

9-5

Design of Authentication Infrastructure for the WEB Service Federation between Universities

Kazuhide Kanenishi¹, Kenji Matsuura¹, Yasuo Miyoshi², Kazumi Sagayama³,
Tomohiro Takagi⁴ and Yoneo Yano³

¹Center for Advanced Information Technology, The University of Tokushima

²Faculty of Science, Kochi University

³Graduate School of Advanced Technology and Science, The University of Tokushima

⁴Fujitsu Shikoku Systems

{marukin, matsuura}@ait.tokushima-u.ac.jp, miyoshi@is.kochi-u.ac.jp,
{sagayama, yano}@is.tokushima-u.ac.jp, takagi.tomohiro@jp.fujitsu.com

Abstract

Recently the computerization of the higher education progresses rapidly in Japan. A variety of WEB services are developed, and improve the usefulness of user such as students and faculty members. There are ever-increasing amount of web services. Developing the framework that cooperates between the WEB services, and offering it are important. As for the cooperation of the WEB services, the research and development are advanced as WEBSSO (WEB Single Sign On). We also develop the framework that cooperates between the WEB services and verify it. In addition, the demand on the cooperation interorganizational the WEB services are increase in these days. Such cooperation is called federation. Therefore, a new framework different from existing WebSSO architecture is needed. So, this study proposes the new model of the authentication and authorization. We achieve the federation by using OSS middleware Shibboleth that is developed at Internet2. However, the function is insufficient only the Shibboleth. Then, we have enhanced the Shibboleth. In addition, to verify the effectiveness of federation based on the management of the authentication and authorization, a prototype environment was constructed. The federation model is verified on the experimental environment.

Keywords

Single Sign On(SSO), Authentication Infrastructure, Federation, Authorization, WEB Services

Introduction

Informatization is advancing rapidly in higher education facilities in Japan. The ever-increasing

amount of web services such as course registration system, library system, a LMS (Learning Management System) has been introduced. On the other hand, managing several services appropriately for user is becoming a problem. For example, the user has to manage more than one set of user ID and password, generating a need to unify those user accounts. This has made very important to develop and offer a framework that coordinates each WEB service, encouraging the research and development of WEBSSO (WEB Single Sign On) that is a framework to liaison between the WEB services (Kanenishi et al., 2006).

In addition, the request for the cooperation among WEB services (credit transfer system, sharing of electronic educational materials) is increasing in these days. Servicing beyond organization is called Federation. Up to now, Federation has the related standard like SAML (SAML, Id-FF), however, it does not have its own standardization and a clear definition. Therefore, a new framework different from existing WebSSO architecture is needed. It is also necessary to strictly correspond to user's management and to share the authentication information among several organizations. For example, the library system can be used by other universities by achieving interorganizational federation. This does not mean that the public service is used. The students at other universities are treated just like the students at the own university. Adaptive management of the authentication and authorization is necessary to achieve the federation.

This study proposes a new model for authentication and authorization to realize Federation in higher education institutions. We achieve Federation by

using OSS middleware Shibboleth developed by Internet2 (Shibboleth). However, the Shibboleth still cannot provide sufficient functions.

For the Federation, personal information provider and service provider should cooperate appropriately. The policies should be exchanged among both providers beforehand and data (personal information) should be dynamically exchanged based on these policies. Processing such as switching service between student and teacher becomes possible at the stage of the authentication. Management function of the authorization information is not enough in the current Shibboleth. Therefore, we have enhanced that function of Shibboleth (Kanenishi et al., 2007).

To verify the effectiveness of the Federation enhanced the management function of authentication and authorization, a prototype environment was constructed. Two or more WEB service servers and a personal information server were constructed as the experimental environment then the Federation model was verified on the environment. We confirm the certain effectiveness by indicating that the authentication and authorization continued to function normally based on this model.

1 Realization of federation during WEB service

The cooperation of Web services by SSO mainly using the authentication infrastructure has advanced because of the introduction of Web Services to the university. As a result, it became clear that the higher educational facilities lack the aspect of sharing information among the internal departments. Here, we describe the model of the cooperation among the information systems at the university. The cooperation of the information systems operated at the university on WEB basis can be achieved by offering the following three kinds of functions:

1. Management of personal information
2. Management of authentication information
3. Management of cooperation among services

The function 1 and 2 are on the server side that manages and offers the authentication information and function 3 is on the general web server side that offers service. User's browser exists besides these functions. SSO in the organization is achieved by these three functions.

At present SSO at the university, there are a lot of cases where functions 1 and 2 are undifferentiated. Recently, the idea of personal information management (Identity Management : IdM) is accepted widely. The IdM distinguishes the data base containing original record of personal information from the data base containing account information and the idea of IdM dynamically generates account

information. Function 1 indicates the operation of the data base that stores the personal information managed by the student affairs section and a personnel section. Function 2 is an authentication infrastructure (mostly LDAP Service) generated from function 1, and also a function of authentication information management to check whether a user has been authenticated to the WEB service for SSO. Function 3 is implemented on various WEB server sides. Each WEB server does not manage the authentication information by itself and it requires the function to manage the authentication information working in concert with SSO server. The authentication information is managed among SSO server, WEB server and user's browsers. When a user moves among WEB services, the user does not have to input the password each time because the SSO server maintains authentication information during fixed time. In this way it is possible to assume SSO model within a single organization. However, this model cannot be applied directly to SSO among the universities. The model should be enhanced. We describe how to coordinate WEB services among the universities and realize Federation below.

The distinction between authorization and authentication, in addition to the function 1, 2 and 3, is important for realization of the Federation.

The authentication information management is to temporarily store the information whether the user is certified. Of course, managing authentication information is the essential function of SSO. On the other hand, higher educational facilities consist of several groups provided different attributes such as teachers, students and staff. In the service among different universities these attributes are complexly intertwined (i.e. a student of X University and a faculty member of Y University). The contents of the service provided by a system differ depending on the attributes. For instance, the e-Learning service provided is quite different depending on if the user logged in as a teacher or as a student.

In fact, the contents of the service are decided depending on attribute information. A framework for unifying the management of the attributes and for sharing the attribute information is necessary to realize dynamic authorization management. For instance, a student has the same attribute as a student in the library system or in the course registration system. The desire to unify the management of authorization information sharable among the systems is caused. Attribute information is personal information and it is possible to manage intensively by LADP server. Authorization is decided on the WEB service side based on the attribute information. The WEB service side decides on authorization from some personal

individual attributes in case of the authorization for the service provided only for the student taking the class of X experiment. Therefore, it is necessary to define the protocol to transmit the individual attribute among WEB server, SSO server and the browser in Federation.

In many higher educational facilities, a lot of WEB services are working now and of course, the existing system doesn't assume Federation. Therefore, a framework to share individual attribute among WEB services and decide authorization dynamically is not implemented. The individual attribute (authorization information itself) is stored on the WEB server. It is difficult to realize the Federation in disregard for the existing systems. When a user want to built in the existing systems, it is necessary to convert the unified user ID to the unique ID of each WEB service on the WEB server. This process of the conversion is important. To realize SSO the IDs are unified in the organization. On the other hand, the existing service is being operated by original user ID before the introduction of the unified ID. It's difficult to unify user IDs and renew the system operation.

We propose the two methods that enable to cooperate with the existing system on Federation as follows. One is a method that stores the individual information on each WEB services (authorization information) in the individual attribute of the authentication infrastructure (like LDAP server) (Fujiwara, 2007). The other is a method that converts the authorization information sent from the SSO server inside the WEB service. In that case, it is preferable to mount trans-

ducer function on the WEB server like a conversion server than to mount it on each WEB services.

The first method is feasible by increasing the entry of the database of the authentication infrastructure without changing the frame of Federation. The second method requires changing the frame in the WEB service. However, there is a lot of flexibility on the WEB service side. In this paper, we propose a method to enhance the WEB service.

2 Federation using Shibboleth

Shibboleth is a middleware of the open source to realize framework of Federation between the WEB services for higher educational facilities developed in Internet2 project. The Federation among the universities based on Shibboleth has realized in Switzerland (SWITCH), Finland (Linden, 2005) and United Kingdom (UK Access Management Federation).

Shibboleth is developed based on SAML as OASIS standard, and is open source middleware that offers solid security and Federation. Federation in Shibboleth is realized by two modules, IdP (Identity Provider) and SP (Service Provider). The source codes of IdP and SP are open to the public by Shibboleth project of Interenet2. IdP is implemented by Java and runs on Tomcat WEBserver. SP is developed by C++, however, there are other implementations. IdP is equivalent to authentication information management agent. IdP cooperates with LDAP servers and takes charge of managing authentication information in each organization. IdP is required to use the database such as LDAP as a repository of per-

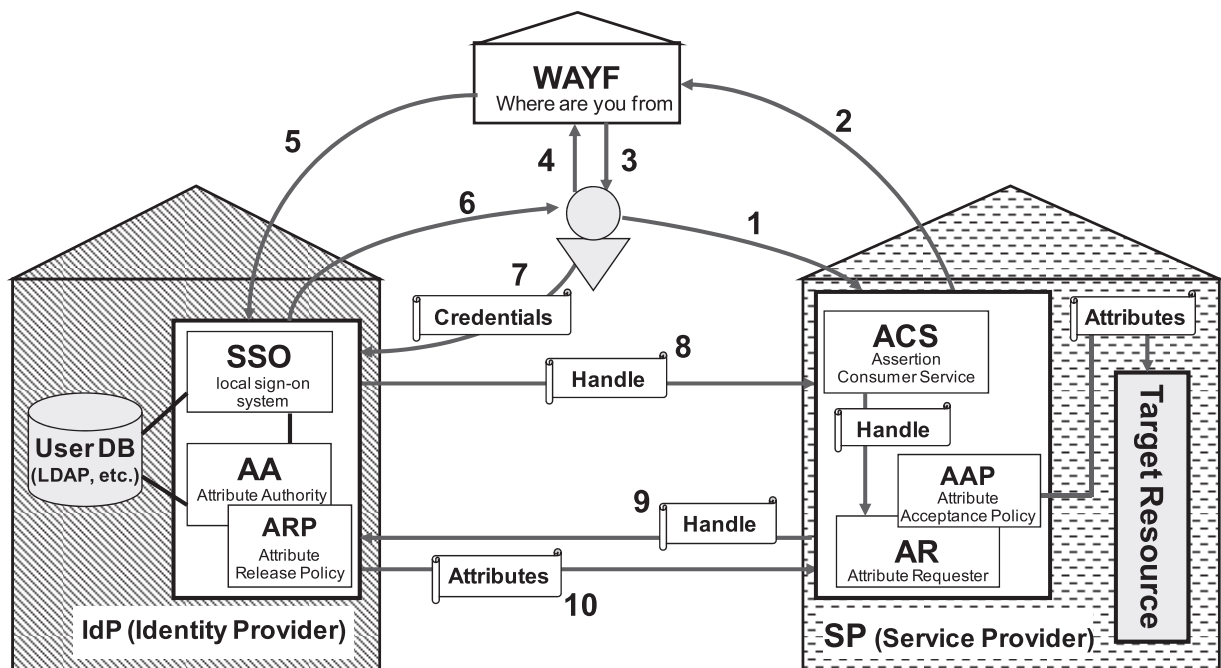


Figure 1: Outline of Shibboleth and Federation.

sonal information. SP corresponds to Service Provider agent and correspond one-to-one with WEB server that provides service called resource. SP usually runs with the same server as WEB server. The outline of Shibboleth is shown in Figure 1.

Shibboleth can put WAYF (Where are you from server) if necessary. WAYF bridges between SP and IdP. Concretely, HTTP access redirects from SP to WAYF. WAYF shows a list of IdPs. The user chooses an IdP where her/his authentication information is registered from the list of IdPs. There is another redirection to the chosen IdP from WAYF. Because it is assumed that several IdPs exist in framework of Federation, the WAYF lead to IdP in Shibboleth. WAYF is defined as the specification but it not included in a distribution. The user will implement WAYF for oneself.

First, the user accesses WEB service from a browser in Shibboleth. On the WEB server, SP redirects http access to IdP through WAYF. IdP certifies the user's authorization. An input screen of the user ID and password is generally shown on a browser. The result of the authentication is stored temporarily, and, in the meanwhile SSO becomes possible. After authentication, IdP acquires individual attribute from LDAP. IdP also correspond to TLS. In the future, authentication by PKI will be more popular than by password entry.

IdP notifies SP of an authentication result. The XML format called "handle" is used for the communication between SP and IdP. SP receives the handle then requests attribute information to IdP. At that time, attribute information is exchanged between IdP and SP according to the policy described beforehand (AAP,ARP). The policy defines the SP corresponding to IdP and the limitation of disclosure of the personal attribute. SP also defines what kind of attribute information should be requested to which IdP. A policy can control authorization partially. If attribute information is not transmitted to SP from IdP even if the authentication is approved, the WEB service cannot decide the authorization. As a result, it cannot start the service actually. Thus, it is possible for the IdP side to control the servicing providing side. When there are no specific problems, the individual attribute is sent to SP from IdP on a request from SP. SP transmit the authentication result and individual attribute to the WEB server. WEB server start to provide the service based on the received information.

When the user moves to new WEB service, the handle is exchanged between the destination SP and IdP. User's previous authentication information has been stored in IdP. It is transmitted to SP that the user is already certified. In this way, SSO is carried out. A user does not have to entry password every time

changing the services.

In Shibboleth, each WEB service is required to synchronize with SP. Therefore, it is necessary to change the program in an authentication part of WEB service.

3 Control of authorization by individual attributes conversion

3.1 Consideration of a method for authorization control

The conversion of individual attributes is necessary to achieve flexible Federation. There are two methods. One is to process the conversion on the IdP side and the other is to process the conversion on the SP side.

We think a conversion on the SP agent side is desirable and attempt to expand the SP agent. Management of authorization is primarily the matter on the side offering the service. Then it is not desirable to put individual information possessed by the servicing side on the IdP side. Moreover, there is a problem with putting authorization information on the personal information repository in other universities.

Therefore, we prepare a conversion server for converting the individual attributes. This conversion server cooperates with a SP agent and rewrites the individual attribute. We assume that more than one WEB services are operated in the organization. An individual attribute conversion server can be shared in the single organization. The administrator's load of management increases because the number of individual-attribute conversion servers increases. The administrator of WEB service defines a rewriting rule for the individual attribute on the organization's own conversion server. Then the SP agent is connected with the individual-attribute conversion server. The SP agent and the conversion server cooperate so that the individual attribute of each WEB service might be converted appropriately. Preparing the individual-information conversion server makes it easy to shift existing WEB service to Federation.

3.2 Add the conversion server

We describe the extension method for SP as follows: The outline of extension is shown on figure 2.

We propose the individual-attribute conversion server MICS (Mapping Information Control Server) for conversion of the real individual attribute in this expansion. So it is necessary to make the SP agent communicate with MICS. It necessary to extend SP in Shibboleth as our research is based on Shibboleth. SP can be changed directly, however, whenever SP is upgraded, SP has to be changed. Considering the actual operation, the method of changing SP directly is not practical. Therefore, instead of directly chang-

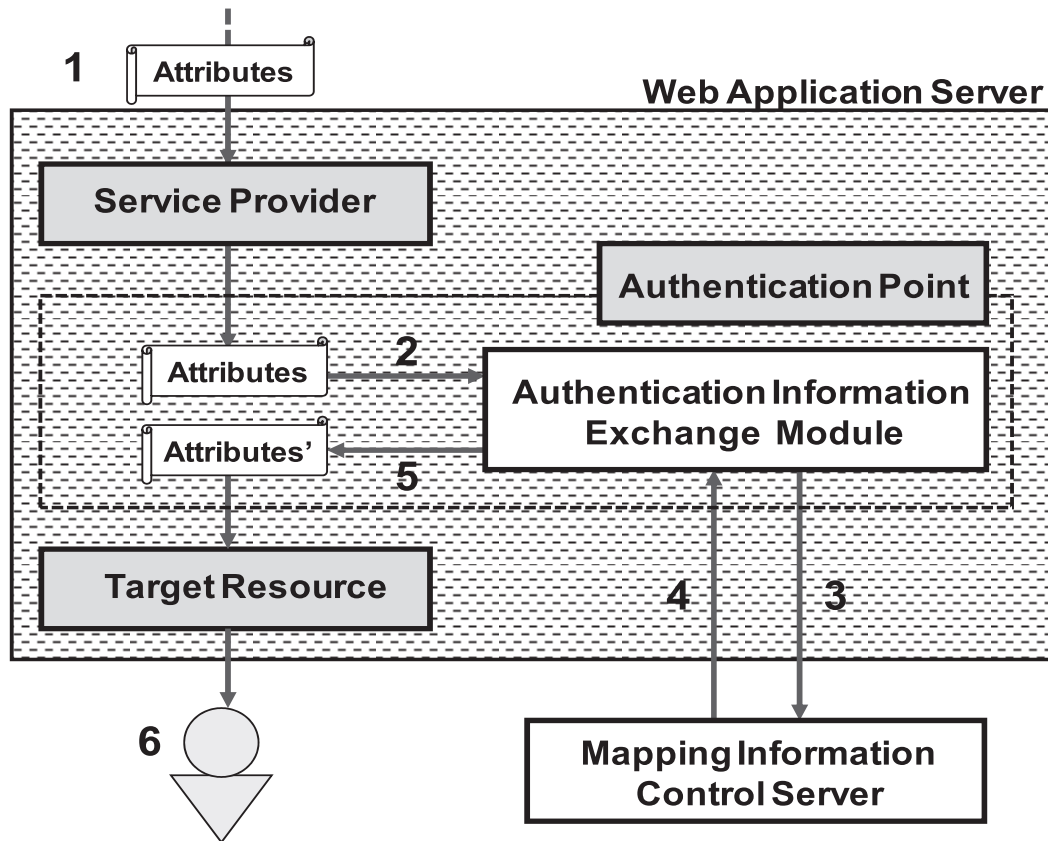


Figure 2: Extension of SP agent.

ing SP we adopt the method to hook data temporary at the phase of the data delivery between SP and WEB server. The interface that gives authentication and attribute information to WEB service exists in SP. An authentication result and attribute information are delivered via this interface. Therefore an entry point for connecting MICS is made at the interface. The information is converted just before the data is conveyed to the WEB service.

Concretely, we modified the authentication module of WEB service. The authentication part is a library form for Shibboleth in a great number of WEB services. Therefore, the cooperation with MICS can be realized by improving this library. In this experimental environment, we focused on Moodle (LMS system) as a target WEB service. Then we changed the authentication library of PHP for Moodle and realized communication function with MICS.

We implemented MICS as an independent server. We assumed to cooperate with more than one SP in the organization and made the function of conversion become independent as a server. MICS was implemented by Ruby in this experimental environment. An administrator of the WEB service defines the procedure of conversion beforehand with the rule based formula. The administrator defines the rule expressed by XML format on MICS. An example of a conver-

sion rule is shown in figure 3. Currently, a regular expression is adopted to describe the conversion rule.

The administrator of WEB server grasps the contents of the individual attribute exchanged between IdP and WEB server. The conversion rule that we assume consists of the condition clause and the action. If the condition is satisfied, the action is carried out. When the data satisfied the condition is sent (this condition is the combination of the name of individual attribute and its value), then MICS converts the value. The action does not only convert but also add and delete the attribute value. For example, when a student of X University receives WEB service provided by Y University, Y University firstly gets the individual attribute from IdP of X University. Next, MICS of B University collates the value of "University Name" and "User Account" in the condition clause of the conversion rule, and converts the value of the account to "x_user". In this example, all users of X University are integrated into the account of "X_user" in the server of Y University. Such operation will be carried out to judge if the student is a user of A University (it is not necessary to distinguish an individual user).

An example of the converted individual attribute is shown in Figure 2. This example shows the converted data sent to the WEB server on MICS. This

```

1 <?xml version="1.0" encoding="UTF -8"?>
2 <match>
3   <condition>
4     <pattern>
5       <id type='string'>0001</id>
6     </pattern>
7     <pattern>
8       <id type='regexp'><![CDATA[^\t.*]]></id>
9     </pattern>
10    <result>
11      <id>staff</id>
12      <lastname>staff</lastname>
13      <firstname>staff</firstname>
14      <mail>staff@example.edu</mail>
15      <authorization>1</authorization>
16    </result>
17  </condition>
18  <default>
19    <result>
20      <authorization>0</authorization>
21      <description><![CDATA一致しません]]></description>
22    </result>
23  </default>
24 </match>

```

Figure 3: Example of conversion rule.

```

1 <match>
2   <info>
3     <lastname>tarou</lastname>
4     <firstname>yamada</firstname>
5     <id>0001</id>
6     <mail>yamada@test.ac.jp</mail>
7     <dn>urn:mace:shibboleth.test:ldap.example.edu</dn>
8     <sysid>moodle</sysid>
9   </info>
10  <result>
11    <id>staff</id>
12    <lastname>staff</lastname>
13    <firstname>staff</firstname>
14    <mail>staff@example.edu</mail>
15    <authorization>1</authorization>
16  </result>
17 </match>

```

Figure 4: Example of conversion result.

data corresponds to the arrow 4 in Figure 2. The attribute values before and after the conversion are stored in this data. The authentication result is also stored together. Here a user account is converted from “0001” to “staff.” In Figure 4 information of arrow 3 received from IdP are sent to MICS. WEB service uses a necessary part from the data shown in Figure 4.

4 Experiment and consideration

4.1 Experiment

We developed an experimental environment to verify the framework of Federation we proposed in this paper. The outline of the experimental environment is shown in Figure 5.

One server (Celeron D, 3.20GHz, 512Mbyte, Vine Linux) was prepared for IdP and OpenLADP in the experimental environment. There is only one IdP server, therefore, WAYF of simple type was prepared in the same server as IdP. Two Moodle servers (Pentium 4, 1.4GHz, 256Mbyte, Vine Linux and CentOS) were prepared as WEB service. The Moodle server and SP run on each WEB server. SP extended to work in conjunction with MICS. A server (Celeron D, 3.20GHz, 512Mbyte, Vine Linux) for MICS and some PCs (Core 2 Duo, 2.66GHz, 2Gbyte, Windows XP) were prepared. The framework of Federation was verified by this configuration. First, we experimented on whether the user could log in. The user’s authentication information is managed by one IdP server, and the user should be able to login by the same user ID and password to two Moodle servers. As a result, the all user could log in two Moodle servers without any problem.

Next, we attempted to convert the individual attribute by MICS. The user tried to connect to two Moodle servers and we checked whether user ID was converted. As a result, we examined whether a user was able to log on with different authorizations of administrator and guest. An individual attribute will be converted based on the conversion rule defined on MICS beforehand. As a result of the experiment, the user was able to log on to each Moodle server using single user ID. In addition, the user was able to log on with different authorizations such as administrator and guest.

We confirmed that MICS could be converted without any problem.

The experiment on the simultaneous access by approximately 100 users was also conducted. In this experiment a large number of simultaneous logins were generated by the program, however, any significant delay was not caused for login.

4.2 Consideration

We checked the operation of the system and conducted a simple load experiment.

There were basically no problems with both check and experiment. Although we were concerned about more than hundred simultaneous accesses to IdP, there were no serious problem by the access concen-

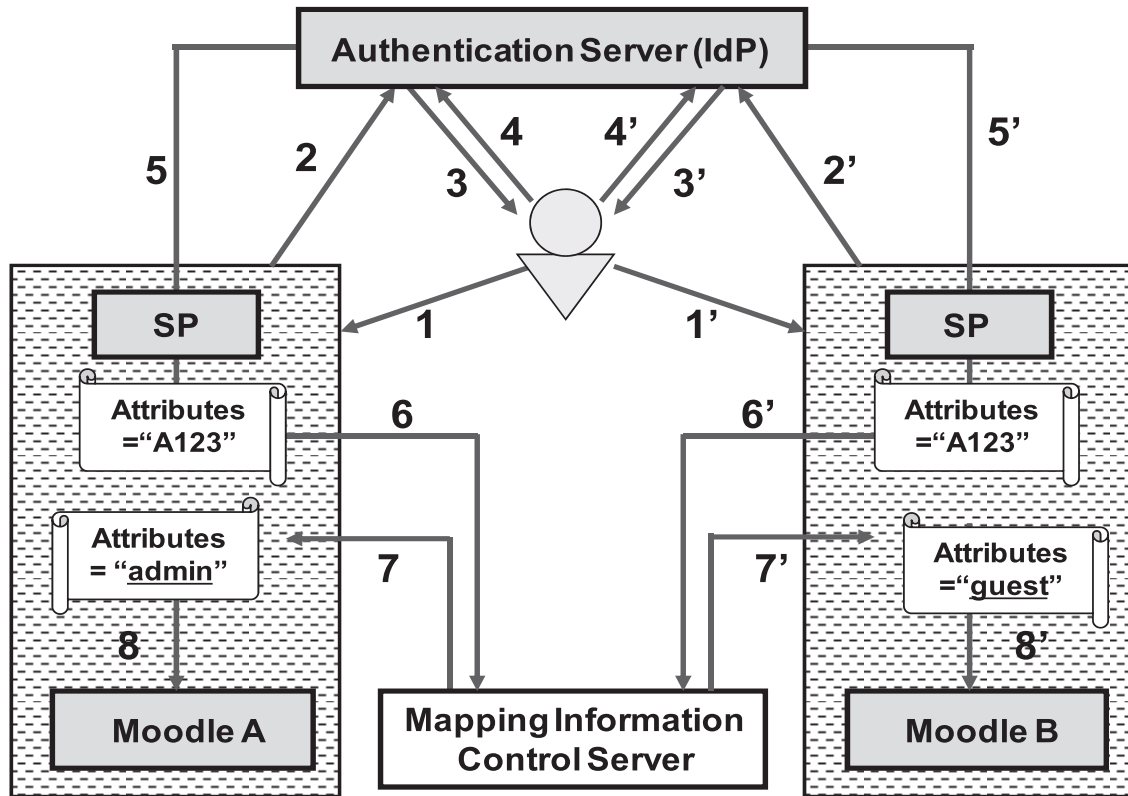


Figure 5: Outline of experimental environment.

tration. However, because IdP is based on Tomcat, the load is a concern when login concentrates simultaneously. Because this problem largely depends on the hardware, it will be possible to handle.

OPenID (OPENID) also offers SSO. However correspondence to security is not always enough in OPENID. The way of cooperation during organization like a university is not also clear.

CAS is also the framework which achieves SSO (CAS). However, CAS targets SSO in the organization. CAS dose not describe the Federation. Pubcookie is in the same frame as CAS (Pubcookie). Architecture is the same as CAS. Implementation is only different.

Several software vendors provide SSO frameworks (ADFS, Icewall SSO, Sun Java System Access Manager). These frameworks offer general-purpose Fedearion. These are not most suitable as Federation for higher educational facilities. It is important to consider the Federation in the higher education organization.

5 Conclusion

This paper described a framework of Federation aiming at WEB service cooperation among the universities. The more the number of WEB services increase, the more the necessity of cooperation beyond the boundary of each university will increase.

The establishment of the Federation technology is highly expected.

For achieving Federation, this paper indicated the importance of the management of authorization information as well as the sharing of authentication information. Then, we described that it was possible to achieve the management of authorization by exchanging individual attributes in Federation. In addition, we proposed to convert individual attributes to realize a flexible system. The flexibility of Federation increases by adding the function of converting individual attributes.

We constructed an experimental environment by using Shibboleth that was the middleware of open source. In the experimental environment, the proposed conversion function of the individual attribute was implemented. The result of verification confirmed that the cooperation of the system ran correctly in the experimental environment. Constant effectiveness was confirmed about the proposed method

In future we plan to introduce Federation into The University of Tokushima based on the proposed method.

Acknowledgement

This research was partially supported by the Grand of Strategic Information and Communications

R&D Promotion Programme (SCOPE), Ministry of Internal Affairs and Communications, Japan.

References

- ADFS , Microsoft,
http://www.microsoft.com/japan/windowsserver2003/R2/identity_management/ADFSwhitepaper.mspx
- CAS, JA-SIG Central Authentication Service,
<http://www.ja-sig.org/products/cas/>
- Icewall SSO, HP,
<http://h50146.www5.hp.com/products/software/security/icewall/sso/feature/flexibility.html>
- Id-FF, Liberty Alliance Project,
<http://www.projectliberty.org/>
- Kanenishi, K., Matsuura, K., Oie, T., Miyoshi, Y., Sano, M. and Yano, Y., (2006), Construction and Operation of a Portal System at Tokushima University, *Proceedings of E-Learn 2006*, pp.642-647.
- Kanenishi, K., Matsuura, K., Sagayama, K., Miyoshi, Y., Minato, J., Takagi, T. and Yano, Y. (2007), Progress of the Federation for Campus SNS Using the Shibboleth, *ICCE2007 Supplementary Proceedings*, Vol.2, pp.309-311.
- Linden, M., (2005), Organizing Federated Identity in Finish Higher Education, *TERENAS Networking Conference 2005*,
http://tnc2005.terena.org/programme/presentations/show.php?pres_id=77.
- OpenID ,Open ID Foundation, <http://openid.net>
- Pubcookie , Pubcookie Project,
<http://www.pubcookie.org/>
- Sun Java System Access Manager, Sun Micro Systems
http://jp.sun.com/products/software/identity/access_mgr/
- SAML , OASIS(Organization for the Advancement of Structured Information Standards),
<http://www.oasis-open.org/specs/index.php#samlv2.0>
- Shibboleth ,Shibboleth Project,
<http://shibboleth.internet2.edu/>
- Fujiwara, S., Komura, T. and Okabe, (2007), Y. A Privacy Oriented Extension of Attribute Exchange in Shibboleth, *2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p.28.
- SWITCH, Serving Swiss University,
<http://www.switch.ch/>
- UK Access Management Federation,
<http://www.ukfederation.org.uk/>