InCommon® camp
Campus Architecture & Middleware Planning

The Big Picture - Introduction to Federated Identity Management

June 21, Raleigh, NC

Larry Conrad, Vice Chancellor for Information Technology and Chief Information Officer, University of North Carolina at Chapel Hill

Mark Scheible, Manager of Identity and Access Management, North Carolina State University

Pre-Conference Meeting Schedule

8:30 AM – Introductions

8:50 AM - Session 1: Overview of Concepts

9:20 AM – 1st Breakout Session – Discussion and Report Out

9:55 AM - BREAK (15 min)

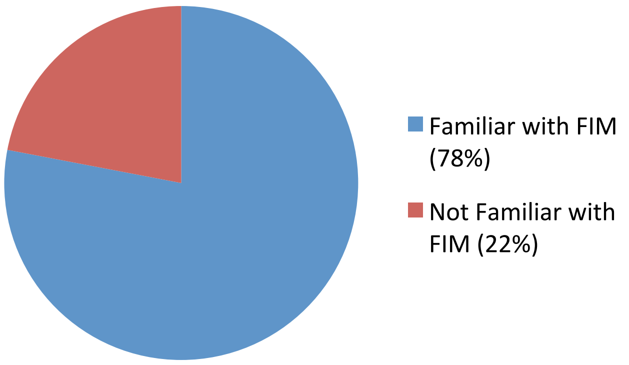
10:10 AM - Session 2: Policy and Security

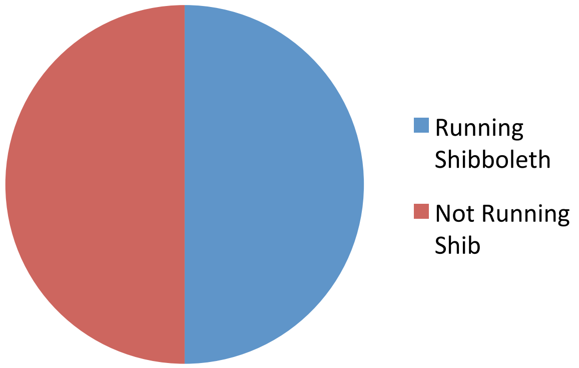
10:40 AM – 2nd Breakout Session – Discussion and Report Out

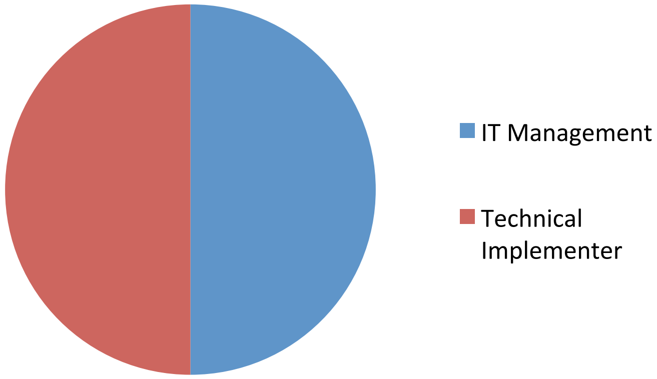
11:15 AM – Wrap-up: Q&A

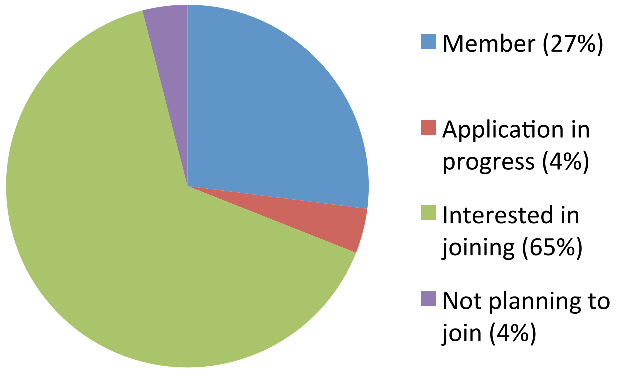
Survey Results (tweaked)

Familiar (Very and Somewhat) with IAM – 100%









Survey Results (Requested Topics/Questions)

1. Shibboleth and Microsoft (FIM?)
2. Managing multiple relationships (affiliations?) per individual and implications for authorization(s) (policy decision – primary affiliation)
3. Influencing business processes (HR and Student) to enable data-driven provisioning (de-provisioning could be an added benefit!)
4. How [where] do institutions capture LoA in their local data models? In their SoRs or only in their [enterprise] directory or data store? (capture and use?)
5. Advice on choosing an IAM software suite for an institution? (discussion lists and collaboration groups)
6. A roadmap for moving from a centralized but fragmented and poorly documented IdM program to one that is compatible with InCommon requirements (you're NOT alone)
7. Implementation Roadmap (for ?) – InC Toolkits, Shibboleth Checklist

* Discussion lists for: IDM, Shibboleth-Users, other MI products

Introductions

1. Who are you and what's your role?

2. Where are you from?

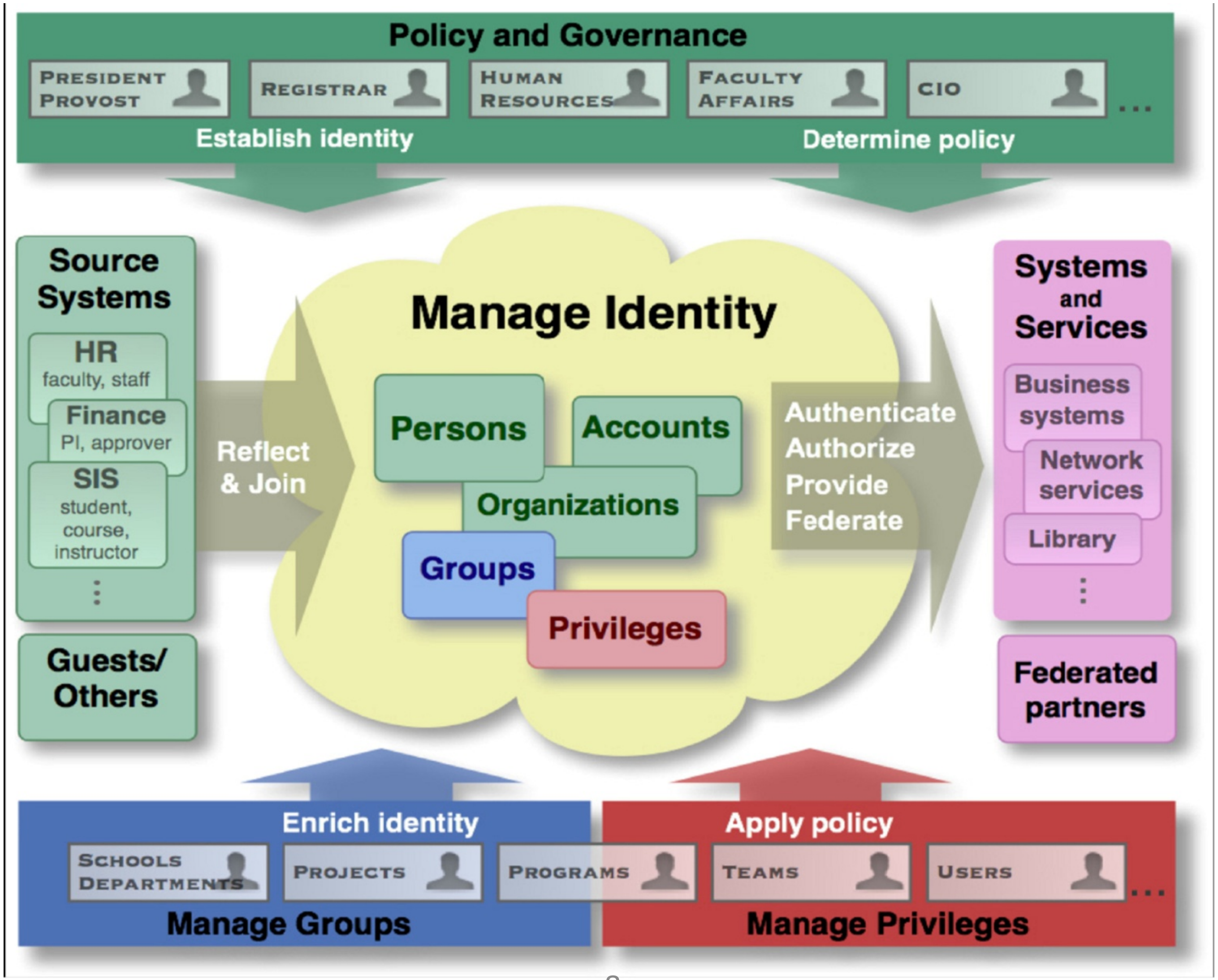
3. Why are you here (Pre-Conference)?

Overview of IAM and FIM Concepts

Identity and Access Management (IAM)

- Policies and Governance
- Authoritative Data Sources (Student, HR, ?)
- Establishing and managing user identities
- Identity Data – Enterprise Directory Service
  - Person Registry – unique record per user
  - Identity Attributes
  - Groups/Roles
  - Entitlements
- Authentication – Credential(s)
- Authorization

Internet2 Model of IAM



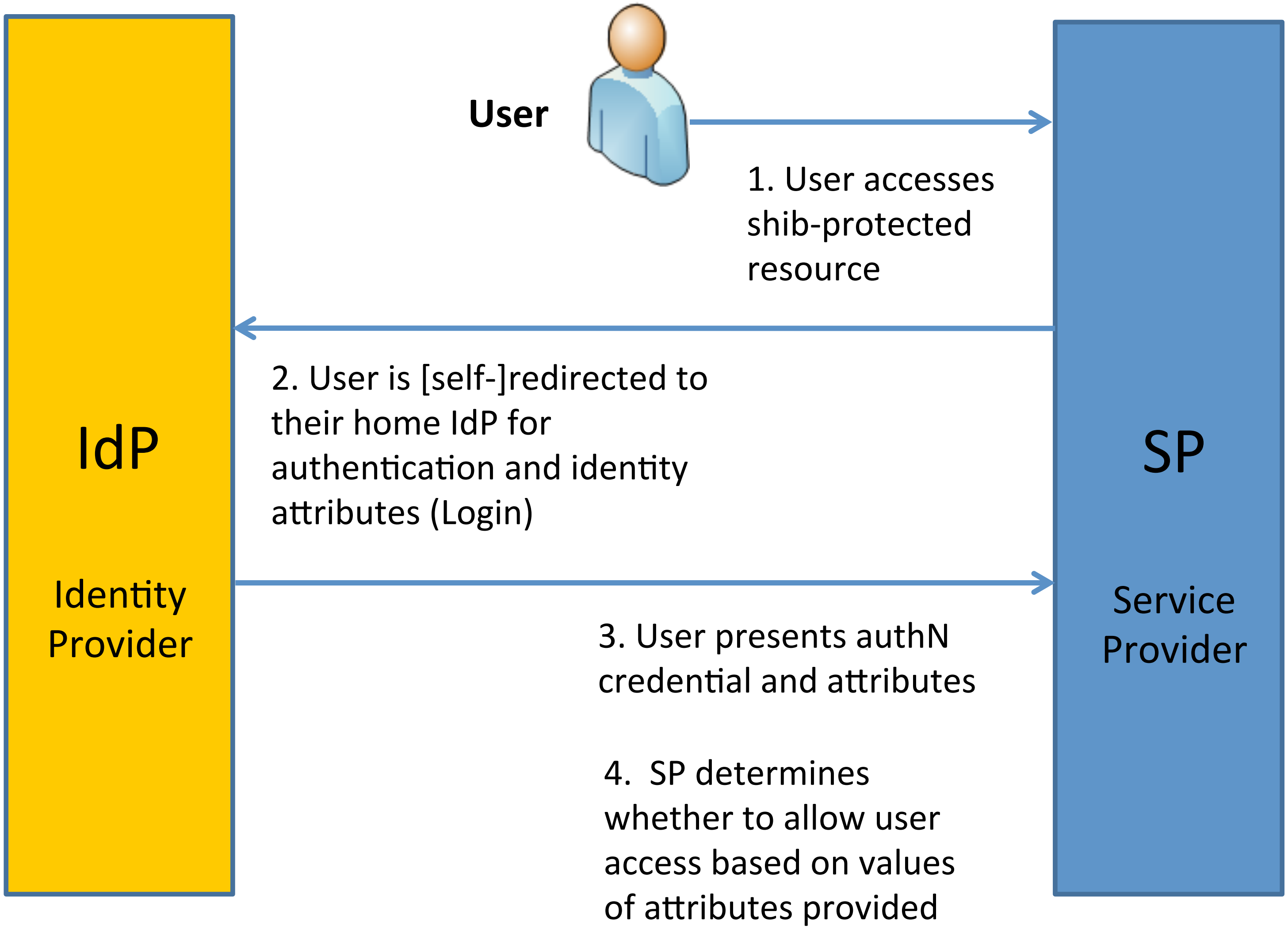
Federated Identity Management (FIM)

- Authenticate Locally - Access Globally
- Within a Federation
  - Trusted identity information from others
  - Presumed "authoritative"
  - Privacy protected when needed
  - Saves lots of work

Shibboleth. - based on SAML standards

- Identity Provider (IdP)
- Service Provider (SP)

How Does it Work?



User

IdP

Identity Provider

SP

Service Provider

1. User accesses shib-protected resource

2. User is [self-]redirected to their home IdP for authentication and identity attributes (Login)

3. User presents authN credential and attributes

4. SP determines whether to allow user access based on values of attributes provided

Attributes (eduPerson)

Some Common eduPerson Object Class Attributes

- eduPersonPrincipalName [EPPN] (single)
- eduPersonAffiliation (multi)

  (faculty, student, staff, alum, member, guest etc.)
- eduPersonScopedAffiliation [EPSA] (multi)
- eduPersonPrimaryAffiliation (single)
- eduPersonEntitlement (multi)

Examples:

student@ncsu.edu; guest@ncsu.edu (EPSA)

fsf@unc.edu; jdoe4@unc.edu (EPPN)

A Bedtime Story for Student Services

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.

She takes a deep breath, wondering if any of those job applications had yielded an interview. She clicks on her shortcut to the job placement service and again is presented with the status of her applications, without having to identify herself. One company is requesting an interview, so Bianca purchases a cheap airline ticket offered by an online service that sells only to students. In the past, she had to provide proof of enrollment, but now the technology handles this in the background.

Bianca occasionally wonders what the institution is giving out to other service providers like the financial aid, job placement, and other companies on her behalf. She cares about her information and doesn’t like her address and cell number available. She decides to check how this is done and clicks on the “Control your information” link provided on the web single sign-on page. She is presented with the campus information release policy that includes the policy and specific information about online transactions. Bianca knows that each of the transactions she has completed tonight implied that the institution was passing identity information on her behalf to the other sites so they could authorize her to access her information there. She opens the list of sites that she has visited and reviews the type of information that is sent. No, that all looks okay to me. She notices that there’s a music site that her institution has an agreement with, but she doesn’t use. She clicks the “do not pass information” box, knowing she now can’t access the service, but that they won’t know anything about her either.

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.

UNC
INFORMATION
TECHNOLOGY SERVICES

Federated IdM
CIO Perspective

Larry Conrad
Vice Chancellor for IT and CIO
UNC Chapel Hill
June 17, 2010

Key Benefits

- Efficient collaboration with a spectrum of entities in and out of higher education
- Ability to deliver services more quickly
- For example, the new course evaluation SaS offering at UNC
- Facilitates delivery of cloud-based services
- Supports improved/eased integration with commercial service providers

Key Benefits

- Ease of providing access to center-of-excellence or working groups, regardless of where the services reside
- Supporting collaboration across institutions for faculty (and others)
- Fine-grained (role-based) access to resources and services
- Access to a pre-defined “trust fabric”

Key Benefits

- Ability to provide access without accepting further risk of exposing private/sensitive data
- Access to tools such as Grouper (Internet2-MI), which helps manage groups
- Leverage InCommon with commercial providers to get them to adopt standards based provisioning

Breakout Session 1

Question:

Why is Federated Identity Management important to your organization and what business challenges does it address?

(20 minutes to discuss – 15 minutes for group reports)

InCommon® camp
Campus Architecture & Middleware Planning

Break!

NC STATE UNIVERSITY

Policy and Security in Federated Identity Management

(Things you need to think about)

oit

IdM Governance

It's critical to establish a governance function for IdM to allow your community to "socialize" the relevant issues.

IdM Governance

It's critical to establish a governance function for IdM to allow your community to "socialize" the relevant issues.

IdM Governance Issues (Sample Set)

- Figuring out the various roles
- What data elements are needed (EduPerson add-ons)
- Who gets access to what data
  …and who decides
- Who do you federate with
  …who do you trust
- Who gets to utilize federated access
- Securing IdM data

Are You Ready?

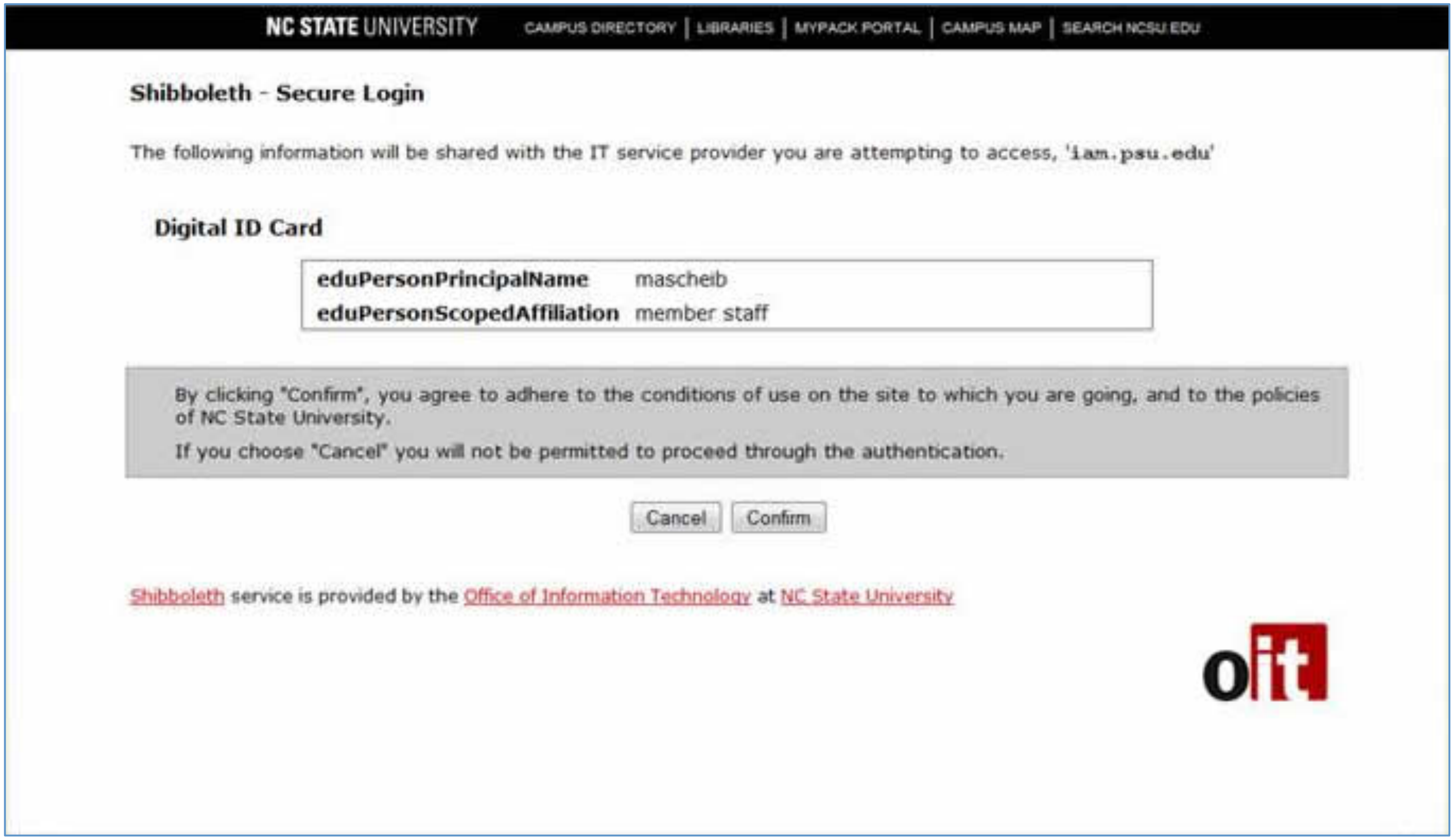
Policy-related Decisions

- FERPA
- Privacy Laws
- Attribute Release Policy (ARP)

Implementation Decisions

- Authentication environment
- User Attributes
- Authoritative Source / Data Integrity
- User Approval of Attribute Release (uApprove)

uApprove Digital ID Card


NC STATE UNIVERSITY
CAMPUS DIRECTORY | LIBRARIES | MYPACK PORTAL | CAMPUS MAP | SEARCH NCSU.EDU

Shibboleth - Secure Login

The following information will be shared with the IT service provider you are attempting to access, 'iam.psu.edu'

Digital ID Card

eduPersonPrincipalName	mascheib
eduPersonScopedAffiliation	member staff

By clicking "Confirm", you agree to adhere to the conditions of use on the site to which you are going, and to the policies of NC State University.

If you choose "Cancel" you will not be permitted to proceed through the authentication.

Shibboleth service is provided by the Office of Information Technology at NC State University

What's Required for Federation?

Identity Provider (IdP)

- Data repository of who your users are with basic attributes (directory or db)
- Web-based AuthN
- Federation Software (can use Shibboleth for above)
- Documented IdM Processes, Policies and Approaches
- Often a Contract/Agreement for participation
- Submit Metadata

What's Required for Federation?

Service Provider (SP)

- Ability to use attributes provided by IdP (AuthZ)
- Federating Software
- Documented SP Processes, Policies and Approaches (for use of attribute data)
- Often a Contract/Agreement for Interaction
- Submit Metadata

Shibboleth Deployment Checklist:

http://shibboleth.internet2.edu/shib-checklist-final-website.pdf

Breakout Session 2

Question:

What Governance, Policy or Security challenges might you encounter in establishing Federated Identity Management in your organization?

(20 minutes to discuss – 15 minutes for group reports)

QUESTIONS?

Larry Conrad	-	larry_conrad@unc.edu
Mark Scheible	-	mark_scheible@ncsu.edu

Wrap-Up:

InCommon® camp
CAMPUS ARCHITECTURE & MIDDLEWARE PLANNING

CAMP Format:

- *Exploring Track*
- *Production Track*
  - *Management*
  - *Technical*
- *General Sessions*

Links:

InCommon: www.incommon.org
Shibboleth: www.internet2.edu/shibboleth