PROCEEDINGS OF SCIENCE

A Method for Remote Initial Vetting of Identity with PKI Credential

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

With the growth of large-scale distributed computing infrastructures, a system that enables researchers – not only international collaborative research projects but also small research groups – to use high performance computing resources in such infrastructures is established. For the computing resource use system which invites researchers in the world to submit the research proposal, it is tough to carry out initial vetting of identity based on a face-to-face meeting at a service desk for the system if the researcher whose proposal is accepted lives in a foreign country. The purpose of this paper is to propose a method to solve the difficulty of initial vetting of identity for a remote user.

An identity management (IdM) system vets the identity and reality of a user by checking the beforehand registered personal information against the identity documents. After the identity vetting, the user can obtain a credential used in the infrastructure. Suppose that the IdM system(A) needs to initially vet the identity of a user and that the user already possesses a credential issued by the other IdM system(B). The basic idea of this paper is that the IdM system(A) uses the credential issued by the IdM system(B) for the initial identity vetting if the level of assurance of the IdM system(B) is the same as or higher than the IdM system(A). However, the IdM system(A) cannot always check the identity against the attribute information provided by the credential. In a trust federation, the IdM system will be able to finish vetting the identity by making reference to the other IdM system that issued the credential for the necessary and sufficient identity data.

As the credential handled in this paper, we focus on Public Key Infrastructure (PKI) credentials that often used in large-scale high performance computing environments. We discuss necessary condition and procedure for ensuring that the remote initial vetting of identity with a PKI credential is the same assurance as the one based on a face-to-face meeting. The proposed method can be introduced to an existing PKI without large changes. The basic idea of the proposed method can be also applied to an infrastructure based on another authentication technology. The applicability of the basic idea is also considered.

International Symposium on Grids and Clouds 2017 -ISGC 2017-
5-10 March 2017
Academia Sinica, Taipei, Taiwan

[*] Speaker.

1. Introduction

With the growth of large-scale distributed computing infrastructures, a system that enables researchers – not only international collaborative research projects but also small research groups – to use high performance computing resources in such infrastructures is established. For computing resource providers which invite researchers in the world to submit the research proposal, it is tough to carry out initial vetting of identity based on a face-to-face meeting at a service desk for the system if the researcher whose proposal is accepted lives in a foreign country. For example, anyone can apply for a research project proposal to HPCI (High Performance Computing Infrastructure) [1] that is a nation-wide distributed computing infrastructure in Japan. Under the HPCI authentication policy the HPCI system needs to vet the identity of a foreign researcher based on a face-to-face meeting if his/her proposal is accepted. Namely, the researcher needs to come to a service desk of the HPCI identity management system located in Japan. However the foreign researcher cannot always come to the service desk just only for the identity vetting due to a means of transportation. It is an important issue to establish a remote initial identification procedure.

This paper discusses how identity management (IdM) system vets the identity of a remote user who cannot come to a service desk for the system. In general, an IdM system vets the identity and reality of an end-entity by checking the beforehand registered personal information against the identity documents. After the identity vetting, the end-entity (user) can obtain a credential used in a computing infrastructure. The basic idea of this paper is that an IdM system(A) uses the credential issued by the other IdM system(B) for the initial identity vetting if the level of identity assurance of the IdM system(B) is the same as or higher than the IdM system(A).

This paper proposes a method of identity vetting for a remote user with a credential. As the credential handled in this paper, we focus on Public Key Infrastructure (PKI) credentials that often used in large-scale high performance computing environments. We discuss necessary condition and procedure for ensuring that the remote initial vetting of identity with a PKI credential is the same assurance as the one based on a face-to-face meeting. The proposed method can be introduced to an existing PKI without large changes, and therefore will promote international use of computing infrastructure. The basic idea of the proposed method can be also applied to an infrastructure based on another authentication technology. The applicability of the basic idea is also considered.

The remainder of this paper is organized as follows. In Section 2 we describe a basic idea about initial vetting of identity for remote users and issues to be addressed. Section 3 describes a solution to resolve the difficulty of initial vetting of identity for remote users. Section 4 makes discussion about the proposed identification procedure and its generalization. Section 5 refers to related work. Finally, Section 6 concludes the paper.

2. Basic Idea and Issues

This section describes a basic idea about initial vetting of identity for a remote user and issues to be addressed. First, we do a brief review of initial identity vetting based on a face-to-face meeting (F2F identity vetting). After that, we discuss a remote initial vetting of identity.

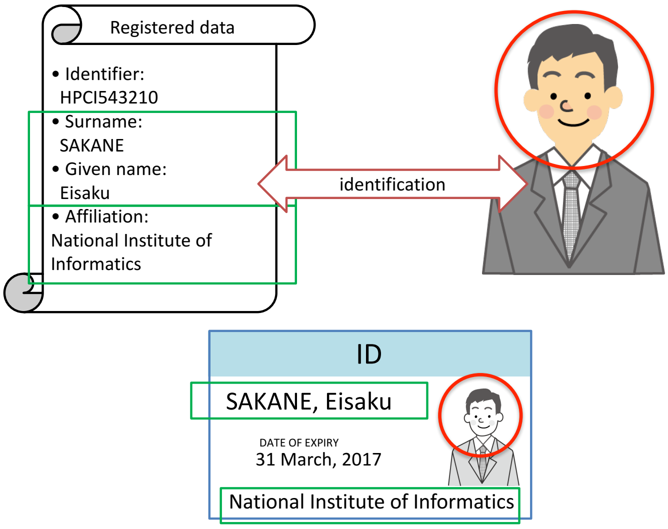

Figure 1: Identity vetting based on face-to-face meeting.

2.1 F2F Identity Vetting

Identity vetting is to check data registered beforehand against photo-ID and/or valid official documents. Its purpose is to ensure that the association between identity data and an end-entity is correct.

Suppose that personnel of a certain system try to perform initial identity vetting for an end-entity based on a face-to-face meeting. In general, initial identity vetting will be conducted as follows (Fig. 1):

1. The personnel of the system prepare the beforehand registered user data to be vetted.
2. The applicant comes to a service desk for the system and presents a photo-ID or official documents to the personnel.
3. The personnel check whether the presented photo-ID card is valid. The other official documents are also checked if needed.
4. The personnel confirm that the photo printed on the ID card/document is the user who is *in the presence of* the personnel.
5. The personnel confirm that the data printed on the ID card/document agree with the registered data.
6. The identification procedure is completed.

A presented photo-ID is often issued by the organization to which the applicant belongs. If an ID card does not print the photo of the applicant, the combination of the applicant's passport and the certificate of enrollment will be used. The date of expiry is printed on the ID card in Fig. 1, whereas there are ID cards on which the date of expiry is not printed due to the running costs of ID card.

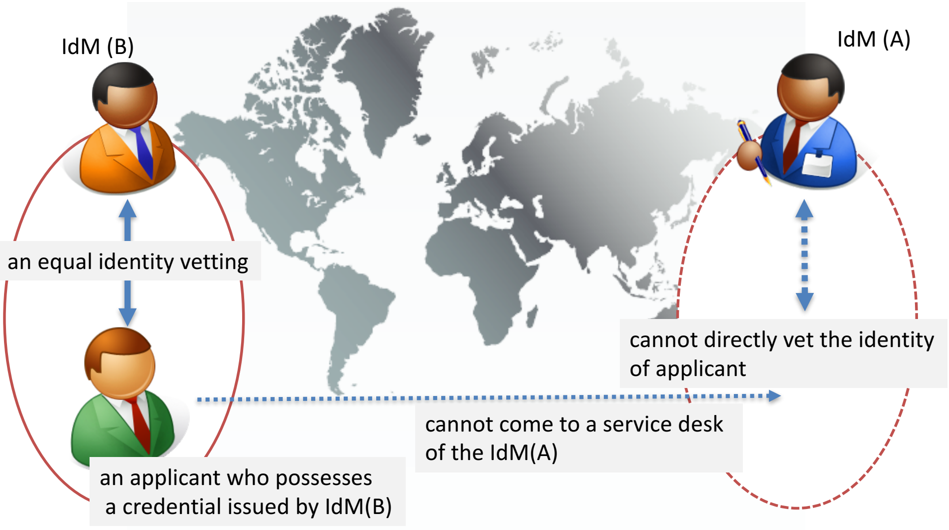
IdM (B)
IdM (A)
an equal identity vetting
cannot directly vet the identity of applicant
cannot come to a service desk of the IdM(A)
an applicant who possesses a credential issued by IdM(B)

Figure 2: An attempt to vet the identity of an applicant by using an existing credential.

2.2 Remote Identification Consideration

We need to consider a situation where the applicant is *not* in the presence of the personnel. Under the situation, we must realize a remote initial identification procedure equal to the one based on a face-to-face meeting. In this case, the personnel of the IdM system cannot take an ID card by the hand and cannot see the applicant directly. Established identification procedure should satisfy the following requirements:

1. A photo-ID presentation should be equivalent to being shown directly.
2. An applicant check against the photo-ID by sight should be equivalent to being checked in the presence of the personnel.

One of solutions to fulfill the above requirements is that the personnel of the IdM system visit the applicant in the opposite direction. However, this is more difficult than the applicant visits the service desk of the IdM system. Another solution is that service desks of the IdM system are opened in the world. This is actually realized in a certain worldwide research community such as high energy physics. However, for a nationwide project that allows general use of computing resources without limitation of research theme it is not easy to establish a service desk of the IdM system to the world at one's own expense.

Now we take note of trust federation. A trust federation is composed of identity providers (IdP) – of course including an IdM system – and service providers. It is considered that each IdP in the trust federation observes the requirements for IdP by mutual agreement. Namely, each IdP ensures the same level of identity vetting. Thus, we can abandon an attempt for the IdM system itself to vet the identity of the applicant. Instead, we try to conduct initial identity vetting by using a credential generated by the identity data already confirmed based on an equivalent identity vetting conducted by the other IdM system.

Figure 2 shows the situation in question. Let us suppose that the IdM system(A) needs to initially vet the identity of an applicant and that the applicant already possesses a credential issued

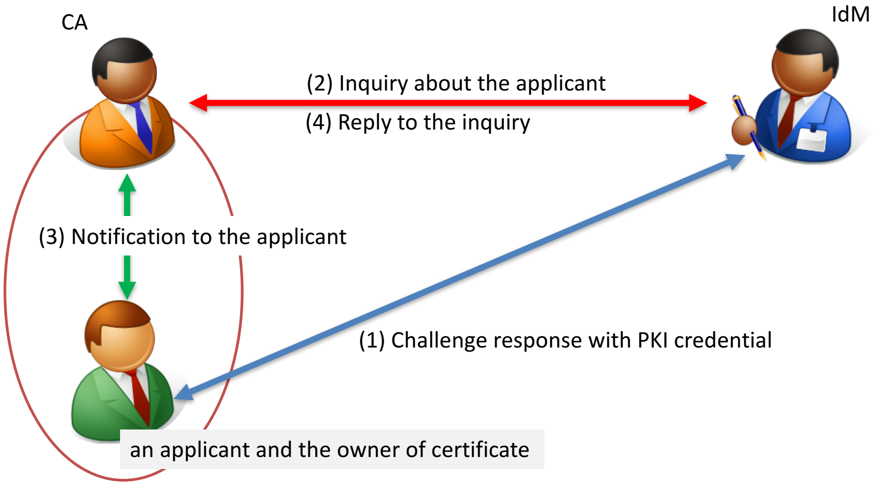
CA
IdM
(2) Inquiry about the applicant
(4) Reply to the inquiry
(3) Notification to the applicant
(1) Challenge response with PKI credential
an applicant and the owner of certificate

Figure 3: Initial identification procedure with PKI credential.

by the other IdM system(B). An initial identity vetting for the applicant was completed by the IdM system(B) based on a face-to-face meeting. If the IdM systems(A and B) join a trust federation, the IdM system(B) has already vetted the identity of the applicant with the same condition as the IdM system(A) imposes. Also, let us suppose that each IdM system is independently operated by each organization. To realize a remote initial identification procedure, now we have the issues to be addressed:

- How do we establish a protocol between the IdM system(A) and the applicant?
- How do we establish a protocol between the IdM systems(A and B)?
- How do we establish a protocol between the IdM system(B) and the applicant?

We consider these protocols with a concrete credential in the next section.

3. Identity Vetting with PKI Credential

This section presents an initial identification procedure for a remote applicant with a PKI credential as a solution to the issues mentioned in the previous section.

Figure 3 demonstrates the outline of protocols among the persons concerned. The IdM system needs to vet the identity of the applicant in Fig. 3. The certificate authority (CA) already completed the initial vetting of identity for the end-entity based on a face-to-face meeting, thus the applicant possesses a credential (digital certificate) issued by the CA. Also suppose that the level of identity assurance of the CA is the same as the one of the IdM system.

The initial identification procedure for the remote end-entity is proposed as follows:

1. The IdM system relies on the CA that ensures the same level of identity assurance. The CA also consents to reply to an inquiry from the IdM system.
2. The IdM system does a challenge response to the applicant.

3. The IdM system keeps a record of the subject distinguished name (DN) of the applicant.
4. The IdM system makes inquiry about the applicant information such as full name and affiliation, based on the subject DN of the verified certificate.
5. The CA notifies the inquiry from the IdM system to the applicant, that is, the owner of the digital certificate.
6. The CA replies to the inquiry after receiving the response from the owner of the certificate.
7. The IdM system checks the identity data against the information provided by the CA.
8. The identification procedure is completed.

The CA needs to make an agreement with the IdM system for the acts of the inquiry from the IdM system in the step 1, the notification and confirmation to the certificate owner in the step 5, and the actual reply to the IdM system in the step 6. Note that there is generally no obligation of the CA to carry out those acts, that is, the CP/CPS (Certificate Policy/Certification Practice Statement) that the CA obeys may not describe the acts.

First, trusting relationship between the IdM system and the CA should be made beforehand with an out-of-band method. In particular, the CA should authenticate the IdM system, understand the contents of the inquiry from the IdM system and its purpose beforehand, and then consent to reply to the inquiry. Step 2 is actually the same one as usual SSL/TLS client authentication. However there is no authorization for the applicant in this step. The IdM system verifies the presented certificate and confirms that the applicant is just the owner of private key associated with the certificate. The subject DN of the certificate is used to make inquiry about the applicant to the issuing CA because the subject DN is a unique identifier to the applicant (the end-entity).

The protocol between the IdM system and the CA in the step 4 should be secure. It can be considered that this secure connection has been established the same as the secure communication among the members of a trust federation. The inquiry to the CA is a necessary process because the IdM system cannot always obtain the necessary attribute information provided by the certificate for checking. For example, the organization name of the subject DN does not always present the organization to which the applicant actually belongs. Since the applicant is not in the presence of the personnel of the IdM system, even if necessary information used in checking can be read from the subject DN or the attribute information, the IdM system should make the inquiry about the applicant and the CA should notify the inquiry from the IdM system to the owner of the certificate (the applicant).

In the step 5 it is very important to ask the owner of the certificate whether the inquiry about the owner is valid as part of the identity vetting being conducted by the IdM system. This will certainly be subject to the law of the country where the CA is organized. For example, Japan has a private data protection law [2]. According to the private data protection law it is recognized that an identity provider (the CA in this case) must reply the inquiry with the owner's consent. It is necessary to verify that the reply to the IdM system obeys the law of the country where the CA is organized. A memorandum of understanding for the proposed identification procedure between the IdM system and the CA should be exchanged after careful consideration of the laws that each organization obeys.

4. Discussion

In this section we discuss the feasibility in the Interoperable Global Trust Federation (IGTF) of the proposed method described in the previous section. We also consider the generalization of the proposed identification procedure.

4.1 Feasibility in IGTF

The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-infrastructures and cyber-infrastructures, identity providers, and the other qualified relying parties [3, 4]. The IGTF consists of three regional Policy Management Authorities: the TAGPMA [5], the APGridPMA [6], and the EUGridPMA [7].

HPCI certification authority [8] is a member of the APGridPMA and issues certificates to users who are authorized to use computing resources in the HPCI. There is an IdM system in HPCI because the HPCI CA is operated based on the MICS authentication profile [9]. The HPCI IdM system vets the identity of the HPCI user based on a face-to-face meeting. Since the HPCI system receives the research project proposal from not only Japanese research groups but also foreign ones, the HPCI IdM system may need to conduct the identity vetting for the foreign users.

For concrete discussion below, let us suppose that a researcher living in the Asia-Pacific region, but outside of Japan, has submitted a project proposal, which has subsequently been accepted. Thus the HPCI IdM system needs to vet the identity of the foreign researcher. Also let us suppose that the researcher cannot come to a service desk of the HPCI IdM system in Japan and that he/she already possesses or will be able to obtain a certificate issued by an IGTF-accredited CA located in the country where he/she lives.

It is self-evident that the HPCI IdM system relies upon the IGTF-accredited CA. However the HPCI IdM system needs to negotiate beforehand with the CA for necessary acts of the CA (the steps 1, 5 and 6 mentioned in Sec. 3) because those acts are not required of the IGTF-accredited CAs by any IGTF authentication profiles. Nevertheless, there can be room to negotiate with the CA for the required acts by the proposed method because CAs concerned are the members of the APGridPMA. If there is agreement that the CA replies to the inquiry from the IdM system and if it is not contrary to the laws that each CA obeys, secure communication for the proposed method between the HPCI IdM system and the CA can be established. The CA can notify the inquiry from the HPCI IdM system to the certificate owner because the CA ensures the traceability to the owner according to an authentication profile published by the IGTF. Therefore, the proposed method is feasible in the APGridPMA without large changes as long as the participants in the method agree and legal problems are solved.

It should be noted whether the certificate used in the initial vetting of identity can be used for authentication in services, for example access to computing resources, is a different problem. The proposed method is for *initial* vetting of identity, thus the certificate is initially used only once.

4.2 Generalization

We can generalize the proposed method with PKI credential to the one with the other credentials by considering a trusted third party such as a CA and an IdP.

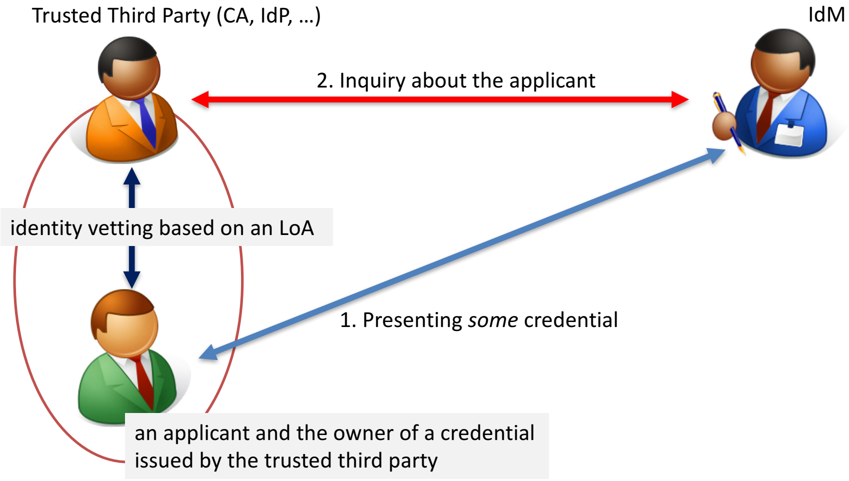
Trusted Third Party (CA, IdP, ...)
IdM
2. Inquiry about the applicant
identity vetting based on an LoA
1. Presenting *some* credential
an applicant and the owner of a credential issued by the trusted third party

Figure 4: A generalization of the proposed method.

A generalization of the proposed method is shown in Fig. 4. The trusted third party should have the same level of identity assurance as the IdM vets the identity of an applicant. The applicant should already possess a credential issued by the trusted third party. In this generalization, the details of the protocol between the IdM system and the applicant depend on the credential issued by the trusted third party. It is unchanged that the IdM system verify the credential of the applicant. The communication for the inquiry about the applicant between the IdM system and the trusted third party will be established if the policies of them can be harmonized. Conversely, it is difficult to adjust the differences of the level of identity assurances without the harmonized policy that they obey. The protocol between the trusted third party and the end-entity (the applicant) should also be carefully considered based on the laws that the trusted third party observes. This is the same situation as Sec. 3.

5. Related Work

This section refers to a video-supported identity vetting, and policy harmonization by the Authentication and Authorisation for Research and Collaboration (AARC).

5.1 Video-supported identity vetting

A video-supported identity vetting guidelines [10] is under discussion in the EUGridPMA. This guideline prescribes a process of identity vetting for a remote person. The advantage of the video-supported identity vetting is to be able to vet the applicant without a trusted third party. However, to satisfy the requirements mentioned in Sec. 2.2, the defined process via a video-supported conference system should be carefully considered and evaluated. The idea of the process between the IdM system and the applicant is essentially the same as ‘challenge response’ in SSL/TLS client authentication. Figure 5 shows the outline of the video-supported identity vetting.

Our proposed method can avoid the difficulties in establishment of the video-supported identity vetting because the directly identity vetting of the applicant has been conducted somewhere

Figure 5: A video-supported identity vetting.

based on a face-to-face meeting. However the proposed method will be not available if the applicant does not have any credential. Thus, the video-supported identity vetting can coexist with the proposed method in this paper and it is worthwhile introducing the video-supported method to the IdM system in question.

5.2 Policy Harmonization

Authentication and Authorisation for Research and Collaboration (AARC) is an EC funded project that brings together 20 different partners from among National Research and Education Networks (NRENs) organizations, e-Infrastructures service providers and libraries in EU [11].

Among five work packages the AARC project has a networking activity on 'Best Practices and Policies Harmonization' to define a cost-effective operational and policy framework to create a secure framework in line with resource providers' requirements, national identity federations' frameworks and compliant with privacy laws. In general, it is hard to harmonize policies between independent trust federations. Therefore, the research result of the policy harmonization work package should be very useful for generalization of the proposed method in this paper. It is also noteworthy for the work package to take up compliance with the privacy law. To confirm whether operation in question be contrary to the privacy law, support from lawyer will be needed. Although the privacy law in EU is different with the one in Japan, the work of the AARC project about compliance with the privacy law should be very instructive.

6. Summary

In this paper, we consider a method for remote initial vetting of identity with PKI credential. Our contribution in this paper is as follows:

- We proposed an identification procedure for foreign researchers with PKI credentials.
- We discussed the feasibility of the proposed method in the IGTF.
- We considered generalization of the proposed method to the one with the other credential.

Although there are several matters that should be coordinated in operation policies, the proposed method with PKI credential can be technically feasible in a trust federation for academic and research communities. The proposed method could be extended to initial vetting for other credentials such as SAML assertion, though the implementation of the proposed method depends on the credential used for the initial identity vetting.

We will evaluate the proposed method as well as the video-supported identity vetting and discuss application to the identity vetting in the HPCI IdM system in the near future.

Acknowledgments

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

References

[1] High Performance Computing Infrastructure (HPCI), http://www.hpci-office.jp

[2] Personal Information Protection Commission in Japan, *Amended Act on the Protection of Personal Information (Tentative Translation)*, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

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

[4] 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

[5] The Americas Grid Policy Management Authority (TAGPMA), http://www.tagpma.org

[6] The Asia Pacific Grid Policy Management Authority (APGridPMA), https://www.apgridpma.org

[7] The European Policy Management Authority for Grid Authentication in e-Science (EUGridPMA), https://www.eugridpma.org

[8] HPCI Certification Authority, https://www.hpci.nii.ac.jp/ca

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

[10] EUGridPMA, *Vetting Model Guidelines*, http://wiki.eugridpma.org/Main/VettingModelGuidelines

[11] The Authentication and Authorisation for Research and Collaboration (AARC) Project, https://aarc-project.eu

[12] Policy Harmonisation Work Package of AARC, https://aarc-project.eu/workpackages/policy-harmonisation/