Trust and Identity Services – an introduction

KEVIN MOROONEY
Vice President, Trust and Identity Services

OCTOBER, 2016

PACIFIC NORTHWEST GIGAPOP (PNWGP)
ADVISORY COUNCIL MEETING
Background

- Me
- trust and identity
Trust and Identity Services core portfolio

- InCommon
- TIER
- eduroam
- Certificate Service
Trust and Identity Services core portfolio

- InCommon
- TIER
- eduroam
- Certificate Service
Ever present axioms for T&I

- Reduction in the variances of technologies leveraged and policies developed - among the membership/participants - increases the collective ability to trust, to collaborate.

- Participants need flexibility

- Assets and services must constantly become more trustworthy
Introduction to InCommon
Some terminology and connections

- There are identity providers (IdPs) and service providers (SPs)
- IdPs and SPs are connected by
  - technology (SAML, Shibboleth, Grouper, simpleSAMLphp, etc.)
  - contracts (Participation Agreement, Participants Operational Practices, etc.)
  - business practice “requirements”
  - technology practice “requirements”
- A reasonable reference point is the Payment Card Industry (PCI)
Why do you use them?

Why do you trust them?
Payment Credit Cards

- You know and trust how the cards are distributed
- You know and trust the merchants who accept the cards, to do the right thing with your data - among other things
- There’s a contract between you and the card provider
- There’s a contract between the card providers and the merchants who accept the cards
- There are laws that guide practices and behaviors
The InCommon Trust Federation

• About 600 “card providers”, (mostly) universities who distribute and curate tens of millions of userids and passwords (credentials, “cards”) for faculty, students and staff

• About 450 “merchants” who accept those “cards”/credentials
Let’s take a look at how it works
Federation Operator

Operates the internals of the federation, Internet2 staff. Boards federation participants, curates the metadata, etc.

Identity Provider. *Almost always:* a campus, identity management staff in the CIO organization operate it, policy interpretation or navigation come from CIO. Contributes metadata.

Service Provider. *Often:* a vendor with services or data of interest. *Often:* a campus providing a service to others in a scholarly context. *Sometimes:* a campus serving itself. Contributes metadata.

Identity Provider and Service Provider. *Almost always:* a campus that offers services to others in the federation and has consumers of services in the federation. Contributes metadata.
• **Looks like a hub and spoke network**
  
  • daily, nodes on the network download the federation map from the federation operator
  
  • the trust network is *built* in a hub and spoke fashion
- Acts like a mesh network
- once nodes have the “map”, nodes interact with one another directly
- We call the “federation map”, the InCommon metadata or sometimes the InCommon metadata aggregate
An example
Log in with your partner institution — no signup is necessary.

University of Michigan

CANCEL  CONTINUE

Don’t see your institution listed? »

Not with a partner institution? Create or log in with a "Friend" account to create collections. »

What are the benefits of logging in? »
Please enter your Access Account ID or Friends of Penn State ID (e.g. xyz5000).

User ID: kxm
Password: ************
Log in

Change Access Account Password  Change FPS Account Password

The Pennsylvania State University ©2015. All rights reserved.
Nondiscrimination Policy  -  Privacy and Legal Statements
Additional authentication is required via Penn State's Two-Factor Authentication service.

Enrolled Devices
- iPhone (XXX-XXX-7583)
- Duo Push **RECOMMENDED**
- Phone Call
- Passcode
  (Send SMS passcodes)

Log In

Change Access Account Password  Change FPS Account Password

The Pennsylvania State University ©2015. All rights reserved.
Nondiscrimination Policy - Privacy and Legal Statements
That’s me!

I can get cool stuff.

Because I’m me.
Remember this?
• InCommon Federation Operating Principles and Practices (FOPP)
• InCommon Participation Agreement (PA)
• Campus identity and access management policies and technologies (Participant Operational Practices - POP)
a. Participant agrees to respect the privacy of and any other constraints placed on identity information that it might receive from other Participants or any CoFederation Participants. In particular, Participant understands that it may not permanently store, share, disclose or use for any purpose other than its intended purpose any identity information that it receives from another Participant or Co-Federation Participant without express written permission of the other Participant or Co-Federation Participant. Participant understands that the storing and sharing of resources is between the Participant and the other Participants and/or Co-Federation Participants and is not the responsibility of InCommon.

b. InCommon strongly recommends that Service provider systems may temporarily cache identity attributes/credentials that are supplied by IdPs for operational efficiency or sequential, repeated authentication purposes within a given session or reasonable length episode. InCommon further recommends that any shared attributes/credentials should not be used for any purpose other than the original purpose or intent, and that such attributes/credentials should be destroyed at the end of the session or episode in which they are needed. This temporary storage of credentials shall not be deemed as permanent storage for the purposes of this Agreement.
Identity and Access Management (IAM)

INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

Participation in the InCommon Federation ("Federation") enables a federation participating organization ("Participant") to use Shibboleth identity attribute sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system fall under the purview of the organization's executive or business management, and (2) the system for assuring end-user credentials (e.g., PKI certificates, username/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., authentication and authorization standards, security practices, risk assessments, change management controls, audit trails, etc.).

InCommon expects that Service Providers, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission(s) of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below. Additional information to help answer each question is available in the next section of this document. There is also a glossary at the end of this document that defines terms shown in italics.

1. Federation Participant Information
   1.1 The InCommon Participant Operational Practices information below is for:
      InCommon participant organization name University of Alaska
      The information below is accurate as of this date 2021-08-21
   1.2 Identity Management and/or Privacy Information
      Additional information about the Participant’s identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s)
   UA Board of Regents Policy and University Regulation:
   http://www.alaska.edu/boe/policy-regulations/
   UA Student & Enrollment Services documentation on FERPA compliance:
   http://www.alaska.edu/student-services/ferpa/
technology, contracts, business processes, law

University polices, digital lifecycle practices

FOPP, PA, POP
Current InCommon Participants

Below is a complete list of InCommon Participants. There are also lists available for:

- **Identity and Service Providers** deployed in the federation (and other metadata-driven pages)
- **Certificate Service** subscribers
- **Duo Security multifactor service** subscribers

The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. **InCommon serves 8 million end-users through federated identity management (IPEDS data; October 2014)**

<table>
<thead>
<tr>
<th>Higher Education Participants (597)</th>
<th>Government and Nonprofit Laboratories, Research Centers, and Agencies (31)</th>
<th>Sponsored Partners (257)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. T. Still University</td>
<td>Ames Laboratory</td>
<td>12Twenty Inc.</td>
</tr>
<tr>
<td>Adventist University of Health Sciences</td>
<td>Argonne National Laboratory</td>
<td>3D Control Systems, Inc.</td>
</tr>
<tr>
<td>Aims Community College</td>
<td>Brookhaven National Laboratory</td>
<td>9STAR</td>
</tr>
<tr>
<td>Allan Hancock Joint Community College District</td>
<td>ESnet</td>
<td>Aastra USA</td>
</tr>
<tr>
<td>Allegheny College</td>
<td>Fermilab</td>
<td>Academic Works, Inc.</td>
</tr>
<tr>
<td>American Museum of Natural History - Richard Gilder Graduate School</td>
<td>GENI Project Office</td>
<td>Acatar</td>
</tr>
<tr>
<td></td>
<td>Internet2</td>
<td>Accessible Information Management, LLC</td>
</tr>
</tbody>
</table>
How does TIER fit in?
TIER background

- 49 CIO investors, all Internet2 members. 25K/year for three years.
- ~9 months of requirements gathering among the investors institutions, generating 200+ use cases and ~30
- We’re getting close to the half way mark for the three year uplift
• InCommon Federation Operating Principles and Practices (FOPP)
• InCommon Participation Agreement (PA)
• Campus identity and access management policies and technologies (Participant Operational Practices - POP)
technology, contracts, business processes, law
TIER was established to:

- sustain the investment the community has made in developing a set of critically important identity-related software components;
- integrate them together with common APIs, data structures, development and release practices and schedules, and facilitative and flexible deployment packaging;
- extend their features to support the common functionality in the set of the campus contributed use cases.
Core components
- Shibboleth, Grouper, COManage

New components, capabilities
- APIs, Entity Registry, Scalable Consent, Packaging, interoperability profiles, etc.
TIER Release One - April 2016

- Shibboleth Single Sign-On and Federating Software (Identity Provider version 3.2.1)
- Grouper enterprise access management system (version 2.3)
- COmanage Registry (version 1.0.3)
- First Look Containers and Virtual Machine Images
- COmanage Registry 1.0.2 (VM/Container)
- Grouper 2.2 (Container)
- Shibboleth 3.2.1 (VM running Container)
- Application Programming Interfaces (APIs) - to enable extension and flexibility
- Data Structures and API documents
- Entity Registry documents
- InCommon Multifactor Authentication (MFA) Interoperability Profile (draft)
- InCommon SAML V2.0 Implementation Profile for Federation Interoperability v20160303
- InCommon Global Interfederation (in production through InCommon Federation)
- MACE-Dir eduPerson 201602 (including ORCID Identifier)
TIER at Technology Exchange 2016
<table>
<thead>
<tr>
<th>Categories</th>
<th>Timing / Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Application Programming Interfaces / Campus</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>2  VO De/Provisioning and Invitation Svcs (Comanage)</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>3  Student Applicant Identity Provider (CommIT)</td>
<td>“Beta” / Suspended</td>
</tr>
<tr>
<td>4  Community IdP (Identity Provider of Last Resort)</td>
<td>Community Solution / External</td>
</tr>
<tr>
<td>5  Entity Registry (Person and Object Registry)</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>6  Group Management and Group Administration</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>7  InCommon Federation Operations and Management</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>8  Component Packaging and Deployment</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>9  Component and Operations Security and Audit</td>
<td>Near-Term / Recommendations</td>
</tr>
<tr>
<td>10 Scalable Consent Services</td>
<td>Near-Term / Grant-Funded</td>
</tr>
<tr>
<td>11 Identity Provider and Service Provider (Shibboleth)</td>
<td>Near-Term / In Progress</td>
</tr>
<tr>
<td>12 Community Training and TIER Program</td>
<td>Mid-Term / Under Evaluation</td>
</tr>
</tbody>
</table>
In Our Last Episode … (Global Summit 2016)

Proposed Milestones

- Backbone usage scenario (BUS) proof of concept
- An open IAM testbed based on the proof of concept
- A containerized version of the IAM testbed for local experimentation
- Well-instrumented code that can reveal behavior and health of the IAM infrastructure components and their interactions
- First edition of a living guidebook: architectural patterns for IAM integration
Actual Progress

- Backbone usage scenario (BUS) proof of concept
- An open IAM testbed based on the proof of concept
- A containerized version of the IAM testbed for local experimentation
- Well-instrumented code that can reveal behavior and health of the IAM infrastructure components and their interactions
- First edition of a living guidebook: *architectural patterns for IAM integration*
In Our Last Episode … (Global Summit 2016)

Proposed Milestones

- Testing and enhancement of the container/vm distributions
- Exploring Instrumentation
- Prioritize usability enhancements
  - Setup automation and pre-configuration
  - Campus metadata
  - etc., etc.

- Build on the packaging foundation
  - Automate the container and VM builds
  - Operationalize the build process; produce regularly scheduled updates
  - Start the process of automating testing
  - Complete the work with the initial components
Actual Progress

- Testing and enhancement of the container/vm distributions
- Exploring Instrumentation
- Prioritize usability enhancements
  - Setup automation and pre-configuration
  - Campus metadata
  - etc., etc.

Build on the packaging foundation
- Automate the container and VM builds
- Operationalize the build process; produce regularly scheduled updates
- Start the process of automating testing
- Complete the work with the initial components

Today … (TechEx 2016)
DevOps Model: Enabling Autonomy

Workbench Path 1: Development and Iteration / Ideation

Workbench Path 2: UAT/QA/Security Audit/Performance Assessment/Release
Things we didn’t talk about but could have

- edugain (global interfederation)
  - interfederation interoperability
- Stewards Program (federation extension to regionals to enable support of K-14)
- SIRTFI (security incident response in a world with global interfederation)
- Community conversations for sustainability of trust and identity services
- Baseline Expectations implementation
- Support for “Research and Scholarship” Tags
- Moving to a dynamic distribution of federation metadata
- Emerging support for OpenID Connect (OIDC)