Enabling Inter Institutional Collaboration with Shibboleth

InCommon Library/Shibboleth Project
Steve Carmody, Brown University

INTERNET®

Overview

- The Changing Environment
- Some Problems…
- A New Approach

The Changing Environment

- Scholarship is now done via the Net..
  - Both teaching (cross registration) and Research
  - Allegiance is to the discipline, not the campus
  - Joint work with worldwide peers is now the norm
- Access to Federal Agency Web Sites
- Access to Higher Ed Specific Services
  - National Student Clearinghouse http://www.studentclearinghouse.org/
- The rise of Virtual Organizations
  - Local and distributed environments supporting cross-institution collaboration

The Changing Environment

- Courses Using More Electronic Services + Resources
  - LMS + other local services + outsourced services
- Expectation of Controlled access to
  - Collaboration services
  - Information services
  - Communication services
- Growing Dependence on Outsourced Services by various Business Departments

INTERNET®

The Changing Environment

- Desire for seamless user experience (SSO)
  - Across a wide range of distributed services
- Integration of resources
  - Linked resources (Openurl, deep links)
- Mobility /new devices
- Access to a broader range of electronic resources
  - Licensed
  - Campus-based repositories

INTERNET®

The Changing Environment

- New Communities, with broader membership
  - Team/Course Membership coming from multiple Institutions
  - Applicants, Alumns, Affiliates
- Role of personal privacy when using outsourced services

INTERNET®

Some Problems…

- Managing Access
  - Identity
    - “Real”
    - Attributes
    - Pseudononymous
    - Anonymous
  - Privileges
  - Level of Assurance
- Identity within Virtual Organizations

INTERNET®

Problems

- Beyond IP Address based authorization
  - Mobility, ubiquitous access
  - Traditional approaches break down
- Web SSO across the universe
  - Distributed services
  - Asserting privileges to gain access
  - Personalized instance of a service

INTERNET®

A New Approach

INTERNET®

In an ideal world …

- Many fewer identities
- Consistent user experience for authentication
- Integrated access to licensed library resources regardless of user location
- Reduced maintenance overhead for library resources
- Reliable authentication for service providers and vendors

A New Model

- Federated Model
- Shibboleth -- an implementation of the Federated Model
- Managing privileges within a VO (CoManage)
- Accessing Licensed Information Services

INTERNET®

The Federated Model

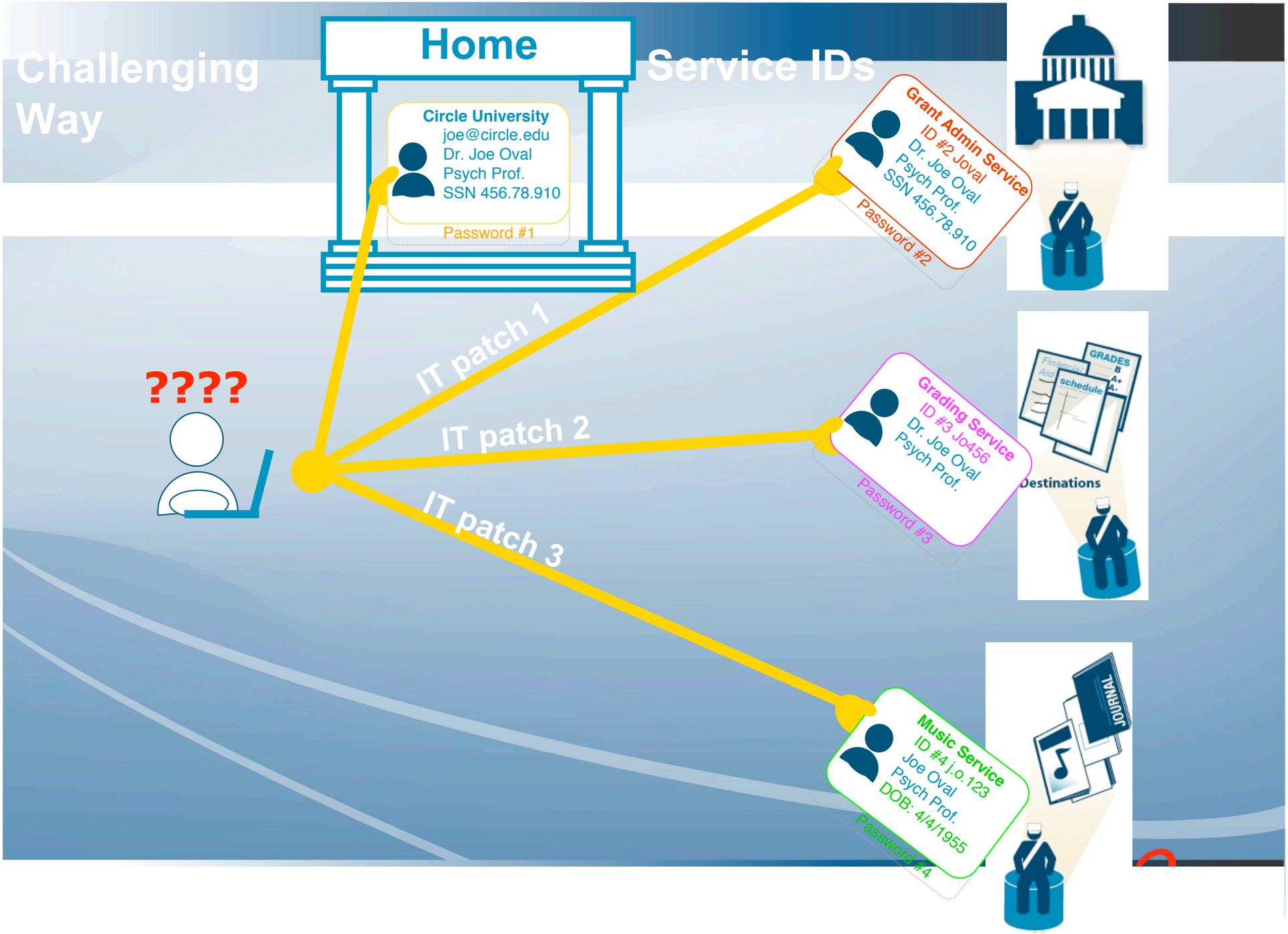
- The Players
  - –Identity Provider (IdP) authenticates the browser user, and provides Attribute Assertions describing the user
  - –Service Provider (SP) validates the Assertions, makes an Access Control decision, and provides Resources
- How is it Implemented
  - –Message sequences between the IdP andSP
  - –Most message move through the user's Web Browser
- –Metadata
  - –Defines trust framework
  - –Defines trusted parties
  - –Defines the attributes that SPs want
- Importance of
  - –Policy
  - –Trust

INTERNET®

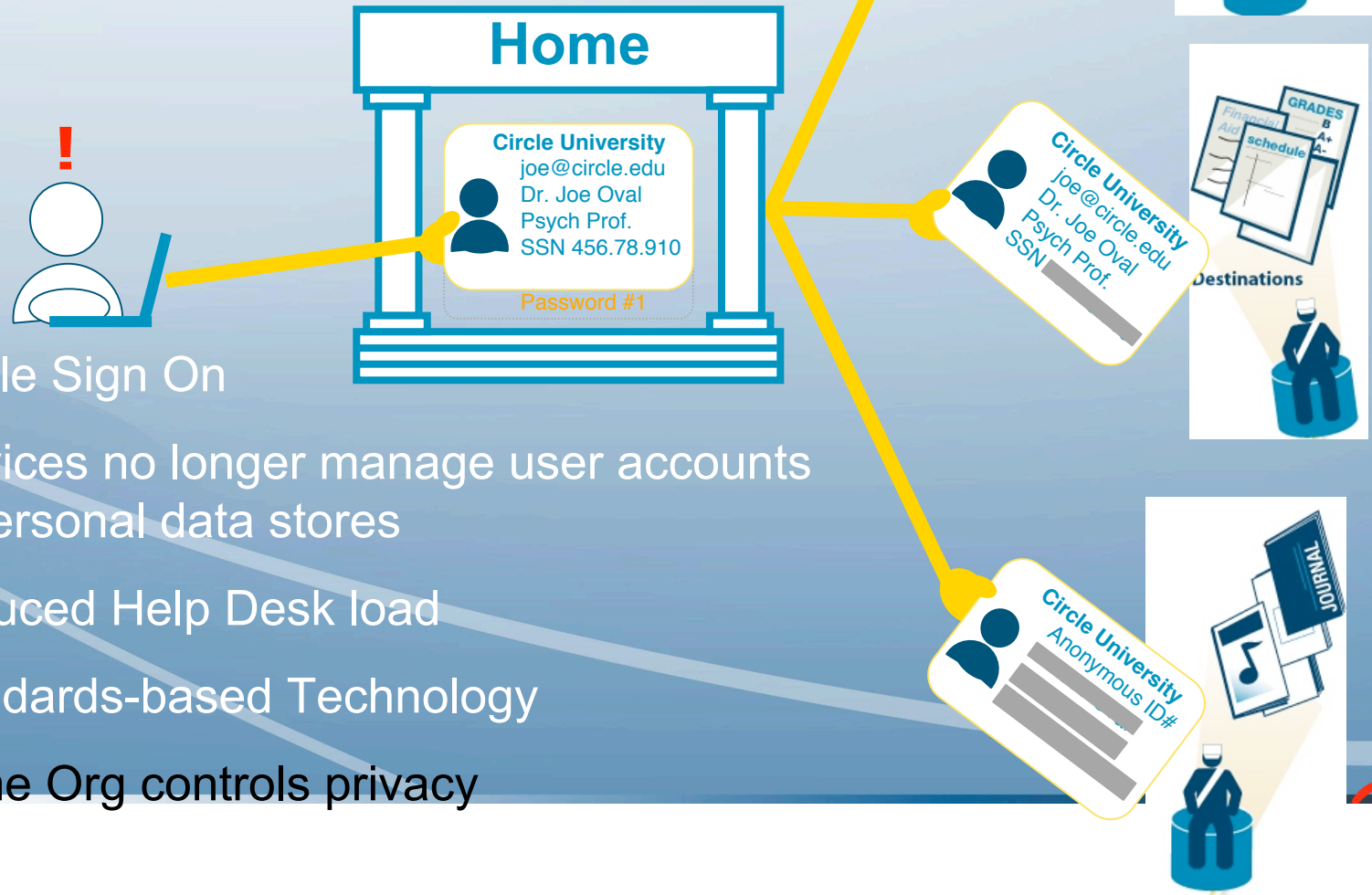
What is a Federation

- Members are campuses and vendors
- Provides
  - Common policy base
  - Common standards
    - Attribute definition and usage
  - Framework for technical trust

INTERNET®


Challenging Way
Home
Service IDs
Circle University
joe@circle.edu
Dr. Joe Oval
Psych Prof.
SSN 456.78.910
Password #1
Grant Admin Service
ID #2 Joval
Dr. Joe Oval
Psych Prof.
SSN 456.78.910
Password #2
????
IT patch 1
IT patch 2
IT patch 3
Grading Service
ID #3 Jo456
Dr. Joe Oval
Psych Prof.
Password #3
GRADES
schedule
Destinations
Music Service
ID #4 j.o.123
Joe Oval
Psych Prof.
DOB: 4/4/1955
Password #4
JOURNAL

Federated Way



1. Single Sign On
2. Services no longer manage user accounts & personal data stores
3. Reduced Help Desk load
4. Standards-based Technology
5. Home Org controls privacy

What is Shibboleth ?

- An open source standards-based Web Single Sign-on package (SAML)
- Leverages local Identity Management system to enable access to campus and external applications
- Tools to Manage Privacy -- protects your data and your users' privacy
- Helps your service partners
- Scaleable to the thousands of Higher Ed members and partners
- Plays well with others
- Extra functionality -- outside the standards -- to address the unique needs of Higher Ed

INTERNET®

Why Choose Shibboleth ?

- Framework for a Variety of Policy and Management Models
  - Intra-campus
  - Federations
  - Bilateral
- Extensible Authentication and Attribute Sharing
  - Federation defines syntax and semantics of common Attribute/Value pairs
  - Two parties can define custom attributes
- Provides functionality outside of SAML to allow a site + a user to manage personal privacy
- Scaleable to thousands of campuses
- Use same SSO for intra- and inter-campus

Attributes.. With Shibboleth

- Identity
  - Name
  - Uid
  - Pseudononymous
- “Others”
  - Department
  - Groups
- Privileges
  - Represented as Attribute values

INTERNET®

Value of the Federated Model

- To Campuses
  - One solution for intra- and inter-domain SSO
  - Ability to manage access control for small groups, roles
    - Courses, departments, projects, etc
  - Implement Shibboleth once…
    - And then just manage attributes that are released to new targets
- To Service Providers
  - Unified authentication mechanism built on open standards
    - Much more scalable
    - Much less integration work required to bring a new customer online.
  - More flexible and more secure than current methods
    - IP address based control open to many forms of abuse
    - Attribute-based approach allows more licensing options
  - Ability to implement fine-grained access control
    - License material to courses, departments, virtual organizations, etc

Value of the Federated Model

- To Users
  - Allows personalization of services, without releasing identity
  - Web SSO across a worldwide set of sites
  - Fewer passwords
  - Tools to manage privacy
  - A trusted party is asserting values + eligibility
  - NOT tied to IP address of browser

Managing Privileges in a VO

- The Problem
  - Members come from multiple institutions
  - Need to manage permissions within a suite of applications supporting their collaborative work
- Currently
  - Management of collaboration a real impediment to collaboration, particularly with the growing variety of tools

INTERNET®

Collaboration Management Platforms

- Goal is to develop a “platform”for handling the identity management aspects of many different collaboration tools
- Platform includes a framework and model, specific running code that implements the model, and applications that take advantage of the model
- This space presents possibilities of improving the overall unified UI as well as UI for specific applications and components.

CoManage - one example…

- A collaboration management platform, supported in part by a NSF OCI grant, being developed by the Internet2 community, with Stanford as a lead institution
- Open source, open protocol
- Uses Shibboleth, Grouper, and Signet
- COmanage can be deployed by a campus, a department, a VO, a VO service center; COmanage instances communicate with each other by the “attribute ecosystem”voodoo

Information Services

INTERNET®

What is the Library/Shibboleth Project?

- Established 2007
- Six universities + Internet2
- Campus IT, Library IT, Librarians

Focus of the Library/Shibboleth Project

- Improving access to licensed electronic resources
- Identify user scenarios
- Document business practice and technology issues
- Test proposed solutions

Technologies investigated

- Federated Access
  - Shibboleth
- Shibboleth-enabled Rewrite Proxy
  - EZProxy

The Model

- A hybrid environment
  - Leveraging Shibboleth where possible
  - Falling back to EZProxy when necessary
- Browser users authenticate to EZP with Shibboleth
  - Provides consistent user experience
  - Allows library staff to manage transitionof services to “Shib-enabled” without affecting user experience

Shibboleth + SSO enabled rewrite proxy

Benefits to users
- Single password for campus service and proxy access
- Integration with personalized vendor functionality

Benefits to librarians
- Reduced cost of support
- Less IP and proxy maintenance with 80% case
- Easier breach investigation
- Permits rollout of Shib-enabled resources while keeping user experience consistent.

Benefits to vendors
- Authoritative validation
- No maintenance of password information

Benefit to library administration
- Central usage statistics (“foot traffic”)

Campus Repositories - Access Control

- Grant Access to
  - A member of the department
  - Friends of the department
  - Members of the project team
  - Instructor gives students access to a “slice” of their research data
  - External reviewers, during departmental re-accreditation

INTERNET®

In Brown's case…..

- Use Fedora
  - Already supports federated access
  - Use XACML to write access rules
  - Use Shibboleth to provide permissions

Questions ?