

# Federated Identity: Leveraging Shibboleth to Access On and Off Campus Resources

Paul Riddle

University of Maryland Baltimore County  
EDUCAUSE Mid-Atlantic Regional Conference  
January 16, 2008

Copyright Paul Riddle, 2008.

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

# Introduction

- Campuses are managing an increasing array of in-house and third-party self-service tools
- Lots of services, lots of authentication schemes
- Goal is to provide end users with a “seamless” web browsing experience
- To address this, many campuses have implemented single sign-on (SSO) systems
- It is often difficult to extend SSO systems to manage access to providers external to the campus

# How are providers addressing SSO?

- Some support popular systems like CAS and Pubcookie
- Some have established ad-hoc schemes that schools can follow to set up SSO (ex. National Student Clearinghouse)
- Others do nothing, leaving SSO integration up to the customer (ex. PeopleSoft)
- More and more are supporting Shibboleth and other related technologies

# Common problems

- Can't expect providers to support every single sign-on system out there
- Integrating ad-hoc SSO schemes is often cumbersome and insecure
- Providers still need to maintain user accounts
  - This often means storing users' personal data on the provider's remote site. This is a big privacy concern.
- Ideally we'd like to send user information to providers on an “as-needed” basis only

# Shibboleth Addresses These Issues

- Extends single sign-on to include services external to the University
- Takes providers out of the authentication business
- Protects individuals' privacy
- Based on open standards
- Straightforward for Universities and providers to adopt

# What is Shibboleth?

*shibboleth* (n) -

1. a peculiarity of pronunciation, behavior, mode of dress, etc., that distinguishes a particular class or set of persons
2. ~~a common saying or belief with little current meaning or truth~~

-dictionary.com

# What is Shibboleth?

- A secure framework for exchanging user attributes between institutions
- Provides single sign-on service that works with a campus' existing authentication system
- Allows campuses to build and manage locally, access globally
- Sends user attributes to providers at the time the user accesses the service

# Technical Info

- Based on SAML v1.1 specification (forthcoming version 2.0 will implement SAML 2.0)
  - Interoperates with other SAML-based providers
- Uses SSL certificates to securely transmit authorization data to remote providers
- Works with any authentication service that can provide the HTTP *REMOTE\_USER* environment variable.

# Some Providers who Support Shibboleth

- WebCT
- Symplicity Student Career Services
- WebAssign
- NSF FastLane grant administration system
- Elsevier ScienceDirect online scientific journals
- TurnItIn
- Napster
- Google Apps (coming soon with Shib 2.0)

# How Shibboleth Works

# Two Major Components

- **Identity Provider (IdP)**
  - Runs at the end user's site
  - Verifies the identity of the user (usually via SSO)
  - Asserts user's relevant attributes to the remote site
- **Service Provider (SP)**
  - Runs at the remote site
  - Verifies that the remote user is allowed to access the remote service

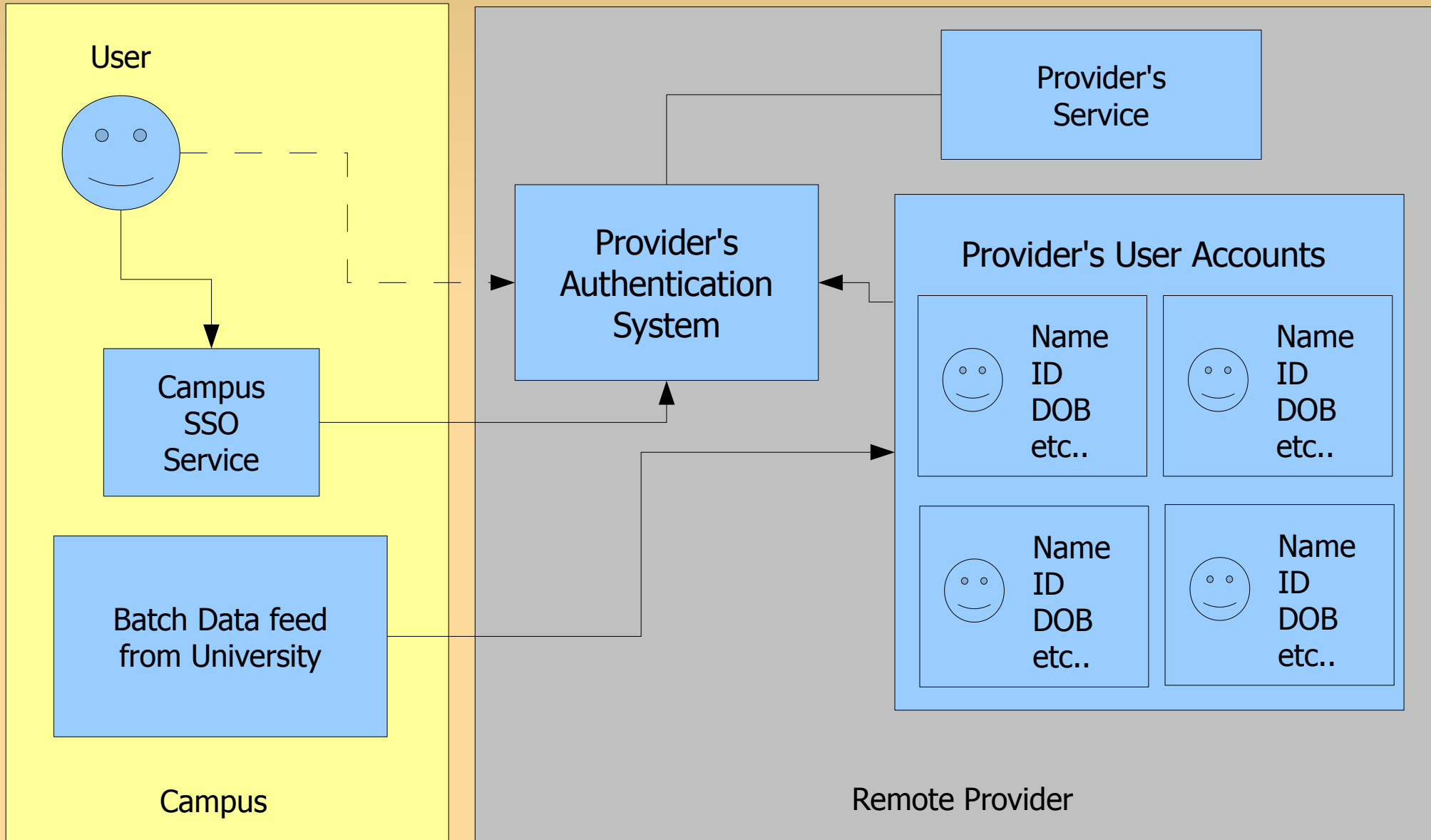
# High Level Work Flow

1. User browses to a Shib-authenticated web site
2. Remote site contacts the IdP at the user's site
3. User authenticates via site's SSO (if necessary)
4. IdP passes a “handle” back to the remote site
5. Remote site sends an attribute request back to the IdP
6. IdP queries and returns user attributes that the remote site is entitled to know

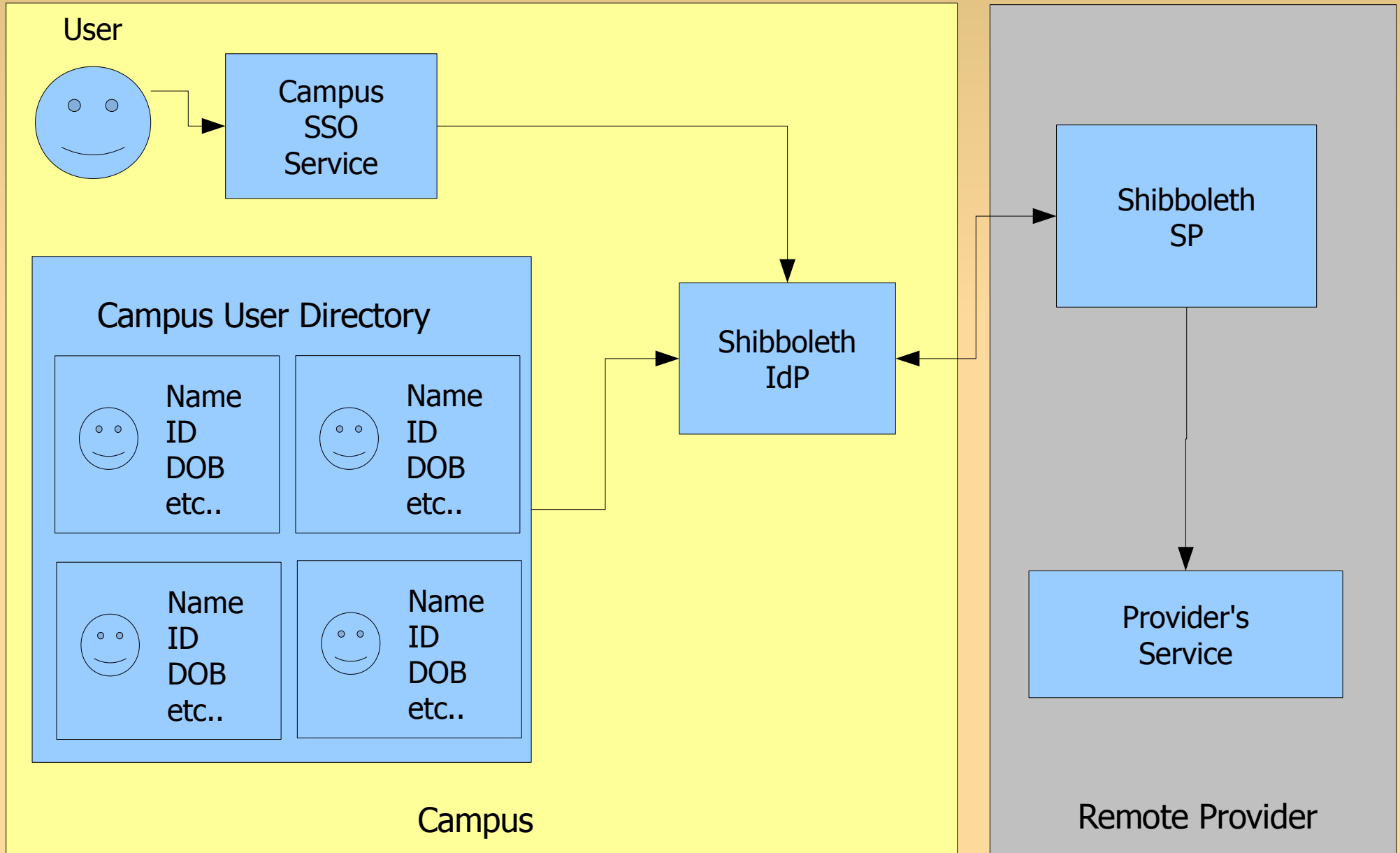
# Things to Note

- It's not necessary to release the user's actual identity
- Users can control what information is released about them
- Remote service providers no longer need to maintain user accounts or track identities

# The Old Way



# The Shibboleth Way



# Federations

# About Federations..

- Shibboleth is a nice starting point, but it doesn't enforce any specific attribute policies
- A federation brings like-minded organizations together and defines a standard vocabulary of attributes
- This eliminates the need to come up with “one off” solutions for each service provider
- In many cases, things will “just work”

# InCommon

- InCommon is a popular federation for higher education institutions in the U.S.
- Many providers who support Shibboleth in higher ed have joined InCommon
- InCommon's attributes are based on the popular eduPerson specification
- InCommon also provides an SSL Certificate-Signing Authority

# Some InCommon Attributes

- eduPersonScopedAffiliation
- eduPersonPrincipalName
- eduPersonEntitlement
- eduPersonTargetedID
- sn
- givenName
- displayName
- mail

# Case Study: Shibboleth at UMBC

# About UMBC

- Roughly 15,000 users
- Home-grown single sign-on service (WebAuth)
- (Mostly) eduPerson-compliant user directory based on OpenLDAP
- Many in-house and third-party applications ported to use our SSO (*myUMBC* portal, PeopleSoft Finance and HR, Blackboard, etc)
- Several outsourced services (National Student Clearinghouse, Campus Card Services, etc)

# Shibboleth at UMBC

- We want to “Shibbolize” as many of our in-house applications as possible, to de-couple them from the SSO system.
- Third-party applications are another story. Ideally, we'd like all of our vendors to support Shibboleth out of the box. Some are beginning to do this, but for the others, we'll still need custom solutions.
- The more customers ask, the more likely vendors will be to offer support.

# UMBC and Symplicity

- Symplicity Corporation provides services to students seeking employment, internships etc.
- We chose Symplicity over several competing products partly because of their support for open standards like Shibboleth/SAML
- All services run on Symplicity's own, off-site web servers
- We use Shibboleth and InCommon to facilitate single sign-on into Symplicity for our users. It has been a big success.

# What's next?

- “Shibbolize” services such as PeopleSoft and Blackboard
- Single sign-on for Alumni portal
- Explore the idea of creating a federation of schools within the University System of Maryland
  - This opens up some very interesting possibilities, such as cross-campus course registration, library services, etc.

# Next Steps

# Shibboleth Infrastructure Requirements

- An authentication or single sign-on (SSO) service capable of providing HTTP *REMOTE\_USER*
- A user directory (LDAP or other) that ideally complies with eduPerson specification
- Apache (preferably 2.x) and Tomcat
- Java 1.5 or better

# Getting Started

- Download and deploy the Shibboleth IdP
- Integrate the IdP with your existing SSO and Directory services
- If you want to “Shibbolize” locally-managed services, deploy the Shibboleth SP
- Join a federation such as InCommon
- Encourage vendors to adopt Shibboleth and support those who do.

# References

- <http://shibboleth.internet2.edu>
- <http://www.incommonfederation.org>
- <http://www.oasis-open.org>
- <http://www.opensaml.org>
- <http://www.educause.edu/eduperson>
- <http://www.symplicity.com>

# Contact Information

Paul Riddle  
paulr@umbc.edu