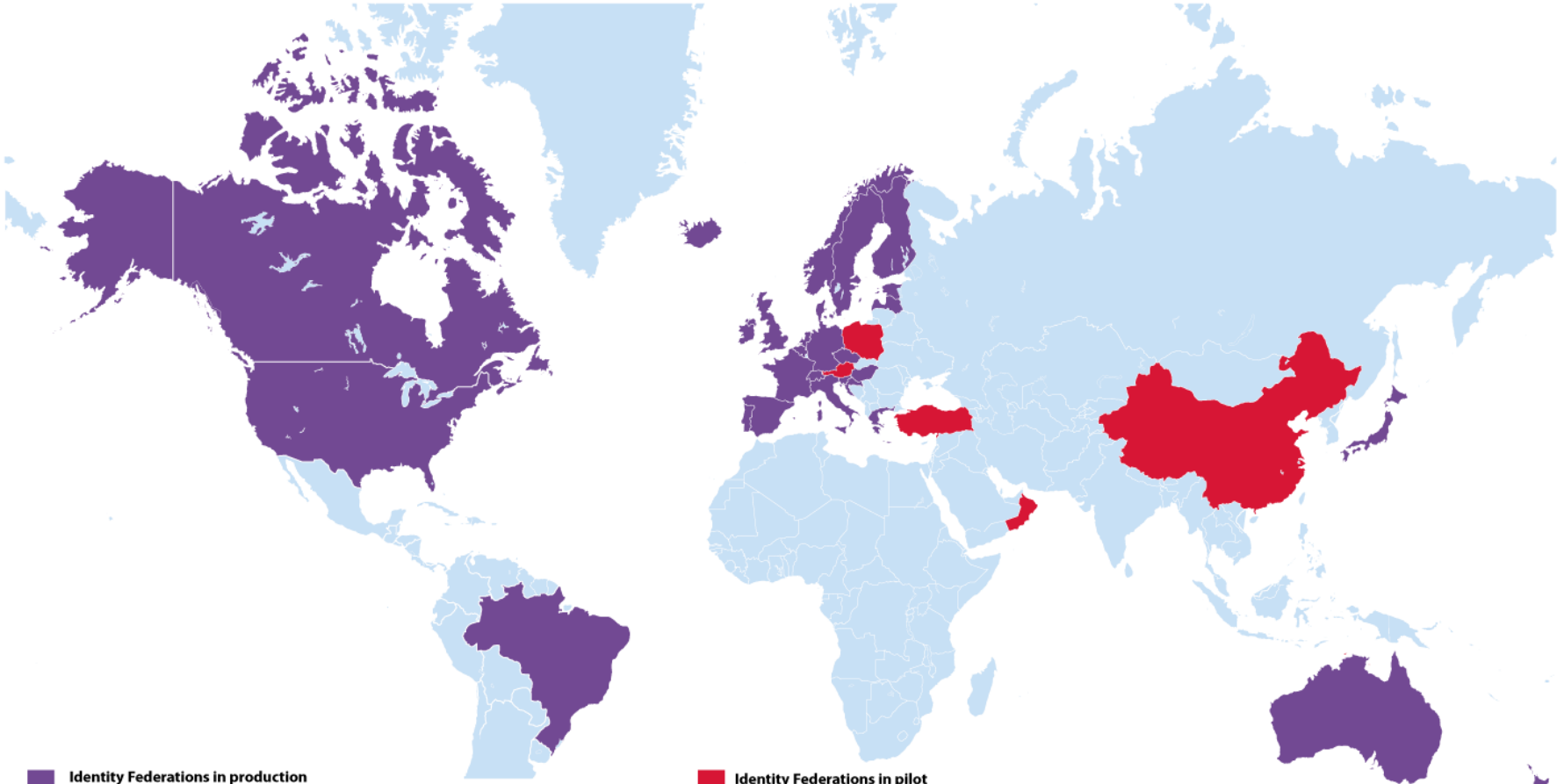

DigitalMeasures

SO WHAT ARE THE BENEFITS?

- A network of identity
- Vertical and horizontal support of the academy
- Federal agency funding research, not IT support
- Richness of privacy support
- Granularity of access controls
- International support

Research and Education Identity Federations

REFEDS



Identity Federations in production

AU	Australian Access Federation AAF
BE	Belnet R&E Federation
BR	CAFe
CA	Canadian Access Federation CAF
CH	SWITCHaai
CZ	eduID.cz
DE	DFN-AAI
DK	WAYF
ES	SIR
FI	Haka
FR	Fédération Éducation-Recherche
GR	GRNET
HR	AAI@EduHr
HU	eduID.hu
IE	Edugate
IT	IDEM
JP	GakuNin
LV	LAIFE
NL	SURFfederatie
NO	FEIDE
NZ	Tuakiri New Zealand Access Federation
PT	RCTSaai
SE	SWAMID
SI	ArnesAAI Slovenska
UK	UK Access Management Federation for Education and Research
US	InCommon
int	IGTF

Identity Federations in pilot

AT	ACOnet-AAI Federation
CN	CARSI
OM	OMAN_KID
PL	Poland Identity Federation
TR	ULAKAAI

UPDATE 14 April 2011

SERVICE PROVIDER PERSPECTIVE

I get that federations provide a way for inter-organizational online transactions to happen at scale, but my SP provides access to sensitive data or export-controlled computing power.

How can I manage my risk when users are vetted and authenticated by campuses?

National Student Clearinghouse	student transcripts
TeraGrid/OSG/CILogon	ssh access to HPC, sensitive data
NSF & NIH Virtual Orgs	sensitive data and equipment
Funding Agency	grant and report submission
ADP	employee payroll information
TIAA-CREF	employee retirement accounts
DoE Labs	classified programs

IDENTITY ASSURANCE

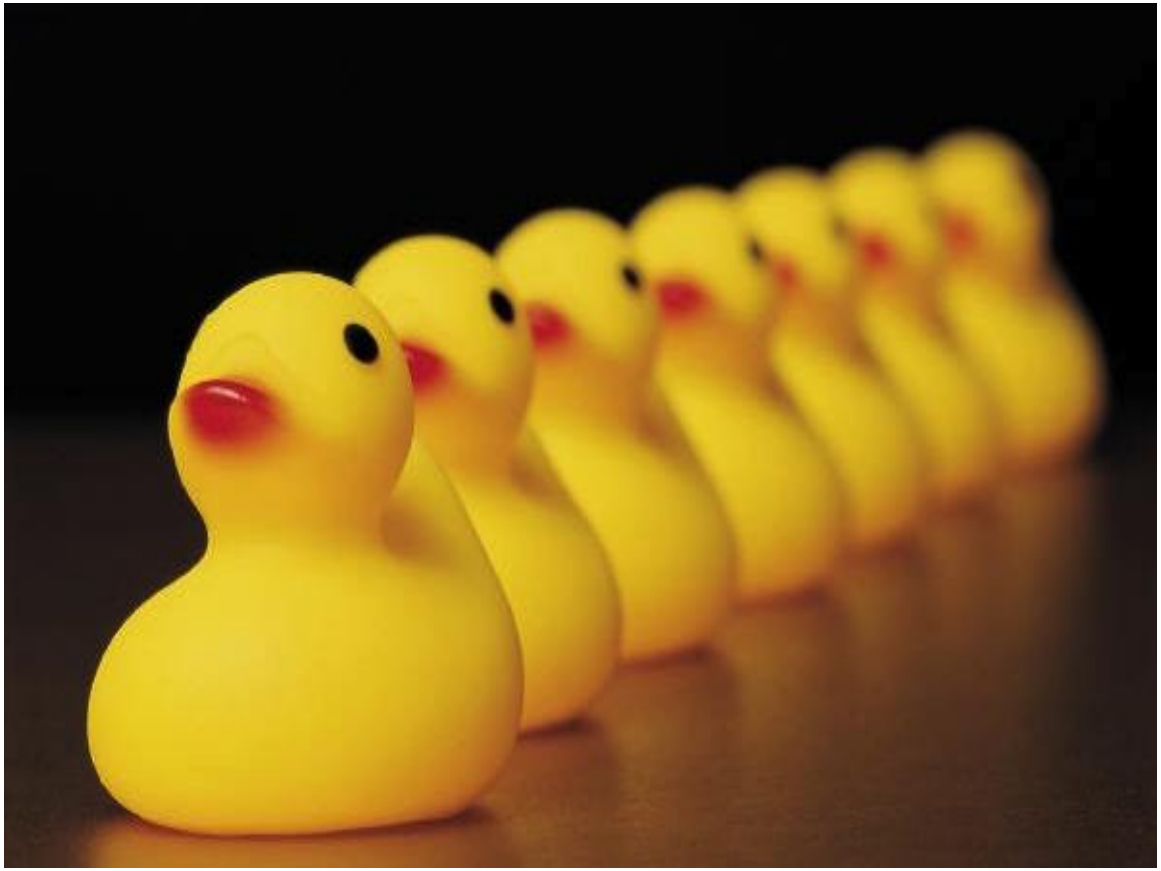
- Helping the community deal with complex federated identity risk issues is one part of simplifying and promoting federation (along with protocols, attributes, metadata, etc)
- Starting point is risks to applications/services
  - applications seek to manage risks cost-effectively
  - identity risks are only one class of risks ...
- What is "identity"?
  - from app point of view, it is anything about a requesting party on which access decisions can be made
  - maybe just a userid, maybe lots of other info: name, group, role, authentication method, usage history, location, etc

ONE SIZE DOESN'T FIT ALL

- 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

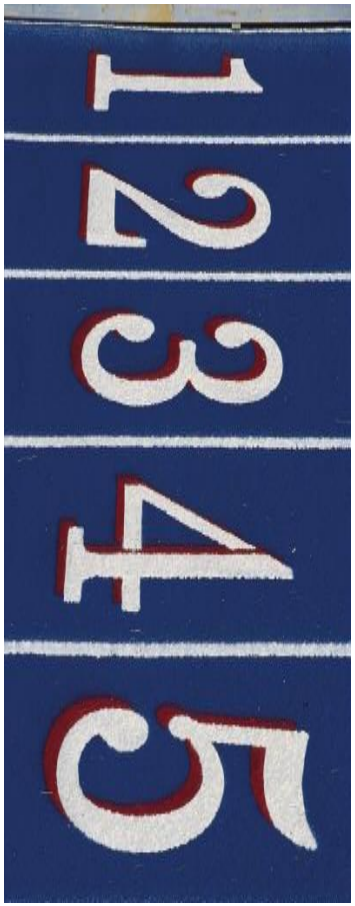
ASSURANCE "LEVELS"

- US government proposed 4 levels of risk (low, medium, high, very high), hence 4 levels of IdM practice
  - roughly: Internet; regular business; two-factor; military
- InCommon adapts these materials for HE environment
  - Assurance Framework and Assurance Profiles (Bronze and Silver)



INTERESTED?
LET’S GET STARTED

GET STARTED TODAY



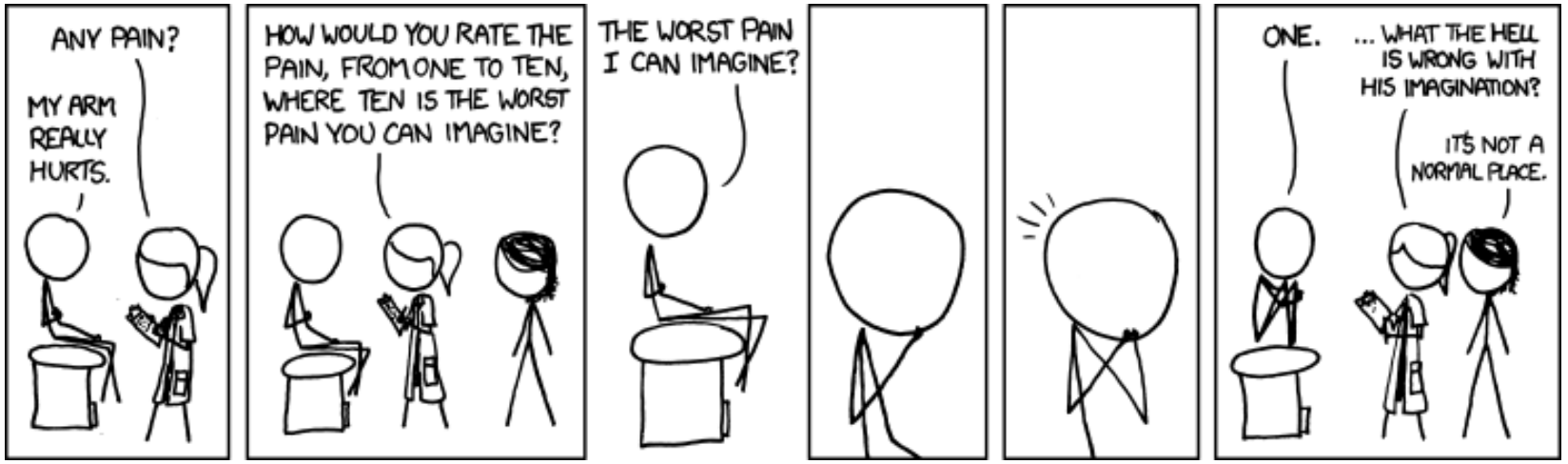
- Review and Prepare Campus Identity Management
- Review, Create, Establish Relevant Business Processes
- Install/Configure SAML2 software
- Support the eduPerson schema
- Join InCommon

REVIEW, CREATE, ESTABLISH RELEVANT BUSINESS PROCEESES

REQUIREMENTS

- What items of documentation are collected from a new user prior to granting access?
- How is the identity of the new user verified (e.g., independent validation of data supplied, personal knowledge, etc.)?
- If passwords are used in your authentication procedures, describe how they are selected, assigned and delivered to new users.
- What information do returning users enter to gain access?

ANY PAIN?


ANY PAIN?
MY ARM REALLY HURTS.
HOW WOULD YOU RATE THE PAIN, FROM ONE TO TEN, WHERE TEN IS THE WORST PAIN YOU CAN IMAGINE?
THE WORST PAIN I CAN IMAGINE?
ONE.
... WHAT THE HELL IS WRONG WITH HIS IMAGINATION?
IT'S NOT A NORMAL PLACE.

BEST PRACTICES FOR FIDM

- Account provisioning
- Account de-provisioning
- Security of credentials
- Accuracy of information
- Governance over attribute release
- Problem resolution
- Educating stakeholders
- RFP language requiring federation

ACCOUNT PROVISIONING

- How do you determine who gets NetIDs?
- How do you validate new users?

ACCOUNT DE-PROVISIONING

- How do you remove accounts once users leave?
- How long do you keep identities?

SECURITY OF CREDENTIALS

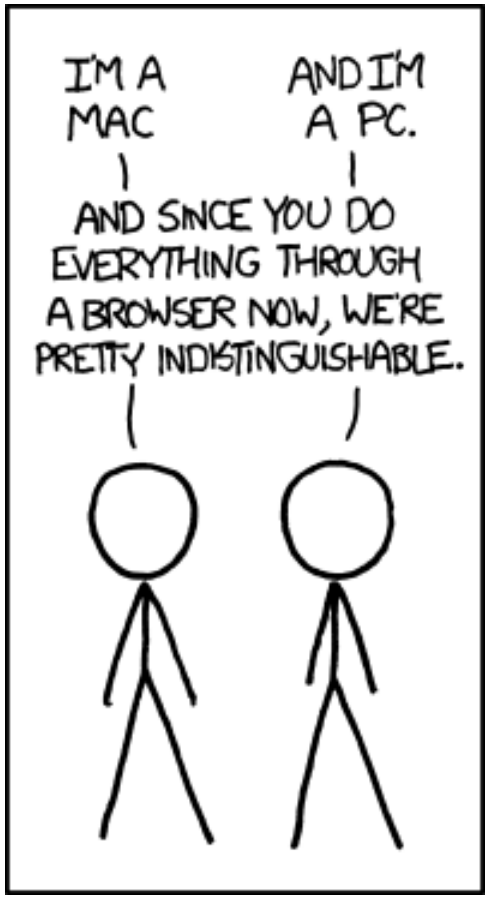
- How do you keep identities secure in the directory?
- How do you keep identities secure in transmission?

ACCURACY OF INFORMATION

- What processes do you have to maintain audit trails?
- How reliable is the attribute information?
- How do you update the person registry?
- Who can update the person registry?

ATTRIBUTE RELEASE

- Who gets to say what attributes can be released and when?
- How can the process be streamlined?
- Can you agree to a default set of attributes to release?



PROBLEM RESOLUTION

- How do you train and empower the helpdesk to manage forgotten password issues?
- What will be the process to board new service providers?

EDUCATING STAKEHOLDERS

- How can you best communicate and collaborate with stakeholders?
- What is the best way to get executive level buy-in?
- How do I make business case for this?

RFP LANGUAGE

- How can I craft RFPs with language that embraces federation?
- How can I convince other services that I want to do business with to federate?

REVIEW AND PREPARE CAMPUS IDENTITY MANAGEMENT

What is a POP?

Participant Operating Practices

More Simply: How do you do IdM?

Why do I care about your IdM system?

Federation == Trust

Two parts: one for IdPs and one for SPs

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

2.2 “Member of Community” is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is “current student, faculty, or staff.”

What subset of persons registered in your identity management system would you identify as a “Member of Community” in Shibboleth identity assertions to other InCommon Participants?

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

2.7 Are your primary electronic identifiers for people, such as “net ID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

2.9 What information in this database is considered “public information” and would be provided to any interested party?

2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

INSTALL SAML2 SOFTWARE

BREAKOUT DISCUSSION

JOIN INCOMMON

CASE STUDIES

LAFAYETTE COLLEGE CASE STUDY

2011 EDUCAUSE: ANNUAL CONFERENCE
THE BEST THINKING IN HIGHER ED IT

EDUCAUSE

ABOUT LAFAYETTE

- Private Liberal Arts & Engineering
- 2360 Students
- 213 Faculty
- 500 Staff
- Central IT (30 Staff)
- Endowment driven

WHAT KEEPS US UP AT NIGHT?

- Access to increasing amounts of digital information
- Enabling ad-hoc, social media-like communication/collaboration
- Changes to federal regulations
- Boarding process for non-traditional accounts
- Growing number of cloud services
- Security and privacy of digital identities

HOW FIDM HELPS US SLEEP

- Used InCommon's guidelines as a cookbook
- Effective attribute collection and maintenance has enabled other projects
- Secure and automated credentialing
- Good attributes allow for robust access to services

THE BEGINNING

- Net@EDU 2003
- Many Systems, Many Logins (2005: 11 different username/password combinations)
- No account creation or termination procedures were codified

MOVING TOWARDS FIDM

- Implemented eduPerson schema extensions (for Moodle, iTunesU)
- Added other schema extensions (L-Number)
- Developed account creation/termination procedures
- Used Shibb/InCommon as a guide
- Implement Shibboleth March 2007
- Joined InCommon June 2007

LYNDA.COM

- Online training need
- Lynda.com in beta test with only 5 accounts
- Implemented May 2011
- 335 users by September

LAFAYETTE UNIVERSITY TICKETS

- Student life used this vendor
- Wanted to validate users for ticket purchase
- University Tickets joined InCommon
- Sending basic attributes
- Expanded to Athletics

universitytickets

LAFAYETTE E2CAMPUS

- Spam-like emails sent to campus prompted project
- Worked with Public Safety
- Go-Live October 2009

LIBRARY APPLICATIONS

- Jstor
  - Looking to move away from proxy service
  - IT/Library collaboration in merged organization
  - our first production use of Shibboleth

- RefWorks
  - Cumbersome login process
  - Users complained
  - Hatai Trust

OTHER FEDERATED PARTNERS

- Internet 2 Wiki
- University of Washington Wiki
- Moodle Spaces
- Google Apps for Education?

PROJECTS ON THE HORIZON

- Examine Silver LoA and explore what needs to be done
- Encourage others to implement Shibboleth
- More hooks and info into identity vault
- Implement Grouper for group management
  - Extending credential to alumni and prospects
  - Collaborations with other institutions (LVAIC)

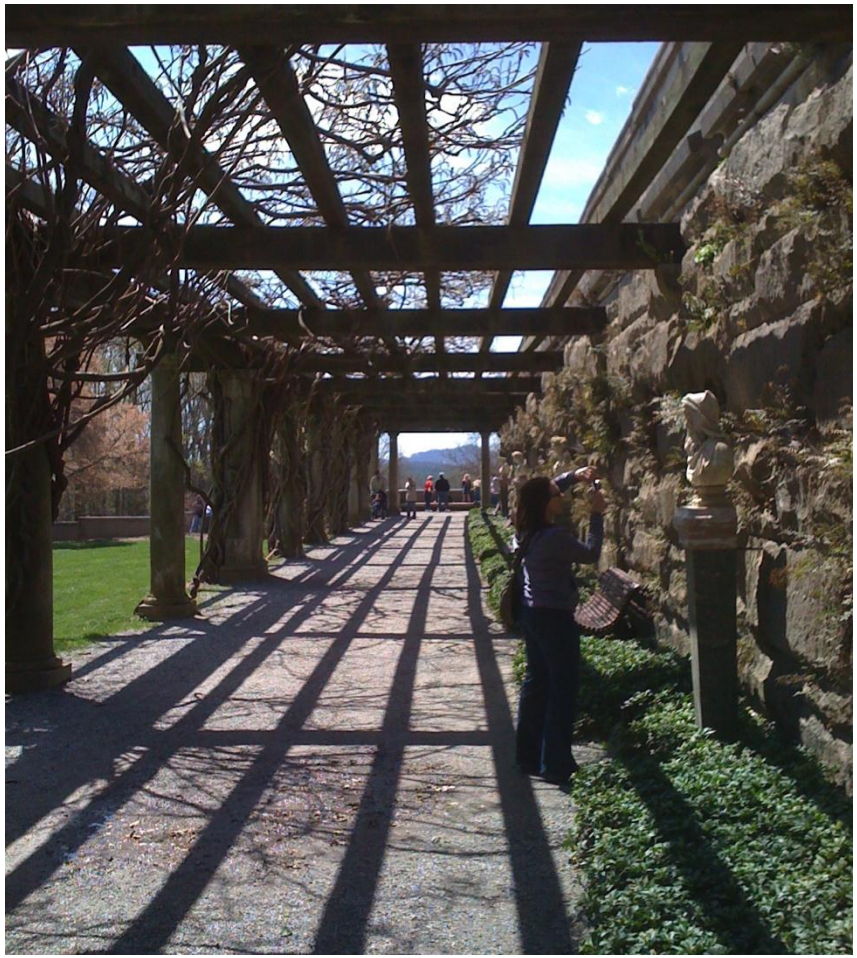
JOINING: THE ROAD IS PRETTY EASY

Degree-Granting Institutions & Research Labs

- Agreement
- Pay fee

Corporate Partners

- Sponsor letter
- Evidence of annual revenue
- Agreement
- Pay fee

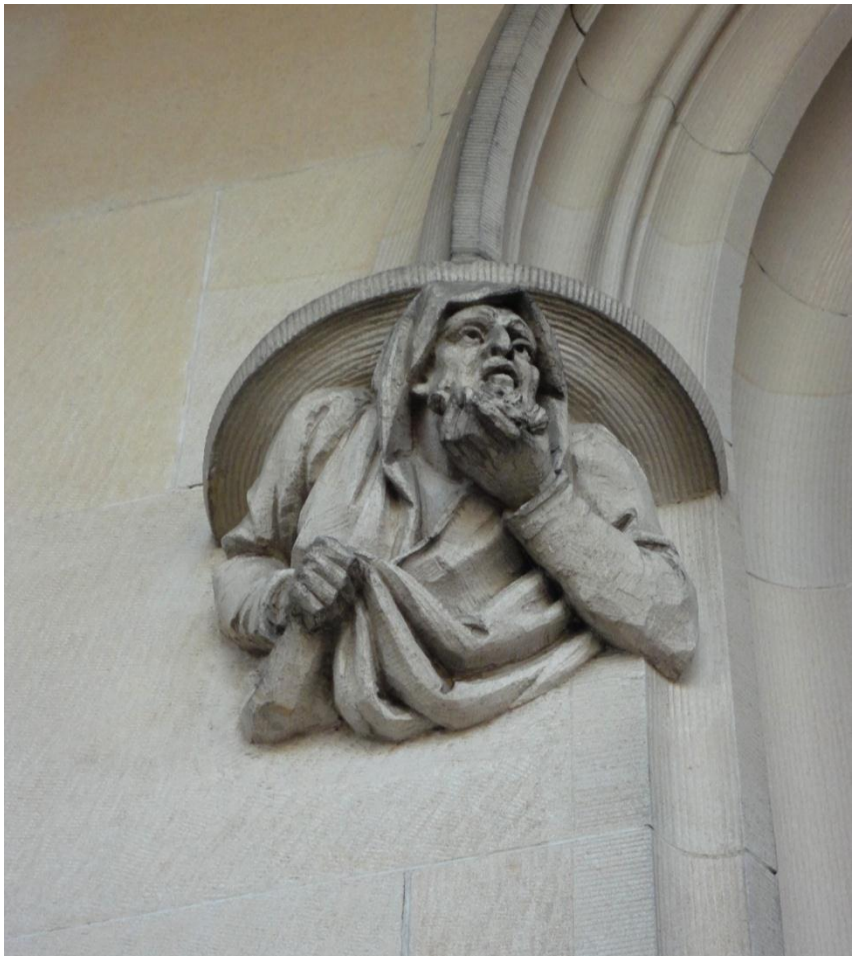


JOINING: INCOMMON AFFILIATES

- Want help?
- Affiliates provide:
  - Cloud IdP services
  - Integration help for service providers
  - Identity provider appliances
  - Shibboleth consulting
  - Federation software

FINAL QUESTIONS?

- Jacob Farmer
  - jpfarmer@indiana.edu
- John O’Keefe
  - okeefej@lafayette.edu
- Ann West
  - awest@internet2.edu



THANK YOU


2011
EDUCAUSE:
ANNUAL CONFERENCE
THE BEST THINKING IN HIGHER ED IT
EDUCAUSE