Day CAMP: Getting Started with the InCommon Federation

The Why and What of Federations

John Ellis, Emory University
Jacob Farmer, Indiana University
Elliot Kendall, Emory University
Ann West, InCommon/Internet2

November 4-5, 2010 Atlanta

A Bedtime Story

It's 3:00 am and Bianca is sitting in a 24 hour Starbucks in the spring semester of her senior year, working on her Physics 456 homework. In a browser, she clicks on the link to the course management system, logs in with her University web single sign-on userid and password, and starts viewing the course information.

Next, she clicks on the homework link hosted by a third-party provider and "Welcome Bianca" appears along with her new homework assignment for that class. After finishing that, she decides to check her loan status and surfs to the web site of her financing agent. She clicks "Access your record" and is presented with an aggregation of her loan liability without having to identify herself or login.

In April, Bianca graduated. One day she was a student and the next, an alumna. She noticed her access changed too. She now could get to an alumni networking service where she put out a query about apartments in the Bay Area. Her loan status had changed on the financing agent's site. She now was out in the wide world of opportunity and responsibility.

Looking for any of these?

- Business Functions
  - Benefits
  - Human Resources System
  - Career Services
  - Asset management
  - Talent management
  - Visas & INS compliance
  - Mobile alerts
  - Travel management
  - Energy management
  - Surveys and market analysis
  - Student loan eligibility verification

- Learning and Research
  - Journals (Lots of Content)
  - Databases and analytical tools
  - Multi-media access
  - Homework labs
  - Quiz tools
  - Plagiarism detection
  - Software downloading
  - Alcohol awareness education
  - Student travel discounts
  - Transportation and ride-share services.
  - Course sharing and video streaming
  - NSF/NIH Grant Submission

The New IT

- IT is shifting from developing technical solutions to enabling efficient solutions through a mix of sourced technology services.
- How do we do that?
  - Embrace change
  - Streamline adoption
  - Provide integration
  - Facilitate reuse
- While protecting privacy, reducing institutional risk, ensuring continuity, meeting regulatory compliance and high availability requirements.

....And do it all for less $$$.

What’s your story?

Identity Management

Who are you?
(identification)

How can you prove it?
(authentication)

Key Roles

Three roles are involved in gaining access to a resource:

- Subject (i.e. user) – The person identified and the subject of assertions (or claims) about his or her identity.
- Identity Provider – Typically the college or university that maintains the identity system, identity-proofs the subject and issues a credential. Also provides assertions or claims to the service provider about a subject's identity.
- Service Provider (sometimes called the relying party) – Owner/provider of the protected resource to which the subject would like to access. Consumes the assertion from the identity provider and makes an authorization decision.

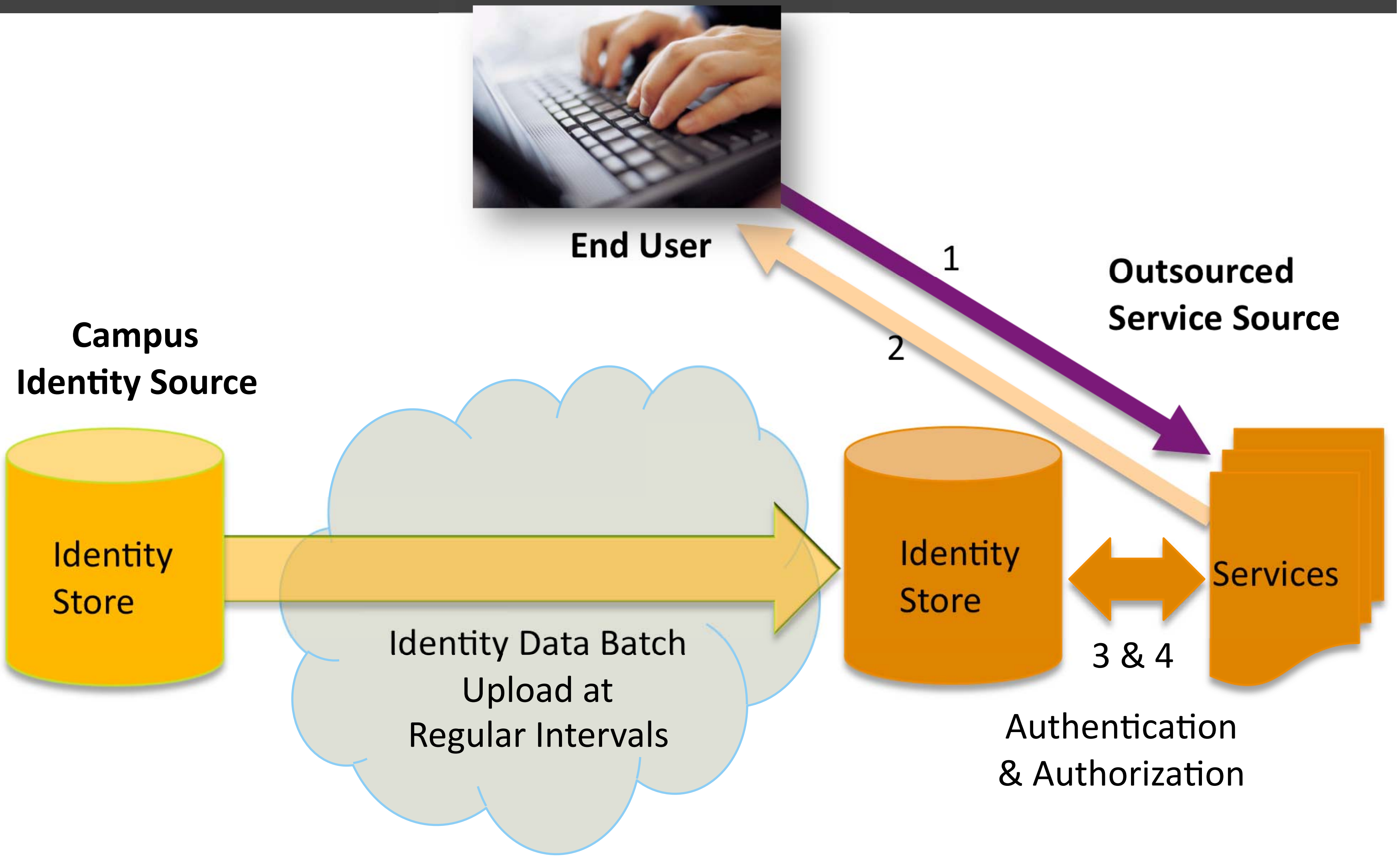
Traditional Two-Party Approach

- The Relying Party (i.e., college/university) must do it all –
  - Identify the employee/student/guest
  - Determine whether person is acceptable for specified purpose
  - Issue a credential (e.g., employee/student ID card, UserID)
  - Establish method to correlate identified individual to the credential – e.g., a picture, a password
  - Authenticate individual for remote access e.g., does picture match?, is password correct?

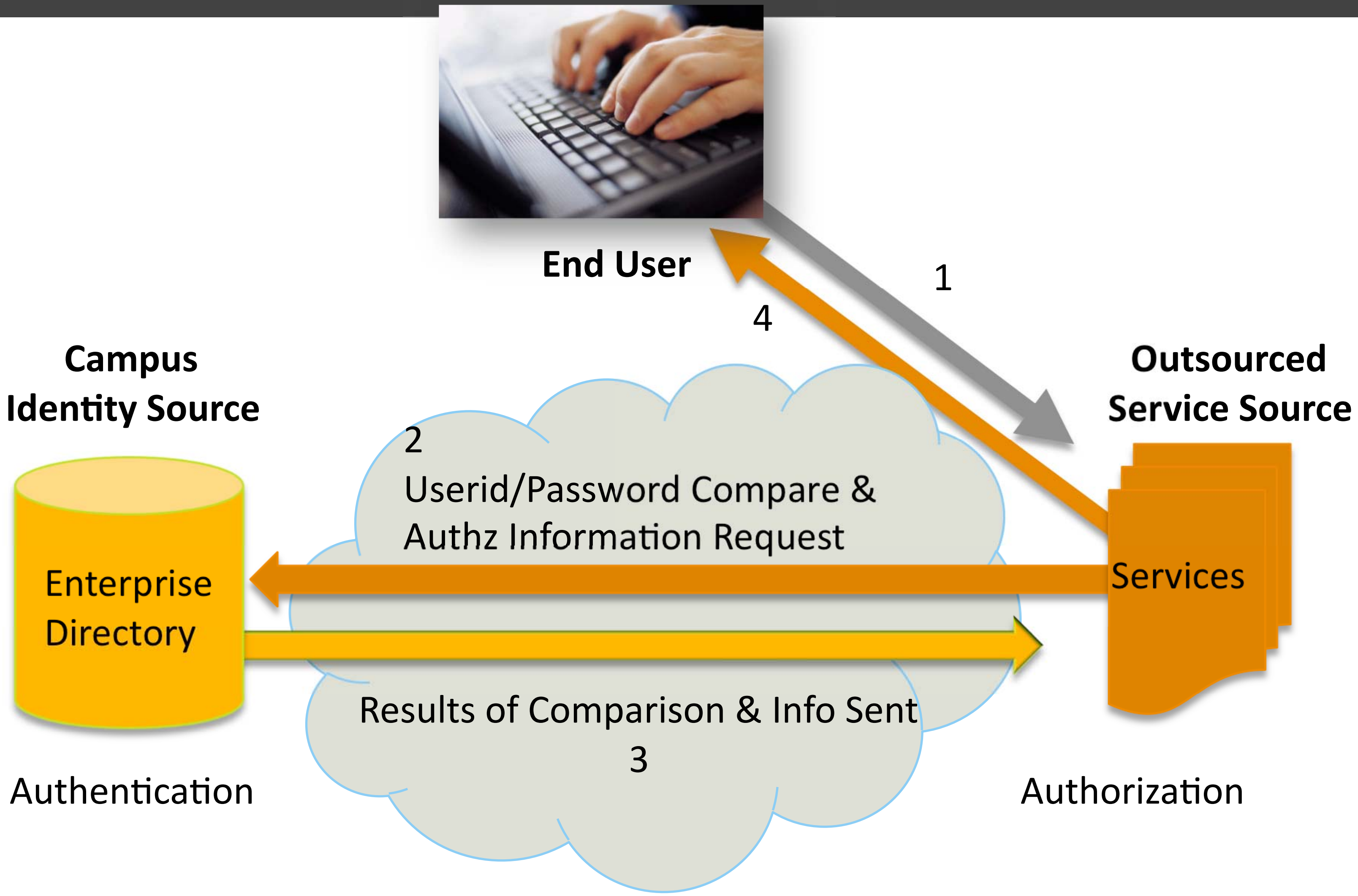
But Here’s The Problem

- How many off-campus applications do you have?
- How do these service providers
  - Verify the identity of your community?
  - Know who’s eligible to access the service?
  - Know the subject is active and hasn’t left the institution?
- How comfortable are you with the security and privacy of the identity data?

Data Upload


End User
1
2
Outsourced
Service Source
Campus
Identity Source
Identity
Store
Identity Data Batch
Upload at
Regular Intervals
Identity
Store
Services
3 & 4
Authentication
& Authorization

Directory Access



End User

1

4

Campus Identity Source

Outsourced Service Source

2

Userid/Password Compare & Authz Information Request

Enterprise Directory

Services

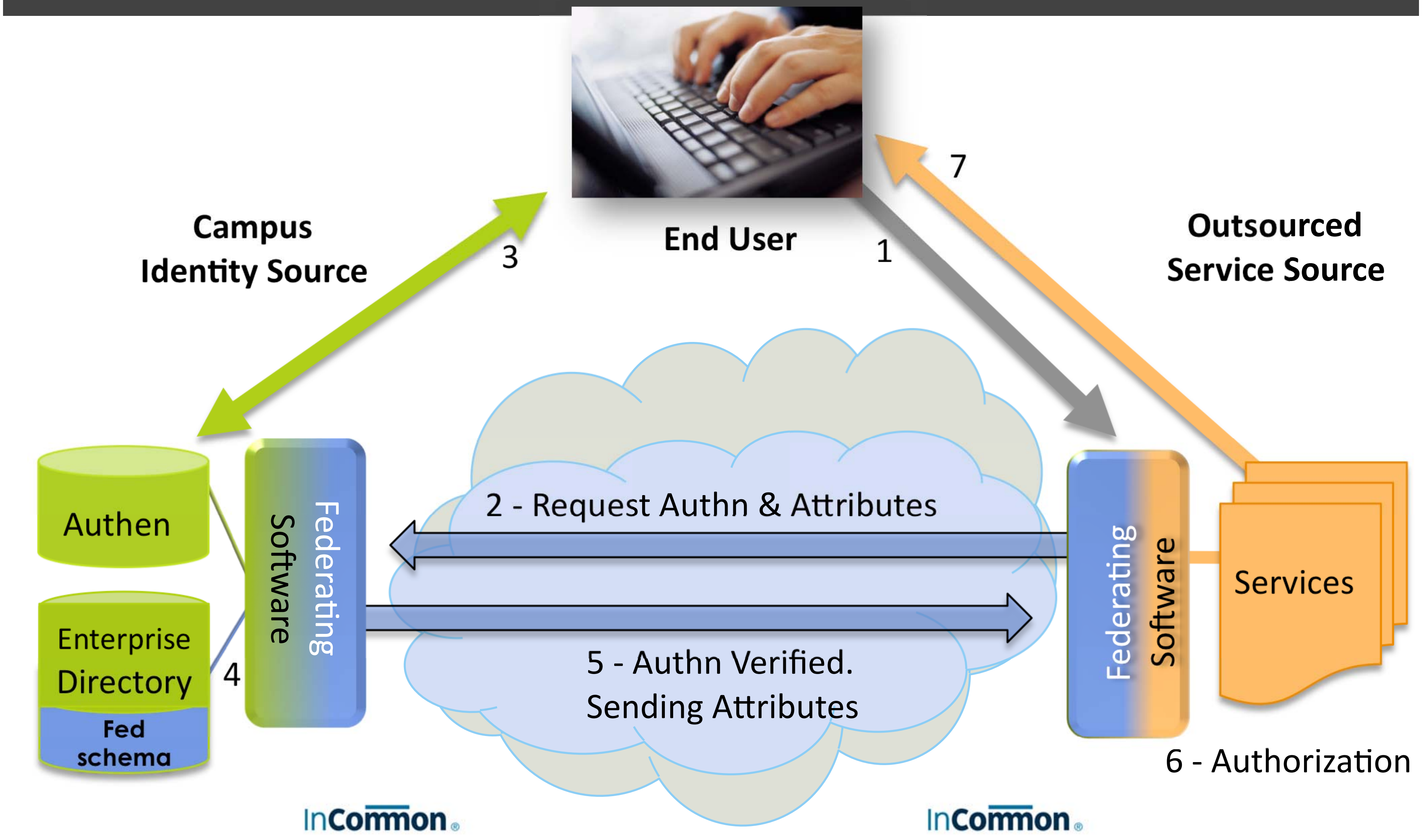
Results of Comparison & Info Sent

3

Authentication

Authorization

Federated Identity



The Answer:
Federated Identity Management

- Federation: An association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.
- All participants in a federation agree on the same policies and procedures related to identity management and the passing of attributes.
- Instead of one-to-one relationships, the federation allows one-to many relationships.

Federated Identity Management

- Users no longer register with the service provider, using their university credentials for transactions
- Single sign-on convenience for users
- Identity provider does the authentication; service provider does the authorization
- Attributes are the key – enable access while maintaining privacy and security

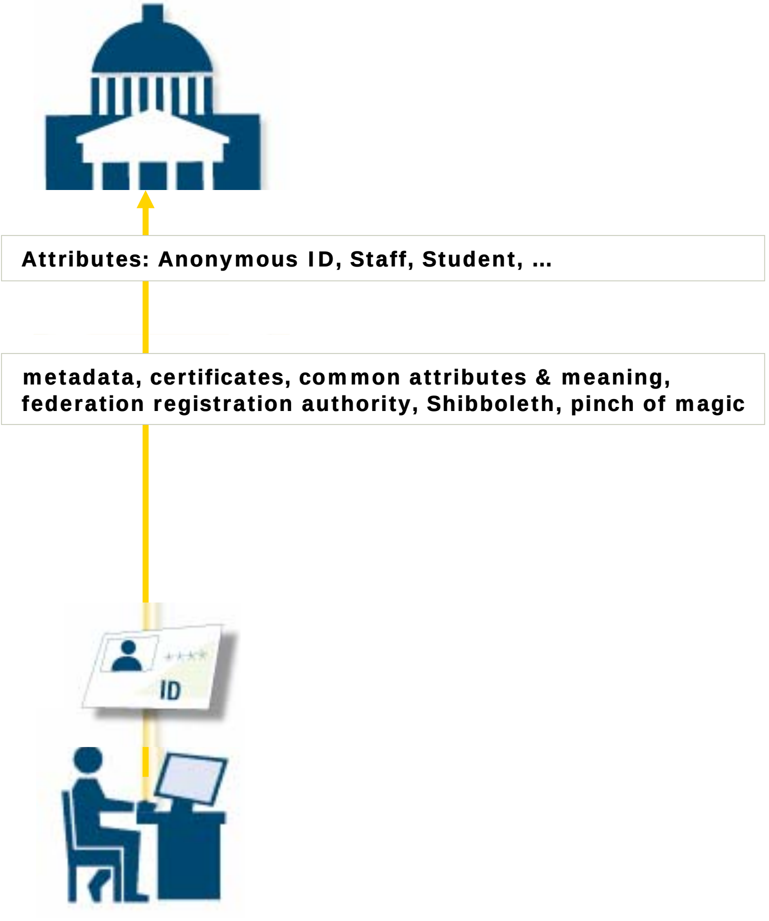
Brief Federated Access

4. If attributes are acceptable,
   Access is granted!

3. Privacy preserving exchange

2. Federation-based Trust Exchange to establish and verify partners & locations

1. Single Sign On : Log In to existing home system



Attributes: Anonymous ID, Staff, Student, …

metadata, certificates, common attributes & meaning, federation registration authority, Shibboleth, pinch of magic

SAML and Shibboleth

- Security Assertion Markup Language (SAML)
  - Standard for the formation and exchange of authentication, attribute, and authorization data as XML.
- Shibboleth Single Sign-on and Federating Software
  - Open source software uses SAML to perform this exchange across boundaries

Getting Started

How Do I Start?

- **Identify your business case (Thursday)**
- Review your campus IdM system (Thursday)
- Post your Participant Operating Practices (Thursday)
- Install/Configure a SAML2 Identity provider (Friday)
- Support the eduPerson schema (Friday)
- Sign/Pay InCommon Agreement and Fee (Friday)

Federating Your Campus Identity Management System

Jacob Farmer, Indiana University