Institutional authentication platform for trustful inter/intra-institutional ubiquitous services

Ito, Eisuke
Research Institute For Information Technology, Kyushu University : Associate Professor : Information Science

Kasahara, Yoshiaki
Research Institute For Information Technology, Kyushu University : Assistant Professor : Information Science

Nogita, Megumi
Research Institute For Information Technology, Kyushu University : Research Technician : Information Science

Suzuki, Takahiko
Research Institute For Information Technology, Kyushu University : Associate Professor : Information Science

出版情報：pp.103-108, 2007-12
バージョン：
権利関係：

Institutional authentication platform for trustful inter/intra-institutional ubiquitous services

Eisuke Ito, Yoshiaki Kasahara, Megumi Nogita and Takahiko Suzuki
Research Institute for Information Technology, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581, JAPAN.
E-mail: {itou, kasahara, megumi, suzuki}@cc.kyushu-u.ac.jp

Abstract

To realize trustful inter/intra-institutional ubiquitous services, we must consider not only information security but also identity federation between institutions. User authentication mechanism must be implemented for secure and personalized services. For inter-institutional services or nationwide services, it needs inter-institutional user authentication, but it is very difficult to manage inter-institutional identity database. ID federation is a solution for this problem. Each institution constructs an IdM (Identity management) system as an IdP (Identity provider), and provides user identity data to SP (service provider) for user authentication and authorization. In this paper, the authors describe about background and design of IdM and IdP in a institution. This paper also describes a case study about ID federation such as UPKI and eduroam.

1. Introduction

Recently a variety of information services are being provided, and they can be classified into two types, one is open service, and the other one is closed service. For instance, Google's web search service is one of the most major open services. Everyone can use the service without user registration or user authentication. On the other hand, Google's "iGoogle" is a closed service because it needs user authentication to provide personalized service.

Usually a university provides some internal information services, such as course registration, grade point checking, and official announcement about lectures. These services are usually closed and non-members can't use the services. These services often deal with private information such as grade points of a student, so it is necessary to consider security and it is difficult to open the end point of user access to the outside of the institutional network. The university issues a pair of ID and password to each student/staff. Each internal service has a user authentication mechanism. A user enters his/her credential (user ID and password, in many cases) into the authentication system. When the credential is valid, the service is provided to the user.

Conventional authentication system uses password [3][4]. The more membership oriented closed service systems are provided, the more ID/password pairs are issued. Then user authentication procedure becomes complicated, and it causes security level decline because users forget their ID/password easily. To solve the problem, a centralized or federated authentication platform is required.

Recently, demand for inter/intra-institutional ubiquitous service is arising, for example, cooperation of services in a university or institution, unit exchange programs between cooperated universities, grid computing, and so on. However, to realize trustful inter/intra-institutional ubiquitous services, we must consider not only information security such as prevention of packet sniffing and data tampering, but also implementation of identity federation between institutions. So, IdM (identity management) and identity federation are researched and developed.

In this paper, we describe the intra-institutional IdM and the campus wide authentication platform in Kyushu University. The IdM and the authentication platform are developed for intra-institutional services, but they can be used as an identity provider for nationwide or worldwide inter-institutional services. We describe their mechanism, our policy and plan of them. After that, we describe UPKI, eduroam, and implemented eduroam system in Kyushu University.

2. IdM and campus wide authentication platform in Kyushu University

We are developing an IdM (identity management) system and a campus wide authentication platform for

intra-institutional information services. In this section, we describe our policy, action plan, and system overview of the IdM and the authentication platform.

2.1. Demand for IdM and SSO in institution

In a large-scale organization, multiple information services are often provided for members. Information service needs user authentication mechanism if it is a membership oriented closed service, and conventional authentication system uses password. Consequently, a member has many ID/password pairs, because information service is developed independently and each system developer issues a pair of user ID and password independently.

This situation is introducing complications to both end-users and administrators. There are three complications about user account management; the first is end-user's authentication complication, the second is end-user's password management complication, and the third is administrator's user account management complication.

Figure 1 shows three complications of user account management.

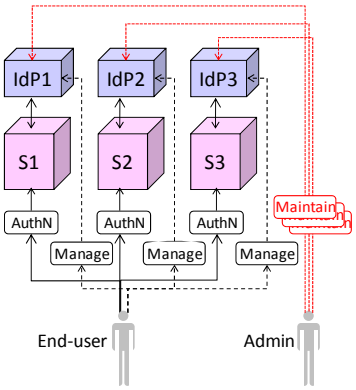

Figure 1. Three complications

The same situation which is showed in Figure 1 is occurred in Kyushu University. It's so complicated that both end-users and administrators request to reduce complexity. A centralized identity management system and a campus wide authentication mechanism were necessary to solve this problem.

2.2. Policy and action plan

We decided a policy and made an action plan to achieve safe and enhanced information services.

2.2.1 Policy. We decided basic policies for the campus wide authentication system.

- Reduce complications and complexity
- Easy to use
- More secure (or keep present security level)
- Applicable to existing service systems

We must reduce complications and complexity about user authentication and user account management because this is the motivation of our plan. The new authentication mechanism must be easy to use. If it is difficult to use, it's meaningless. Additionally, the new authentication system should be more secure than present system security level, or at least it should keep present security level. Finally, the new authentication system should be applicable to existing service systems. If it's not applicable, then additional development will be needed and the cost of development becomes high.

2.2.2. Action plan. According to the policies, we decided the following action plan.

- Construct an IdM (identity management) system (including a central member database).
- Provide a single user ID and password pair for one member.
- Construct a campus wide authentication mechanism
- Implement SSO (single sign-on).
- Introduce e-tokens for authentication and security
- Realize an authorization mechanism for sophisticated access control

Firstly, we decided to construct the IdM (identity management) system. IdM manages the identity life cycle of entities (members in this case). The identity life cycle includes establishment, description and destruction of identity. In the establishment stage, a name (or number) is bound to a member. In the description stage, one or more attributes which are applicable to the particular member may be assigned to the identity. The description may be changed according to the member's situation change. In the destruction stage, the identity of a particular member is destroyed. In case of disappearance of a member, such as retirement or resignation of the staff, or graduate and dropout from school, his/her identity record will be removed from IdM.

Secondly, we issue a single pair of user ID and password for a member[1][2]. So, we want to assign a "true identifier" for a member, that is, an identifier which always refers to the same entity (a member in this case).

Next, we construct a campus wide authentication mechanism for intra-institutional services [2]. By centralizing user authentication system, it is possible to reduce complexity and to realize a simple system.

We also want to install a web SSO system and e-tokens. SSO enables a user to authenticate once and

gain access to the resources of multiple service systems. E-token is a good solution to reduce complications in authentication procedure and to enhance security level. We consider IC-card with PKI certificates for user authentication.

Finally, we want to realize an authorization mechanism for sophisticated access control. For attribute based or role based authorization, the IdM has to keep various kinds of attribute.

Figure 2 shows the image of simplified system.

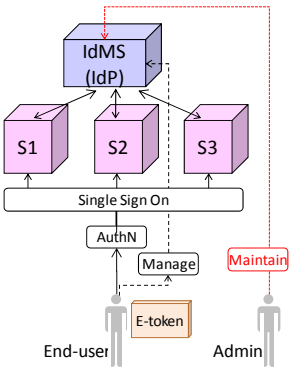

Figure 2. Simplified authentication system

2.3. System overview

Figure 3 shows the overview of the implemented IdM and campus wide authentication platform. Member data is exported from personnel databases and imported to the meta-directory (the member DB) through data cleansing and scheme matching. Staff data is exported by the personnel division, and student data is exported by the student division. Some other member data, such as guest researchers or short time international students, is added by each school. The meta-directory has additional attributes for attribute based authorization.

We construct two directories with LDAP server and MS active directory. The LDAP server is referred by web based systems, and network service systems such as SSL-VPN and 802.1X access control. The MS active directory is referred by MS products such as Windows PC.

Web SSO system is not installed yet. Web SSO solutions are abundant at the intranet level, for example, using cookies or a reverse proxy. Some free and commercial SSO or reduced sign-on solutions are currently available. In the near future, we will install a Web SSO system.

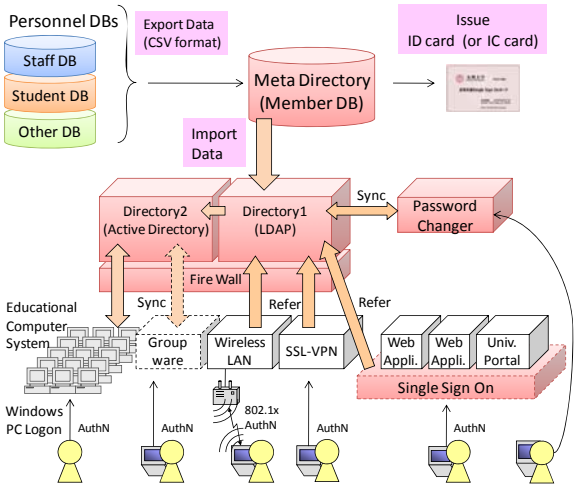

Figure 3. Overview IdM in Kyushu Univ.

3. ID-federation for inter-institutional services

As mentioned in previous sections, requirement for membership oriented inter-institutional service is arising, for instance, grid computing, web based service cooperation, and wireless LAN roaming. Web based service cooperation is the most required.

To realize ubiquitousness for membership oriented closed service, you must consider not only information security such as prevention of packet sniffing and data tampering, but also implementation of identity federation between allied institutions. In this section, we describe some ID federation mechanisms.

3.1. SAML

SAML is an XML standard for exchanging authentication and authorization data between security domains. Where, security domain means an IdP (identity provider) which is a producer of assertions, or an SP (service provider) which is a consumer of assertions. SAML is developed to solve the web browser SSO. SAML has become the definitive standard underlying many web SSO solutions in the enterprise IdM problem space.

Figure 4 shows the service model of SAML. SAML assumes that a user has enrolled with at least one IdP (identity provider). This IdP is expected to provide local authentication services to the user. However, SAML doesn't specify the implementation of these local services. Thus an SP (service provider) relies on the IdP to identify the user. At the user's request, the IdP passes a SAML assertion to the SP. On the basis of this assertion, the SP makes an access control decision.

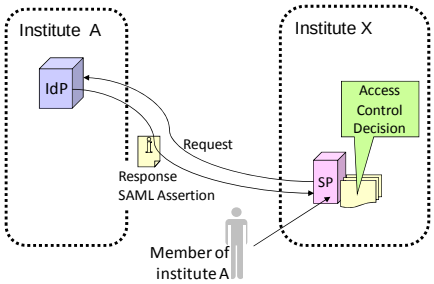

Figure 4. The service model of SAML

SAML v1 is a product of the OASIS[6] Security Services Technical Committee, but SAML v2 is a unification of SAML v1 and ID-FF provide by the Liberty Alliance[7] which is a large consortium of companies, non-profit and government organizations.

3.2. Shibboleth

Shibboleth[8] is a project of Internet2/MACE, and it is also standards-based, open source middleware software. The project develops architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow inter-operation within the higher education community. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The Shibboleth software implements the OASIS SAML v1.1 specification, providing a federated SSO and attribute exchange framework.

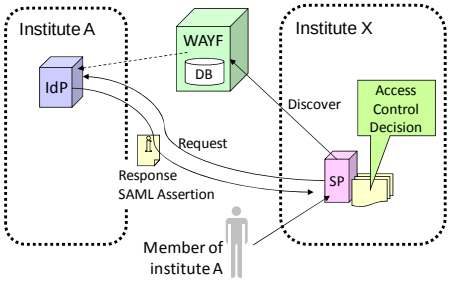

Figure 5. The service model of Shibboleth

Shibboleth proposed WAYF (Where Are You From?) mechanism to discover user's IdP. Figure 5 illustrates the WAYF mechanism. If a member of institute A uses an SP of institute X, then the SP sends a query to WAYF to discover the member's IdP. The WAYF server replies the member's IdP using user identifier.

Furthermore, Shibboleth group develops a new middleware "GridShib" which can cooperate with the grid middleware "Globus Toolkit" to realize cooperation with grid computing services [9].

3.3. OpenID

OpenID[5] is a decentralized SSO system. Using OpenID-enabled sites, web users do not need to remember traditional authentication tokens such as username and password. Instead, they only need to be previously registered on a website with an OpenID IdP. In OpenID authentication mechanism, user's identifier is represented as URL format, then it is easy to keep uniqueness in decentralized distributed control.

Since OpenID is decentralized, any website can employ OpenID software as a way for users to sign-in; OpenID solves the problem without relying on any centralized website to confirm digital identity. OpenID is increasingly gaining adoption among a lot of sites.

3.4. UPKI in Japan

National Institute for informatics in Japan started a project of CSI (Cyber Science Infrastructure) since 2005[12]. The CSI project aims to realize a platform for inter-institutional services in Japan. The CSI project has four sub-project groups; grid computing, advanced high speed broadband network, UPKI and institutional repository for libraries.

The UPKI (University PKI) project researches and develops the nationwide electronic certification platform[11]. UPKI aims to achieve the inter-institutional exchange of user authentication and to construct mutual trust among institutions. The UPKI project tries to realize PKI-like trust framework, but it isn't limited to PKI. Password based authentication exchange is also researched.

4. Comparison of trust styles

For inter-institutional ID federation, it is necessary to consider federation style. There are two styles for trust in ID federation.

One is credential exchange style. Figure 4 and Figure 5 show the models of SAML and Shibboleth respectively, and those two models assume to exchange user's credential between an SP and an IdP. In this style, communication is necessary for authentication. Therefore, if the IdP of an institute is down or network to the IdP is broken, then all members of the institute can't use any services.

In the model of Shibboleth, all authentication requests are relayed by the WAYF server. The more SPs increase, the more requests are sent to the WAYF. So, the WAYF server becomes the bottleneck of authentication process. Scalability is up to processing performance of the WAYF server.

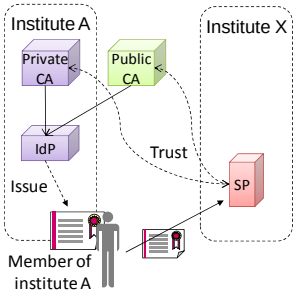

Figure 6. PKI style trust

Figure 6 shows trust style of PKI. Members are issued a PKI digital certificate by the enrolling institute. When a member of the institute *A* uses an SP in another institute, the member sends his/her digital certificate to the SP. If the SP trusts the CA which signed the certificate, then user authentication process finishes within the SP. An SP can decide whether provide service or not based on the attribute in the certificate without communication. So, PKI style is scalable for authentication. However, PKI style is weak for user's identity destruction. If a member quits institute before estimated retirement/graduation date, then the IdP of the institute must send a CRL (certificate revocation list) to all related SPs. It is difficult to send identity destruction data immediately with the CRL mechanism.

5. Eduroam

5.1. What is eduroam

Eduroam[13][14] is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming. Being part of eduroam allows users, who are visiting another eduroam connected institution, to logon to the wireless LAN using the same credentials (username and password) which is used at the home institution. Visitor's available network resources depend on local policies. Eduroam was mainly deployed by TERENA[16], and APAN[17] joined eduroam recently.

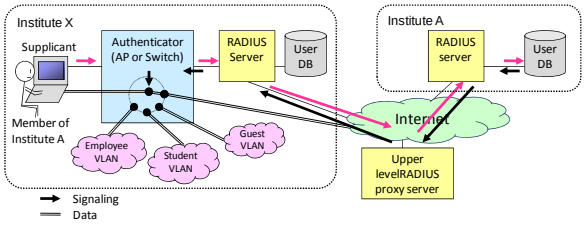

Figure 7. Eduroam basic setup

Figure 7 shows the typical operation for a guest user at an eduroam participant site[14]. When a user, who belongs to the institution *A*, comes to an eduroam participant institute *X*, he/she provides one's credentials to the RADIUS server in the institute *X*. The RADIUS server discovers that it is not responsible for the realm of the institution *X*, and then, the server proxies his/her credentials to the upper level RADIUS proxy server. The upper level server proxies the credentials to the RADIUS sever of the institute *A*, according to the realm described in the credential. More specifically, the text string of a user identifier is represented as the format of network access identifier defined in RFC2486[18]. The network access identifier is described as 'userID@realm', where '@' is a delimiter.

5.2 Eduroam system in Kyushu

We constructed the eduroam system in Kyushu University[2]. Figure 8 shows the outline of the system.

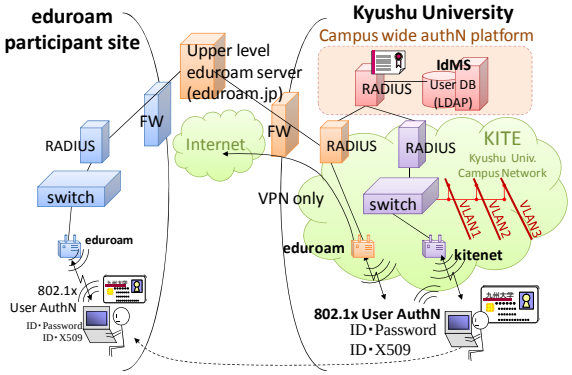

Figure 8. Eduroam system in Kyushu University.

5.2.1. Connection policy. Eduroam service resource depends on local policies at the visited institution. The eduroam standard connection policy requests to allow visitors the following protocols: IPSec VPN, PPTP VPN, SSH, HTTP, HTTPS, IMAP2/3/S, POP/POP3, Passive FTP, SMTP/SMTPS, RDP. If the connection service policy is the eduroam standard, then visitor can

access internal resources. This is often undesirable for network security.

If only VPN is allowed for visitors, visitor must connect to his/her home institute network before accessing any other servers. The visitor accesses any server from his/her institutional IP address. In this case, it is not necessary to change IP address based access control policy for internal information services.

5.2.2. Two layered RADIUS server. Network service and authentication service should demarcate their responsibility. To demarcate responsibility, we designed two layered RADIUS servers. By dividing RADIUS servers, it may be easy to shoot troubles.

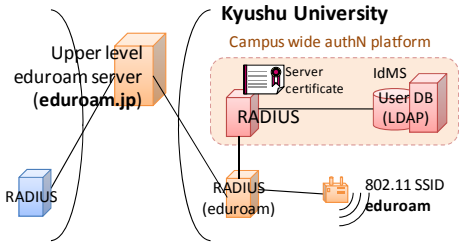

Figure 9. Two layered RADIUS servers

Figure 9 shows the RADIUS servers composition which we are constructed for eduroam. To prevent a phishing access point, the top level RADIUS server has a certificate issued by a public CA (certificate authority) to show its genuineness, because if a malicious person sets a phishing wireless LAN access point with the same SSID 'eduroam', then he/she can collect user ID and password pair.

6. Conclusion

In this paper, we discussed about institutional authentication platform for trustful inter/intra-institutional ubiquitous services. We analyzed the present situation, and made a policy and an action plan to construct the campus wide IdM and authentication platform. We considered ID federation mechanism for inter-institutional services. We also described our eduroam system as an example of inter-institutional service.

In the future, we will do the following things. We will issue PKI certificates for users and provide some applications through PKI based authentication. Additionally, we will install certificates into IC cards, and construct user authentication system with IC cards. We must install web SSO system to reduce complexity. Finally, we want to construct a pretty good authorization mechanism. Attribute based authorization is a challenging problem.

References

[1] Megumi Nogita, Yoshiaki Kasahara, Eisuke Ito and Takahiko Suzuki, "A study of identifier naming conventions suitable for user authentication," *Tech. report of IEICE SIG-ISEC2006-112*, Dec. 2006, pp.67-72. (in Japanese)

[2] Eisuke Ito, Yoshiaki Kasahara, Megumi Nogita and Takahiko Suzuki, "Wireless LAN roaming on ID-Federation environment - A case study for UPKI and eduroam in Kyushu University -", *IPSJ SIG Technical Report 2007-DPS-132/2007-GN-65/2007-EIP-37*, Sep., 2007, pp.141-146. (in Japanese)-

[3] Simson Garfinkel, Gene Spafford, and Alan Schwartz, *Practical Unix and Internet Security*, Oreilly & Associates Inc, 2003.

[4] Masatoshi Itakura, *What Internet Security Really Is*, Nikkei BP Inc. Tokyo, 2002. (In Japanese)

[5] OpenID, http://www.openid.ne.jp/ .

[6] OASIS (The Organization for the Advancement of Structured Information Standards), http://www.oasis-open.org/ .

[7] The Liberty Alliance, http://projectliberty.org/, 2005.

[8] The Shibboleth Project, http://shibboleth.internet2.edu/ .

[9] Tom Barton, Jim Basney, Tim Freedman, Tom Scavo, Frank Siebenlist, Von Welch, Rechana Ananthakrishanan, Bill Baker, Monte Goode, Kate Keahey, "ID Federation and Attribute-based AuthZ through the Globus Toolkit, Shibboleth, GridShib, and MyProxy," *Proc. of Internet2 5th Annual PKI R&D Workshop*, April 2006.

[10] Globus Alliance, http://www.globus.org/, 2003.

[11] UPKI Initiative, https://upki-portal.nii.ac.jp/ , 2005.

[12] National Institute for Informatics, "CSI Cyber Science Infrastructure," http://www.nii.ac.jp/research/project-j.shtml, 2005.

[13] Eduroam web site, http://www.eduroam.org/ .

[14] Licia Florio, Klaas Wierenga, "Eduroam, providing mobility for roaming users," *Proc. of EUNIS2005*, June 2005.

[15] Eduroam.jp web site, http://www.eduroam.jp/, 2006.

[16] TERENA: The Trans-European Research and Education Networking Association, http://www.terena.org/ .

[17] APAN: Asia-Pacific Advanced Network, http://www.apan.net/ .

[18] RFC 2486, "The Network Access Identifier", 1999.