# ARchive system for Cross-reference Across Distributed Environment (ARCADE) Applicable to Sharing of Educational Materials among Inter-University Consortium

TAKUYA MATSUHIRA, YOSHIYA KASAHARA, and YOSHIHIRO TAKATA
Information Media Center
Kanazawa University
Kakuma-machi, Kanazawa-shi, Ishikawa
Japan
takusng@kenroku.kanazawa-u.ac.jp

*Abstract:* - Today, opportunities are increasing for collaboration between universities in many areas such as education, research and business. Against this background, we have developed "ARchive system for Cross-reference Across Distributed Environment (ARCADE)", by which user can share files in safe and secure way with other users over boundaries of different organizations. It is worthy of notice that even a user who does not have sufficient ICT skill can manage the system as ARCADE is implemented as a Java GUI application. We have attempted to apply this system for exchanging educational materials between universities. In the present paper, we introduce the configuration of our system and discuss its adaptation to an educational setting.

*Key-Words:* - shibboleth, single-sign-on, authentication, authorization, attribute, federation

## 1 Introduction

Recently, opportunities have increased for collaboration between universities in many areas such as education, research and business. In such situations, files such as reports, documents and research papers need to be shared; however, authenticating users belonging to different universities remains a challenge. For this reason, file sharing is difficult. It is also pointed out that it is not sufficient to define data access policy of their files simply as fully open access or subscribers only. That is to say, there are many types of data access policy depending on the file.

Against this background, we have developed "ARchive system for Cross-reference Across Distributed Environment (ARCADE)", which allows the data owner to share data easily with appropriate users across organizational boundaries. This system uses the open-source Shibboleth software package, which is based on the SAML2.0 protocol for single-sign-on across or within organizational boundaries. This software can be used to share, upload and download data files among closed communities. Systems similar to ARCADE have also been developed [1]. However, ARCADE is implemented in Java and has a GUI. Therefore, regular users can utilize the system simply by using drag-and-drop action. In addition to this feature, user can easily control access policies on the basis of Attribute Based Access Control (ABAC) [2].

This system is expected to be highly useful; thus, we attempted to apply the system to an educational setting. Recently, institutions of higher education have seen considerable changes in student education. Previously, a student belonged to one university and could not take a course at other universities. Today, in contrast, the student can take courses at other universities. As it becomes more common for students to transfer credit between universities, the difficulty of dealing with grade reports and teaching materials will increase. Accordingly, we adapted ARCADE to the sharing of educational material.

In this paper, we introduce the mechanism of ARCADE and present an example of adapting ARCADE to an educational setting.

## 2 ARCADE Specifications

This section presents an overview of the ARCADE specifications.

### 2.1 About Shibboleth

We use the Shibboleth [3] architecture as the ARCADE framework.

Shibboleth is a project of the Middleware Architecture Committee for Education of Internet2 [4].

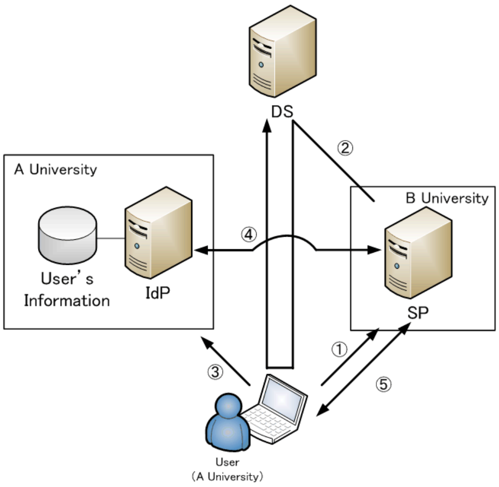


**Fig.1 Conceptual image of Shibboleth**

It is based on SAML2.0 [5], and so we can implement single-sign-on and sharing of attributes among different information systems. Shibboleth consists of three systems. Identity Provider (IdP) authenticates the user and sends the user's attributes to Service Provider (SP). SP requests the user's authentication for IdP and sends attributes to the application running on the SP server. Discovery Service (DS) provides information to ensure that the user chooses the correct IdP when multiple IdPs are available.

The operation of Shibboleth is presented schematically in Fig.1. First, a user at University A accesses the SP of University B. Second, SP redirects to DS so that the user chooses the IdP of the user's organization. Third, the user selects the proper IdP and is authenticated by their ID/Password. Fourth, the IdP returns the result of authentication; when the result is true, the SP requests the attributes that the SP needs to authorize the user. Fifth, the SP offers the service requested by the user.

## 2.2 Usability of ARCADE

In this subsection, we discuss the usability of ARCADE. High usability is essential because ARCADE users may have only basic IT skills. Concretely, we have attempted to hide from users the existence of servers such as IdP, SP, DS and LDAP. Thus, we developed ARCADE as a Java application.

ARCADE has been implemented by using the Standard Widget Toolkit (SWT) [6], which is constructed by Eclipse [7]. One of the best features of SWT is that it uses the native OS's widgets, such as buttons and textboxes. As a result, ARCADE runs quickly and its appearance is like that of the OS. Furthermore, ARCADE is started up by Java Web Start [8]. Thus, users can start ARCADE via a Web browser. The advantages of Java Web Start are as follows.

- Users only click a link to start ARCADE.
- Users can use the latest version.
- Users do not need to install or update software.

For these reasons, users can use ARCADE easily.

## 2.3 How to use ARCADE

In this subsection, we describe the use of ARCADE.

### 2.3.1 Authentication

When the user accesses ARCADE via a Web browser, the user is redirected to DS in order to authenticate his own organization's IdP. The user selects the correct IdP (Fig.2). Then, the user inputs an ID and password (Fig.3).

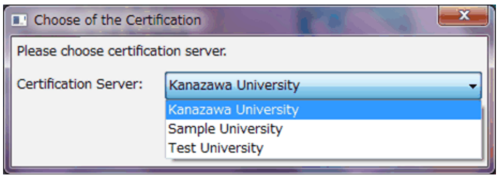
After the user is authenticated, ARCADE can retrieve the SP's information.

### 2.3.2 Method of access control

We next discuss access control in ARCADE. An overview of data management in ARCADE is shown in Figure 4. Data management consists of three parts: display of directories, display of files and setting access control.

All SPs accessible to a user are displayed in the same manner that the OS displays disk drives. The user can view the directory tree if the user has appropriate permissions. The user can create/delete directory simply by right-clicking on a directory, and a subtree can be created.

Second, we explain the display of files. When the user selects a directory, ARCADE displays information about files in the directory. The user can

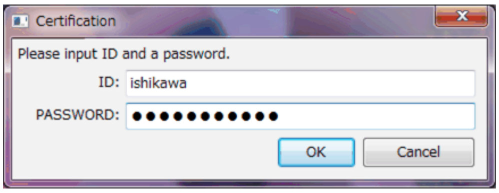

Choose of the Certification

Please choose certification server.

Certification Server: Kanazawa University

Kanazawa University
Sample University
Test University

**Fig.2 Snapshot of DS page (IdP selection)**

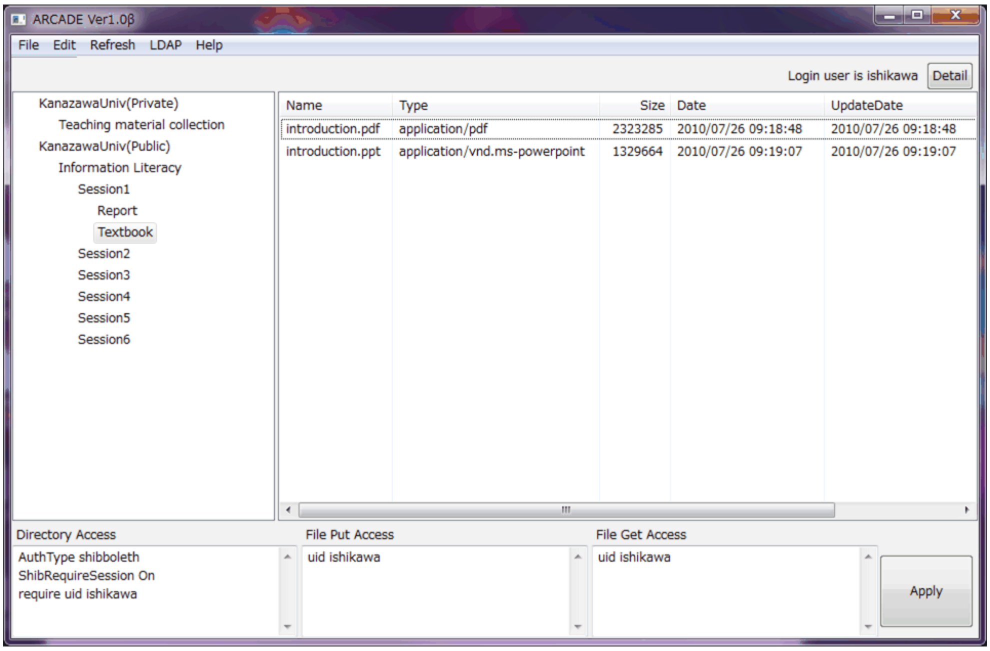

Certification

Please input ID and a password.

ID: ishikawa

PASSWORD: ●●●●●●●●●●●

**Fig.3 Snapshot of authentication page**



Login user is ishikawa

KanazawaUniv(Private)
Teaching material collection
KanazawaUniv(Public)
Information Literacy
Session1
Report
Textbook
Session2
Session3
Session4
Session5
Session6

| Name | Type | Size | Date | UpdateDate |
|---|---|---|---|---|
| introduction.pdf | application/pdf | 2323285 | 2010/07/26 09:18:48 | 2010/07/26 09:18:48 |
| introduction.ppt | application/vnd.ms-powerpoint | 1329664 | 2010/07/26 09:19:07 | 2010/07/26 09:19:07 |

Directory Access

```
AuthType shibboleth
ShibRequireSession On
require uid ishikawa
```

File Put Access

```
uid ishikawa
```

File Get Access

```
uid ishikawa
```

**Fig.4 Snapshot of ARCADE page**

drag and drop files if the user has appropriate permission.

Third, we discuss the display of files and the setting of access control. The user can set three types of restriction on each directory. All settings are controlled by the attributes of the user. These nine attributes include the user's e-mail address, organization name and user ID. "Directory Access" can control whether to display the directory on the position of "Display of directories". This can be set for each directory.

"File put access" can control whether the user is permitted to upload files to the directory. Also, "File get access" can control whether the user is permitted to download files from the directory. These control settings can also be set for each directory.

## 3 Application to Educational Setting

This section presents a demonstration of the proposed system in a university setting.

### 3.1 Example of using ARCADE

We next present an outline of a proof of concept. The test was carried out as follows.

- There are three organizations: Kanazawa University, Sample University and Test University.
- Kanazawa University's user, whose ID is *ishikawa*, offers a course called "Information Literacy".
- Sample University's user, whose ID is *sample01*, takes this course.
- Test University's user, whose ID is *test01*, collaborates with *ishikawa* for this lecture.
- This course ended session3, so *sample01* can download the textbook and upload the report until session3.
- *Test01* can download and upload textbooks and access the private teaching materials of *ishikawa*.

### 3.2 Result of using ARCADE

The directories displayed to each user are shown in Fig.5. The user *ishikawa* can access all SPs and directories, and can set all permissions. The user *test01* can access "Teaching material collection" and textbooks for all sessions. "Teaching material collection" can only be downloaded by *test01*, and textbooks can be both downloaded and uploaded by *test01*. The student's report cannot be accessed by *test01*. The private SP of Kanazawa University is not displayed to *sample01,* who can download the textbook and upload a report until Session3. Neither *test01* nor *sample01* can change the access control for each directory.

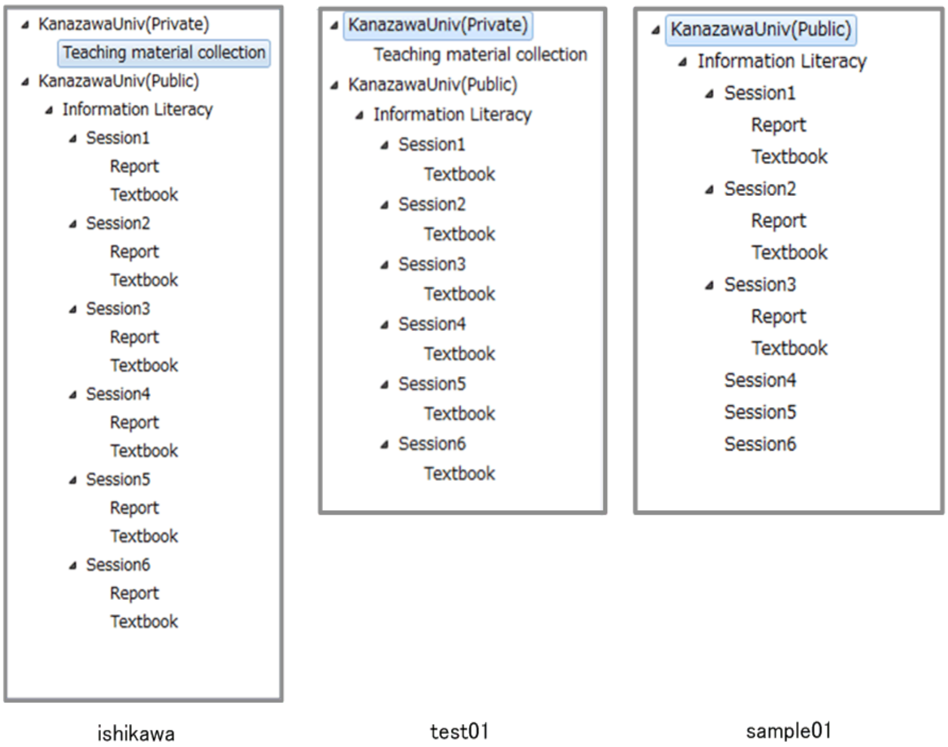


**Fig.5 Folders according to user access control policies**

## 4 Conclusion

In this study, we developed the ARCADE system, with which user can share files easily and safely across organizational boundaries. Furthermore, ARCADE is implemented as a Java GUI application; thus users with only basic IT skills can use the system to share and access files.

In a demonstration, we adapted ARCADE for an educational setting. The proof of concept was successful and therefore ARCADE can be used in many situations relating to education.

Looking toward the future, we plan to actually implement ARCADE, and to work to spread its use.

## 5 Acknowledgements

This work was supported by a Grant-in-Aid for Young Scientists (B) from the Japan Society for the Promotion of Science (22700809).

*References:*

[1]L. Ngo and A. Apon, Using Shibboleth for Authorization and Authentication to the Subversion Version Control Repository System, *International Conference on Information Technology (ITNG'07)*, 2007, pp. 760-765.

[2]E. Yuan and J. Tong, Attributed Based Access Control (ABAC) for Web Services, *IEEE International Conference on Web Services (ICWS'05)*, 2005, pp. 561-569

[3] Shibboleth, http://shibboleth.internet2.edu/

[4] MACE, http://middleware.internet2.edu/MACE/

[5] SAML2.0, http://www.oasis-open.org/specs/index.php

[6] SWT, http://www.eclipse.org/swt/

[7] Eclipse, http://www.eclipse.org/

[8] Java Web Start, http://java.sun.com/javase/technologies/desktop/javawebstart/index.jsp