



MIAMI FL



SEPTEMBER 25-28

INCOMMON TRUST FEDERATION

The Basics

Kevin M. Morooney

Vice President, Trust and Identity
Internet2

Caveats

Some terminology and connections



Some terminology and connections

- There are identity providers (IdPs) and service providers (SPs)



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” and technology practice “requirements”



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” and 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

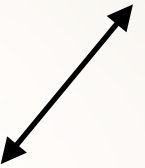
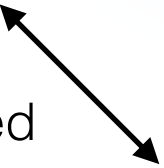


Payment Credit Cards

- You know and trust how the cards are distributed



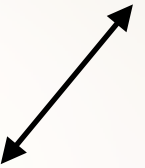
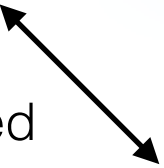
amazon



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

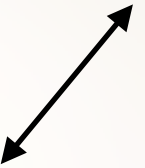
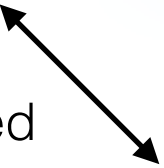
amazon



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

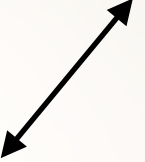
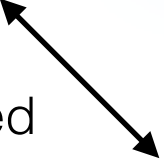
amazon



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

amazon



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

amazon

technology,
contracts,
business processes,
law



technology,
contracts,
business processes,
law

technology,
contracts,
business processes,
law



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.

IdP

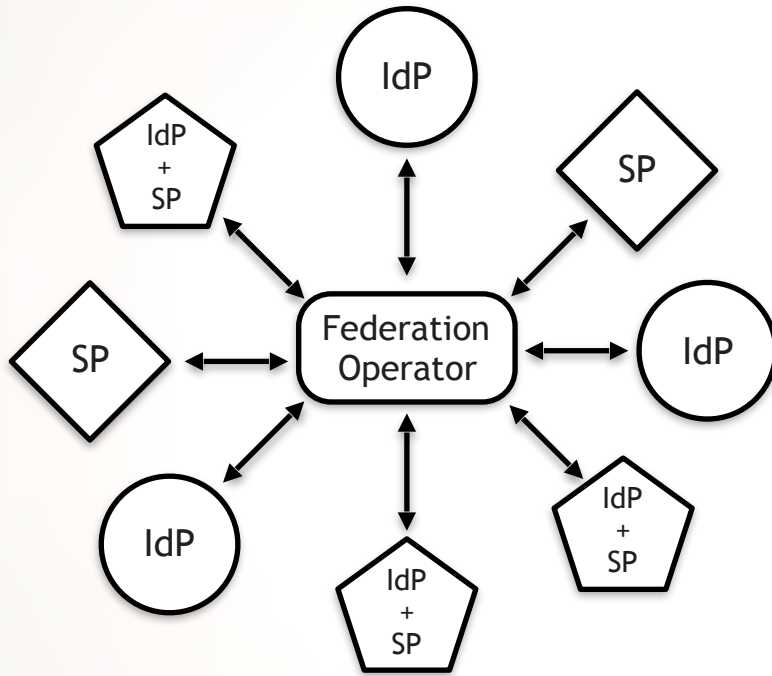
Identity Provider. *Almost always:* a campus, identity management staff in the CIO organization operate it, policy interpretation or navigation come from CIO. Contributes metadata.

SP

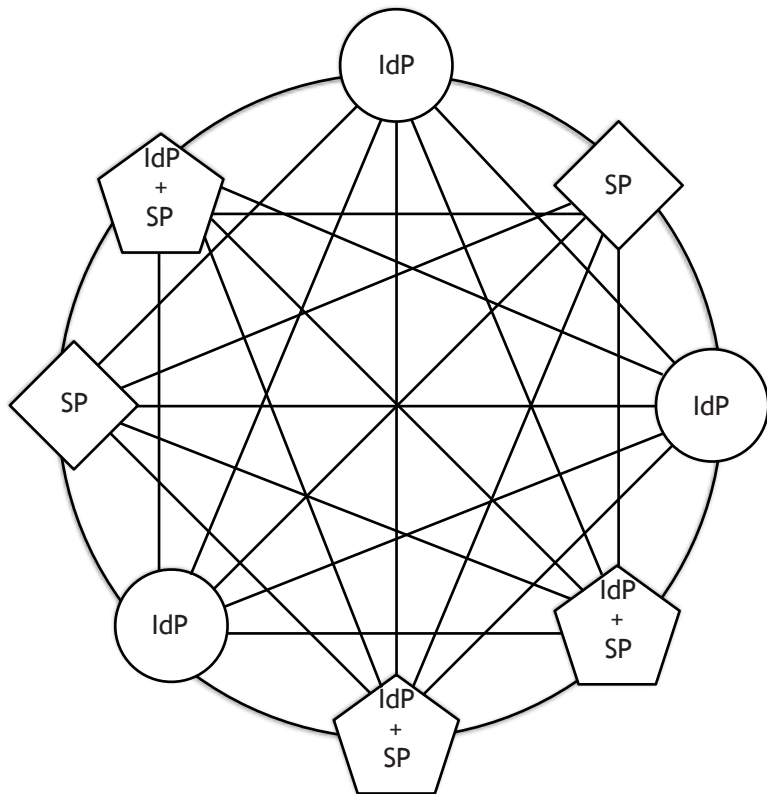
Service Provider. *Often:* a vendor with services or data of interest. *Often:* a campus providing a service to others in a scholarly context. *Sometimes:* a campus serving itself. Contributes metadata.

IdP
+
SP

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



https://www.hathitrust.org

Home About Collections Help Feedback



Search HathiTrust's digital library FULL-TEXT CATALOG

Search words about or within the items Search

[Advanced full-text search](#) [Search tips](#) [Full view only](#)

[Should I search combo or full-text?](#)

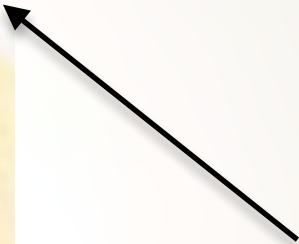
HathiTrust is a partnership of academic & research institutions, offering a collection of millions of titles digitized from libraries around the world.

WHAT CAN YOU DO WITH HATHITRUST?

- BROWSE COLLECTIONS**
Explore user-created featured collections
- READ BOOKS ONLINE**
Read millions of titles online -- like this one!
- READ BOOKS ON THE GO**
Take the library's books anywhere with our mobile website.
- DOWNLOAD BOOKS* & CREATE COLLECTIONS**
*requires institutional login

LOG IN

Want to get the most out of HathiTrust? Log in with your partner institution account to access the largest number of volumes and features. Not with a personal institution? -



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? »](#)

https://www.hathitrust.org

UNIVERSITY OF MICHIGAN
HATH TRUST

Search HathTrust's digital library

University of Chicago
University of Connecticut
University of Delaware
University of Florida
University of Houston
University of Illinois at Chicago
University of Illinois at Urbana-Champaign
University of Iowa
University of Kansas
University of Maine
University of Maryland, College Park
University of Massachusetts Amherst
University of Miami
University of Michigan
University of Minnesota
University of Missouri - Columbia
University of Nebraska - Lincoln
University of Nevada - Las Vegas
University of New Mexico
University of North Carolina at Chapel Hill
University of Notre Dame
University of Oklahoma
University of Pennsylvania
University of Pittsburgh
University of Queensland
University of Rochester
University of South Florida
University of Tennessee, Knoxville
University of Texas Health Science Center at Houston
University of Texas M.D. Anderson Cancer Center
University of Texas at Arlington
University of Texas at Austin
University of Texas at Dallas
University of Texas at El Paso
University of Texas at San Antonio
University of Utah
University of Vermont
University of Virginia
University of Washington
University of West Florida
University of Wisconsin - Madison



MIAMI FL



SEPTEMBER 25-28



Please enter your Access Account ID or Friends of Penn State ID (e.g. xyz5000).

User ID

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](#)

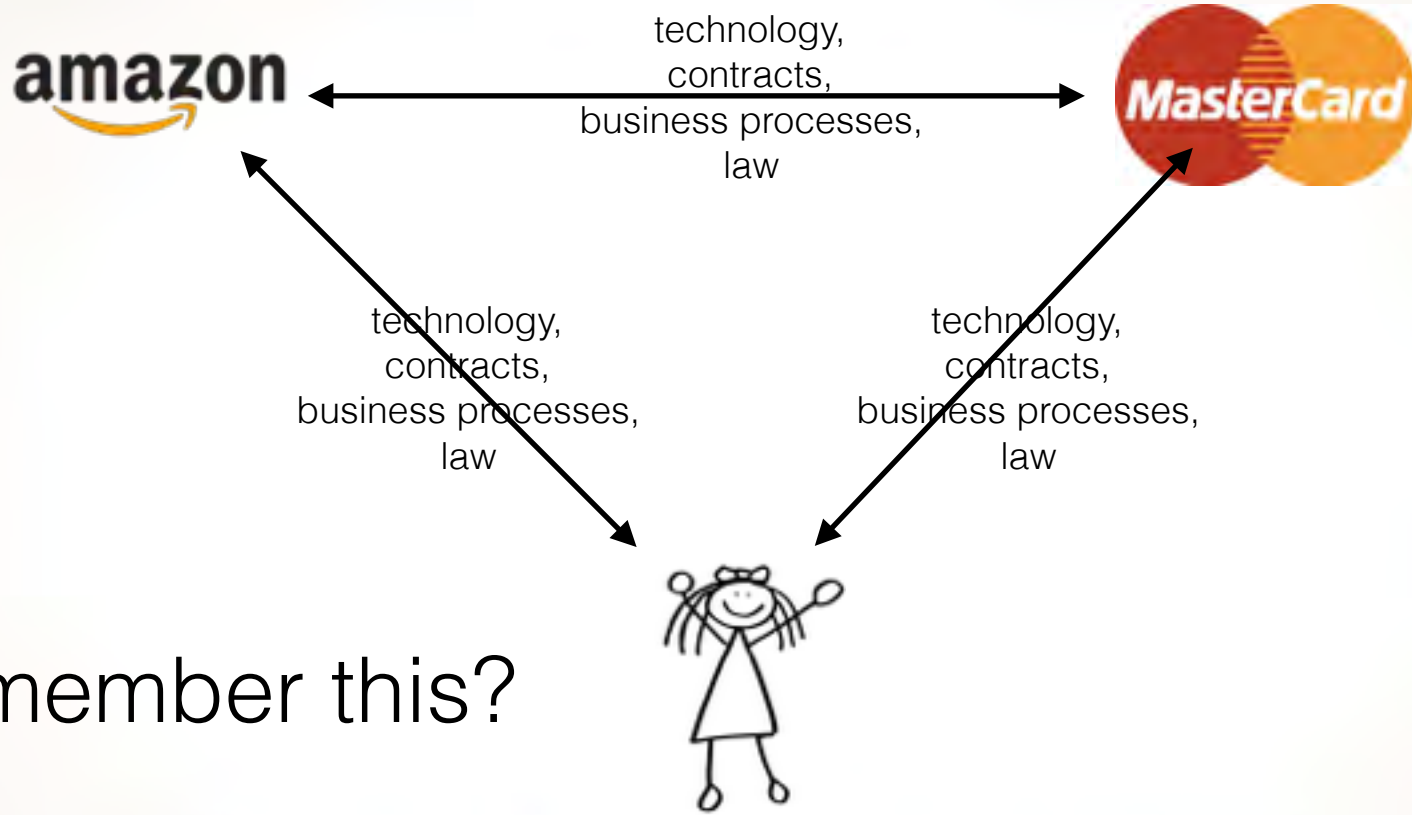
The Pennsylvania State University ©2015. All rights reserved.
 Nondiscrimination Policy • Privacy and Legal Statements

The screenshot shows the HathiTrust Digital Library website. At the top, there is a navigation bar with links for Home, About, Collections, Help, and Feedback. The user is logged in as KEVIN M MOROONEY1, with links for My Collections and Logout. The main content area features a search bar with the text "Search HathiTrust's digital library" and buttons for "FULL-TEXT" and "CATALOG". Below the search bar is a search input field and a "Search" button. A sidebar on the right displays a personalized greeting: "Hello, KEVIN M MOROONEY1" and "You are logged in, which ensures you get the most out of HathiTrust." Below this, there are four icons representing different services: "Browse Collections", "Read Books Online", "Read Books on the Go", and "Download Books & Create Collections".

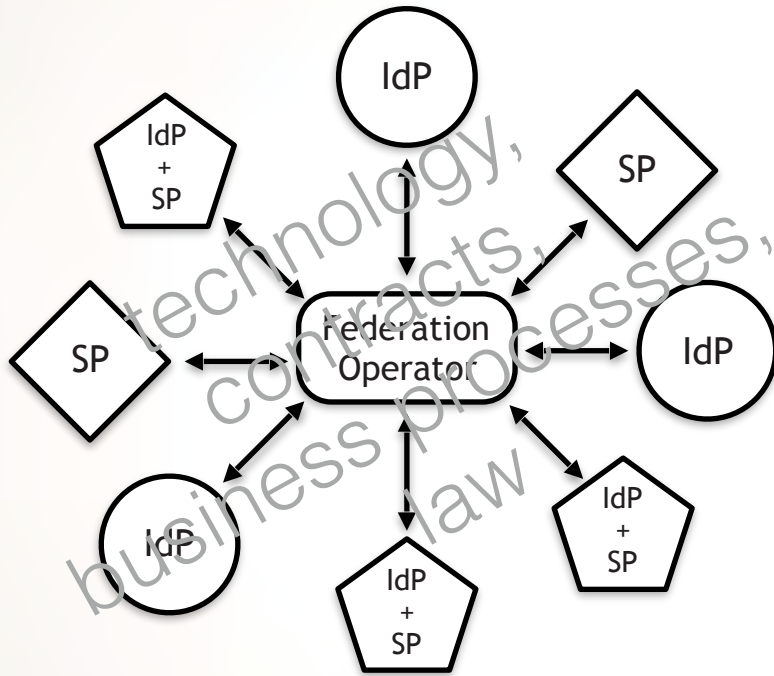
That's me!

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)

**INCOMMON:
FEDERATION OPERATING POLICIES AND PRACTICES**

TABLE OF CONTENTS

1.1	The InCommon Assurance Program	1
2	ORGANIZATIONAL STRUCTURE	2
2.1	Membership	2
2.2	Committees	2
2.3	Meetings	2
2.4	Offices and Regions	2
2.5	Principles	3
3	POLICIES, REQUIREMENTS, AND STANDARDS	3
4	APPLICATION FOR PARTICIPATION IN INCOMMON	3
4.1	Eligibility Criteria	3
4.1.1	Eligibility to Become a Participant	3
4.1.2	Eligibility for the Assurance Program	3
4.2	Submission and Processing of Applications	3
4.2.1	Application to Become a Participant	3
4.2.2	Application for Participation in the Assurance Program	3
5	FIDP	3
6	REGISTRATION, IDENTIFICATION AND AUTHENTICATION OF PARTICIPANT'S TRUSTED OFFICERS	6
7	REGISTRATION AND MANAGEMENT OF PARTICIPANT POLICIES, SYSTEMS, AND TECHNICAL COMPONENTS	6
7.1	Technical Resource Services, Incident Procedures and Service Procedures	6
7.2	Registration or Renewal of Participants	6
7.3	Participant System/Service Components	6
7.3.1	Participant Operating Practices	6
7.3.2	Minimality	6
7.3.2.1	Confidence in Minimization	7
7.3.2.2	Declaration of Participant Assurance Program Compliance	7
8	DISPUTE RESOLUTION PROCEDURES	8
8.1	Dispute Resolution Procedures	8
8.2	Dispute Resolution Procedures for Participants and Trust Providers	8
8.3	Dispute Resolution Procedures for Participants and Trust Providers or Participants and Trust Providers	8
9	OPERATIONS	8
9.1	Operational Address Lists	8
9.1.1	General Operations	8
9.1.2	Operational Staff Credentials and Authentication	8
9.2	Communication and Security	8
9.3	Participant Technical Interactions	8
9.3.1	Discovery Service (DS)	8
9.3.2	Minimality Distribution	8
9.3.3	Participant Administrative Interface	8
9.3.4	Registration of Participant Services	8
9.4	Operational Reviews	8
10	PARTICIPATION STATUS: RENEWAL, WITHDRAWAL, TERMINATION, AND SUSPENSION	11
10.1	Renewal	11
10.1.1	Renewal of Participant Status	11
10.1.2	Renewal of Assurance Program Compliance	11
10.2	Withdrawal or Termination	11
10.3	Suspension of Participant Services	11
10.3.1	Suspension for Failure of Security	11
10.3.2	Suspension of Assurance Compliance	11
11	FURTHER RISK ASSESSMENT	12

Participation Agreement snippet - Section 9

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.

<mdui:InformationURL xml:lang="en"><https://iam.alaska.edu/trac/wiki/UAIInCPOP.html></mdui:InformationURL>

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 authenticative 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 issuing end-user credentials (e.g., PKI certificates, usernames/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.).

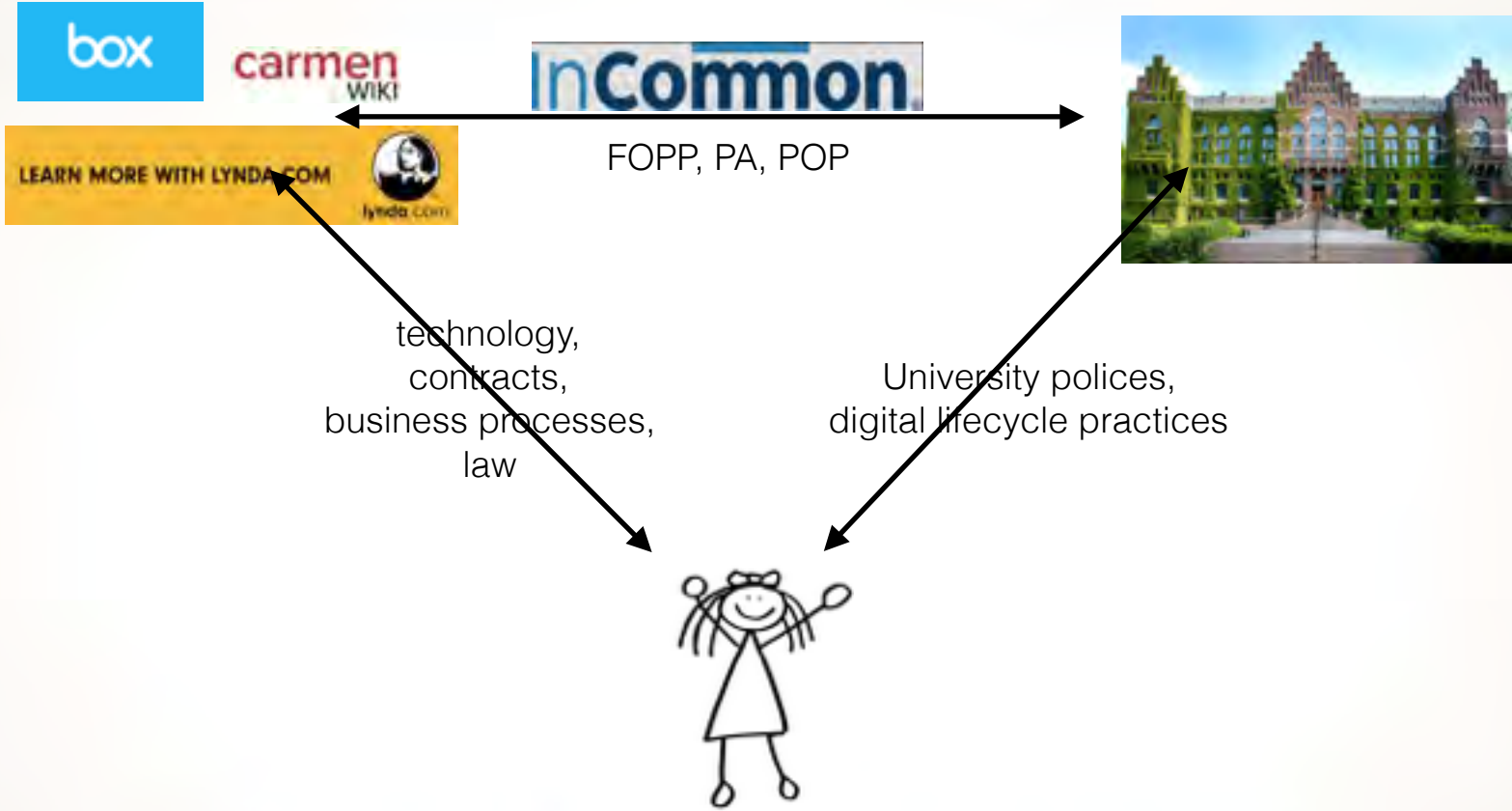
InCommon expects that Service Providers, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission 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 final 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 2011-06-21

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 address(es):
URL(s)
UA Board of Regents Policy and University Regulation:
<http://www.alaska.edu/ua-board-reg-conv>
UA Student & Enrollment Services documentation on FERPA compliance:
<http://www.alaska.edu/student-services/ferpa/>





INTERNET
2

2016
TECHNOLOGY
exchange

MIAMI FL



SEPTEMBER 25-28

Why?



INTERNET
2

2016
TECHNOLOGY
exchange

MIAMI FL

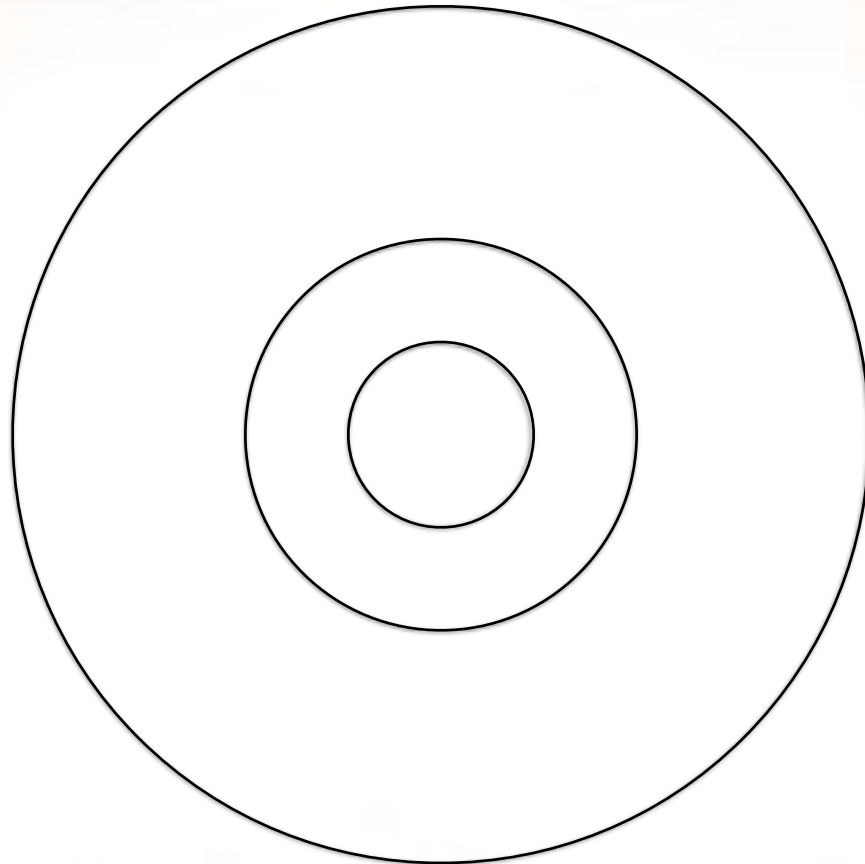
SEPTEMBER 25-26

Why?

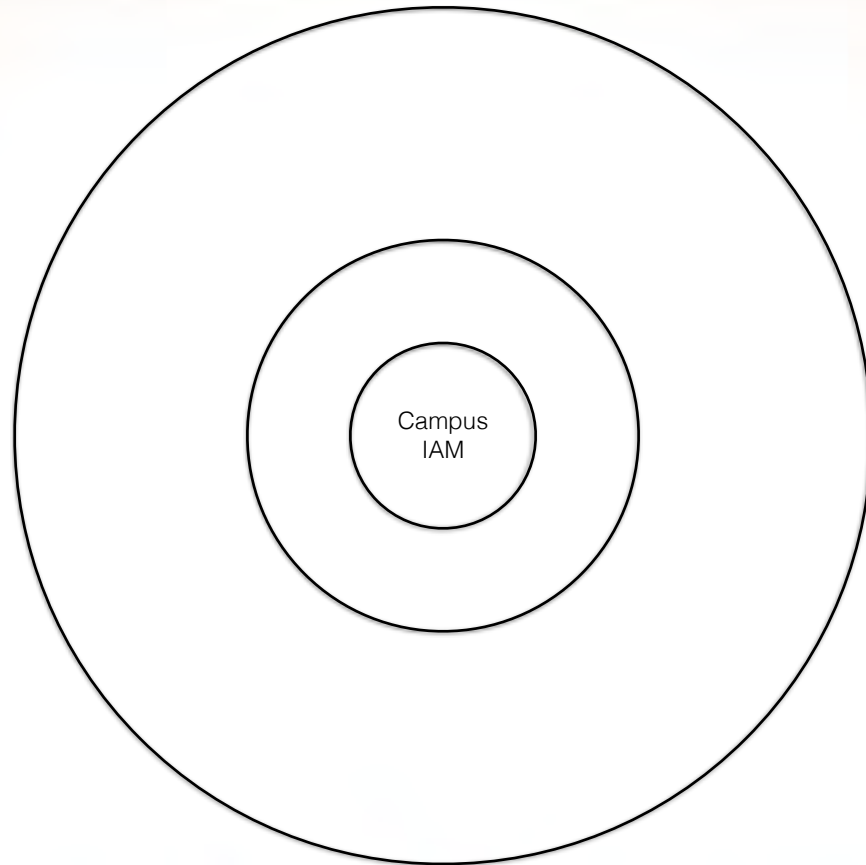
- People: use familiar, trusted identifiers to consume and access information and workflows relevant to their scholarly journey. Enable future access by being at an institution that vibrantly participates in a collaboration enabling infrastructure.
- University/IdP IT staff: Publish metadata one time, integrate many times
- Service Providers: Publish metadata one time, integrate many times
- Everyone: reduce hassle and cost for everyone, improve privacy and security

One last thing

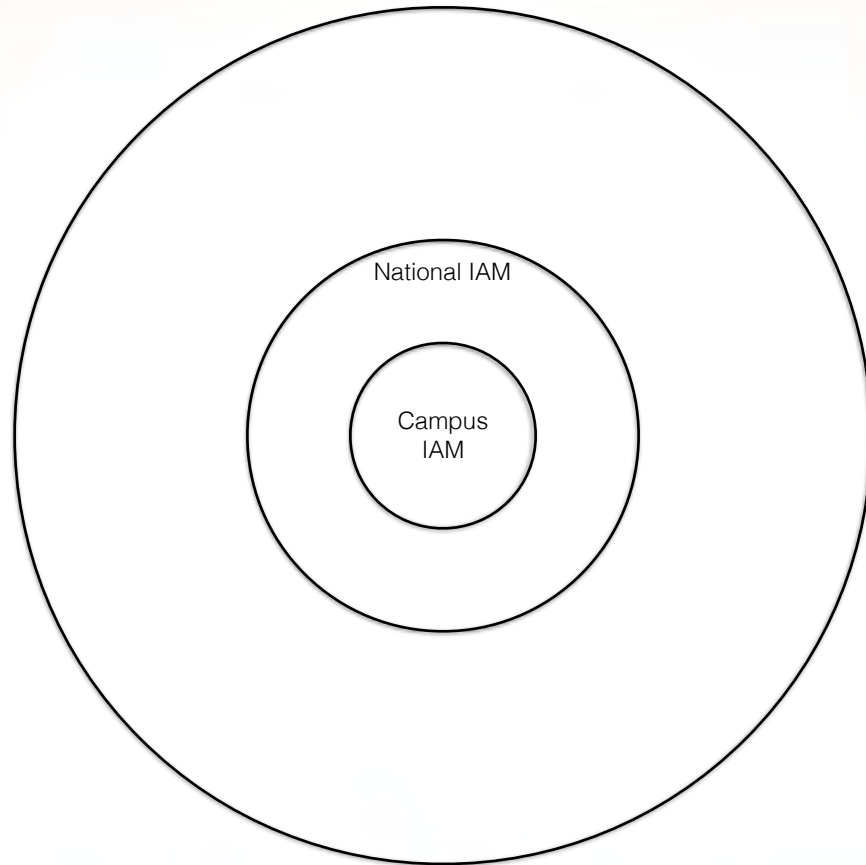
How does everything fit together?
(An IdP perspective)

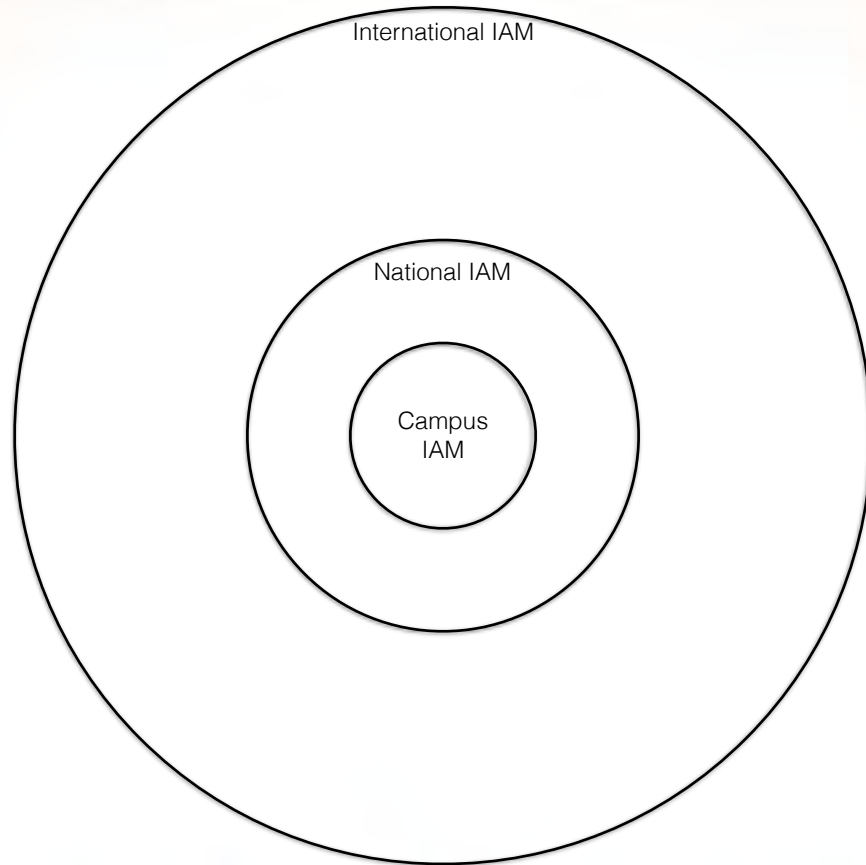


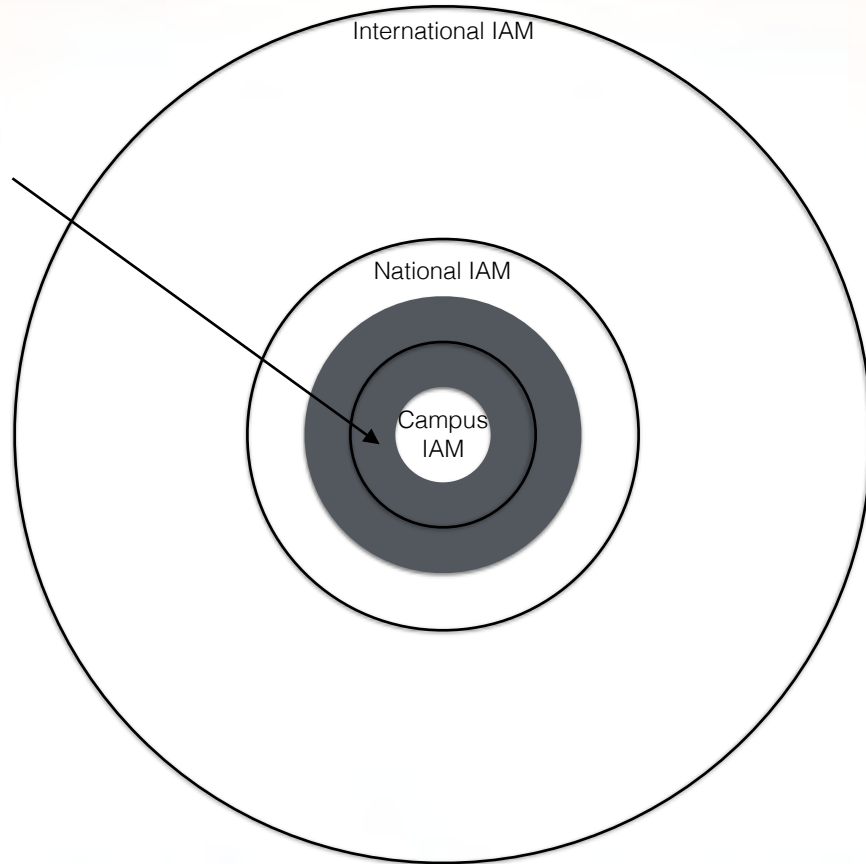
MIAMI FL SEPTEMBER 25-28



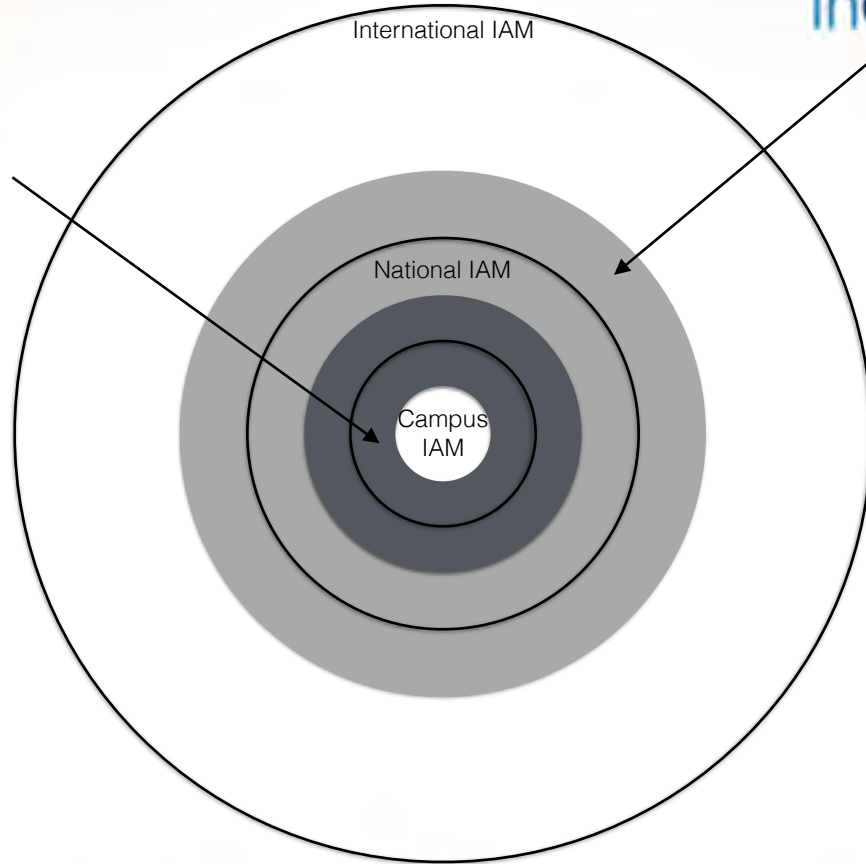
MIAMI FL SEPTEMBER 25-28

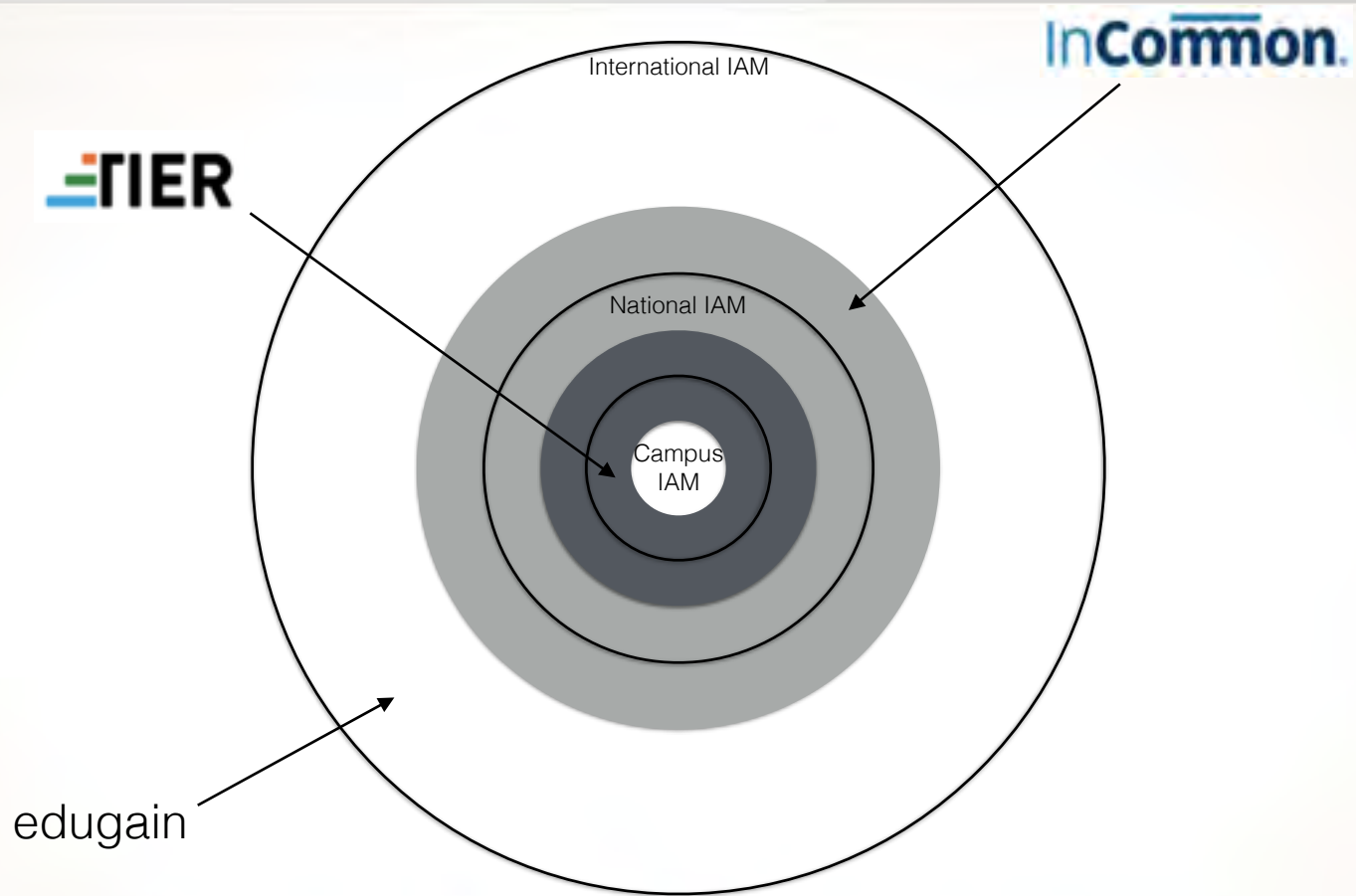






MIAMI FL SEPTEMBER 25-28







INTERNET2

2016
TECHNOLOGY
exchange

MIAMI FL

SEPTEMBER 25-28