SP / IdP cases

Ito, Eisuke
Research Institute for IT, Kyushu University

Abe, Eiji
Research Institute for IT, Kyushu University

Kasahara, Yoshiaki
Research Institute for IT, Kyushu University

http://hdl.handle.net/2324/17780

出版情報：29th APAN meeting, 2010-02-09
バージョン：published
権利関係：
UPKI update from Japan

SP / IDP CASES

Eisuke Ito, Eiji Abe, Yoshiaki Kasahara
Kyushu University
ito.eisuke.523@m.kyushu-u.ac.jp
Outline

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
1. Introduction

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
1. Introduction

- 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

2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011
--- | --- | --- | --- | --- | --- | ---

**Joined UPK**

- **Kyushu Univ.**
  - LDAP
  - Password manager
  - University authN platform
  - University ID
  - kitenet (Wireless LAN)

- **NII, Japan**
  - UPKI
  - UPKI Initiative
  - Server Cert. service
  - eduroam.jp
  - GRID
  - SSO trial

**ID Integration**

**Shibboleth IdP**

- Join UPKI-Fed (JP Federation)

**UPKI**

**UPKI-Fed Trial**

**UPKI-Fed Federation**
In this presentation,

- Show a case study of shibboleth IdP and SP operation in Kyushu University
- Report some problems of shibboleth IdP operation.
- Report results of two month operation.
2. Shibboleth SSO

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
2. Shibboleth SSO

- Before Shibboleth
  - Kyushu U
    - Students 18,000
    - Staffs 7,000 (prof. 2500)
  - Campus wide authentication system (since 2007.)
  - IDM and LDAP server
    - IDM: Identity management system (Meta Directory)
    - LDAP server is used as password authenticator.
System Overview

Other worker
Personnel DB
Student DB

ID card
IC Card (User ID)

Active Directory
Active Directory

Enterprise system for officials
Education system for students

Password manager
Matrix code DB
LDAP

ID/PW, or Matrix code

Critical Service
Critical Service
Matrix code authN

Secure

Shibboleth IdP (SSO)

IDM

Federated SPs

E-Journal
Refworks
MS DS

Shibboleth SSO

E‐Journal
WebCT
EZproxy
MyLibrary

Personnel DB
Student DB

kitenet (WiFi)

Shibboleth SSO

Mail

ID/PW

Critical Service

ID/PW, or Matrix code

IC Card (User ID)

E‐Journal
WebCT
EZproxy
MyLibrary
Dataflow of IDM

Students
- Student DB
- Student list
- Learning System (PCs, Server, WBT)
- Twice in a Year

Staffs
- Personnel DB
- Staff list
- IDM (Identity Management Sys.)
- Daily

- ID Card
- Account activation
- Staff
Integrated Services

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

<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>• University portal</td>
<td></td>
</tr>
<tr>
<td><strong>Security oriented</strong></td>
<td>• Financial system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Grade point management system</td>
<td></td>
</tr>
</tbody>
</table>

Shibbolize!
3. Problems of IdP

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
3. Problems of IdP

- Attributes matching
- Attribute filtering

Diagram:
- LDAP
- IdP
- SP
Attributes matching

Existing schema (attributes)

mismatch

eduperson schema

LDAP

Open LDAP (rewrite)

IdP

Solutions

Add/Change schema

Attributes Translation

Schema Matching

OpenLDAP’s rewrite module

attribute-resolver.xml
Attribute filtering

OK
Serves all attributes

IdP

No
Against privacy policy

Internal SPs
- MyLibrary
- EZproxy
- WebCT

External SPs
- Google
- RefWorks
Solutions for attribute filtering problem

1. Write filter rules for each SP.

2. Two IdPs

3. Filtering script

LDAP (rewrite)
4. Analysis

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
4. Analysis

Shibboleth IdP and SPs in Kyushu University

LDAP
SJSDS (Solaris)

Open LDAP (rewrite)
OpenLDAP, CentOS.

IdP
Shibboleth IdP, Tomcat (CentOS), VMware, Windows XP

Internal SPs
MyLibrary
EZproxy
WebCT
Kyushu University Library
http://www.lib.kyushu-u.ac.jp/
Results

- Two months operation
- 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.

<table>
<thead>
<tr>
<th></th>
<th>Students</th>
<th></th>
<th>Staffs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1815</td>
<td>18000</td>
<td>467</td>
<td>7000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(2500)</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>2291</td>
<td>25000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Top 200 users (10% users) occupy 41.2% access.
Statistics: Daily access
Statistics: Hourly access

Most user access at afternoon.
5. Conclusion

1. Introduction
2. Shibboleth SSO
3. Problems of IdP
4. Analysis
5. Conclusion
5. Conclusion

- A case study of Shibboleth IdP in a university
- Two problems for IdP construction
  - Attribute matching
  - Attribute filtering
- Two months operation
  - No serious trouble.
  - Got statistics
    - No over load
Thank you for your attention.