Web app AAI Integration

How to integrate web applications with AAI in general?

SWITCH
Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Zurich, 8. February 2009

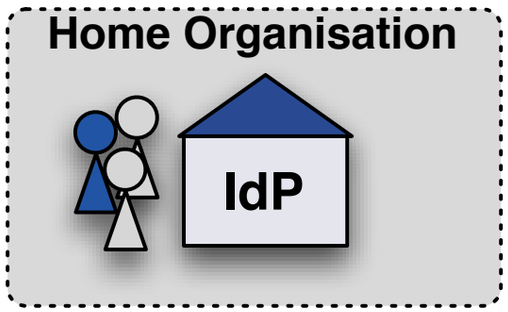
Goal of this presentation

1. List the general requirements for integrating AAI into a general web application (not SAP-specific)

2. Out-line what “AAI Integration” means and involves

3. Describe some technical aspects of the integration

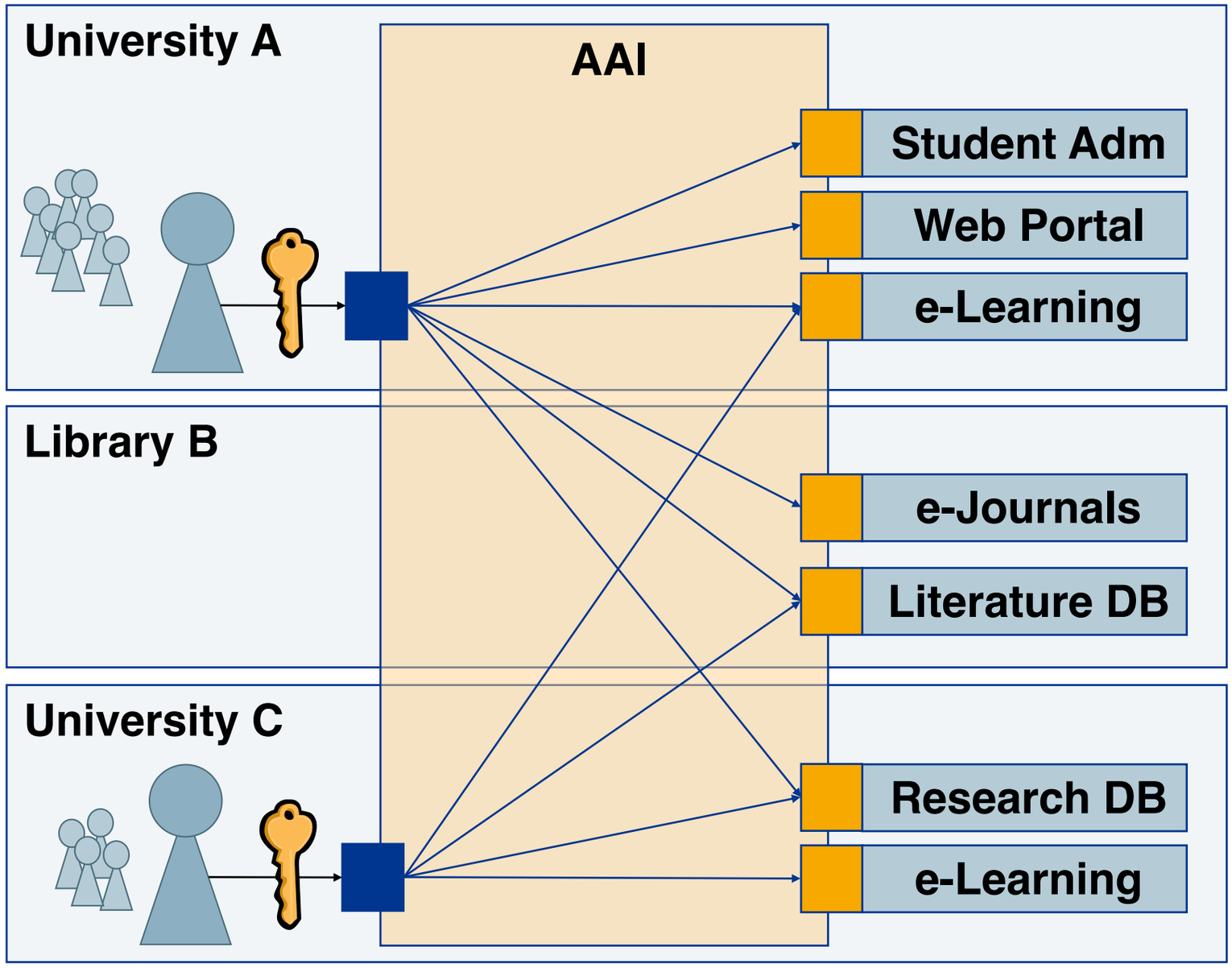
Some Terminology



Home Organisation
Operates an Identity Provider that authenticates a user and asserts identity information about this user in form of SAML assertions

Resource
Consists of Service Provider that protects one or more web-applications by enforcing authentication. Provides SAML identity assertions in form of attributes to the application(s).

The Advantages of AAI



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Authorization independent of location
- Efficient implementation of inter-institutional access

User Administration Authentication | Authorization | Resource | Credentials

Shibboleth - The Software Behind AAI

- Open Source developed by

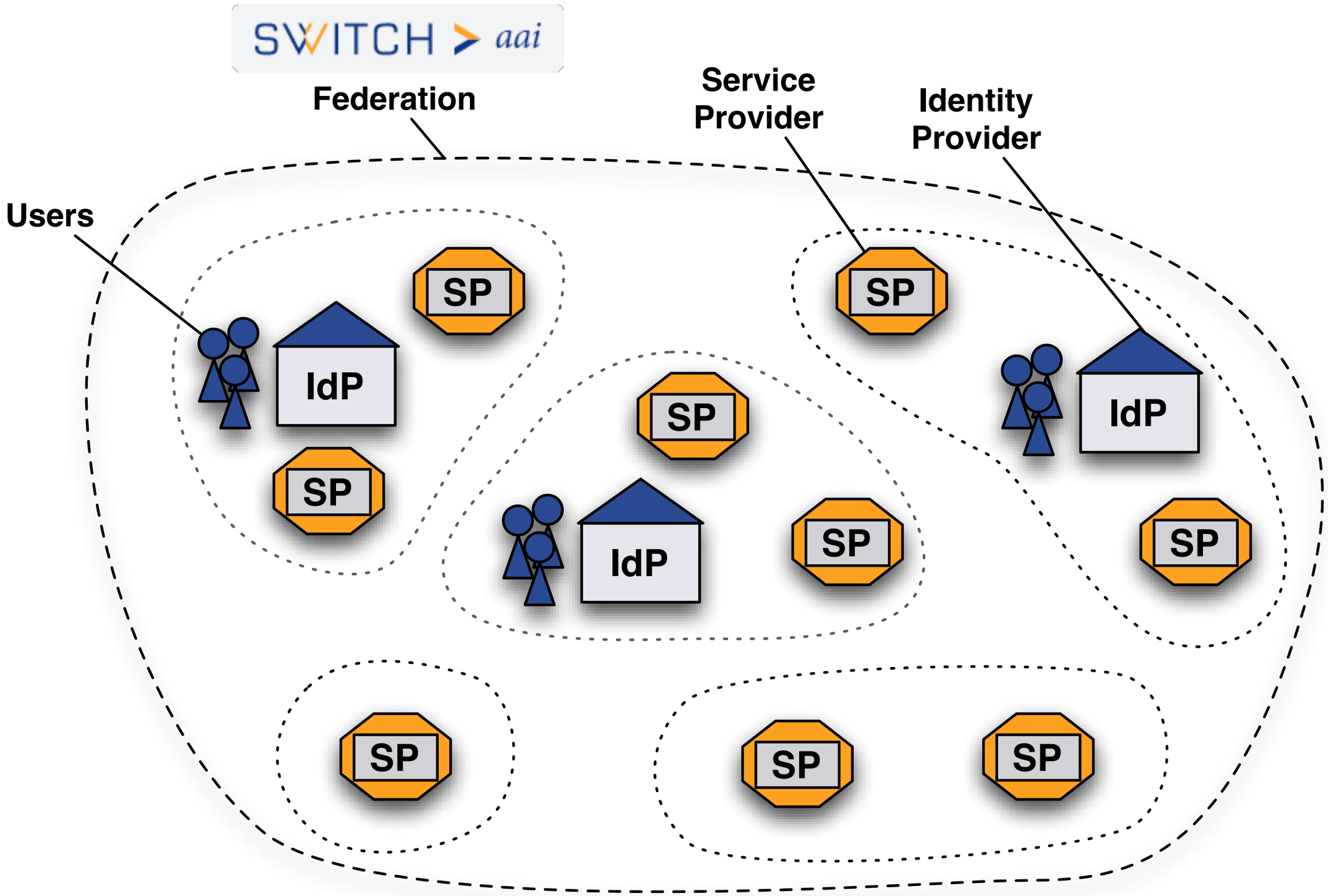
- Word **Shibboleth** was used to identify members of a group

- Based on Security Assertion Markup Language (SAML)

- Internationally used (mostly in academic sector)

http://shibboleth.internet2.edu

AAI - Authentication and Authorization Infrastructure



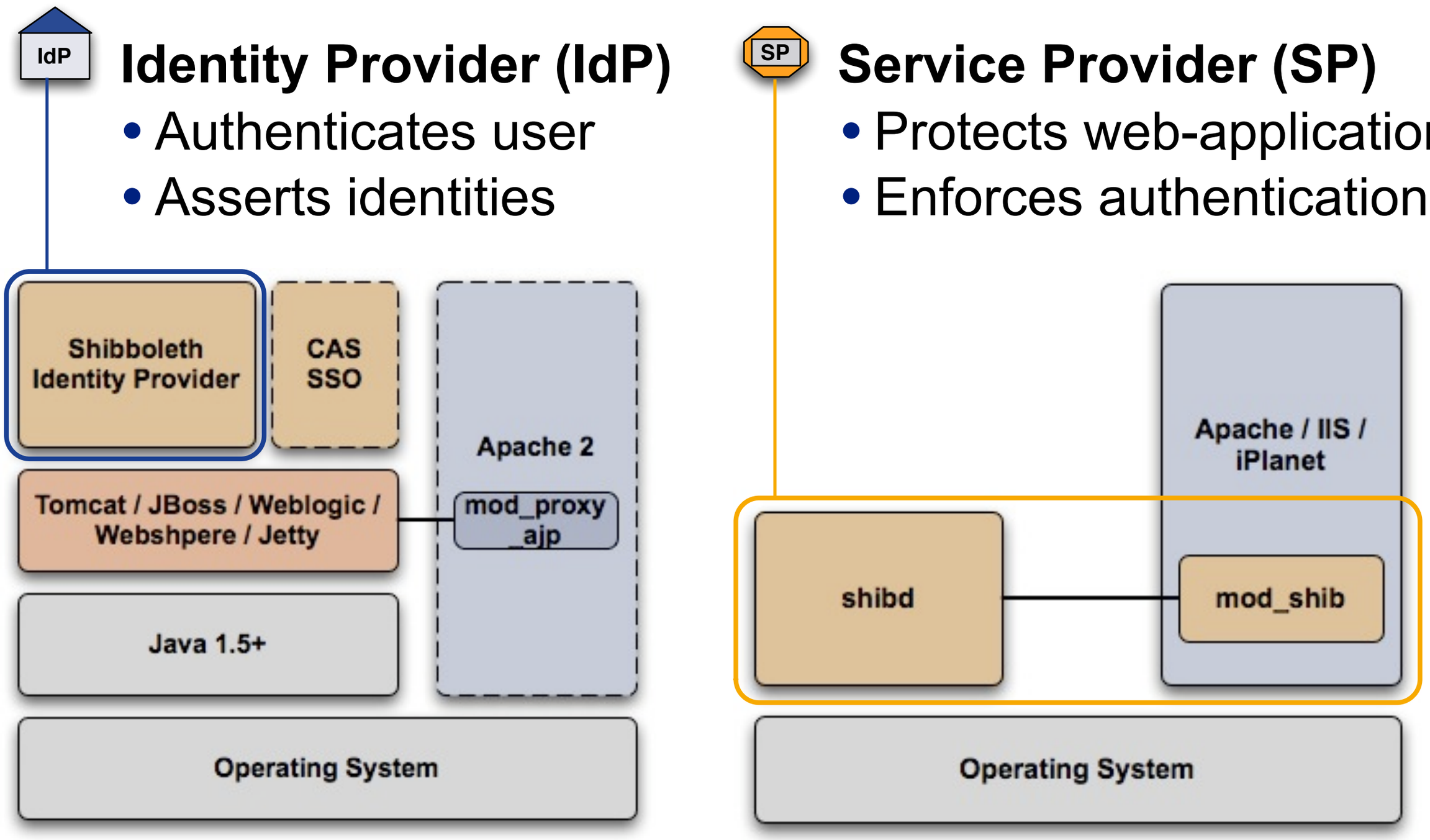
Shibboleth – The components

Identity Provider (IdP)

- Authenticates user
- Asserts identities

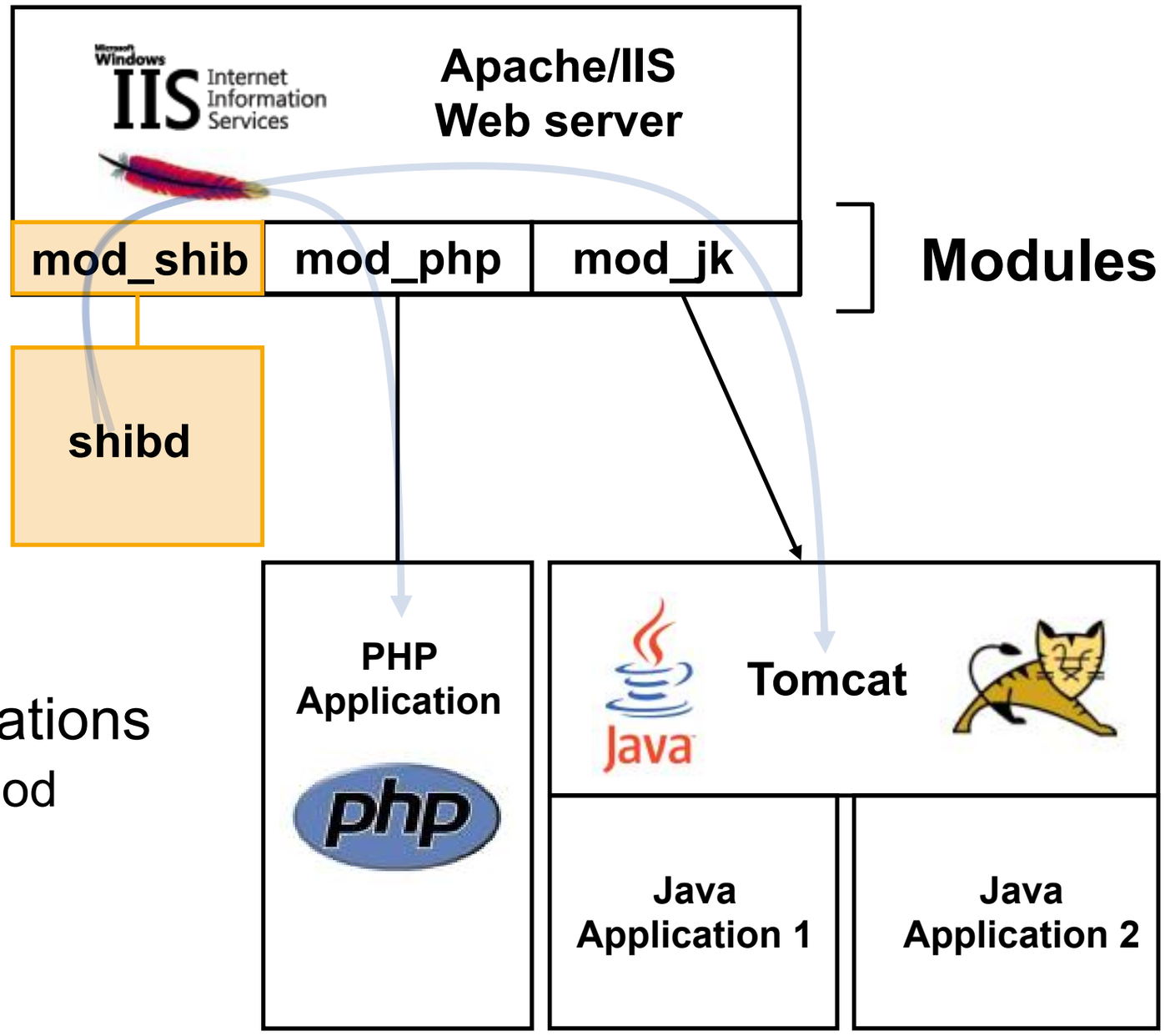
Service Provider (SP)

- Protects web-application
- Enforces authentication

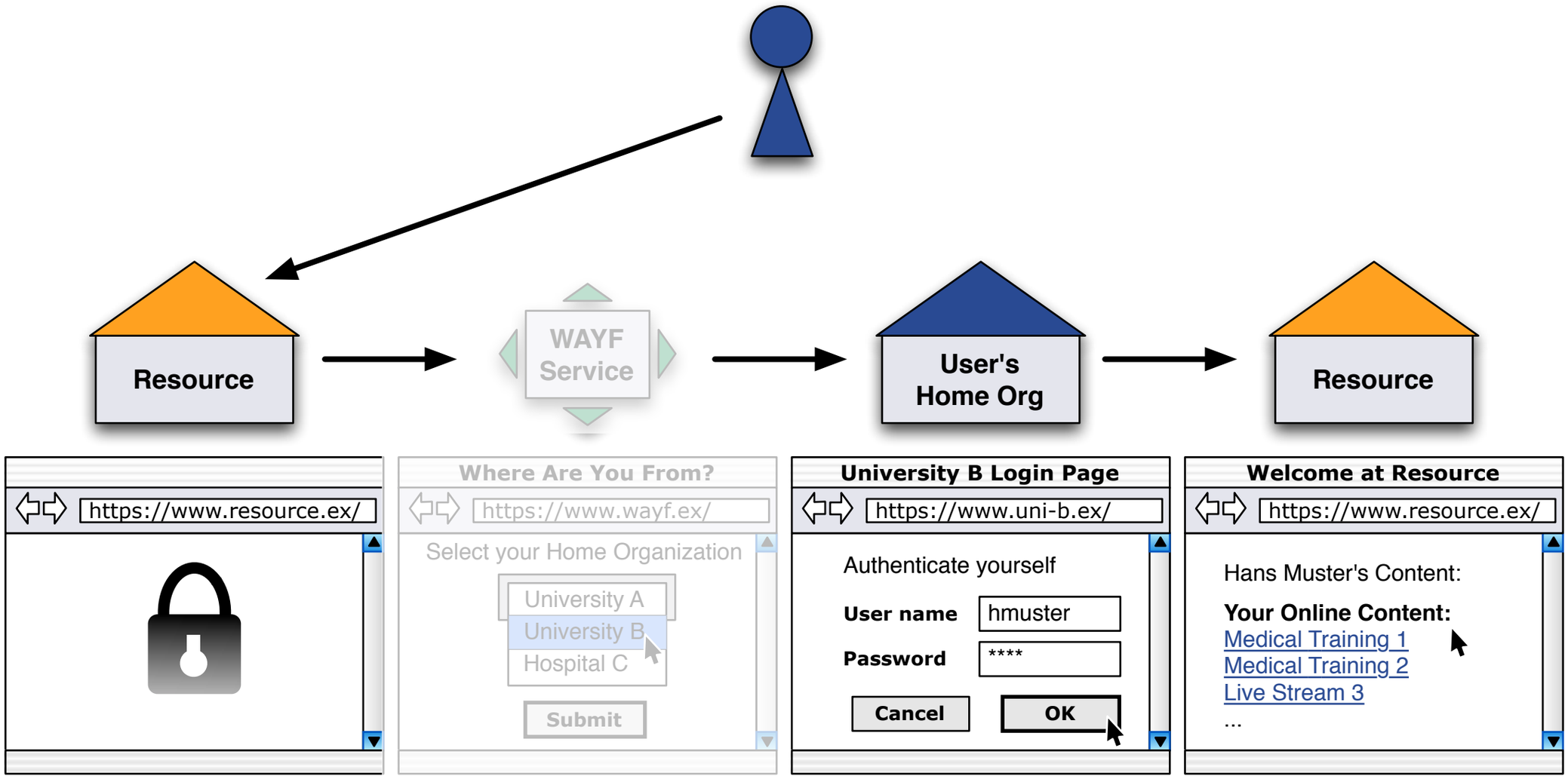


Shibboleth Service Provider for Apache/IIS

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, …
- Protects static content and web applications
- **shibd** fetches attributes
- Authorizes users using
  - Apache directives
  - Shibboleth XML Access rules
- Provides attributes to applications
  - Alternative authorization method



Login Procedure from User's View



Access Resource

Choose Home Org.
(not always necessary)

Provide credentials

Use Resource

Application receives user's attributes

How to Use AAI Attributes in Application

On Shibboleth-protected pages, user attributes can be directly read from web server environment.

PHP

```
$email = $_SERVER['Shib-InetOrgPerson-mail'];
```

Perl

```
$email =$ENV{'Shib-InetOrgPerson-mail'};
```

Java

```
String email = "";
email = request.getHeader("Shib-InetOrgPerson-mail");
```

Attributes That Are Available in AAI

Personal

Unique Identifier

Surname

Given name

E-mail

User ID

Matriculation number

Employee number

Address(es)

Phone number(s)

Preferred language

Date of birth

Gender

Group Membership

Home Organization Name

Home Organization Type

Affiliation

Study branch

Study level

Staff category

Group membership

Organization Path

Organizational Unit Path

Implementation of Attributes

- Mandatory
- Recommended or optional

Based on

- eduPerson Attributes
- “Schweizerisches Hochschulinformations-system” (SHIS)

NO password (in general)

http://www.switch.ch/aai/attributes

Some Already Shibbolized Applications

Information Providers:		Learning Management Systems:	Other Systems:	
• American Chemical Society	• NSDL	• Blackboard	• Bodington.org	• JISCmail
• ArtSTOR	• OCLC	• CLIX	• Condor	• LionShare
• Atypon	• Ovid Technologies Inc.	• Fronter	• Confluence Wiki	• Media Wiki
• CSA	• Project MUSE	• ILIAS	• Darwin Streaming Server	• Microsoft
• Digitalbrain PLC	• Proquest Information and Learning	• INSTRUCT	• Drupal	• MyProxy
• EBSCO Publishing	• Serials Solutions	• Moodle	• DSpace	• Napster
• Elsevier ScienceDirect	• SCRAN	• OLAT	• eAcademy	• PHEAA
• ExLibris	• Schweizerisches Bundesgericht	• Sakai	• Fedora Repository	• Sharepoint® from Microsoft
• H.W. Wilson	• Thomson Gale	• WebAssign	• Google Apps/Email	• SYMPA
• JSTOR	• Thomson Reuters	• WebCT	• GridSphere	• Symplicity
• The Literary Encyclopedia	• Useful Utilities - EZproxy		• GridShib	• TurnItIn
• Metapress			• Higher Markets	• TWiki
			• Horde	• uPortal
			• Hupnet	• WordPress
				• Zope + Plone\

More up-to-date and comprehensive list:

https://spaces.internet2.edu/display/SHIB2/ShibEnabled

Questions to Consider Before Integration

Feasibility

- Can I modify the application logic/code at all?
- Is the application open source or is there an API?

Level of Integration

- How much shall be integrated?
- Authentication? Authorization? Enrollment? Logout? De-provisioning?

Sustainability

- Can changes be included in official source tree?
- What happens after version 1.0 or in cases of bugs?

Levels of Integration

How deep shall the integration go?

1. Authentication
2. Registration/Provisioning
3. Enrollment
4. (Single) Logout
5. Account Deletion/De-provisioning

1. Authentication

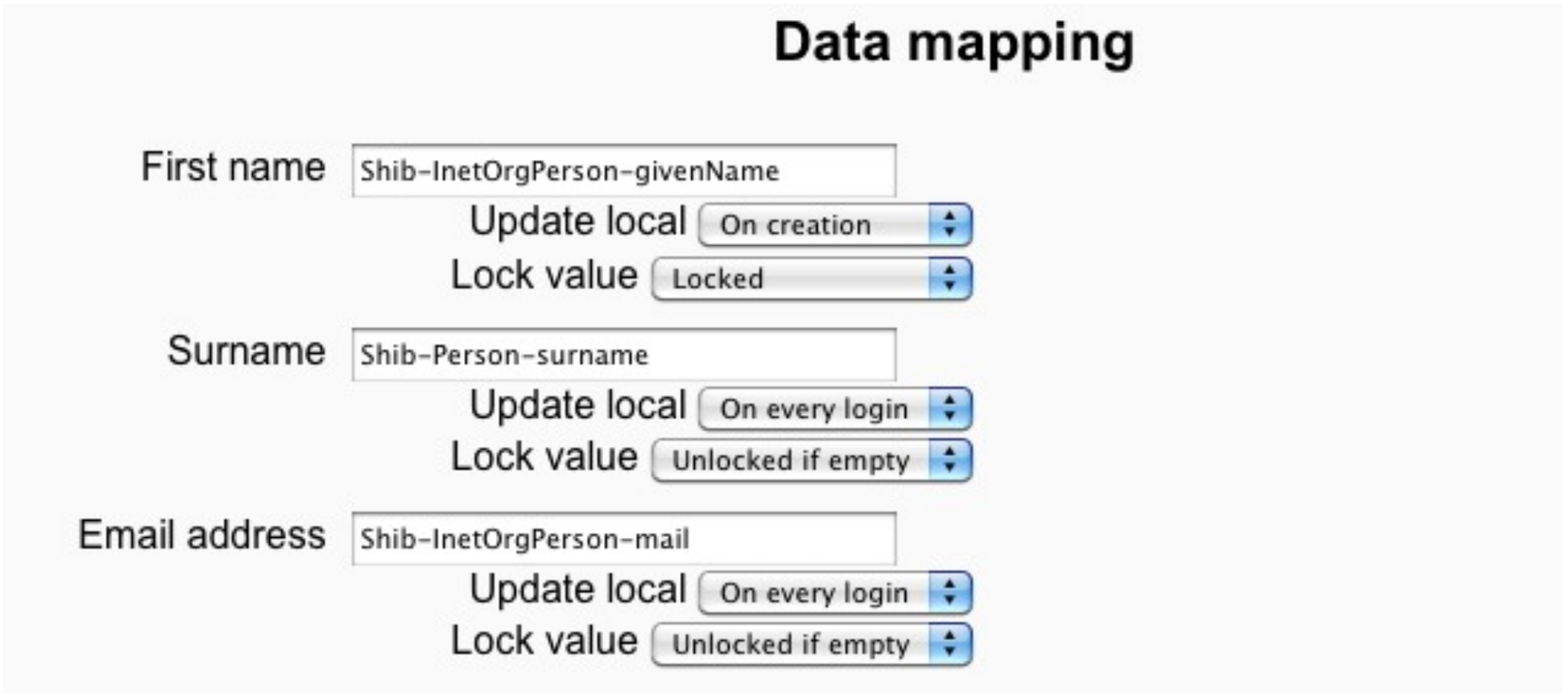
- **Simple case:**
  Application relies on external session management like HTTP Basic Auth.
  Shibboleth can then set the REMOTE_USER header variable with an AAI attribute.
  (This is one of the presented approaches for SAP)

- **More complex case:**
  Application uses it's own session management.
  Application code must be extended to set up application session using AAI attributes.
  Examples: Almost all e-learning applications

2. Registration/Provisioning

- Create a user entry within the application based on AAI attributes the first time a user accesses the application.
- Update user data using AAI attributes
- Available already in quite some web applications: Moodle, BSCW, ILIAS, ...

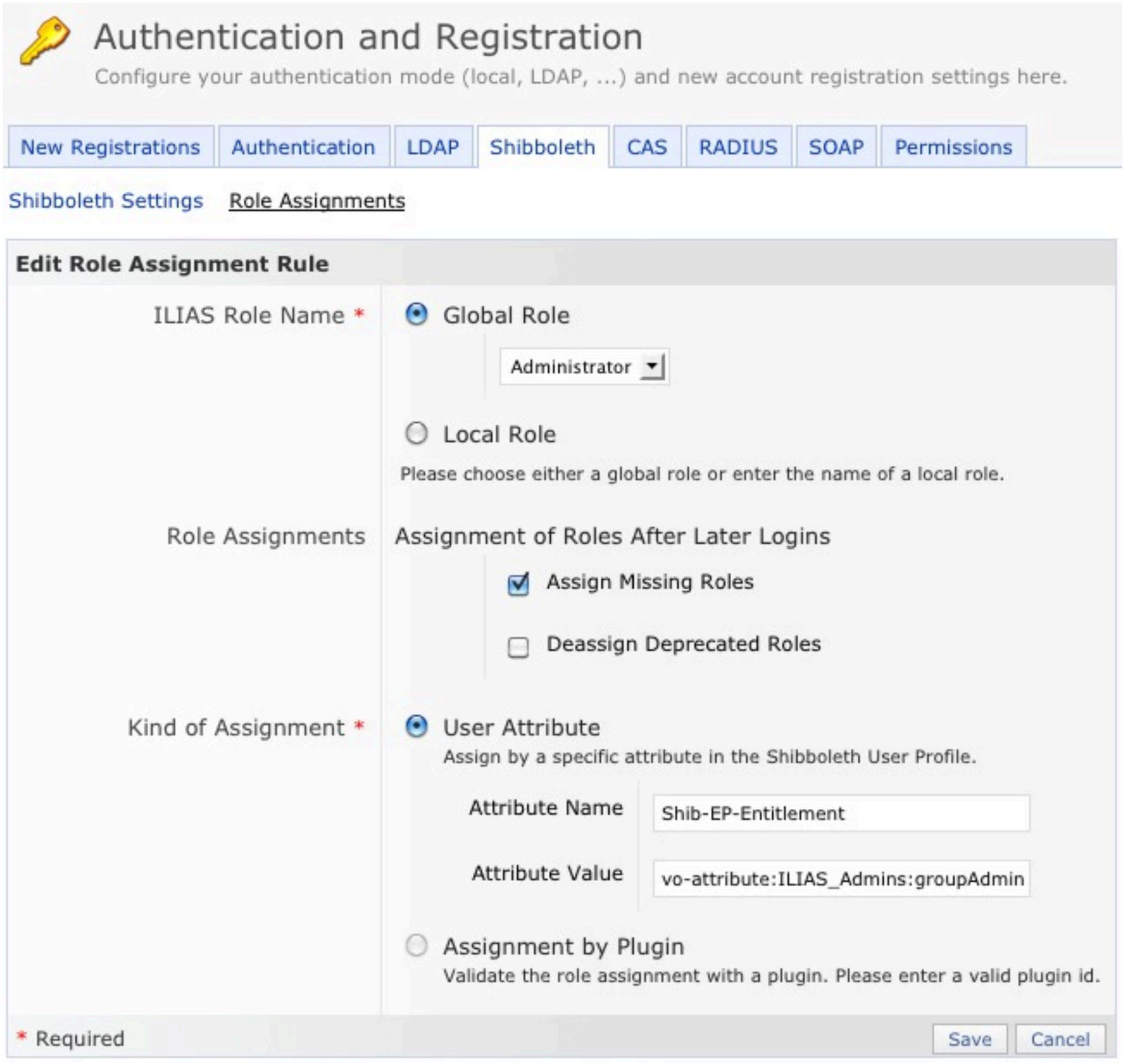
- Example: Moodle Shibboleth Settings



3. (Auto-) Enrollment

- Assign a user privileges or roles based on attributes
- Not available in many web applications yet:
  Available e.g. in ILIAS (see next slide)
- Should become more common in the future with the establishment of Virtual Organizations (VO)

(Auto-) Enrollment Example (ILIAS)



4. (Single) Logout

- Single-Log-In is “easy” but what about logout?

- Only concerns applications with own session management
- Logout implemented in Moodle, ILIAS and a few other web applications but support in Identity Provider still missing.
- **“Inedible cookies, sticky sessions and false hopes”** http://switch.ch/export/sites/default/uni/security/aai/event/aai-info-day-2009/slides/AAI-ID09-51-SLO.pdf

5. Account Deletion/De-Provisioning

- How to get rid of user entries of users who left an organization on application side?

- No solution in production yet!
  “How to find and kill zombie users”
  http://switch.ch/aai/support/presentations/opcom-200909/AAI-OpCom-Account-Checking.pdf

Technical Integration Issues

- **Login name vs user name vs screen name**
  Sometimes no attribute can be used as username
  - Generate screen name (e.g. ILIAS) or ask user for one (e.g. OLAT)
- **Password is not available as attribute**
  - Generate random password. Won't be used in general.
- **Related Non-Web services are not (yet) Shib-enabled**
  - Provide way for user to set password for that service
- **Federation-specific attribute names and values**
  - Provide mapping between Shibboleth and application attributes
  - Provide hook or API to do conversion/transformation

Short Summary for Developers

- **Shibboleth works with anything running behind Apache/IIS**
  CGI, PHP, Perl, Python, Java (via Tomcat), .Net, Ruby, ...

- **Shibboleth enforces authentication and authorization**
  Files, Directories, Sub-Directories, Locations

- **Shibboleth attributes available in web server environment**
  No API or library is needed to read them.