Federated Identity:
What is Federation?
How does it work?
Why is it secure?

Ardoth Hassler
Senior IT Advisor
National Science Foundation
April 16, 2009
Agenda for Today

• Establish a common vocabulary
• What are the business needs?
• What is InCommon?
• What is “Federation”?
• How does it work?
  – Why is it more secure?
• What does it mean for the research community and NSF?

If we have time…

• What’s happening with the research community and Federal eAuth?
Some terminology…
What is identity management?

- **Organization**: The policies, processes, and tools used to “assure” that IT systems and applications are made available only to appropriate persons.

- **Individual**: The persons I am working with and the systems I am using really are who/what they say they are. And no one can impersonate me, or read or change my information.

- **Identity Management**: Has greatly increased in importance as IT systems and applications are used to perform more and more of the work of society and commerce.

- **Today**: NSF requires an NSF ID and password to access FastLane and Research.gov.

-G. Strawn
What is federated identity?

• “Federated identity management allows users to log in using their local authentication credentials (username and password assigned by their institution) to access electronic resources hosted at other institutions belonging to the same identity federation.” ([www.incommonfederation.org](http://www.incommonfederation.org))

• Designed to address:
  – multiple passwords required for multiple applications
  – scaling the account management of multiple applications
  – security issues associated with accessing third-party services
  – privacy
  – interoperability within and across organizational boundaries
“Identity Providers”

• End user organizations act as ‘identity providers’ (IdPs) and optionally ‘service providers’ (SPs defined on next slide)

• Identity providers (IdPs) supply user information
  – Universities
  – NSF should be the IdP for its employees

• Benefits
  – Enhances security
    • IdP controls what information is shared
    • Users need to remember only one username and password
  – Users and organizations are responsible for their own information
  – Ease of use
“Service Providers”

- Service Providers (SPs) “consume the IdP’s information and get access to secure content in order to provide the appropriate access to services

- Benefits
  - No need to maintain your own user database
    - Authentication is performed by the IdP
    - Can authorize per institution, role, and/or entitlement
  - Reduced user support requirements
  - Reduced compliance burden
    - Less storage/processing of personal data
  - Accurate implementation of license conditions
  - Users take better care of credentials
  - Organizations take better care of assertions
Authentication vs. Authorization

• Authentication: the process of verifying that you are who you say you are
• Authorization: the process of verifying that an authenticated person has the authority to perform a certain operation
• Authentication must precede authorization
Levels of Assurance

• Electronic Risk and Requirements Assessment (e-RA) Tool (http://www.cio.gov/eauthentication/drilldown_ea.cfm?action=ea_ea)
Short Summary of the Asserted Identity’s Validity

Level of Assurance

• Level 1: Little or no confidence
• Level 2: Some confidence
• Level 3: High confidence
• Level 4: Very high confidence
It’s About Trust…
What are the business needs?
The Changing Environment

• Many more services require authentication
  – At work
    • Travel
    • Emergency Alerts
    • HR-related
    • Training
    • Benefits
    • Professional organizations
  – At home
    • Shopping (Lands End, Amazon, eBay, airlines…)
    • Google Email/Apps, Yahoo, AOL…
    • Social networking: Facebook, LinkedIn, Twitter, MySpace…
    • Financial management: Banking, credit cards, investment, bill paying
The Changing Environment (more)

- Many more services require authentication
  - At school/university
    - Scholarship is done via the net
    - Access needed within the institution
      - Library, food services, HR, registration…
    - Access needed outside the institution…
      - Collaboration is worldwide
      - State agencies
      - Federal agencies
The Challenge....

• More and more services
• More and more “trusted” partners
• Dependent on assertion of “eligibility”
  – Various criteria and representations
  – Who can assert “student-ness” ? “research-ness”? 
• More Personal Identifying Information (PII) --> less personal privacy AND a higher level of service
  – Varying levels of assurance required
• Anonymity sometimes required
• Broader constituencies to worry about
What problems are we trying to solve?

• Reduce the need for multiple usernames and passwords
• Reduce amount of personal data held by third parties
• Reduce the duplication of effort across multiple institutions
• Enable publishers, service and network providers to have a common interface for multiple systems
• Ease the difficulty in sharing resources between institutions and organizations
• Make revocation of access/services easier
Challenging Way

Home

Circle University
joe@circle.edu
Dr. Joe Oval
Psych Prof.
SSN 456.78.910

Service Providers

Research.gov
ID #2 Joyal
Dr. Joe Oval
Psych Prof.
NSPID 200123456
Password #2

Grading Service
ID #3 J0456
Dr. Joe Oval
Psych Prof.
Password #3

Music Service
ID #4 J0.123
Joe Oval
Psych Prof.
DOB: 4/4/1955
Password #4

No coordination
Proprietary code
Batch uploads

Slide courtesy of InCommon
Federated Way

1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user controls privacy

Slide courtesy of InCommon
Why does the community want this?

• It’s easier
  – Researchers
    • One username and password to remember (single sign on) for multiple campus applications, access to NIH and NSF and …
    • Ability to use same credentials with other agencies
      – NIH is already accepting InCommon credentials for several external application
    • More control over their own information
  – SPOs
    • After initial authorization, won’t have to retrieve NSF IDs for researchers

• Enhances security
  – Eliminates a lot of “middle people”

• Often-requested new feature for Research.gov
What is the value to the “institution”?

• One solution for intra- and inter-domain single-sign on
• Ability to manage access control by groups or for roles
• Allows personalization of services without releasing identity
• Once implemented, extensions to other applications are much easier
  – Just manage attributes that are released to new targets
What value is there to the user?

- Web single-sign on across a worldwide set of sites
- Fewer passwords
- Tools to manage privacy
- A ‘trusted party’ is asserting values and eligibility
- NOT tied to IP address or browser

-Courtesy of Steve Carmody, Brown University
Why is this important to NSF?

• Provides easier authenticated access to services the research and education community wants and needs to reach
  – Perfect fit for access to Research.gov and FastLane
• Keeps NSF in a leadership role for use of “Federated Identity”
• Enhanced security
  – More work done electronically “behind the scenes”
  – No local IDs and passwords
  – Users won’t need to write down multiple passwords
• Reduces NSF’s need to manage accounts
  – Institutions and individuals at those member institutions become responsible for the integrity of their own information
• Unified authentication methods build on standards
  – Much more scalable
  – Easier to bring new “customers” online
What is InCommon?
and
What does “Federation” mean?
InCommon

“InCommon eliminates the need for researchers, students, and educators to maintain multiple, passwords and usernames. Identity providers manage the levels of their users' privacy and information exchange. InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants.”

• InCommon Federation (www.incommonfederation.org)
  – Mission: create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the US

• US Research and Education Federation
  – Separate entity with its own governance
  – Operations managed by Internet2
  – Members are degree granting accredited organizations and their partners
What is “Federation”? 

• A group of member organizations who agree to a set of rules 
• An independent body, managing the trust relationships between members 
• Publishers, agencies and resource providers act as ‘service providers’ (SPs) 
• InCommon is a Federation
Role of Federation

1. Agreed upon attribute vocabulary & definitions: member of, role, unique identifier...

2. Criteria for identity management practices (user accounts, credentialing, etc.), privacy stewardship, interop standards, technologies

3. Trusted exchange of participant information

4. Trusted “notary” for all universities and partners

Slide courtesy of InCommon
What services does the Federation provide?

- **Rules that binds members:**
  - Make accurate statements to other members
  - Keep federation systems and data secure
  - Use personal data correctly
  - Resolve problems within the Federation
    - Not by legal action

- **Guidance, examples, support**
  - How to comply with the Rules
  - How to work with other members
    - Common definitions, etc.
What services does the Federation provide?

• Operational management
  – Registration mechanism for SPs and IdPs
  – Adding new members to the federation & updating existing members’ metadata
  – Fault finding and trouble shooting
  – Compatibility testing of server certificates and CA Qualification
  – Technical and operational documentation
  – Ongoing federation development
  – Reporting
What does the Federation do?

• Uses shared technology
• Provides “common data” or “attributes” to exchange
• Enables scaling beyond the technology
  – Rules of engagement
  – Information about how to connect
• Performs vetting of organizations and representatives
• Maintains member information
# Levels of Assurance

<table>
<thead>
<tr>
<th>M04-04/ NIST 800-63</th>
<th>Requirement</th>
<th>Application Risk</th>
<th>InCommon</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1:</strong> Little or no confidence</td>
<td>User ID and Password SAML</td>
<td>Low</td>
<td>Bronze</td>
</tr>
<tr>
<td><strong>Level 2:</strong> Some confidence</td>
<td>User ID and Password SAML</td>
<td>Moderate (money)</td>
<td>Silver</td>
</tr>
<tr>
<td><strong>Level 3:</strong> High Confidence</td>
<td>Tokens and certificates PKI</td>
<td>High</td>
<td>Gold</td>
</tr>
<tr>
<td><strong>Level 4:</strong> Very high confidence</td>
<td>Tokens and certificates PKI</td>
<td>Highest</td>
<td>[Platinum?]</td>
</tr>
</tbody>
</table>
Federation Metadata

1. College A
   - IdP: name, key, url, contacts, etc.
   - SP1: name, key, url, contacts, etc.
   - SP2: name, key, url, contacts, etc.

2. University B
   - IdP: name, key, url, contacts, etc.
   - SP1: name, key, url, contacts, etc.

3. University C
   - IdP: name, key, url, contacts, etc.
   - SP1: name, key, url, contacts, etc.

4. Partner 1
   - SP1: name, key, url, contacts, etc.

5. Partner 2
   - SP1: name, key, url, contacts, etc.
   - SP2: name, key, url, contacts, etc.

6. Partner 3

---

Slide courtesy of InCommon
US InCommon Membership and Federation Highlights

• Current InCommon Members
  – 96 Colleges and Universities
    • More every week
    • Growth almost exponential
  – 66 Government and Nonprofit Labs, Research Centers, and Agencies
  – 33 Corporations
  – More pending

• Other Federations
  – State university systems
  – Community college libraries
  – Medical associations
  – DoJ and DoD

• All do SAML; most are Shib

-Source: K. Klingenstein, Internet2/InCommon
## 96 Colleges and Universities

<table>
<thead>
<tr>
<th>Arizona State University</th>
<th>Northwestern University</th>
<th>University of Colorado at Boulder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brown University</td>
<td>Ohio State University</td>
<td>University of Dayton</td>
</tr>
<tr>
<td>California Polytechnic State U - San Luis Obispo</td>
<td>Ohio University</td>
<td>University of Florida</td>
</tr>
<tr>
<td>California State University, Office of the Chancellor</td>
<td>Old Dominion University</td>
<td>University of Houston-Downtown</td>
</tr>
<tr>
<td>Carleton College</td>
<td>Penn State</td>
<td>University of Illinois at Urbana-Champaign</td>
</tr>
<tr>
<td>Case Western Reserve University</td>
<td>Purdue University</td>
<td>University of Iowa</td>
</tr>
<tr>
<td>Clemson University</td>
<td>Ramapo College of New Jersey</td>
<td>University of Mary Washington</td>
</tr>
<tr>
<td>College of William and Mary</td>
<td>Rutgers, The State University of New Jersey</td>
<td>University of Maryland</td>
</tr>
<tr>
<td>Colorado State University</td>
<td>Seattle Central Community College</td>
<td>University of Maryland Baltimore County</td>
</tr>
<tr>
<td>Columbia University</td>
<td>Stanford University</td>
<td>University of Maryland, Baltimore</td>
</tr>
<tr>
<td>Cornell University</td>
<td>Stark State College of Technology</td>
<td>University of Massachusetts Amherst</td>
</tr>
<tr>
<td>Dartmouth</td>
<td>Stevens Institute of Technology</td>
<td>University of Minnesota</td>
</tr>
<tr>
<td>Duke University</td>
<td>Stony Brook University</td>
<td>University of Missouri System</td>
</tr>
<tr>
<td>Emory University</td>
<td>Sweet Briar College</td>
<td>University of Nebraska - Lincoln</td>
</tr>
<tr>
<td>Florida State University</td>
<td>Texas A &amp; M University</td>
<td>University of Nevada, Reno</td>
</tr>
<tr>
<td>George Mason University</td>
<td>The University of Chicago</td>
<td>University of Northern Colorado</td>
</tr>
<tr>
<td>Georgetown University</td>
<td>The University of Findlay</td>
<td>University of Northwestern Ohio</td>
</tr>
<tr>
<td>Hampden-Sydney College</td>
<td>The University of Michigan</td>
<td>University of Richmond</td>
</tr>
<tr>
<td>Indiana University</td>
<td>The University of North Carolina at Chapel Hill</td>
<td>University of Rochester</td>
</tr>
<tr>
<td>James Madison University</td>
<td>University at Buffalo, SUNY</td>
<td>University of South Carolina</td>
</tr>
<tr>
<td>Johns Hopkins</td>
<td>University of Alabama at Birmingham</td>
<td>University of South Florida</td>
</tr>
<tr>
<td>Lafayette College</td>
<td>University of Arizona</td>
<td>University of Southern California</td>
</tr>
<tr>
<td>Liberty University</td>
<td>University of California, Berkeley</td>
<td>University of Utah</td>
</tr>
<tr>
<td>Massachusetts Institute of Technology</td>
<td>University of California, Davis</td>
<td>University of Vermont</td>
</tr>
<tr>
<td>Medical University of South Carolina</td>
<td>University of California, Irvine</td>
<td>University of Virginia</td>
</tr>
<tr>
<td>Miami University</td>
<td>University of California, Los Angeles</td>
<td>University of Washington</td>
</tr>
<tr>
<td>Michigan State University</td>
<td>University of California, Merced</td>
<td>University of Wisconsin - Madison</td>
</tr>
<tr>
<td>Michigan Technological University</td>
<td>University of California, Office of the President</td>
<td>University of Wisconsin - Whitewater</td>
</tr>
<tr>
<td>New York University</td>
<td>University of California, Riverside</td>
<td>Vanderbilt University</td>
</tr>
<tr>
<td>North Carolina State University</td>
<td>University of California, San Diego</td>
<td>Virginia Commonwealth University</td>
</tr>
<tr>
<td>Northern Arizona University</td>
<td>University of California, San Francisco</td>
<td>Virginia Polytechnic Institute &amp; State University</td>
</tr>
<tr>
<td>Northern Michigan University</td>
<td>University of California, Santa Cruz</td>
<td>Virginia State University</td>
</tr>
</tbody>
</table>

---

Large Facilities Workshop
Members: Government and Nonprofit Laboratories, Research Centers, and Agencies

Members
• Energy Sciences Network (ESNet)
• Lawrence Berkeley National Laboratory
• Moss Landing Marine Laboratories
• National Institutes of Health
• TeraGrid
• National Science Foundation as of 1/29/2009

Pending
• LIGO
• OOI
• Department of Education

In the virtual organizations, there is a bit of a “chicken and egg” problem as the member institutions have to adopt SAML and Shib before the VO can make use of it.

Considering
• NEON
• OSG
NSF Large Facilities Are Already Joining InCommon

- Laser Interferometer Gravitational-Wave Observatory
- Ocean Observatories Initiative
- TeraGrid - piloting/test bed now - Expect XD (TG phase 3) to use it in production

Considering InCommon membership:
Long Term Ecological Research [lternet.edu]
National Ecological Observatory Network [neoninc.org]
33 Sponsored Partners

Members
• Absolute Software, Inc.
• Apple - iTunes U*
• Burton Group
• Cengage Learning, Inc.
• e2Campus by Omnilert, LLC
• EBSCO Publishing*
• Elsevier*
• Houston Academy of Medicine - Texas Medical Center Library
• Identit-e
• Internet2
• JSTOR*
• Kuali Foundation*
• Microsoft*
• National Institute for Technology and Liberal Education (NITLE)
• National Student Clearinghouse* (student loan processing)
• NG Web Solutions
• OCLC
• OhioLink - The Ohio Library & Information Network
• Omnilert, LLC
• Outside The Classroom
• PeopleAdmin, Inc.

• ProQuest LLC
• ProtectNetwork
• RefWorks, LLC
• Safari Books Online
• Students Only Inc.
• SumTotal Systems Inc.
• Symplicity Corporation
• Travel Solutions, Inc.
• Trondent Development Corp.
• Turnitin
• UniversityTickets
• WebAssign

Pending
• Google*
• student service companies*
• medical consortia

*Incentive for more colleges and universities to join

The research community will benefit as institutions opt for federated services to meet administrative needs, eg student loan processing.
International Federation Highlights

• International Federation Highlights
  – Numerous countries including Norway, Switzerland, Finland, Spain, France, Sweden, Finland, Switzerland, Netherlands, Germany, Denmark, Norway, Australia, Brazil, Japan, Canada, etc.
  – Several countries at 100% coverage, including Norway, Switzerland and Finland
  – Community served varies somewhat by country, but all are multi-application and include higher education
  – UK intends a single federation for HE and Further Education ~ tens of millions of users
  – Real use cases involving international team science now driving interfederation peering urgency

• All do SAML; most are Shib

• Working to “peer” Federations

-Source: K. Klingenstein, Internet2/InCommon
Peering Parameters

Parameters:

- LOA
- Attribute mapping
- Legal structures
  - Liability
  - Adjudication
- Metadata
  - VO Support
- Economics
- Privacy
How does it work?
Shibboleth

- Shib what?
- Techniques and software developed as part of NSF Middleware Initiative (CISE/NMI)
- Standards based, open source software package for web single sign-on across or within organizational boundaries
- Neither an authentication or authorization system
- Secure exchange of messages between two parties (Identity Provider and Service Provider)
- Authentication handled by institution/LA/RBC (devolved authentication)
- Authorization achieved by an exchange of attributes (such as ‘member of an institution’)
- Providers need to sign up to a ‘trust’ agreement
- Vendor solutions (Oracle, Sun, CA/Netegrity…)
- An implementation of SAML (Security Assertion Mark-Up Language)
SAML

• SAM who?
• Security Assertion Markup Language (SAML)
  – Used for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions)
  – XML-based standard
• OASIS SAML
  [Link]
• Open SAML 2.0 now available
  – Already heavily used by Verisign, Tata, etc.

• NSF is using SAML 1.01
• Federations are migrating to SAML 2.0
• Action item for NSF: migrate to SAML 2.0
  [Link]
How does it work?

• The Players
  • IdP authenticates the browser user, and provides Attribute Assertions describing the user
  • SP validates the Assertions, makes an Access Control decision, and provides resources

• How is it Implemented?
  • Messages sequence between the IdP and the SP
  • Most messages move through the user’s Web browser

• Metadata defines the:
  • Trust framework
  • Trusted parties
  • Attributes the SPs want

• Importance of
  • Policy
  • Trust
R&D to Market

• TCP/IP
  – first as a technology
  – then as a market-maker

• SAML/Shibboleth
  – first as a technology
  – then as a market-maker

• Collaboration tools and collaboration management platforms

• Many of these technologies developed with NSF NMI/CISE (now OCI) support
  – “Shibboleth” and other Middleware
What is WAYF?

- “Where are you from?”
- Verification method for Shib
- Developed in the UK
I don't know you. Not even which home org you are from. I redirect your request to the WAYF.

Please tell me where are you from?

I redirect your request now to the Handle Service of your home org.

OK, I know you now. I redirect your request to the target, together with a handle.

Let's pass over the attributes the user has allowed me to release.

OK, based on the attributes, I grant access to the resource.

I don’t know the attributes of this user. Let’s ask the Attribute Authority.
What does this all mean for NSF?

How are we implementing this here?
What will NSF’s customers be able to do?

- **Research.gov**
  - Login with credentials issued by their home institution
  - View Proposal Status
    - NSF
    - USDA/CSREES
    - Army Research Office
    - More in progress
  - Create and submit Federal Financial Reports to NSF
  - Maintain their user profiles
  - And much more…

- **FastLane**
  - Login with credentials issued by their home institution
  - Access and use current PI/co-PI suite of functions
  - Perform Research Administration
  - Use proposal and award functions
Planned Pilot

- Demonstrate “proof of concept” with Ohio State University - complete
- Research.gov
  - Connect other institutions
    - Pennsylvania State University
    - University of Washington
    - Georgetown University
    - Colorado State University
    - University of California-Davis
  - Expand to other Research.gov institutions
- FastLane
  - Timeline to be determined
  - Successfully demonstrated in December 2006
Shared Data (minimum)

- Common Name
- Given Name
- Surname
- Middle Name (init)
- Business email
- Institutional affiliation of credential issuer
- Authentication LOA (level of assurance of identity) – will be 1 for this round
- a unique identifier for the user
How will it at work at NSF?

Step #1: User logs into his/her home institution portal, and chooses to go to Research.gov or FastLane.

Step #2: Home portal checks that user is authenticated, and hands him/her off to Research.gov, where access is provided only to the user’s own work items.
An example of a current service at an IdP…

Step 1: start

1. User may click from SPO home page or type [http://nsf.georgetown.edu](http://nsf.georgetown.edu), for example

2. User (reads notice) and clicks “Login”
An example of a current service…

Step 2: authentication

“Ardoth Hassler” logs in with unique credential, eg.“hasslera”, and password. After authentication, her information is passed to service provider.
An example of a current service...
Step 3: access

User recognized and now has access to offerings available under license agreement.
Example of “launch” at NSF

User selects login path

Large Facilities Workshop
Example of “launch” from USDA

Or, user logs in
Example of “arrival” at NSF
Example of “arrival” at NSF
Example of “arrival” at NSF “prompted activation”
Next time…

• User
  – “Launches” from home institution
  – Arrives at Research.gov
  – Is not asked for NSF ID and password
What the institutions need to do…

• Five pilot institutions (“beta”)
  – Tech lead: RL “Bob” Morgan U of Washington
  – Ironing out kinks at their end to share experience with others
• Unique user names (pilot institutions have this)
• “Identity proofing”
  – LOA1 (InCommon Bronze)
    • You are who you say you are… vetted by Sponsored Projects Officer
  – LOA2 (InCommon Silver)
    • You will have provided at least the INS (I-9) level of identification of two forms of government-issued ids
    • Anyone hired prior to 1986 may not have done this
• Technical implementation
  – Production “Shib”
  – Login services
  – “application handshakes”
• Sponsored Research Office collaboration
  – “Front end”/“Front door” access
  – User education
  – Ongoing support
A real life example… One University
Two Sponsored Research Offices; Two Administrations

Main Campus

Medical Center

Large Facilities Workshop
Already a resource…
[adding a link to Research.gov]
Example Change: requires collaboration with SRO, IT and, in this case, a contract web developer

Add link for login with GU credentials and link to NSF OR Pass already authenticated GU credentials to NSF

Note: this authentication may also occur off of a special login page initially.
What’s happening in the research community and with federal eAuth?
“InCommon-research-admin” Pilot

• Goal: intended to accelerate the deployment of federated identity and associated attributes in the research management community.

• Participants
  – University: IT organizations and Sponsored Research Offices
  – Federal Agencies: NIH and NSF, with endorsement of GSA eAuthentication initiative
  – National Organizations: the FDP and InCommon

• Objectives:
  – Inform each other - The diverse communities engaged bring different interests, expertise, terminologies, and challenges that they want to address.
  – Improve current business processes by leveraging the emerging federated identity infrastructure – The primary early focus of the activity is to utilize federations such as InCommon to improve the user experience, provide better security, and protect privacy.
  – Develop reengineered business processes to take advantage of the new technologies – Over the course of the work, we hope to better understand how to make other fundamental improvements to the activities of the research administration community through the use of the identity and access infrastructure.
InCommon-research-admin Objectives

- Work with pilot institutions to anchor and extend the use of existing InCommon infrastructure within the research administration community.
  - initial application base is a set of LOA 1 applications (grant status checks, genome db access, etc.)
  - expanded and complement with better defined strategies for cutover, user support, dissemination, etc.

- Develop strategies for campuses to implement InCommon Silver.
  - LOA 2
  - Leverage real business requirements to improve levels of security and ease of use.

- Use role-based access controls to complement identity based controls.
  - Pilot distributed but coordinated management via federated attributes.

- Understand how the InCommon-research-admin activities relate to other important R&E activities for the promotion of leverage and consistency of practice across the research community.
InCommon-research-admin
Expected Outcomes

• A “researchPerson” definition similar to the existing “eduPerson”
• Experiences to share with
  – Other federal agencies
  – Other institutions
National Institutes of Health

- Creating a federation for inside NIH
- All LOA 1
- Enabling lots of applications
  - But, NOT grants management
  - 5-6 in production now
  - National Library of Medicine is coming on soon
- Soon will have 100,000 users in 9,500 institutions worldwide
- Piloting LOA 2 for grants management with InCommon
What’s happening with Federal eAuth?

• 2002: government-wide eAuthentication begun
  – A few early adopters
• March 2009: eAuth PMO disbanded
  – Non viable business model
  – Sunset meeting held January 2009
• Responsibility moving from Federal Acquisition Service to Office of Government Policy
  – Agencies can:
    • Buy services off GSA schedule
    • Make their own alliances with other agencies and organizations
  – Move toward more industry-based certifications of products and technologies
What’s happening with Federal eAuth?

• GSA
  – New Leadership: Peter Alterman, Ph.D., Deputy Associate Administrator for Technology Strategy; Office of Governmentwide Policy, GSA
    • Led NIH initiative (toward higher-ed compatibilities)
    • Advocate for university methodologies for many years
  – Recommending using technologies used by InCommon as their new model as of 11/2008

• CIO Council/New Administration
  – Federal Identity, Credential, and Access Management (ICAM) Working Groups
    • Citizen services
    • F2F Working group

• http://www.cio.gov/eaauthentication/
Background and Supplemental Information
Shibboleth*

• “The term originates from the Hebrew word ‘shibboleth’ (شبולת), which literally means the part of a plant containing grains, such as an ear of corn or a stalk of grain[3] or, in different contexts, ‘stream, torrent’[4][5] It derives from an account in the Hebrew Bible, in which pronunciation of this word was used to distinguish members of a group (the Ephraimites), whose dialect lacked a /ʃ/ sound (from members of a group (the Gileadites) whose dialect did include such a sound.

• “In the Book of Judges, chapter 12, after the inhabitants of Gilead inflicted a military defeat upon the tribe of Ephraim (around 1370–1070 BC), the surviving Ephraimites tried to cross the Jordan River back into their home territory and the Gileadites secured the river’s fords to stop them. In order to identify and kill these disguised refugees, the Gileadites put each refugee to a simple test:

• “‘Gilead then cut Ephraim off from the fords of the Jordan, and whenever Ephraimite fugitives said, Let me cross, the men of Gilead would ask, Are you an Ephraimite? If he said, No, they said, Very well, say Shibboleth. If he could not pronounce it correctly, they would kill him by the ford of the Jordan. Forty-two thousand Ephraimites fell on this occasion.’” – Judges 12:5-6, NJB

Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

The single most important problem that SAML is trying to solve is the Web Browser Single Sign-On (SSO) problem. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. SAML has become the definitive standard underlying many web Single Sign-On solutions in the enterprise identity management problem space.

SAML assumes the principal (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented (although individual service providers most certainly will).

Thus a service provider relies on the identity provider to identify the principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.

*http://en.wikipedia.org/wiki/SAML
OASIS: Organization for the Advancement of Structured Information Standards

- OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.
- Members of note: NIST, NOAA (weather), Internet2, NCSA, etc.
- http://www.oasis-open.org/who/
eduPerson Core Attributes

- **eduPersonScopedAffiliation** – does this institution subscribe to the service in question? e.g. member@netherhall.cambs.sch.uk, or student@keele.ac.uk
  - student (learner), staff (non-teaching staff), faculty (teaching staff), employee (all staff), member (comprises all the previous categories), affiliate (relationship short of full member), alum (ex pupil/alumnus)
- **eduPersonTargetedID** – persistent opaque identifier – can provide personalisation & usage monitoring across sessions
- **eduPersonPrincipalName** – the ‘NetID’ of the user, e.g. user@school.lea.sch.uk – a persistent identifier across different services
- **eduPersonEntitlement** – enables an institution to assert that a user satisfies an additional set of specific conditions that apply for access to a particular resource e.g. “entitled to access financial accounts”

- Where extra attributes are required, the federation has a process for the addition of subsidiary attributes, but...

For most applications a combination of **eduPersonScopedAffiliation** and **eduPersonTargetedID** will be sufficient
Resources

- http://www.incommonfederation.org/
- http://www.incommonfederation.org/assurance/
- http://www.Internet2.edu
- http://shibboleth.internet2.edu/
- http://middleware.internet2.edu/eduperson/
- http://csrc.nist.gov/publications/PubsSPs.html
International Activities

  - A summary of discussions among R&E networks, including a survey of national efforts

- [http://www.jisclegal.ac.uk/access/](http://www.jisclegal.ac.uk/access/)
  - Excellent policy analytics, especially around international issues of privacy, peering, and attributes

  - TransEuropean activities in IdM for use among citizens, governments, and businesses
Acknowledgments

• Bill Altmire, Shauna Benson and David Lotts; NSF
• Steve Carmody, Brown University
• Ken Klingenstein, InCommon
• Ann West, Internet2

Slides from the above used with permission.
Questions?