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

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

Payment Credit Cards

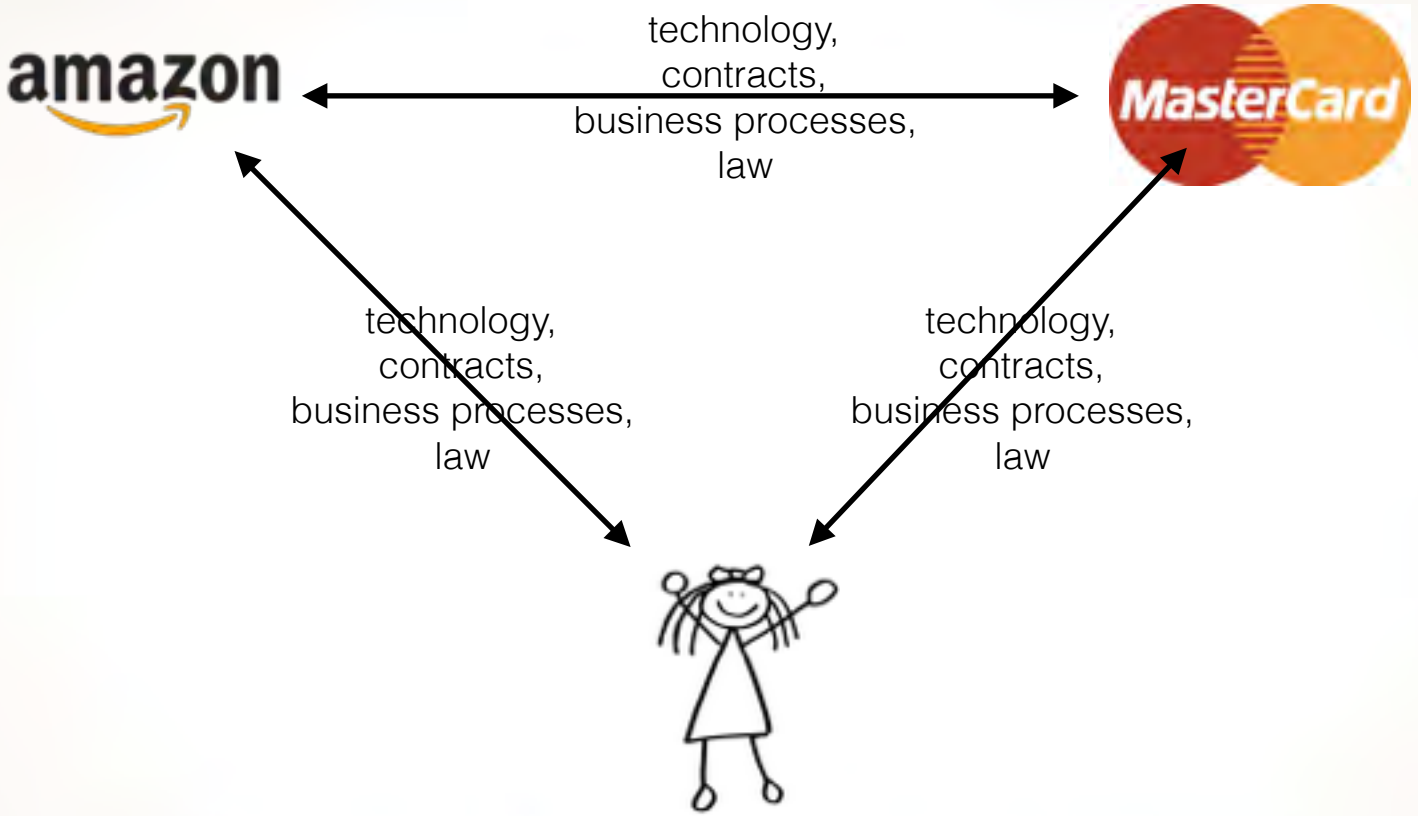
- You know and trust how the cards are distributed
- You know and trust the merchants who accept the cards, to do the right thing with your data - among other things
- There's a contract between you and the card provider

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

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

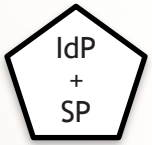
- About 600 “card providers”, (mostly) universities who distribute and curate tens of millions of userids and passwords (credentials, “cards”) for faculty, students and staff
- About 450 “merchants” who accept those “cards”/credentials

Let’s take a look at how it works

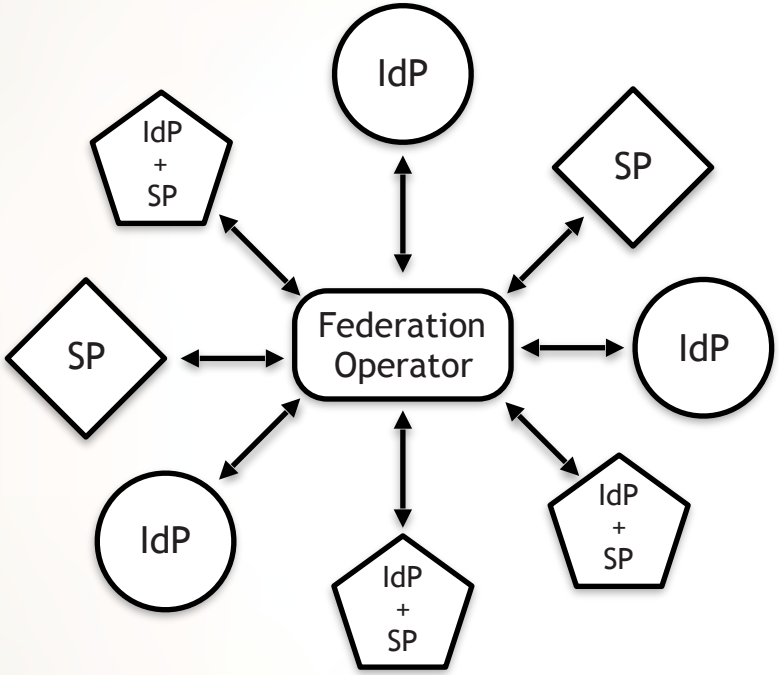
Operates the internals of the federation, Internet2 staff. Boards federation participants, curates the metadata, etc.

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

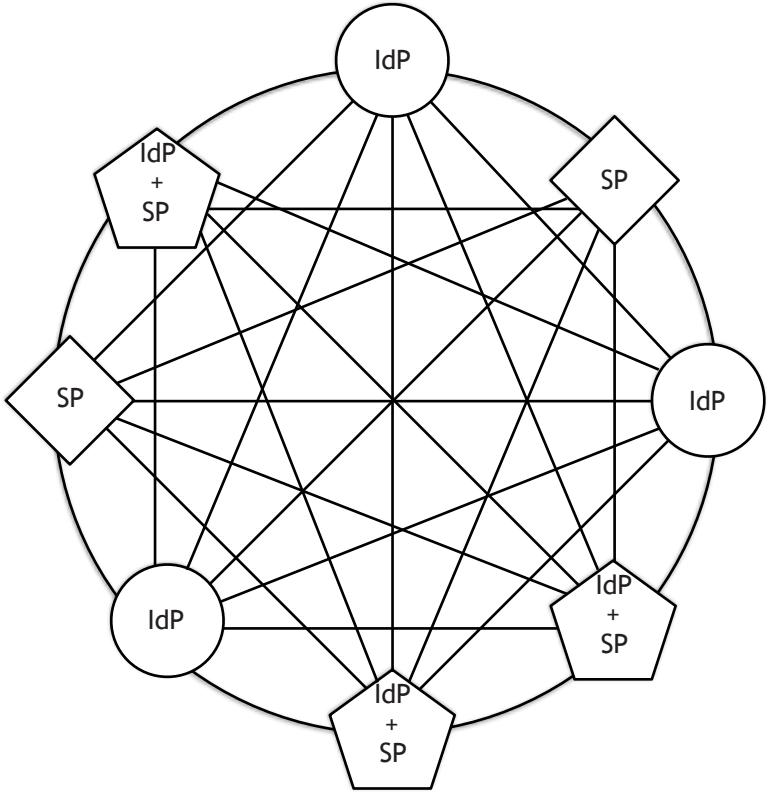
Service Provider. *Often*: a vendor with services or data of interest. *Often*: a campus providing a service to others in a scholarly context. *Sometimes:* a campus serving itself. Contributes metadata.



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.

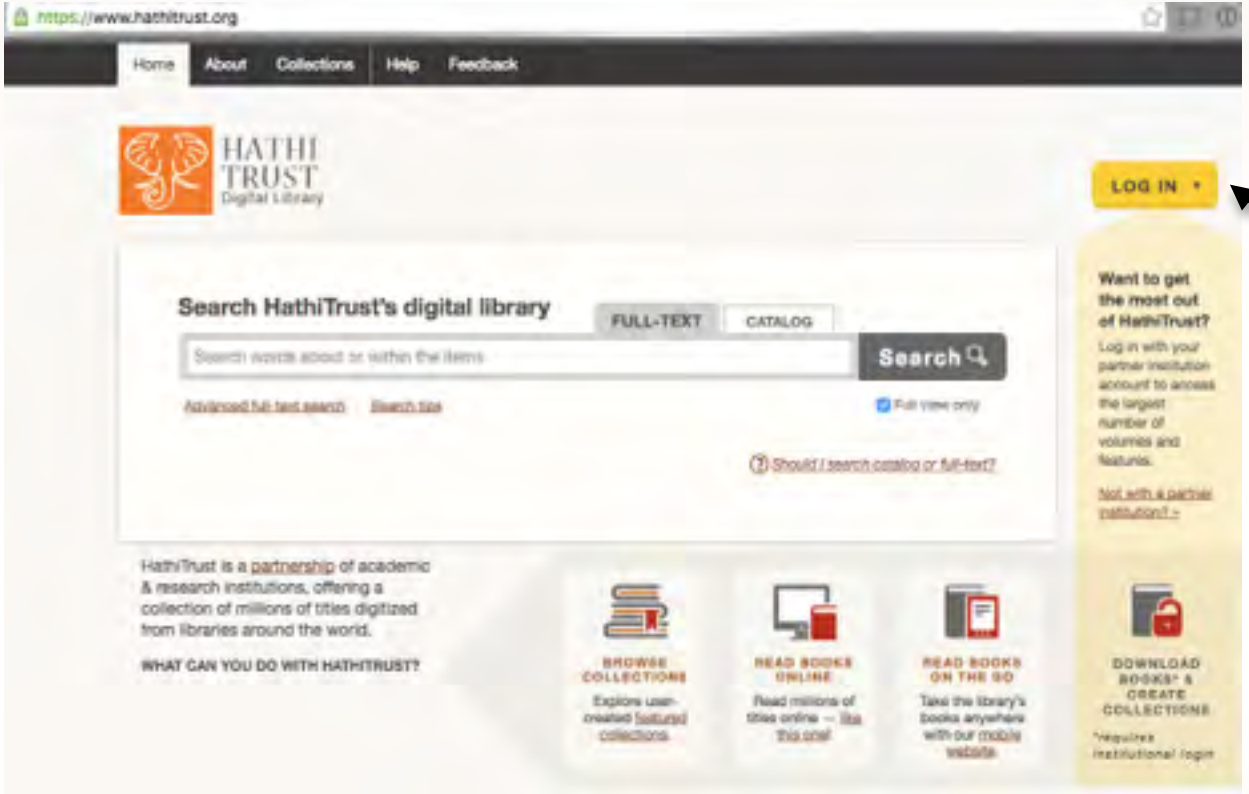


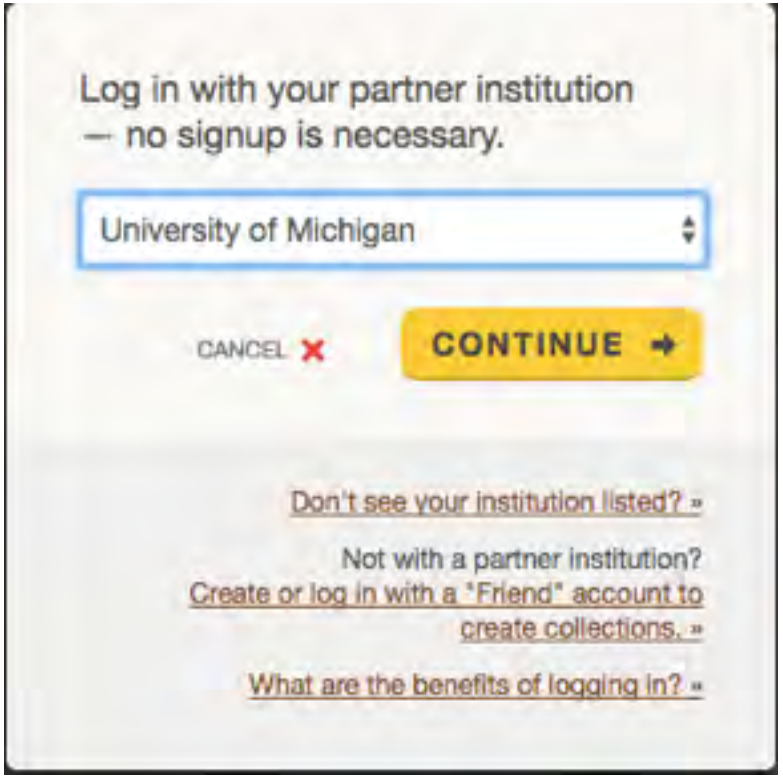
- *Looks* like a hub and spoke network
  - daily, nodes on the network download the federation map from the federation operator
  - the trust network is *built* in a hub and spoke fashion

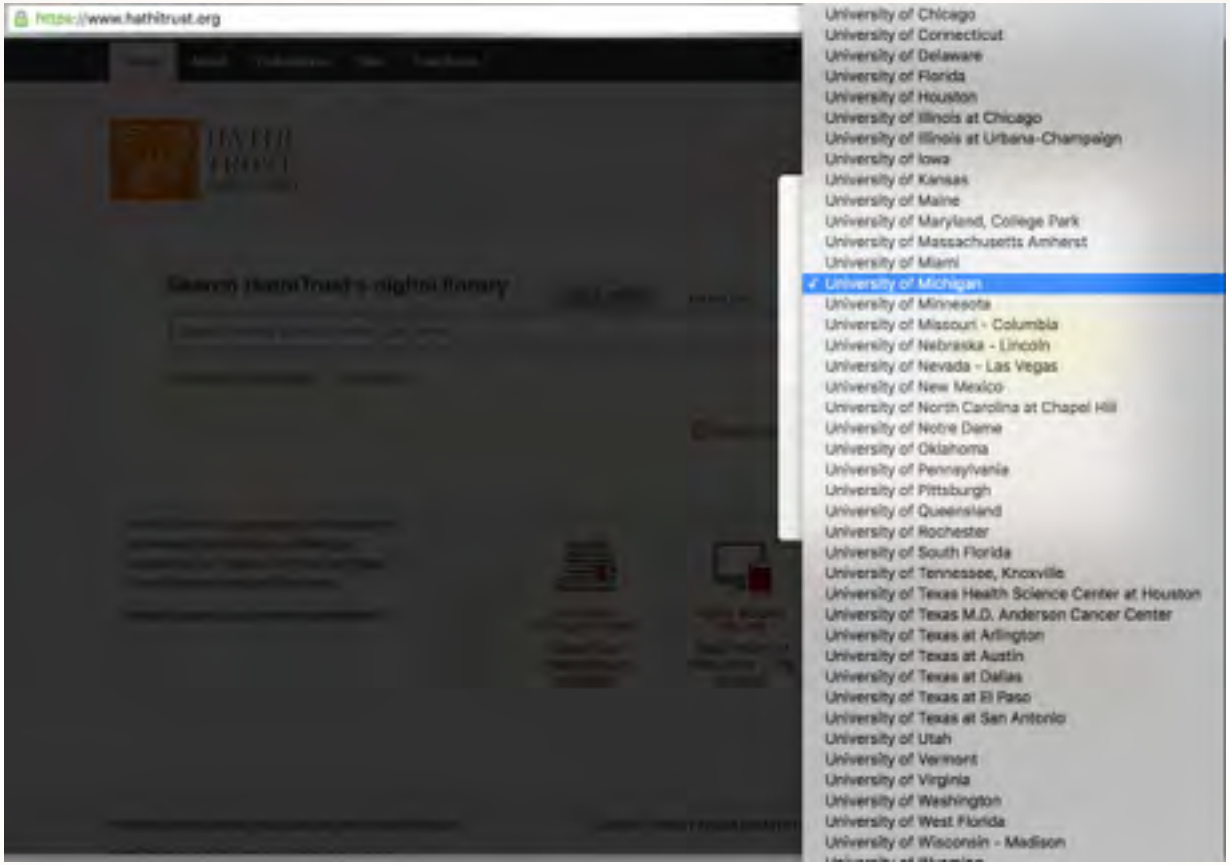


- *Acts* like a mesh network
  - once nodes have the “map”, nodes interact with one another directly
  - We call the “federation map”, the InCommon metadata or sometimes the InCommon metadata aggregate

An example


https://www.hathitrust.org
Home
About
Collections
Help
Feedback
HATHI TRUST
Digital Library
LOG IN
Search HathiTrust's digital library
FULL-TEXT
CATALOG
Search
Advanced full-text search
Search tips
Full view only
Should I search catalog or full-text?
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 partner institution? »
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

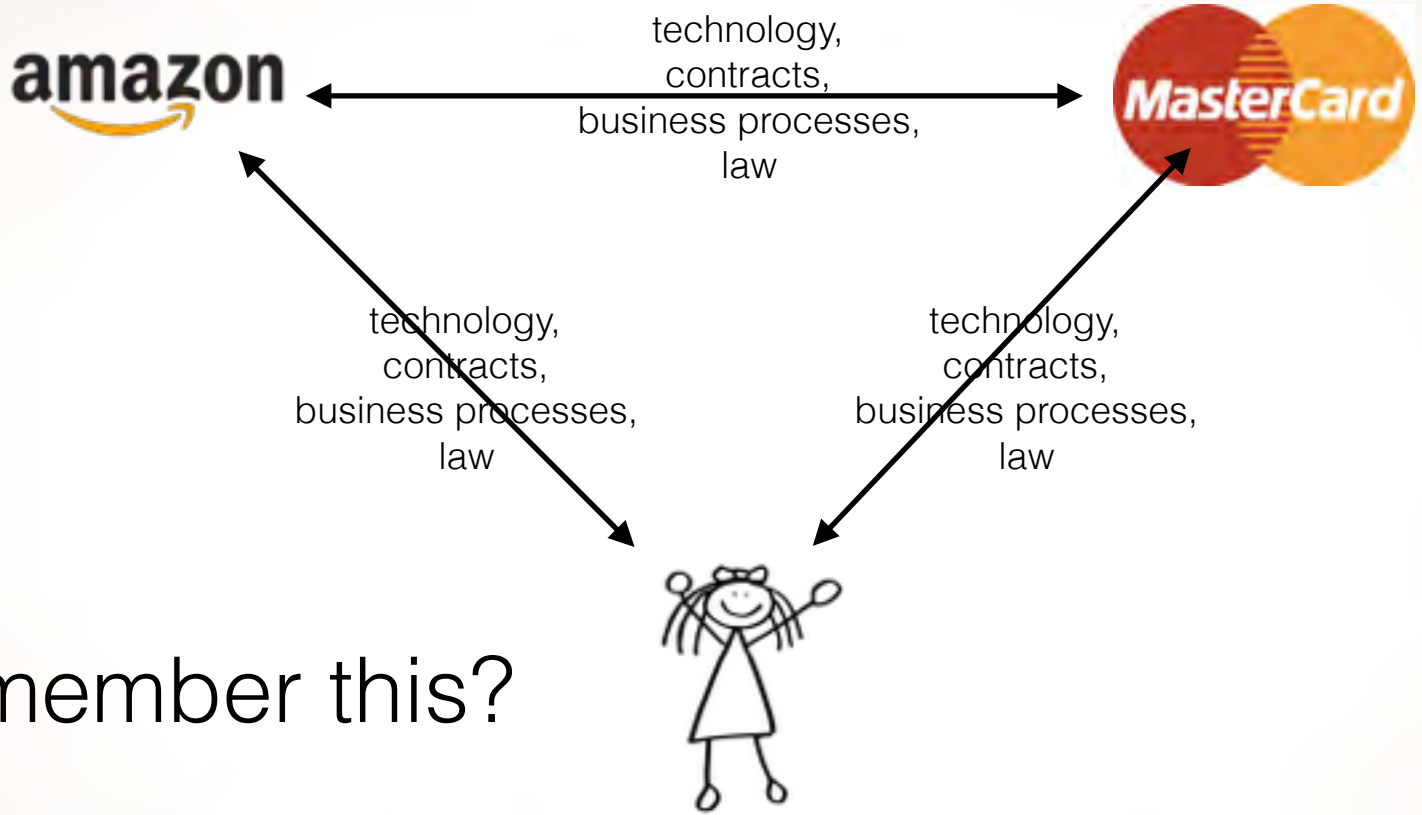

Log in with your partner institution
— no signup is necessary.
University of Michigan
CANCEL
CONTINUE
Don't see your institution listed? »
Not with a partner institution?
Create or log in with a "Friend" account to
create collections. »
What are the benefits of logging in? »



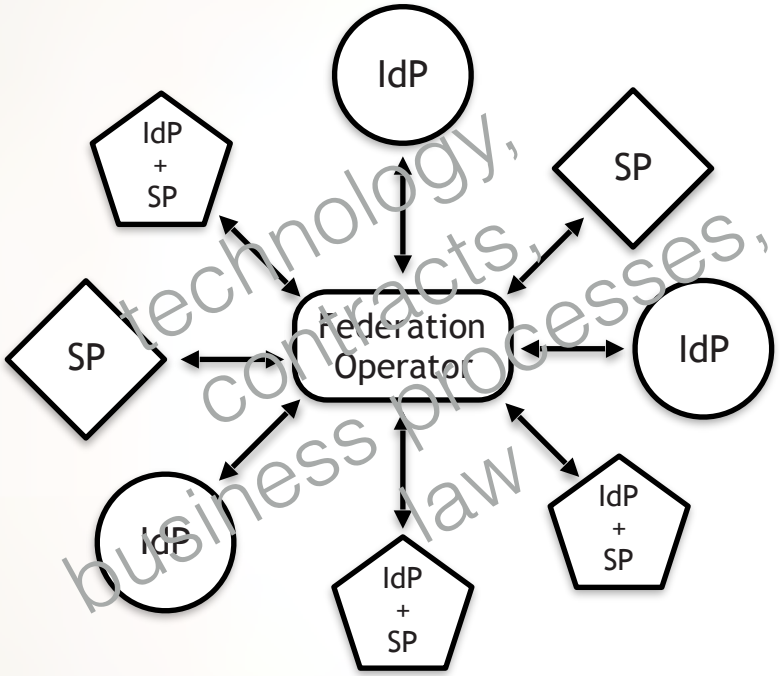
That's me!

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

INCOMMON:
FEDERATION OPERATING POLICIES AND PRACTICES

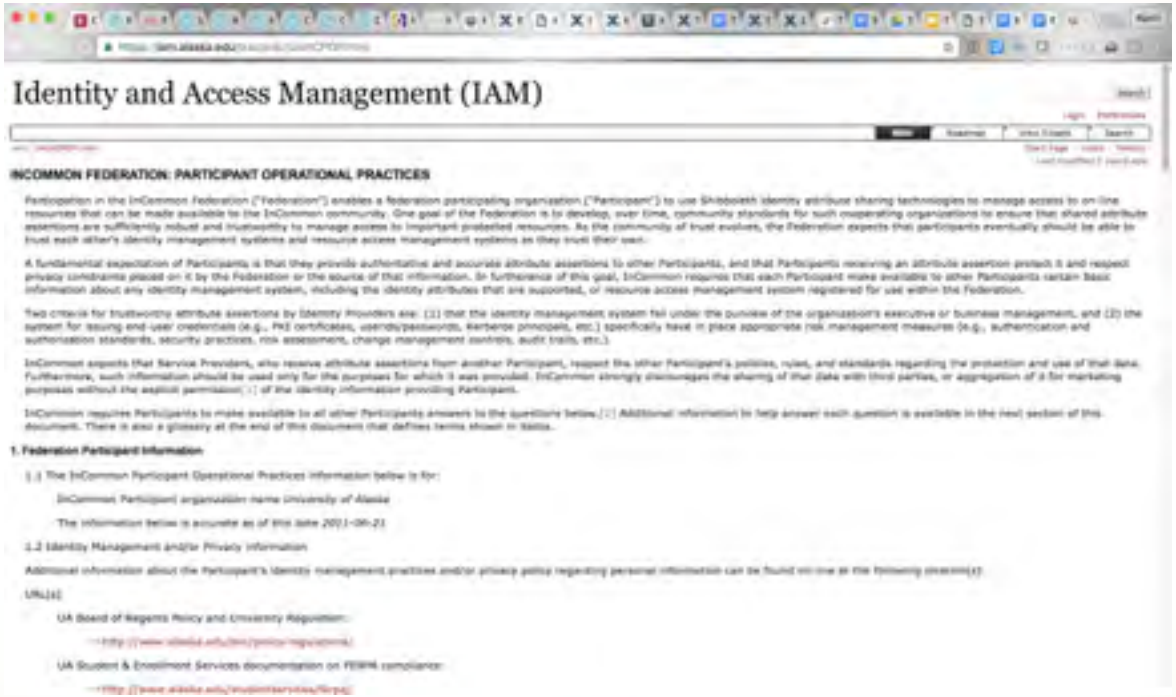
TABLE OF CONTENTS

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/UAInCPOP.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 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 issuing end-user credentials (e.g., PKI certificates, userids/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 [1] of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below.[2] 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 2011-04-21

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 URL(s):

UA Board of Regents Policy and University Regulation:

http://www.alaska.edu/bor/policy-regulations/

UA Student & Enrollment Services documentation on FERPA compliance:

http://www.alaska.edu/studentservices/ferpa/

box

carmen WIKI

InCommon

LEARN MORE WITH LYNDA.COM

lynda.com

FOPP, PA, POP

technology,
contracts,
business processes,
law

University polices,
digital lifecycle practices


MEMENTO

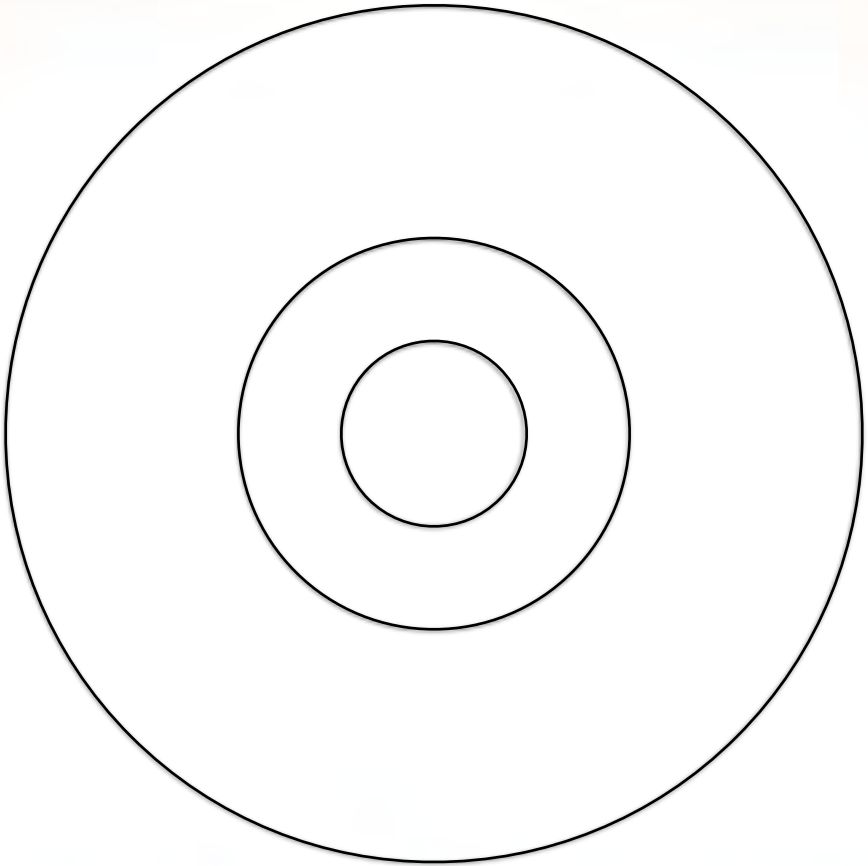

Why?

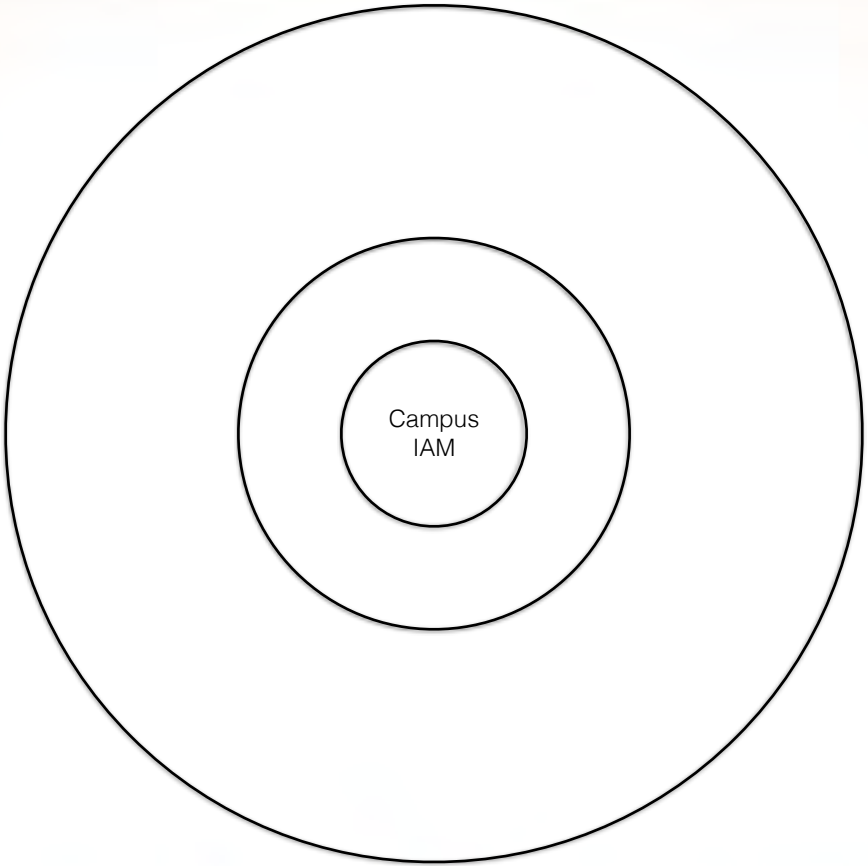
Why?

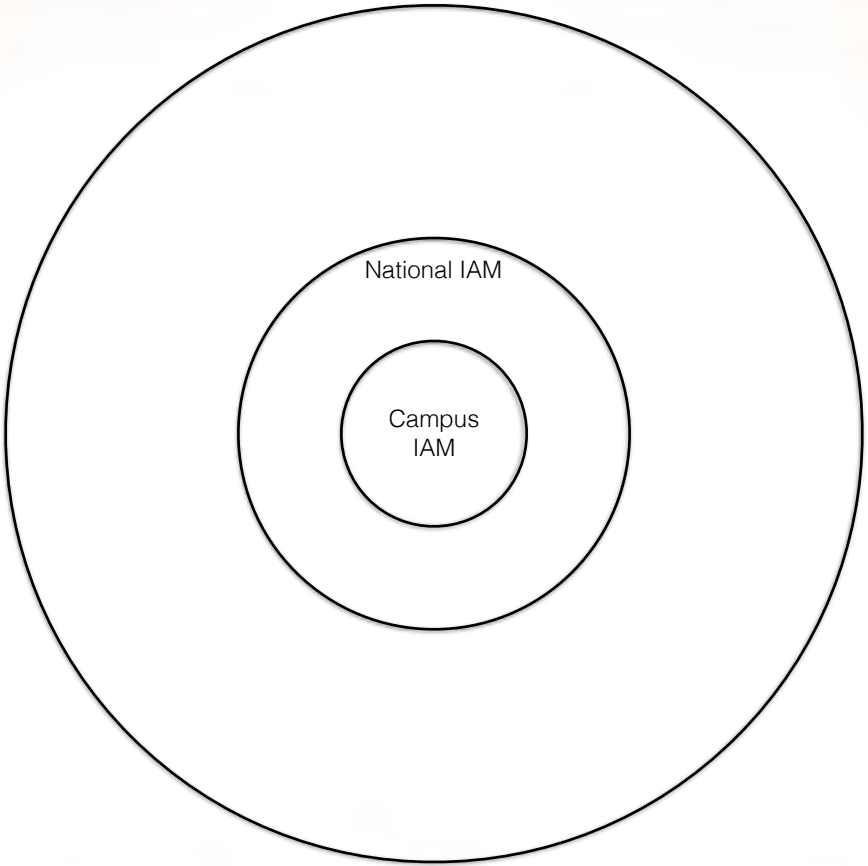
- People: use familiar, trusted identifiers to consume and access information and workflows relevant to their scholarly journey. Enable future access by being at an institution that vibrantly participates in a collaboration enabling infrastructure.
- University/IdP IT staff: Publish metadata one time,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

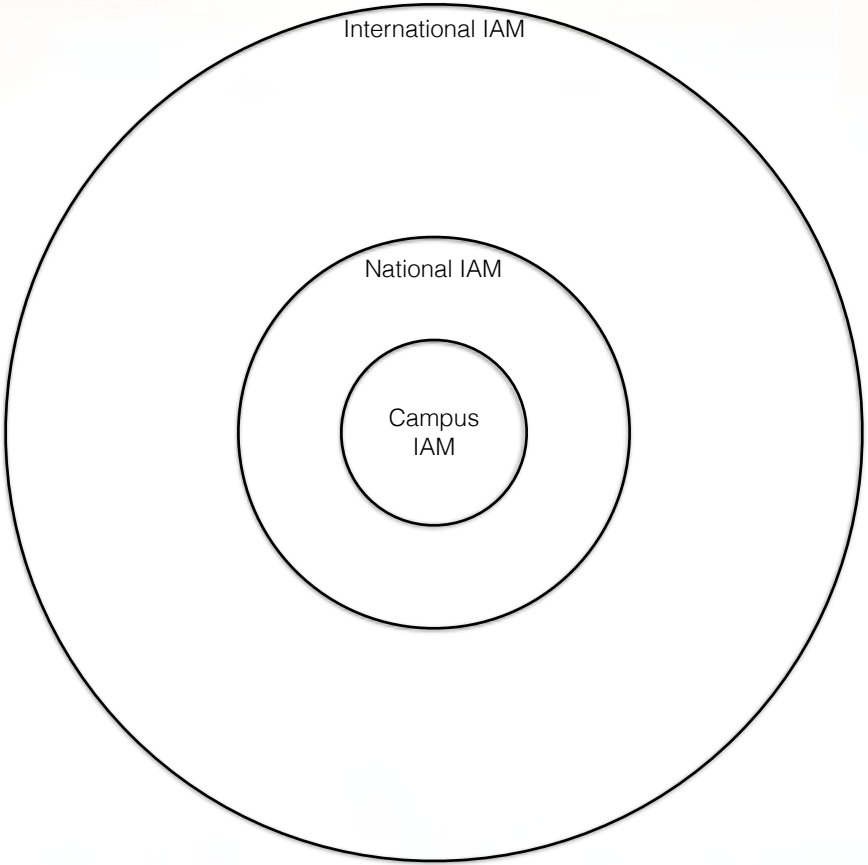
One last thing

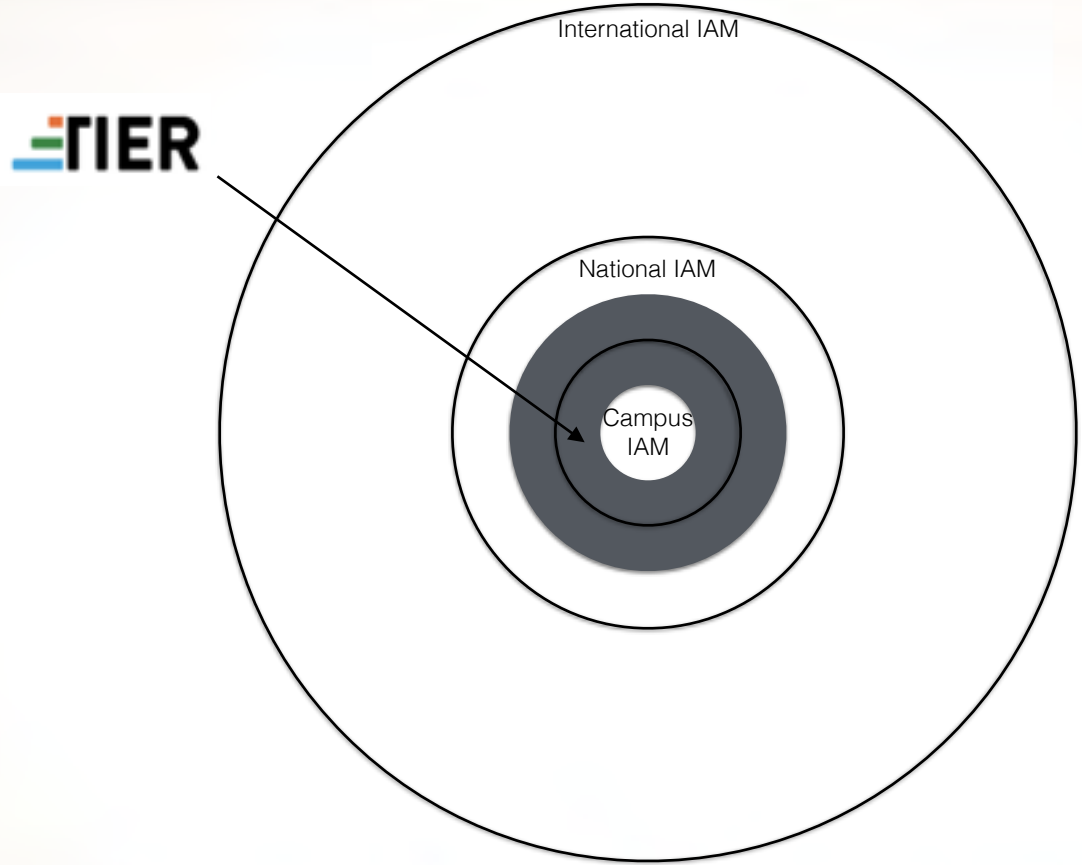
How does everything fit together?
(An IdP perspective)

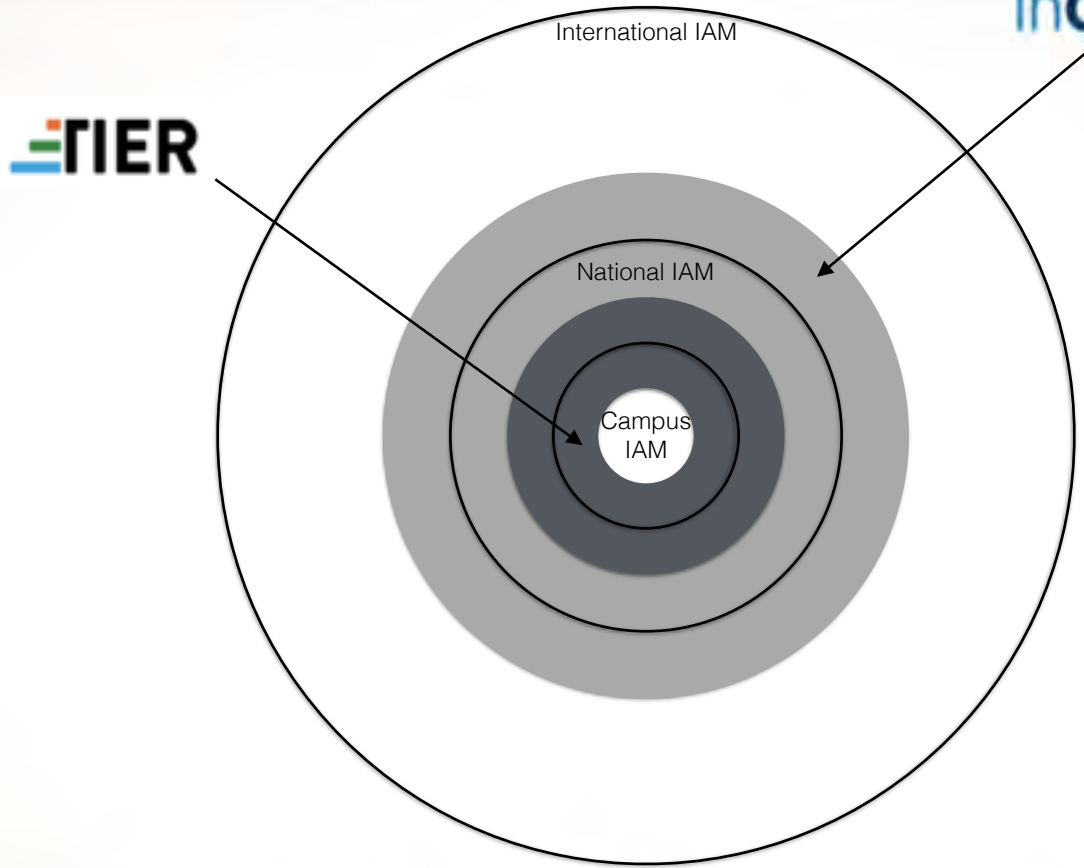


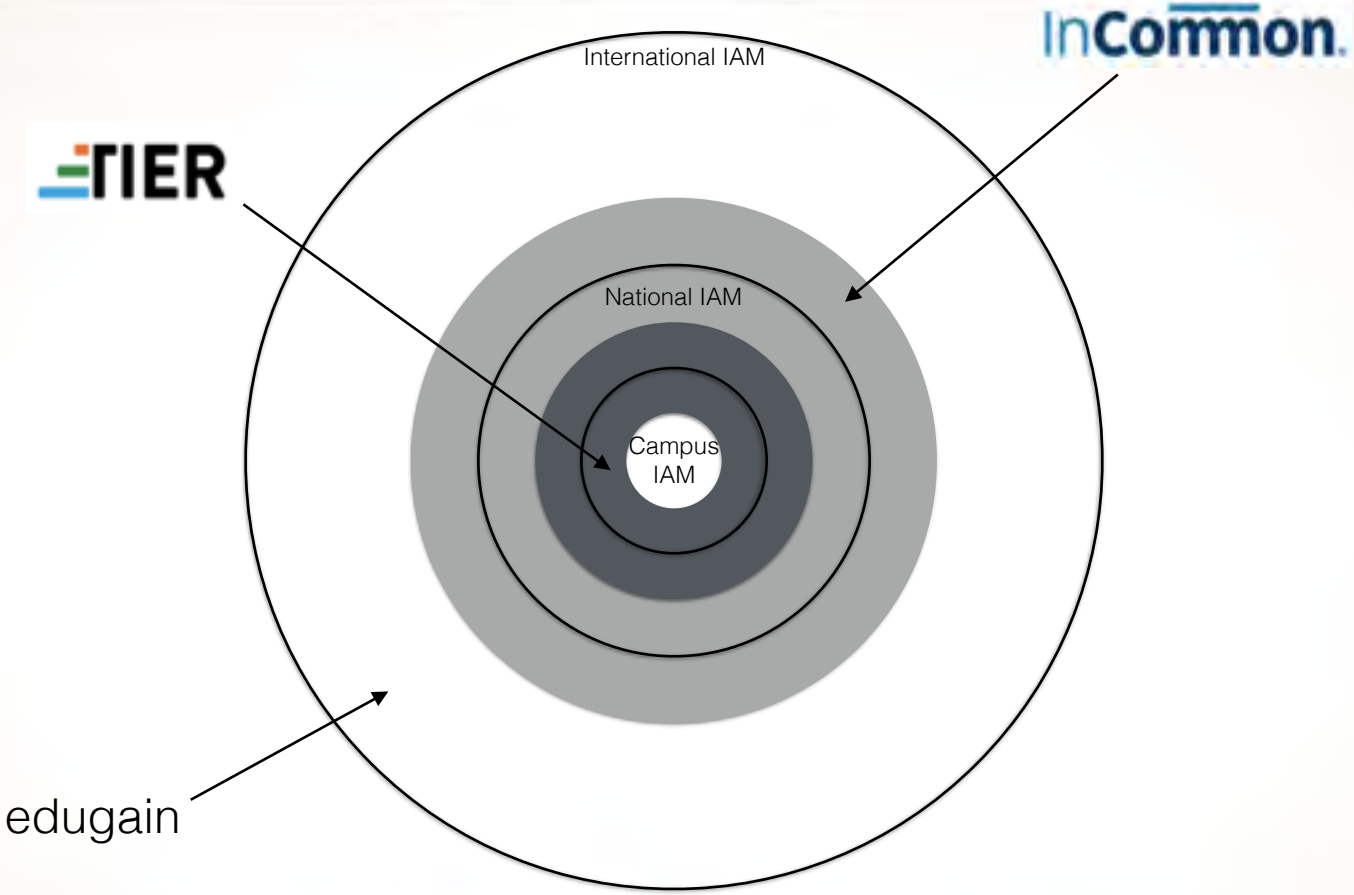

Campus
IAM


National IAM
Campus
IAM


International IAM
National IAM
Campus
IAM


TIER
International IAM
National IAM
Campus
IAM


InCommon
TIER
International IAM
National IAM
Campus
IAM


InCommon
TIER
International IAM
National IAM
Campus IAM
edugain