PROCEEDINGS OF SCIENCE

A Study of Credential Integration Model in Academic Research Federation Supporting a Wide Variety of Services

Eisaku Sakane[*], **Takeshi Nishimura, Kento Aida, and Motonori Nakamura**
National Institute of Informatics, Japan
E-mail: sakane@nii.ac.jp, takeshi@nii.ac.jp, aida@nii.ac.jp, motonori@nii.ac.jp

This paper investigates the situation where users must utilize each credential according to the desired services, and clarifies the problems in the situation and the issues addressed by the concept of "identity federation". Japan has the GakuNin, which is an academic access management federation, and the HPCI, which is a distributed high performance computing infrastructure. For the provision of the HPCI resources, the HPCI cannot simply behave as a service provider in the GakuNin. Consequently, in performing academic research, especially HPCI users belonging to academic institutions are compelled to manage both the GakuNin and the HPCI credentials. In this paper, based on the situation in Japan mentioned above, we discuss a credential integration model in order to more efficiently utilize a wide variety of services. We first characterize services in an academic federation from the point of view of authorization and investigate the problem that users must utilize each credential issued by different identity providers. Thus, we discuss the issues to integrate user's credentials, and consider a model that solves the issues.

International Symposium on Grids and Clouds (ISGC) 2018 in conjunction with Frontiers in Computational Drug Discovery
16-23 March 2018
Academia Sinica, Taipei, Taiwan

[*] Speaker.

PoS(ISGC 2018 & FCDD)016

1. Introduction

Single sign-on mechanism raises usability of Information Communication Technology (ICT) services and is currently an essential technology for distributed computing systems. By separating authentication and authorization, ideally users have only to manage one account for ICT services and service providers (SPs) have only to control authorization such as access privileges. Identity providers (IdPs) manage user accounts based on a level of assurance (LoA) of identity and issue user's credentials after user authentication.

Japan has a nation-wide academic access management federation, called "GakuNin" [1]. The GakuNin built up new ICT infrastructure to support research and education based on single sign-on technologies, provides a trust framework including policies and assessment, and improves usability and security with continuous research and development. The GakuNin utilizes Shibboleth [2, 3] as a technology to provide Web single sign-on. In the GakuNin, under conditions presented by an SP, constituent members of an academic institution can seamlessly utilize services provided by the SP as well as ICT services provided by the home institution. There are many services provided by SPs such as e-journal and e-learning.

Japan also has a nation-wide distributed supercomputing infrastructure, called "High Performance Computing Infrastructure" (HPCI) [4]. The HPCI consists of the K computer operated by RIKEN [5] and supercomputers by eleven academic institutions, and large shared storages. The HPCI utilizes two authentication technologies, the Shibboleth and the GSI (Grid Security Infrastructure) [6, 7]. Users can access the HPCI computing resources by using GSI-enabled client software such as GSI-OpenSSH with GSI proxy certificates. An X.509 certificate used to generate the GSI proxies can be obtained from a Web certificate issuance service operated by the HPCI certificate authority (CA) [8] by using Shibboleth assertion. In this sense, Shibboleth account is primary one in the HPCI and managed by IdP independent of the GakuNin.

Let us consider what difference between the HPCI and the GakuNin is. A GakuNin IdP is managed by an academic institution and covers all constituent members of its institution. An HPCI IdP is managed by a supercomputer center (university or institute) and covers only *HPCI users* who are not only academic researchers but also *industrial ones*. Thus, the GakuNin IdP cannot easily play a role of the HPCI one. Academic users are forced to possess two accounts of the IdP of home institution and the HPCI one. However, it should be an ideal situation that academic users have only to possess one account for the desired services. Therefore, it is an important issue to integrate two different IdPs.

This paper considers how the GakuNin and HPCI IdPs should be integrated. In considering IdP integration models, we regard the GakuNin IdP as principal identity provider because the GakuNin IdP is operated by home organization, which user belongs to. However, the HPCI IdP cannot simply be replaced with the GakuNin one. Therefore, we discuss how a credential issued by the GakuNin IdP is applied to the HPCI services. Among authentication processes in the HPCI, we examine how to apply the GakuNin credential to the initial vetting of identity because the initial vetting of identity imposes a burden on both users and personnel. Indeed, it can be understood that our conception is a feasible approach to IdP integration. Moreover, our proposed integration model can be extended to general cases, although discussed based on the situation in Japan.

The remainder of this paper is organized as follows. In Section 2 we describe common and personal services concerned with this paper and illustrate why there is different IdP for each service. Section 3 considers the possibilities for utilization of the GakuNin credentials for the HPCI system and presents an application to initial vetting of user identity. Section 4 makes discussion about equivalence between the traditional procedure for initial identity vetting and the proposed one, and also considers attribute provider approach. Section 5 refers to related work. Finally, Section 6 concludes the paper.

2. Common and Personal Services

This section organizes common and personal services in an academic trust federation.

Firstly, we consider e-journal service in a university as an example, which is typical of services in the academic federation. The university will desire to enable all constituent members to access the e-journal just as the physical journals stored in the university library. In this sense, this can be regarded as a *common* service. At this time, the SP providing the e-journal service does not basically need detail personal information because the SP does not negotiate with the individuals but with the university as juridical person. Only fundamental identity data which represents a member of the university is sufficient for e-journal access. Therefore the IdP (actually the university) will have only to offer basic information that the person certainly belongs to the university and the management of service authorization by the SP will naturally become simple. However, it is possible that the SP will utilize more personal attributes in order to enrich the service or optimize for the individuals.

There are services that are provided restrictedly to a group of the constituent members. Suppose a special discount of a service for students as an example. In order to authorize a customer, the SP offering the discount service will utilize an identity attribute that indicates that the person is certainly a student, in addition to the attribute that the person is a constitute member of the university. The identity attribute whose value has student, faculty, staff, and so on can be assigned normally by the IdP because the IdP, the university itself, manages the attributes originated from constituent member. Thus, these services, which use the attributes assigned *normally* by the university, are still considered as common services. In other words, a service is regarded as common if the SP offers it to a subset that can be classified by attributes originally assigned by the university. The universal set is composed of all members of the university.

Next, we consider the other services than ones described above. Among such services we will deal with a service that screens applicants and thus offers it the permitted users only. In order to illustrate the situation, we suppose the following players: an SP that offers a restricted service with screening, a user for the service, and the IdP managed by the university, which the user belongs to. After screening, it is obvious that the SP should have a service authorization table that is used to authorize requesters for the service. In this case, however, the management method of the authorization table is not unique because there is no available attribute naturally assigned by the IdP for the service authorization. It is tough for the IdP to assign the user an attribute that indicates permission of the service because the IdP does not originally have the responsibility to assign such attribute and the operation cost of the IdP increases even if the IdP can assign the attribute. In this sense, the service concerned can be regarded as a *personal* service. The SP will conduct a

Service type	Essential attributes for authorization
common	attributes originally assigned by IdP
personal	Other than the above

Table 1: Service type in academia classified by required attributes. The IdP is operated by an academic institution and covers all constituent members of the institution.

procedure with the user rather than the university (IdP). Table 1 summarizes the types of service concerned with this paper.

We discuss the management of the service authorization table for a personal service described above. In order to build such table, initial vetting of user identity is very important. Moreover, since the SP does not possess authentication information, the SP must choose credential for the user authentication. The matters for consideration in building the authorization table will be as follows:

- Which level of assurance does the initial vetting of identity need?
- Which credential does the service employ for authentication?
- Which attributes does the service utilize for authorization?

There are several possibilities for the credential selection. Among such possibilities, it can be considered to build a new dedicated IdP for the personal service. If such dedicated IdP can be built, certainly this approach will have the following advantages: possessing a credential issued by the dedicated IdP naturally means possessing permission of access the personal service. Thus, such credentials will make the authorization table not complicated. Furthermore, the SP does not need to adjust LoA to each IdP or to execute policy matching. Consequently, the approach building the dedicated IdP would be able to smoothly launch the personal service because there is no negotiation with IdPs that do not originally ensure suitable attributes for the personal service. This is one reason why there is different IdP for each service.

Concretely, GakuNin IdP can be considered suitable for the common services in academia. HPCI IdP can be regarded as just a dedicated IdP for the personal service, which offers high performance computing resources in Japan. The HPCI and the GakuNin IdPs are independently operated. Currently there is no cooperation relationship between them. HPCI user applied for the HPCI project and her/his research proposal has been accepted after screening. Such attribute itself as the HPCI user is not essential to characterize a constituent member of her/his home organization. As mentioned in Sec. 1, however, such circumstances are not preferred. We should discuss cooperation between the HPCI and the GakuNin as next step. From SP's point of view, three questions above should be answered in considering cooperation. Next section will discuss answers to the questions.

3. Possibilities for Integration

This section considers the possibilities for integration of authentication mechanisms of the GakuNin and the HPCI, and presents an application of the credentials of the GakuNin IdP to the HPCI system.

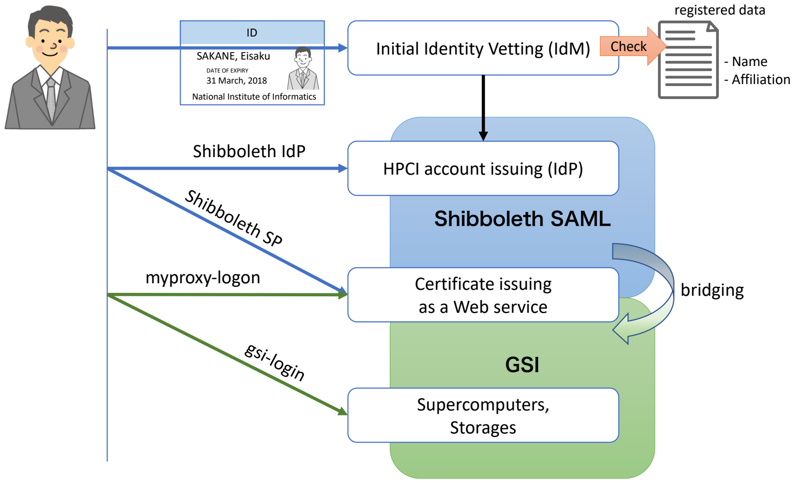

Figure 1: Authentication flow in the HPCI system.

3.1 HPCI Authentication Flow

In considering integration models we first regard the credentials issued by GakuNin IdPs as principal because academic HPCI user's home organization operates the GakuNin IdP and the attribute such as affiliation can be considered as essential for user identification. Thus, we survey authentication flow in the HPCI system. Figure 1 represents the authentication flow for HPCI users. There are three kinds of user authentication in the HPCI system: initial identity vetting, Shibboleth authentication and GSI one. The initial identity vetting is executed just once ordinarily by an identity management (IdM) system. If user personal information varies or when the term of validity of identity vetting expires, the IdM system will again confirm the identity data of the person concerned. The IdM system can be included in the IdP, however, we distinguish them, namely action subjects because we focus on the initial identity vetting below. After the initial identity vetting, HPCI account is issued and utilized to Shibboleth authentication. The HPCI users can access Web services in the HPCI such as content management system (CMS) with SAML assertion issued by the HPCI IdP. For access to supercomputers and distributed storages HPCI users utilize GSI proxy certificates. Certificate issuing system [8] is a Web service in the HPCI, issues certificates to the HPCI users, stores the certificates in a repository, and also issues and stores proxy certificates. The certificate issuing system authenticates the requesters with the SAML assertion and thus bridges credentials between Shibboleth and GSI.

Naively there are three possibilities for utilization of the GakuNin credentials to the HPCI authentication flow (Figure 2). We discuss each possibility in order from the lower part of Fig. 2.

Access to HPC resources The first possibility is to apply the GakuNin credential to authentication at SSH-based access to HPC resources. Actually this tries to replace GSI credential with Shibboleth one. However such attempt is difficult because we do not currently have a de facto standard implementation of command-line user interface for SSH using SAML assertion. Therefore credential bridging approach is still reasonable unless we are forced to change the authentication mechanism for access to HPC resources.

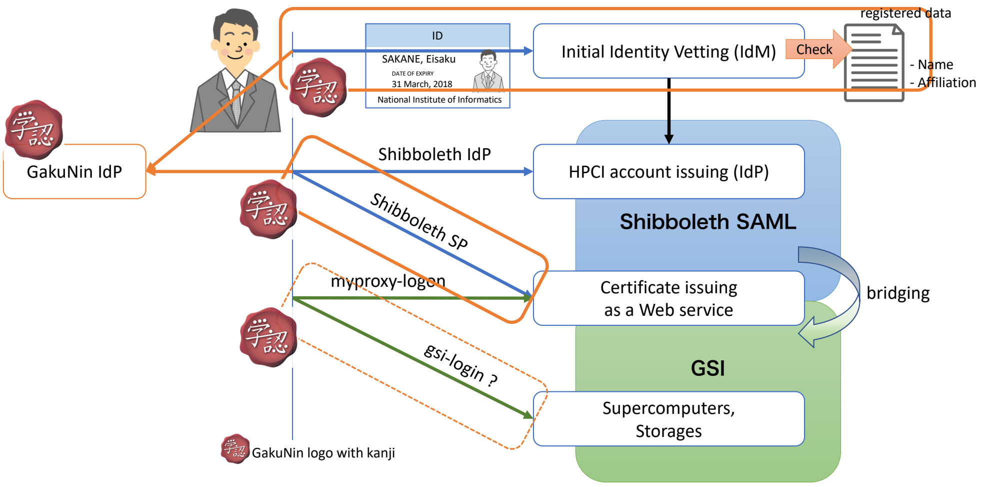

Figure 2: Possibilities for utilization of the GakuNin credentials.

Access to Web services Secondly, we consider applying to authentication for Web services in the HPCI. This application appears to be simple because both the GakuNin and the HPCI utilize SAML assertion. Namely, we can answer easily to the second question mentioned in Sec. 2. However, it will be hard to answer immediately to the third question. Indeed, we can answer that there is no available attribute in the SAML assertion issued by the GakuNin IdP for the HPCI access authorization and that it will be tough for the GakuNin IdP to newly assign such attribute to the person concerned. Thus, the HPCI SP must associate the identity data with the GakuNin credential on the authorization table. Moreover, if the HPCI SP desires to control the access under more rich rules, the authorization table managed by the HPCI SP will be more complicated. Certainly the management of authorization table is one of crucial duties of SP, however, the authorization table based on each person will impose a burden on the HPCI SP.

Initial identity vetting Finally we can consider applying to initial identity vetting. Currently the HPCI IdM vets the identity data of HPCI user based on a face-to-face meeting. At the face-to-face meeting, the HPCI user presents her/his photo-ID to the HPCI IdM personnel. We contemplate the possibility of replacing the photo-ID presentation with the SAML assertion. This attempt does not require the GakuNin IdP to add new attribute to the SAML assertion because the *initial* vetting of identity does not require any HPCI access attributes but only basic personal information. The current HPCI authentication and authorization system is not affected by the attempt. Therefore, to begin with, we should consider applying the GakuNin credential to the initial identity vetting in the HPCI IdM system.

3.2 Application to Initial Vetting of Identity

In this section we propose an effective procedure for initial identity vetting. The basic idea of the proposed procedure is based on our previous work [9]. To begin with, we make brief mention of a method for initial identity vetting with external credential.

The method for initial identity vetting with external credential was originally proposed to resolve the problem that an applicant that lives overseas cannot come in person to a service desk

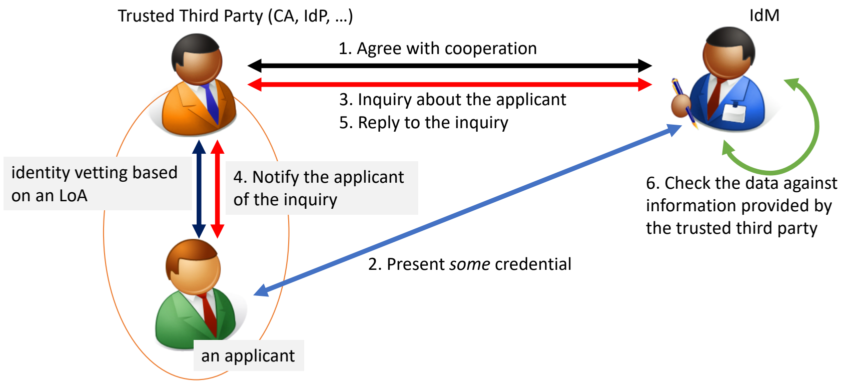
Trusted Third Party (CA, IdP, …)
IdM
1. Agree with cooperation
3. Inquiry about the applicant
5. Reply to the inquiry
identity vetting based on an LoA
4. Notify the applicant of the inquiry
6. Check the data against information provided by the trusted third party
2. Present *some* credential
an applicant

Figure 3: Initial identity vetting with external credential.

of IdM for initial identity vetting. Suppose the following situation: an IdM system must initially vet the identity data of a user, on the other hand a trusted third party such as certificate authority and identity provider has already issued a credential to the user under an LoA requirement. This approach utilizes the credential issued by the trusted third party for the initial identity vetting in the IdM system.

Figure 3 demonstrates the outline of protocols among the players concerned. The initial identification procedure with external credential is as follows:

1. The IdM system relies on the trusted third party that ensures the same level of identity assurance. The trusted third party also consents to reply to an inquiry from the IdM system.
2. The applicant presents her/his credential to the IdM system. The credential was issued by the trusted third party. The IdM system checks the validity of the presented credential.
3. The IdM system makes inquiry about the applicant information such as full name and affiliation, based on the verified credential.
4. The trusted third party notifies the inquiry from the IdM system to the applicant, namely, the owner of the credential, and asks the owner whether the trusted third party can answer the IdM's inquiry.
5. The trusted third party replies to the inquiry after receiving the response from the owner of the credential.
6. The IdM system checks the identity data against the information provided by the trust third party.
7. The identification procedure is completed.

Reference [9] describes in detail the procedure in the case where the trusted third party is a certificate authority and thus the credential is an X.509 certificate.

We apply the method for initial identity vetting with external credential to the situation considered in this paper. The players are the HPCI IdM, the GakuNin IdP, and the HPCI user respectively,

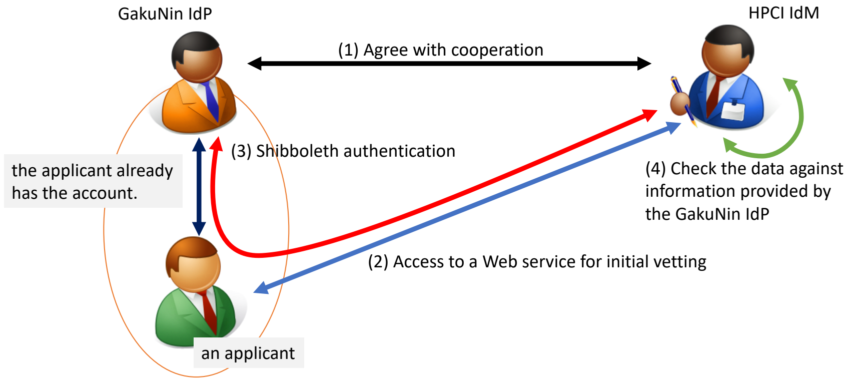
GakuNin IdP
HPCI IdM
(1) Agree with cooperation
(3) Shibboleth authentication
the applicant already has the account.
(4) Check the data against information provided by the GakuNin IdP
(2) Access to a Web service for initial vetting
an applicant

Figure 4: Initial identity vetting with SAML assertion.

and the external credential is SAML assertion. Figure 4 demonstrates the outline of the initial identity vetting with SAML assertion. This case supposes that the HPCI user possesses a Shibboleth account for her/his home organization of which the IdP has joined the GakuNin.

Firstly, the GakuNin and the HPCI IdM negotiate about putting the procedure for the initial identity vetting into practice. The HPCI IdM provides a Web service for the initial identity vetting with SAML assertion and should determine which attributes it utilize in order to confirm the registered data such as name and affiliation. After reaching an agreement the HPCI IdM will join the GakuNin as an SP. In the remainder of this step, an ordinary procedure for an SP to join the trust federation will be executed. For example, the HPCI IdM will submit its metadata for Shibboleth to the GakuNin.

Secondly, the HPCI user accesses to the Web service for the initial identity vetting. Based on ordinary Shibboleth authentication flow, the user selects her/his IdP from the discovery service, and thus accesses the IdP for Shibboleth authentication. If the Shibboleth authentication succeeds, the IdP can ask the user whether it may send the desired attributes to the HPCI IdM before sending the SAML assertion. If the user approves the request, the IdP will send the SAML assertion including the attributes for the identity vetting. Step 5 described above will be completed thus far.

Finally, the HPCI IdM checks the identity data against the SAML assertion provided by the GakuNin IdP. If the check succeeds, the identity vetting will be completed. Note that the HPCI user has only to access the Web service for the initial identity vetting just once.

4. Discussion

In this section we discuss equivalence between an ordinary procedure and the proposed one for initial identity vetting. We also mention attribute provider approach.

4.1 Equivalence between Traditional and Proposed Procedures

The HPCI IdM vets user identity data based on a face-to-face meeting and checks the registered data against photo-ID presented by the user. This traditional procedure essentially arises from the fact that the HPCI certificate authority (CA) obeys the MICS profile [10] managed by the Interoperable Global Trust Federation (IGTF) [11, 12]. In the traditional procedure, an applicant comes

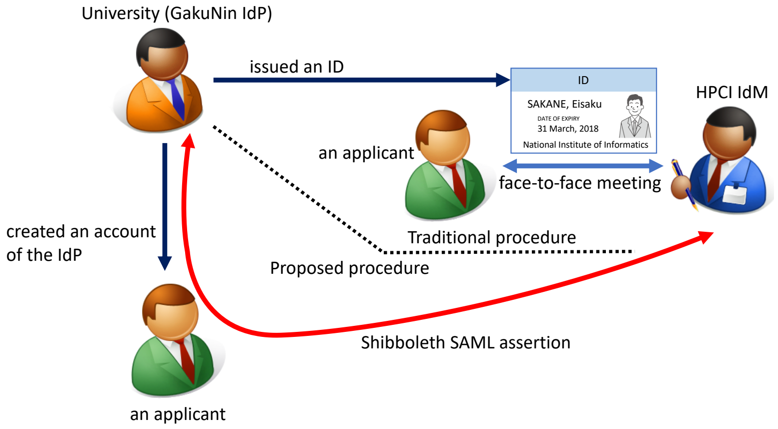

Figure 5: Two procedures for initial identity vetting. The first procedure is traditional based on a face-to-face meeting in which an applicant presents her/his photo-ID, issued by the home organization, to a personnel of the IdM. The other one is proposed in this paper, which utilizes SAML assertion provided by the GakuNin IdP (indeed the home organization).

in person to a service desk of the HPCI IdM, and thus presents her/his photo-ID to a personnel of the HPCI IdM. Note that the presented photo-ID is issued by her/his home organization. Figure 5 demonstrates two methods of initial identity vetting, namely, the traditional identity vetting and the proposed one.

The proposed method replaces the photo-ID presentation in the traditional procedure with SAML assertion transmission. However, the proposed procedure can intuitively be regarded as the almost same level of assurance as the traditional one provides. The reason is that there is no qualitative difference between ID issuance and IdP account creation as long as those acts are done by the same organization. And yet, the traditional procedure and the proposed one are not completely equivalent. In order to treat the traditional procedure and the proposed one equally, we must consider security such as ease of faking the ID and ease of usurping the IdP account. Moreover it is very important that each of Steps 2 and 4 described in Sec. 3.2 is executed on independent channels. For example, for the initial identity vetting with PKI (Public Key Infrastructure) credential [9], even if a cracker steals the private key associated with a certificate and does a challenge response to the IdM in Step 2, the compromising of the private key will be uncovered in Step 4 unless the cracker tampers the contact channels between the CA and the certificate owner. Since the proposed procedure does not ensure the independence of the channels of Steps 2 and 4 clearly, spoofing may be allowed even if the cracker usurps the IdP account only. Thus it is an issue in the future to improve the proposed procedure in order that the procedure can ensure the independence of steps concerned. For example, multi-factor authentication that includes SAML assertion is well worth discussing in the next stage.

4.2 Attribute Provider Approach

This section discusses an approach not changing the type of credential if possible. Namely, we discuss how to widely apply SAML assertion provided by the GakuNin IdP not to only the initial identity vetting but also the Web services in the HPCI.

As described in Sec. 3.1, the authorization table for the HPCI Web service becomes more complicated than one for *common* service because the authorization table for the HPCI should be managed based on each person, in other words, it cannot be simplified with suitable attributes. We consider reducing a burden of the authorization management on the premise that it is difficult for the GakuNin IdP to add appropriate attributes for *personal* services such as the HPCI services. Among solutions to the issue, introducing attribute provider can be considered as feasible approach. This paper defines attribute provider as an action subject that adds attributes to valid credential based on an attribute table. The attribute table is managed by the attribute provider and deals with information such as which person has which attribute.

Because of the attribute provider, the SP can handle the authorization table in terms of suitable attributes and thus the authorization table will become simple. If there are the other SPs that provide the same service, the attribute provider approach will be able to reduce the whole of the cost of service authorization management. This is one of the merits of the attribute provider approach. In order to practice the approach, it is an issue how the attribute provider should manage attributes and add suitable attributes to credential. VO (Virtual Organization) is a standard concept of the attribute provider approach in Grid computing. VOMS (Virtual Organization Membership Service) [13] is an implementation of the approach for GSI credential and still utilized in e-Science communities. Instead, we need an implementation of the approach for SAML assertion. GakuNin mAP [14, 15] (currently Cloud Gateway [16]) is an implementation in Shibboleth SAML and plays a role of the attribute provider. Thus we should examine how suitable attributes for the HPCI service can be handled with the Cloud Gateway service in the future. Furthermore, it may be considered to introduce ECP [17] to the HPCI system in the next stage because the object of ECP is not a Web browser but the other application client.

5. Related Work

This section refers to AARC Blueprint Architecture and Snctfi by Authentication and Authorization for Research Collaboration (AARC).

5.1 AARC Blueprint Architecture

The AARC Blueprint Architecture [18] (AARC-BPA) is a set of software building blocks that can be utilized to implement federated access management solutions for international research collaborations. The AARC-BPA systematizes coexistence between many circulated credentials in the world. Since it is usual for recent authentication and authorization infrastructure to need to handle two or more kinds of credential, the system of the AARC-BPA is very instructive for utilization of large-scale federated services.

The AARC-BPA does not mention a collaboration between identity services. The proposed procedure for initial identity vetting in this paper can be considered as concrete cooperation between IdP and IdM in the User Identity Layer in the AARC-BPA. In this sense the proposed procedure is practical for the AARC-BPA. Furthermore, it is worthwhile to reorganize the authorization mechanism in the HPCI service in terms of the concepts of the Identity Access Management Layer, the User Attribute Services Layer, and the Authorisation Layer in the AARC-BPA.

5.2 Snctfi

Snctfi [19] stands for Scalable Negotiator for a Community Trust Framework in Federated Infrastructures. It proposes a policy framework to assess the 'quality' of service provider and identity provider (SP-IdP) proxies based on the structures of the Security for Collaboration among Infrastructures (SCI) framework [20]. The SP-IdP proxy behaves authentication and authorization infrastructure gateway and mediates between the services in the research/education infrastructure and IdPs in the federation.

It is unclear that the whole of the GakuNin and HPCI authentication and authorization system discussed in this paper can be regarded as a specific example for the SP-IdP proxy model. However, Snctfi framework is expected to corroborate the equivalence between the traditional and the proposed procedures for initial identity vetting discussed in Sec. 4.1. Thus, we should evaluate the proposed procedure for initial identity vetting by means of Snctfi framework in the future.

6. Summary

In this paper, we presents matters for consideration toward a credential integration model in academic research federation in Japan, in particular, between the GakuNin and the HPCI. Our contribution in this paper is as follows:

- We characterized service type in an academic federation from the point of view of authorization and clarified one reason why users must utilize each credential issued by different IdPs.
- We discussed possibilities for credential integration, namely, application of the GakuNin credential to the HPCI authentication and authorization system, and proposed a procedure for initial identity vetting of the HPCI IdM utilizing the GakuNin credential as a feasible approach.
- We discussed the equivalence between the traditional procedure for the initial identity vetting based on a face-to-face meeting and the proposed one.

Although our studies were conducted in the circumstances in Japan, the proposed procedure for initial identity vetting is useful for the other trust federations in the world. Moreover the discussion about credential integration, namely, applying credential suitable for *common* services in academia to *personal* services will provide a helpful suggestion to academic research communities.

We will evaluate the proposed procedure for initial identity vetting toward practice. Also staring fixedly at post-GSI system, we will redesign the next HPCI authentication and authorization system.

Acknowledgments

This work is partially supported by the Ministry of Education, Sports, Science and Technology in Japan.

References

[1] The Academic Access Management Federation in Japan (GakuNin), https://www.gakunin.jp/En-fed/

[2] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein, *Federated Security: The Shibboleth Approach*, *EDUCAUSE Quarterly*, **27**, pp.12–17 (2004).

[3] Shibboleth Consortium, https://www.shibboleth.net

[4] The High Performance Computing Infrastructure in Japan (HPCI), http://www.hpci-office.jp

[5] RIKEN's K computer, http://www.r-ccs.riken.jp/en/k-computer/about/

[6] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, and S. Tuecke, *Security for Grid Services*, in proceedings of *the 12th IEEE International Symposium on High Performance Distributed Computing*, pp.48–57 (2003).

[7] The Globus Security Team, *Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective*, http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf

[8] E. Sakane, K. Aida, and K. Motoyama, *Design and Implementation of Certificate Authority for High Performance Computing Infrastructure*, in proceedings of *the International Symposium on Grids and Clouds (ISGC) 2013*, PoS(ISGC 2013)013 (2013).

[9] E. Sakane, T. Nishimura, and K. Aida, *A Method for Remote Initial Vetting of Identity with PKI Credential*, in proceedings of *the International Symposium on Grids and Clouds 2017 -ISGC 2017-*, PoS(ISGC2017)009 (2017).

[10] D. Simmel (Ed.), *Profile for Member Integrated X.509 Credential Services with Secured Infrastructure*, Version 1.3 (2013), https://www.igtf.net/ap/mics/

[11] Interoperable Global Trust Federation (IGTF), https://www.igtf.net

[12] D. Simmel, S. Rea, and A. Stolk, *An Introduction to The Americas Grid Policy Management Authority (TAGPMA) and the International Grid Trust Federation (IGTF)*, http://www.tagpma.org/files/CLCAR-Paper15-Simmel-Rae-Stolk.pdf

[13] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, K. Frohner, K. Lrentey, F. Spataro, *From gridmap-file to VOMS: managing authorization in a Grid environment*, *Future Generation Computer Systems*, **21**, pp.549–558 (2005).

[14] T. Nishimura, M. Nakamura, K. Yamaji, H. Sato, Y. Okabe, *Privacy Preserving Attribute Aggregation Method without Shared Identifier Binding*, *Journal of Information Processing*, **22**, pp.472–479 (2014).

[15] T. Nishimura, E. Sakane, K. Yamaji, M. Nakamura, K. Aida, and N. Klingenstein, *Virtual Organization Platform Interoperability Provides the Long Tail an eScience Environment*, *Journal of Information Processing*, **24**, pp.609–619 (2016).

[16] Cloud Gateway, https://cg.gakunin.jp

[17] ECP: Enhanced Client or Proxy, https://wiki.shibboleth.net/confluence/display/CONCEPT/ECP

[18] The AARC project, *AARC Blueprint Architecture*, https://aarc-project.eu/wp-content/uploads/2017/04/AARC-BPA-2017.pdf

[19] Snctfi: Scalable Negotiator for a Community Trust Framework in Federated Infrastructures, *The Snctfi framework v1.0*, https://aarc-project.eu/wp-content/uploads/2017/07/Snctfi-v1.0.pdf

[20] D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz, J. Wolfrat, *A Trust Framework for Security Collaboration among Infrastructures*, in proceedings of *the International Symposium on Grids and Clouds (ISGC) 2013*, PoS(ISGC 2013)011 (2013).