Federated Identity & Authentication Workshop

October 22, 2014
## Today’s Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00</td>
<td>Welcome and Introductions</td>
<td>5m</td>
<td>Evans, Beadles</td>
</tr>
<tr>
<td>1:05</td>
<td>Purpose and Goals</td>
<td>5m</td>
<td>Beadles</td>
</tr>
<tr>
<td>1:10</td>
<td>The Problem Today</td>
<td>15m</td>
<td>Beadles</td>
</tr>
<tr>
<td>1:25</td>
<td>Basics of Federation</td>
<td>20m</td>
<td>Beadles</td>
</tr>
<tr>
<td>1:45</td>
<td>Elements of the System</td>
<td>30m</td>
<td>Beadles</td>
</tr>
<tr>
<td>2:15</td>
<td>Implementation Options</td>
<td>30m</td>
<td>Cantor</td>
</tr>
<tr>
<td>2:45</td>
<td>Break</td>
<td>15m</td>
<td></td>
</tr>
<tr>
<td>3:00</td>
<td>The Ohio Landscape</td>
<td>25m</td>
<td>All</td>
</tr>
<tr>
<td>3:25</td>
<td>Solution Requirements</td>
<td>25m</td>
<td>All</td>
</tr>
<tr>
<td>3:50</td>
<td>Call to Action</td>
<td>10m</td>
<td>Beadles</td>
</tr>
<tr>
<td>4:00</td>
<td>Dismissal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Welcome & Introductions
Purpose & Goals
Purpose & Goals

1. Displace legacy access and authentication methods which have become dangerously obsolete

2. Enable OhioLINK members to adopt more secure, extensible authentication framework with OH-TECH's assistance

3. Lay stepping stones to broader adoption

4. Define program, answer questions, recruit participants
IAM Ohio Program Overview

• IAM Ohio: “A Network of Trust”
  – Identity & Access Management for Ohio Public-Serving Institutions
  – Education and Collaboration
• Program Goals
  – Integrating Research at State and Federal level
  – Enabling Shared Services: OhioLINK, BOR, EduRoam
  – Improving Provisioning for automation and efficiency
  – Enhancing the Classroom and Online Teaching
IAM Ohio Program

• Standard agreements/alignments with federation providers
  – InCommon
  – Eduroam
• Education & Training
• Vendor management
  – Vendor identification, testing, pilots
  – Development of favorable vendor business terms
• Federation operations
  – Definition of regional policies and standards
  – Establishment of IDM operations, appropriately scaled, supporting high levels of trust and assurance
The Problem Today
The Identity Crisis

“On the Internet, nobody knows you’re a dog.”

www.oh-tech.org
The Identity Crisis

Multiple logins, multiple passwords

Lack of access to applications and services

Privacy breaches, fraud, theft and noncompliance

Lack of trust in identity and privacy claims

Disconnected silos of information

Duplicated effort and expense
### Ohio Federation Adoption 10/14

<table>
<thead>
<tr>
<th>OH-TECH Member</th>
<th>InCommon Member</th>
<th>InCommon Certs</th>
<th>InCommon Auth</th>
<th>OhioLINK via SAML</th>
<th>Eduroam Member</th>
<th>Active Eduroam</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>23</td>
<td>17</td>
<td>11</td>
<td>9</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

#### KEY

**InCommon Member**: Vetted member in good standing

**Certs**: Subscribes to InCommon cert service

**Auth**: Operates an InCommon IDP

**OhioLINK via SAML**: Authenticates users to Library services through SAML

**Eduroam Member**: Listed by Eduroam: Initiated membership process or testing

**Active**: Authenticating users to wireless

#### Notes:

1. Most Ohio InCommon members are buying certs, not authenticating
2. Most members authenticate to library services using legacy protocols
3. “Open” wireless is more common than Eduroam
Barriers to Federation

- We don’t have the time to set it up / operate it
- We don’t have staff with the right expertise
- It costs too much
- We don’t have the right software tools
- It’s too complex to integrate
- We don’t have servers or data centers to run it in
- We are challenged by Governance/Policy management
- It will disrupt our users
- It will disrupt our business
- There is no reason to care
Basics of Identity Federation
Building Blocks of Federation

• Identity Providers
  – identity management systems storing the user identity data

• Service Providers
  – collaboration, research, education tools, sites, services

• Federation Providers
  – In USA: InCommon for higher education and research
Components of a Federated System

Federation Provider

Service Provider

Identity Provider
How Trusted Identity Federation Works

1. User requests access to App
2. SP contacts User’s IDP
3. IDP authenticates User
4. IDP tells SP of result
5. SP provides access to app

*IDP: Identity Provider  
*SP: Service Provider

www.oh-tech.org
How Trusted Identity Federation Works with Proxy

1. User requests access to App
2. SP contacts User’s IDP
3. IDP authenticates User
4. IDP tells SP of result
5. Proxy provides access to Content Provider

*IDP: Identity Provider  *SP: Service Provider

www.oh-tech.org

Slide 17
Trust is the foundation

Passwords are never disclosed

Institution that issues identity performs the authentication

Only authorized attributes are released

Multiple levels of trust depending on sensitivity of data

Collaborate only with trusted partners

www.oh-tech.org
Elements of the System
Shibboleth

*is not*

SAML

*is not*

InCommon

*is not*

IAMOhio
Elements of the System

- **SAML**
  - Security Assertion Markup Language, a standard protocol for exchanging security claims and attributes with trust and security

- **Shibboleth**
  - Open-source software that implements SAML for web access

- **InCommon Federation**
  - A group of mutually trusting institutions, defined in SAML metadata, that use SAML to federate access

- **Incommon**
  - The entity that runs the InCommon Federation and also provides related services like certs, training, standardization, organizational vetting

- **IAMOhio**
  - A community of interest of OH-Tech members with a requirement to federate access regionally as well as with non-OH-Tech members; not limited to SAML
Without InCommon
- Users have many accounts to access different resources.
- Access is based on a user's identity or location.
- Time spent managing accounts instead of resources.
- Lack of uniform standards among partners.
- Collaborations don't happen because sharing is too difficult or insecure.
- Adding new resources and users may require significant work.

With InCommon
- Users have a single point of signing on to access different resources.
- Fewer user accounts to manage.
- Fine-grained control over the release of identities and other user information.
- Standards-based and open source.
- New resource providers and users can be integrated quickly.
- Access is based on information attributes, not identity or location.

Destinations
Many Managed Accounts
Multiple IDs and Passwords

Single ID at Home Institution

---

www.oh-tech.org
Elements of the System

- **Attribute**
  - A single piece of user data (such as name, affiliation, study branch, etc.) needed to make authorization decisions. Some attributes are general; others are personal. Some combination of attributes defines a unique individual.

- **Attribute Schema**
  - eduPerson

- **Attribute Release Policy**
  - Defines which attributes are going to be released to a requesting resource. It is a mechanism to implement privacy and data protection.

- **Discovery Service (Where Are You From?)**
  - A service that helps a user locate his or her "home" IdP
Current InCommon Sponsored Partners


- 12Twenty Inc.
- 9STAR
- Aastra USA
- Academic Works, Inc.
- Acatar
- Accessible Information Management, LLC
- Active Network
- Advantage Connect Pro Inc.
- ALEGKOS Corporation
- Alexander Street Press
- AliveTek
- American Psychological Association
- AppointLink Portal Solutions, Inc.
- ARTstor
- Association for Computing Machinery
- AT&T Services
- AthenaOnline.com
- Atlas Systems, Inc.
- Atomic Learning
- Axiom Education
- Benelogic
- BioOne, Inc.
- BioRAFT
- Blackboard, Inc.
- Blatant Media Corporation
- Blue Jeans Network
- BoardEffect
- Box, Inc.
- Cambridge University Press
- Campus Quad
- CampusGuard
- Cayuse, Inc.
- Cengage Learning, Inc.
- CENIC
- Center for Research Libraries
- CenturyLink
- Cincinnati Children's Hospital Medical Center
- Cirrus Identity, Inc.
- Cloudpath Networks
- CollegeNET
- Colorado Alliance of Research Libraries
- Comodo
- CounterMarch Systems
- CourseNetworking, Inc.
- CourseSmart
- CSO Research, Inc.
- Data 180, LLC
- Davie County Schools
- Decision Lens
- Desire2Learn
- DigArc
- Digital Measures
- Do Sports Easy
- DocuSign
- DoubleMap Inc.
- Dropbox
- Durham Public Schools
- e-academy, Inc.
- e2Campus by Omnilert, LLC
- EBook Library - EBL
- EBSCO Publishing
- Echo360
- Edublogs
- EDUCAUSE
- Elsevier
- Ensemble Video
- Entligence Corporation
- eRezLife Software
- ESM Solutions
- Evanced Solutions, LLC
- Evogh, Inc.
- Ex Libris
- First Advantage Screening Corporation
- Fluidware Corporation
- Fundriver, Inc.
- FuzeBox Software Corp.
- Give Pulse
- Governet
- GradesFirst
- Great Plains Network
- Halogen Software Inc.
- Hazelbney Betty Ford Foundation
- Higher One, Inc.
- HighWire Press
- Hitachi ID Systems
- Houston Academy of Medicine - Texas Medical Center Library
- IEEE
- iLab Solutions
- Imodules Software, Inc.
- Innitas
- Institute for Advanced Study
- Instructure, Inc.
- Interfolio, Inc.
- JSTOR
- Kaltura Inc.
- Kuali Foundation
- LabArchives
- LCMS Plus Inc.
- Leepfrog Technologies, Inc.
- Library of Congress
- Logistical Athletic Solutions
- Longsight
- Lucid Software
- lynda.com
- Mass. Green High Performance Computing Ctr
- Maxient LLC
- MCNC
- MedHub
- MediaCore Technologies Inc.
- Merit Network, Inc.
- Microsoft
- Modo Labs Inc.
- Moodlerooms, Inc.
- Moofwd Inc
- Moxie Software
- Mozy, Inc.
- MyEvaluations.com Inc.
- Myunidays Limited
- National Student Clearinghouse
- NBC Learn
- NC Live
- Nolij Corporation
- NuPark
- OCLC
- Ohio Technology Consortium (OH-TECH)
- OhioLink - The Ohio Library & Information Network
- OmniUpdate
- OrgSync, Inc.
- Outside The Classroom
- Parchment Inc.
- Pathbrite, Inc
- PeopleAdmin, Inc.
- Ping Identity Corporation
- Portfolio, Inc.
- ProQuest LLC
- Publishing Technology
- Qualtrics
- Rave Mobile Safety
- Reehere
- RefWorks, LLC
- Research Foundation for the SUNY
- RightAnswers
- Rockingham County Schools
- Royal Society of Chemistry
- Sakai
- SAE International
- Safari Books Online
- Sallie Mae Campus Solutions
- SANS Institute
- SciQuest
- SCLogic
- Seelio
- Serials Solutions
- ServiceNow
- SHI International Corp.
- Skillssoft Corporation
- Springshare
- SSB Bart Group
- Sloomify
- Stryder Corp
- Student Success
- SumTotal Systems Inc.
- SympliCity Corporation
- TeamDynamix Solutions, LLC
- TERENA
- Terra Dotta
- The Beans Group
- The CBORD Group
- The Centre Daily Times
- The Solution Design Group, Inc.
- Thomson Reuters
- Tivi
- Topofer
- Top Hat Monocle
- Travel Solutions, Inc.
- Trondent Development Corp.
- Trumba Corporation
- Tumitin
- Ubiquia Inc.
- UHC
- Unicon, Inc.
- United Public Safety
- University of Arkansas, Cooperative Extension Service
- University of Texas Health Science Center At Tyler
- UniversityTickets
- UPIC Solutions
- Upswing International, Inc.
- VoiceThread
- Washington Research Library Consortium
- WebAssign
- WERPA, Inc.
- Yammer
- Zimride, Inc.
Implementation Options
## Alternative Identity Provider Strategies

Source: InCommon Alternate IdP Working Group, [https://spaces.internet2.edu/display/altidp](https://spaces.internet2.edu/display/altidp)

<table>
<thead>
<tr>
<th>IdP Strategy</th>
<th>Description</th>
</tr>
</thead>
</table>
| Shibboleth                 | • Mainstream SAML implementation  
• Open source via [Shibboleth Consortium](https://www.shibboleth.net) |
| Microsoft ADFS (ADFS)      | • Natural approach for Windows shops  
• Proprietary as part of [Active Directory](https://azure.microsoft.com/en-us/services/active-directory/) |
| SimpleSAMLphp              | • Lightweight PHP-based IdP  
• Open source via [Uninett (NO)](https://www.uninett.no) |
| Outsourced Shibboleth      | • 3rd party hosted Shibboleth IdP  
• e.g. [Fischer Identity](https://www.fischer-security.com) Ignite Federation |
| Outsourced other vendor    | • 3rd party hosted non-Shib SAML IdP  
• e.g. [Cirrus Bridge](https://cirrusbridge.com) Social-to-SAML Gateway |
| Hub-and-spoke              | • Group of organizations sharing a trusted IdP  
• e.g. WAYF (DK), SURFnet (NL), FEIDE (NO) |
| Identity-as-a-Service      | • Outsource all or nearly all of IDMS  
• e.g. [Stormpath](https://www.stormpath.com), [Okta](https://www.okta.com), Google, Fischer Suite |
The Ohio Landscape
(handout)
Solution Requirements Discussion
Call to Action
“Federation Package”

• Federated Services
  1. OhioLINK library system access
  2. Eduroam roaming wireless
  3. State Board of Regents Services
     • Higher education student database
     • Supercomputing access
     • OARnet Customer Portal access

• OH-Tech Federation Package
  – SAML server in a box? (Shib/ADFS/Fischer…?)
  – Technical assistance/training (Shibfest II?)
  – Funding? Time? Personnel?

• Standards
  – Ohio “Category” a la R&S
Federated Identity & Authentication Workshop

October 22, 2014