

# IAM and Shibboleth

Shibboleth Planning Team  
June 2, 2008



**UF** | UNIVERSITY of  
FLORIDA

# Shibboleth Planning Team

- Eli Ben-Shoshan, CNS
- John Bevis, CNS
- Dr. Mike Conlon, chair
- Alan Cook, CIO Ofc
- Warren Curry, Bridges
- Tim Fitzpatrick, CNS
- Rodger Hendricks, AT
- Mike Kanofsky, UFAD
- Iain Moffat, CNS
- Erik Schmidt, UFAD
- Barb Sedesse, CNS

# Identity and Access Mgt (IAM)

- Identity
  - UFID – UF Directory
- Authentication
  - GatorLink username and password – managed in myUFL, pushed into PeopleSoft, Active Directory, Kerberos, NDS
- Authorization
  - Affiliations (UF Directory) and roles (PeopleSoft), pushed into UFAD. Declarative authorization: Is person x in group y?

# IAM – Big Picture At UF


## Enterprise Applications

myUFL  
Cognos  
WebCT

ISIS  
WebMail  
Many others

## Local Applications

Many, many, many applications – simple web sites with controlled content, vendor applications, locally developed applications, variety of technologies



**Area of interest – how to improve connection between applications and IAM systems**

## IAM Systems

UF Directory      PeopleSoft      BizTalk

GLAuth      Kerberos      Active Directory      MIIS

LDAP      NDS      Cosign

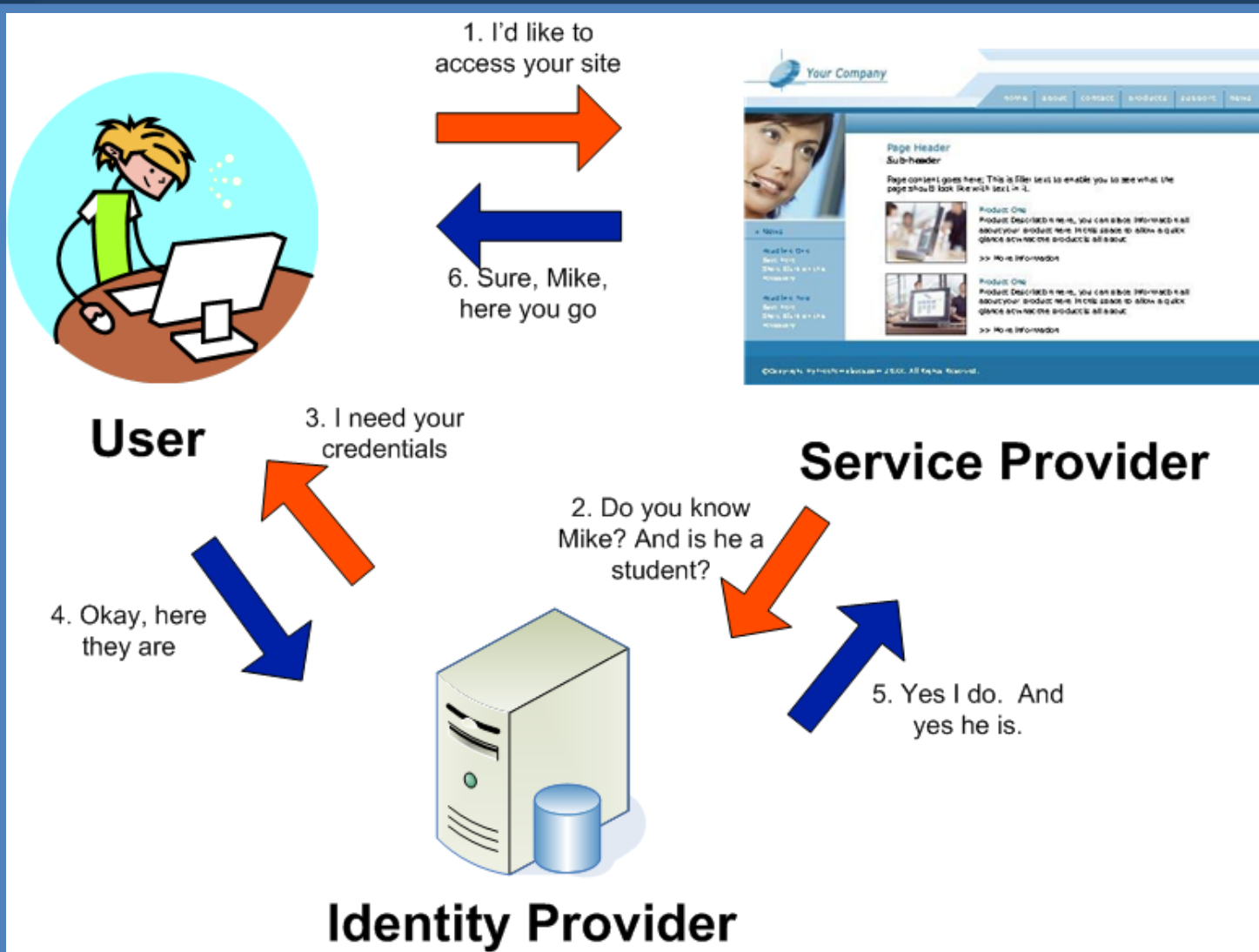
# Opportunities for Improvement

- Symmetric WebISO
- More environments
- Improve Security
- Use group information for declarative authorization

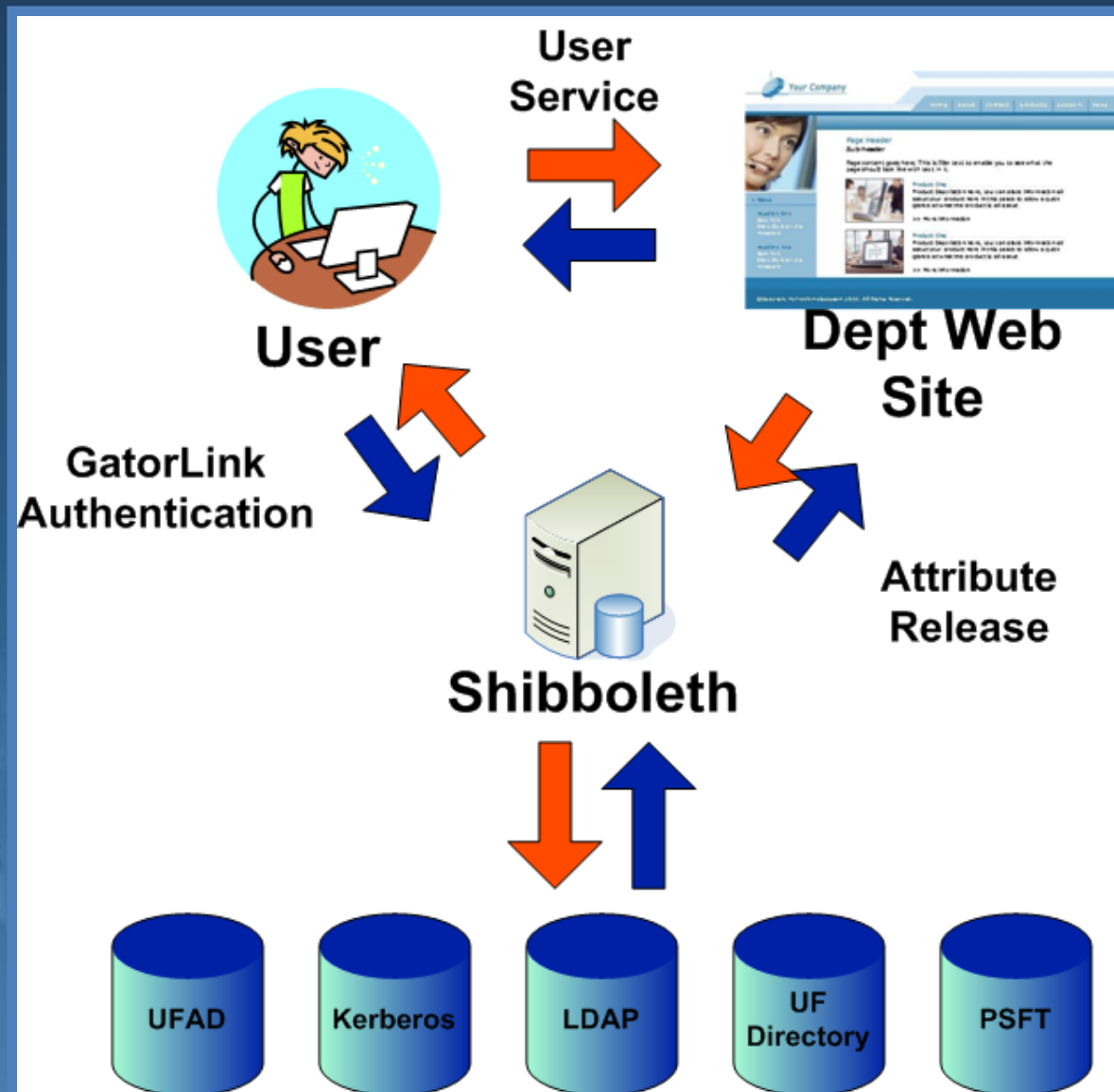
# Shibboleth

- Internet2 project with lead site at Ohio State
- InCommon Trust Federation
- NSF, NIH, Microsoft DreamSpark, Elsevier, Mobile Campus, many more
- Federated identity (multiple identity providers) as well as declarative authorization (attribute release)
- Shibboleth Demo  
[http://shibboleth.internet2.edu/demo/shib\\_demo.html](http://shibboleth.internet2.edu/demo/shib_demo.html)
- See <http://shibboleth.internet2.edu>

# Shibboleth Flow



# UF Shibboleth Flow



# Attribute Release

- Shibboleth is designed to provide data about users (attributes) to authorized requestors
- Attribute Release is governed by Attribute Release Policy
- Attribute Release Policy is associated with an “Application” (typically a URL)
- At UF, an application is associated with a Responsible Party via UFID.

# Attribute Release Control



1. Each Application has exactly one responsible party. A responsible party may have many applications
2. An Attribute Release Policy (ARP) may be assigned to many applications. An application may have more than one ARP.
3. An ARP may release multiple attributes. An attribute may be released via many different policies
4. Many attributes may come from a particular attribute source. Each attribute comes from exactly one source

# Attribute Release Policy Example

- Suppose we have an ARP named UF\_PRIMARY\_AFFILIATION releasing a single Attribute – UF Primary Affiliation
- An Application is registered with a Responsible Party who is authorized to use the ARP.
- The application can then control content via a rule of the form  

```
allow affiliation=(faculty,staff,student)
```
- Note: *the application does not get the identity of the user!*

# ARP – Example 2

- UF\_CID – release primary affiliation along with a service provider specific computed identifier (CID).
- The CID can be used by the service provider as a key to provide persistent access
- The CID is not the UFID. It is managed by Shibboleth.
- An application can assume that if a CID value recurs in a subsequent transaction, that it belongs to the same individual
- CID is not sensitive nor privileged data and can be used outside UF.
- An application such as Mobile Campus could use this policy to verify that the user is a student and then manage preferences within their service for the student based on the CID.
- **Note: The application does not get the user identity!**

# ARP – Example 3

- UF\_PERSON might release UFID, name, campus address, email, telephone, UF affiliations, department id, course/section info along with role info
- Such a collection of attributes might be sufficient to provide customized service without resort to additional enterprise data access.
- Applications using this ARP might remain stateless with respect to these attributes, using values as they are obtained during the Shibboleth transaction

# Memoranda of Understanding (MOUs)

- All ARPs would be governed by MOUs
- Standard MOUs for internal UF responsible parties
- Template, customizable MOUs for external responsible parties
- Primary use of attribute release is to authorize access to services
- In general, secondary use of data from ARPs is prohibited
- All Responsible Parties must sign MOUs. UF entities must provide ISA, ISM and application tech lead contacts.

# IAM Opportunities and Shibboleth

- **Symmetric WebISO** – Shibboleth provides Symmetric WebISO across all Shibbolized applications
- **More environments** – Shibboleth supports both IIS and Apache on Windows and Linux. Also Solaris and Mac servers.
- **Improve Security** – Shibboleth has well-defined ARPs and technical controls to support appropriate data release
- **Use group information for declarative authorization** – ARPs support declarative authorization

# Current State and Next Steps

- Proof of concept complete. Multiple web servers in CNS and Bridges. WebISO. Simple ARPs
- DRAFT ARP management and governance processes
- Production environment planning
- Production launch anticipated fall 2008
- Ready for early beta testing

# Early Beta Testing

- Requirements
  - Web Server with admin rights, commercial SSL certificate and remote access to environment
  - Experience with XML
  - Time to invest in set up and trouble shooting
- Contact Eli Ben-Shoshan ([ebs@ufl.edu](mailto:ebs@ufl.edu)) regarding participation
- There will be a “camp” for the early beta testers at CNS in mid June
- An open beta will follow at a time to be announced

# Production Launch

- Full clustered production infrastructure with dev, test and pre-production by end of July
- Service definitions, documentation, local support in place in August
- Anticipated production service available fall 2008

# Future of GatorLink Authentication

- Shibboleth is the stated direction for GatorLink authentication
- Eventually, all enterprise systems will use Shibboleth for single sign on. CoSign will be decommissioned.
- Intention is to eventually decommission GLAuth, the current system for GatorLink authentication.
- We expect at least one year for GLAuth service after the production launch of Shibboleth in the fall of 2008.
- After GLAuth is decommissioned, Shibboleth will be required for all GatorLink authentication.

# IAM at UF with Shibboleth

## Enterprise Applications

myUFL  
Cognos  
WebCT

ISIS  
UF Exchange  
Many others

## Local Applications

Many, many, many applications – simple web sites with controlled content, vendor applications, locally developed applications, variety of technologies

## IAM Systems

**Shibboleth**

UF Directory

PeopleSoft

BizTalk

~~GLAuth~~

Kerberos

Active Directory

MIIS

LDAP

NDS

~~Cosign~~

# Next Steps

- Finalize ARP governance and control processes
- Finalize infrastructure planning
- Early Beta Testing for service providers
- Open Beta Testing
- Finalize “opening day” ARP collection
- Build production service, including infrastructure and ARPs
- Final testing of production services
- Launch of production services. Support of service providers
- Begin conversion of enterprise systems
- Convert Mobile Campus to Shibboleth
- Add DreamSpark and other external services
- Announce date for sunset of GLAuth

# More information

- Web Sites
  - <http://www.bridges.ufl.edu/directory>
  - <http://www.ad.ufl.edu>
- Discussion – various listservs
  - [Central-posix-l@lists.ufl.edu](mailto:Central-posix-l@lists.ufl.edu)
  - [Activedir-l@lists.ufl.edu](mailto:Activedir-l@lists.ufl.edu)
  - [ccc@lists.ufl.edu](mailto:ccc@lists.ufl.edu)
- Feedback
  - [mconlon@ufl.edu](mailto:mconlon@ufl.edu)