Issues of university shibboleth IdP in national federation

Ito, Eisuke
Research Institute for IT, Kyushu University

Nakakuni, Masanori
Research Institute for IT, Kyushu University

http://hdl.handle.net/2324/17781
Issues of university shibboleth IdP in national federation

Eisuke Ito and Masanori Nakakuni
ito.eisuke.523@cc.kyushu-u.ac.jp, Kyushu University
nak@fukuoka-u.ac.jp, Fukuoka University
Outline

1. Introduction
2. IDM and AuthN system
3. SSO Policy
4. Shibboleth IdP
5. Issues of university shibboleth IdP
6. Conclusion
1. Background

• Protected services in University
  – E-Learning, e-Syllabi, Researcher activity DB, Student portal, ...
  – E-Journal, Google Apps/Windows Live, ...

• Shibboleth SSO (Single Sign-on)
  – Distributed SSO Middleware
  – Identity Providers (IdP), Service Providers (SP). (and Discovery Service (DS))

• Federation
  – A trust relationship between Identity Providers (IdP) and Service Providers (SP).
  – NII of Japan deploys Shibboleth SSO Federation
    • Kyushu University joins this federation
## History

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Joined UPK</td>
</tr>
<tr>
<td>2006</td>
<td>kitenet (Wireless LAN over authN)</td>
</tr>
<tr>
<td>2007</td>
<td>University platform for authN. University ID</td>
</tr>
<tr>
<td>2008</td>
<td>ID Integration</td>
</tr>
<tr>
<td>2009</td>
<td>Shibboleth IdP</td>
</tr>
<tr>
<td>2010</td>
<td>Join UPKI-Fed (JP Federation)</td>
</tr>
</tbody>
</table>

**Joined UPK**

- **Kyushu Uni.**
  - LDAP
  - Password manager
  - University platform for authN.
  - University ID

**NII, Japan**

- UPKI
- UPKI Initiative
- Server Cert. service
- eduroam.jp
- GRID
- SSO trial
- UPKI-Fed Trail
- UPKI-Fed Federation
In this presentation,

- Show shibboleth IdP and SP in Kyushu University
- Report results of 3 month operation.
- Report issues of university shibboleth IdP in national federation
2. IDM and authN system in Kyushu U

- Campus wide authentication system
- IDM and LDAP server
  - IDM: Identity management system (Meta Directory)
  - LDAP server is used as password authenticator.
System Overview

Federated SPs
- E-Journal
- Refworks
- MS DS

Shibboleth SSO
- Shibboleth IdP (SSO)

Secure
- Critical Service
- Critical Service
- Matrix code authN
- Matrix code DB
- LDAP

ID/PW, or Matrix code
- kitenet (WiFi)
- Mail
- WebCT
- EZproxy
- My Library

Login
- System Overview
- IDM (Identity Manager)
- Password manager
- IC Card (User ID)
- ID card
- Personnel DB (staffs)
- Student DB (students)
- Active Directory
- Active Directory
- Enterprise system for officials
- Education system for students
- Other worker

IC Card (User ID)
- Personnel DB (staffs)
- Student DB (students)
- Active Directory
- Active Directory
- Enterprise system for officials
- Education system for students
- Other worker

LDAP
- Shibboleth IdP (SSO)
- IDM (Identity Manager)
- Password manager
- IC Card (User ID)
- ID card
- Personnel DB (staffs)
- Student DB (students)
- Active Directory
- Active Directory
- Enterprise system for officials
- Education system for students
- Other worker

Secure
- Critical Service
- Critical Service
- Matrix code authN
- Matrix code DB
- LDAP

ID/PW, or Matrix code
- kitenet (WiFi)
- Mail
- WebCT
- EZproxy
- My Library

Login
- System Overview
- IDM (Identity Manager)
- Password manager
- IC Card (User ID)
- ID card
- Personnel DB (staffs)
- Student DB (students)
- Active Directory
- Active Directory
- Enterprise system for officials
- Education system for students
- Other worker
Dataflow of IDM

Students

- Student DB
- Student list (Twice in a Year)

Learning System (PCs, Server, WBT)

Info. Infra. Initiative, Kyushu U. (Dept. of IT)

Staffs

- Personnel DB
- Staff list (Daily)

IDM (Identity Management Sys.)

- Account activation
- LDAP

Students and Staffs

- ID Card
Integrated Services

- WebCT (e-Learning)
- NetAcademy2 (English study)
- kitenet (WiFi)
- Campus licensed software download service
- Space management system
- Cute.Anyware (EZproxy, E-journal proxy by Library)
- Webmail (Primary e-mail service)
- Course registration and grade point management system
- Researcher activity DB
# 3. SSO Policy

- **Two categories**

<table>
<thead>
<tr>
<th></th>
<th>Internal service</th>
<th>Out sourced service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usability oriented</strong></td>
<td>• Webmail</td>
<td>• E-Journal services</td>
</tr>
<tr>
<td></td>
<td>• WebCT (e-Learning)</td>
<td>• RefWorks</td>
</tr>
<tr>
<td></td>
<td>• Software download site (licensed software)</td>
<td>• Google Apps</td>
</tr>
<tr>
<td></td>
<td>• Student portal</td>
<td></td>
</tr>
<tr>
<td><strong>Security oriented</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Financial system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Grade point management system</td>
<td></td>
</tr>
</tbody>
</table>

- **Reverse proxy SSO**
- **ID/PW, Matrix code**
- **Shibboleth SSO (SAML)**
Matrix code authN

- A kind of OTP (one time password)
- Matrix code is printed in IC card.
- Enter value of designated cell.

- For only secure services
  - Grade point system
  - Financial system
4. Shibboleth IdP

LDAP

SJSDS (Solaris)

LDAP Proxy (OpenLDAP)

OpenLDAP, CentOS.

Shibboleth IdP

Tomcat (CentOS)

_VMware_

(Winodws XP)

Works as attribute translator

Protected services in Kyushu U.

MyLibrary

EZproxy

WebCT

Shibboleth Web SSO
Kyushu University Library
http://www.lib.kyushu-u.ac.jp/
Results

• Two months
• No serious trouble.
• Some trivial matters.
  – Some users bookmark the IdP site.
    • 404 Not Found: /idp/Authn/Password 7time(s)
    • He/She can’t access to the service which he/she wants.
5. Issues of university shibboleth IdP

- Joins UPK-Fed (Japanese Federation)
- Issue(s)
  - Attribute filtering problem
    - Privacy policy
Attribute filtering problem

OK
Serves all attributes

No.
Against privacy policy.

Internal SPs
- MyLibrary
- EZproxy
- WebCT

External SPs
- Google
- RefWorks

LDAP
LDAP Proxy (OpenLDAP)
Solutions for attribute filtering problem

- **LDAP**
  - **Shibboleth IdP**
    - **Internal SPs**
    - **External SPs**
    - Write filter config. for each SP.

  - **XML Script**

- **LDAP Proxy (OpenLDAP)**
  - **Internal SPs**
  - **External SPs**
  - Write filter config. for each SP.
6. Conclusion

• A case study of Shibboleth SSO and Federation
• Decide SSO Policy
• Internal Services on Shibboleth SSO middleware
  – No serious trouble.
  – Some trivial matters.
    • Some users bookmark the IdP site.
• Joins UPK-Fed (Japanese Federation)
  – Attribute filtering problem
    • Privacy policy