A Method of An Anonymous Authentication For Flat-rate Service

Yoshio KAKIZAKI[†], Hiroshi YAMAMOTO[††], Hidekazu TSUJI[‡]
† Graduate School of Science and Technology, Tokai University, Japan
††, ‡ School of Information Science and Technology, Tokai University, Japan
Email: [†]yoshio@ruby.net.tokai-u.jp, [††]hiroshi@tokai.ac.jp, [‡]htsuji@keyaki.cc.u-tokai.ac.jp

***Abstract*— As the ubiquitous society spreads rapidly, various private information circulates in large quantities. Information increases explosively in recent years, the importance of privacy protection has risen. When the Web services are used, they need not identify who is the user in some cases. In this paper, we propose the authentication method that achieves privacy protection with authorization without identification. Our method makes it possible to protect user's privacy information when the services. We discuss the security of the attacks, and the untraceability from attribute information to identity information. Thereby we show the effectiveness of our method.**

***Index Terms*— role-based access control, anonymous authentication, privacy protection, attribute authentication**

I. Introduction

As the ubiquitous society spreads rapidly, data with various private information circulates in large quantities. Request for the privacy protection has risen in Japan along with the overall enforcement of Act for Protection of Computer Processed Personal Data held by Administrative Organs [1] from April, 2005. Moreover, privacy information is used for purposes other than the original intent. Therefore, it has strong resistance to disclosing needless private information.

The eavesdropping, the spoofing, the modification and the other threats on the network are prevented by the PKI applications. PKI is only a means to lower the threat that exists on the network relatively. Moreover, the eavesdropping prevention by the encryption of the communication is possible. However, the function of anonymity is not provided, so the problem of privacy protection is not solved.

When the Web services are used, there is a case that they need not identify who is the user. However, the authentication and the authorization are done at the same time in ID/password method. In such case, the service provider might record the service usage information: what services are used and who used them. So the authentication scheme becomes more and more necessary.

In this paper, we propose the authentication method that achieves privacy protection by using services based on user's authority without identifying. In this method, the regular user who has a regular authority can receive the services with authority but without identifying by service provider, and service provider does not know who the user is. Therefore, our method makes it possible to protect user's privacy information when the services, such as Web service etc., are used.

II. Related Works

The method of achieving privacy protection is researched with various approaches. Anonymous method and pseudonyms method are typical methods of concealing identity. Anonymous method is an approach that cannot identify an individual from the crowd. Pseudonyms method is an approach that cannot identify by using fake name with untraceability. However, when the same person uses the same fake name, an individual can be specified in this method.

As the research of anonymity using certificate, there is the research that separates authentication and authorization using SPKI (Simple PKI) [2], [3], [4]. SPKI certificate is a kind of authorization certificate that does not contain identity information, and identity information can be prevented from leaking by the access control that uses this. However, we employ PKIX (PKI X.509) from the point of the recycling of infrastructure and the easiness of the implementation, because many PKI applications such as SSL and S/MIME use X.509 certificate.

As the research of anonymous authentication using digital signature, there is *k*-Times Anonymous Authentication (*k*-TAA) [5], [6]. *k*-TAA can achieve the access to the application provider of *k*-times with anonymity by using escrow/group signature. However, it is based on group signature. Its approach is different from our method that aims achievement on PKI.

Attribute certificate is X.509 certificate that proves certificate owner's attribute information, and it includes information as shown in TABLE I. Attribute certificate has holder field and attributes field although the field of attribute certificate looks like the field of public-key certificate. The holder field identifies attribute certificate holder, and the attributes field gives attribute information about attribute certificate holder. The conventional method

This paper is based on "A Proposal of An Anonymous Authentication Method For Flat-rate Service", by Y. Kakizaki, H. Yamamoto and H. Tsuji, which appeared in the Proceedings of International Symposium on Frontiers in Availability, Reliability and Security (FARES), in conjunction with the First International Conference on Availability, Reliability and Security, ARES 2006, Vienna, AUSTRIA, April 2006. © 2006 IEEE.

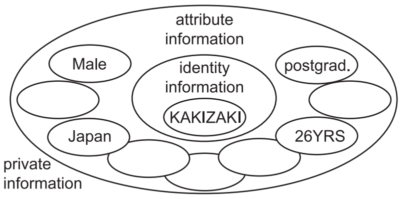

Figure 1. Basic Idea: private information is composed of identity information and attribute information

to contain attribute information is a method of using the extensions field of public-key certificate. However, there is a problem that the reissuing of public-key certificate is needed along with the revocation of attribute information because the lifetime of attribute information is shorter than the lifetime of public-key generally. Attribute certificate solves this problem by containing attribute information to attribute certificate, and make it possible to reduce the cost of public-key generation and management.

RFC3281 [7] just explains the framework of attribute certificate, and details about actual operation are not explained. Chiba et al. examine the details of registration and the use of attribute information [8]. Imaeda et al. consider the problems and the solutions when attribute certificate is linked to public-key certificate with the objectDigestInfo [9]. They took notice of anonymity because attribute certificate does not contain identity information, and they pointed out that additional research is needed. However, the method of achieving anonymity in using attribute certificate remains as a problem. Therefore, it is necessary to examine the authentication method that effectively uses attribute information and the application scene.

III. An Anonymous Authentication Method

A. Basic Idea and Approach

Private information is composed of identity information and attribute information as shown in Figure 1. Identity information identifies the object person, and attribute information shows the qualification and the authority given to the object person. For instance, “KAKIZAKI” is identity information, and “Postgraduate” is attribute information on “KAKIZAKI”. Attribute information is the one component of private information. Thus, attribute information separated from identity information loses value as private information. Attribute information is effective in the case of combining with identity information. If attribute information has no link to identity information, attribute information has the anonymity. When the questionnaires data are processed statistical, identity information is discarded and only attribute information is tallied. This is our basic idea.

Our approach is to apply this basic idea to digital certificate. Our method is an anonymous authentication method that makes it possible that the user can take the services without identifying. The following steps achieve this: identity information and attribute information are separated from private information. Next, public-key certificate with identity information is used to prove the authenticity. Attribute certificate with attribute information is used to prove the authority.

Our method protects user’s usage information by concealing what services are used and who used them.

B. Structure

The structure of our method is shown in Figure 2. Our method is a trusted third party model, and attribute authority, service provider, and user compose it.

1) Entity:

a) Attribute Authority (AA): issues *Attribute Certificate*. *Attribute Authority* and *Service Provider* have the mutual trust. *Attribute Authority* is assigned privilege by *Service Provider* to issue *Attribute Certificate*.

Attribute Authority issues *Attribute Certificate* for the services and the authentication information. *Attribute Certificate* verifier can confirm the user who the regular user is. The hash of the authentication information and attribute information that is user’s authority is contained in *Attribute Certificate*.

b) Service Provider (SP): provides the services that are Web service and others for user. *Service Provider* and *Attribute Authority* have the mutual trust. *Service Provider* assigns privilege to *Attribute Authority* to issue *Attribute Certificate*.

Service Provider verifies that *Attribute Certificate* is from *User*, and that the authentication information is from *Attribute Authority*. *Service Provider* confirms that *User* is *Attribute Certificate* owner by using the authentication information, and that *User* is correct user. *Service Provider* provides the service after confirming that attributes of *Attribute Certificate* is *User*’s.

c) User: takes the services that are Web service and others from *Service Provider*.

User pushes *Public-key Certificate* to *Attribute Authority*. *User* pushes *Attribute Certificate* to *Service Provider* after issuing *Attribute Certificate*, and takes the service which is based on attributes of *Attribute Certificate* after confirming.

2) Certificate: Our method is using public-key certificate and attribute certificate as digital certificate. Two certificates are explained in this section. The features of these are shown in TABLE II.

a) Public-key Certificate (PKC): is X.509 certificate that proves certificate owner’s authenticity. *Public-key Certificate* shows public-key which is signed by Certificate Authority that proves validity.

b) Attribute Certificate (AC): is X.509 certificate that proves certificate owner’s attribute information. It does not contain public-key, but contains attribute information for authorization. It is necessary to bind both *Attribute Certificate* to *Attribute Certificate* owner’s *Public-key Certificate* because information that proves *Attribute Certificate* owner’s identity is not contained in *Attribute Certificate*. The holder field of *Attribute Certificate* is used for this binding.

TABLE I.
PROFILE OF ATTRIBUTE CERTIFICATE STANDARD FIELDS

Fields Name	Definition
version	v2
holder	identity of the holder
issuer	identity of the AA that issued the certificate
signature	algorithm used to sign the certificate
serialNumber	unique identifier of the certificate
attrCertValidityPeriod	time period for the validity of the certificate
attributes	attributes associated with the holder
issuerUniqueID	additional issuer identification
extensions	addition of new fields to the certificate

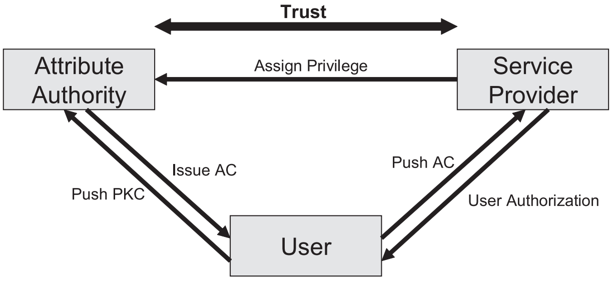

Figure 2. The Structure of Our Method

TABLE II.
A COMPARISON OF PUBLIC-KEY CERTIFICATE AND ATTRIBUTE CERTIFICATE

	Public-key Certificate	Attribute Certificate
Purpose	to prove the authenticity	to prove the authorization
Article	subject name and public-key	attributes
Validity Period	long	short
Issuer	Certificate Authority	Attribute Authority

The holder field has three options as shown in TABLE III: baseCertificateID, entityName, and objectDigestInfo. With the baseCertificateID option, *Attribute Certificate* and *Public-key Certificate* are bound by the holder's *Public-key Certificate* serialNumber and issuer. With the entityName option, *Attribute Certificate* and *Public-key Certificate* are bound by the holder's *Public-key Certificate* subject or subjectAltName. These two options bind *Attribute Certificate* to *Public-key Certificate*, and the verifier can identify an individual by *Public-key Certificate*. With the objectDigestInfo option, *Attribute Certificate* and *Public-key Certificate* are bound by the target object's hash. Therefore, it is possible to bind *Public-key Certificate* or also the other objects by using the objectDigestInfo option.

Attribute Certificate is not bound to *Public-key Certificate* in our method, thus, the objectDigestInfo is used for the holder field of *Attribute Certificate*. *Attribute Certificate* verifier cannot identify who the *Attribute Certificate* owner is though it can confirm that *Attribute Certificate* owner is a regular user, by setting the authentication information to the target object of objectDijestInfo.

AuthInfo is decided as follows. First, two random numbers are generated. One is the authentication key between *User* and *Service Provider*, and the other is the session key for *User*. The user key is calculated with XOR of the authentication key and the session key. *AuthInfo* is made from the authentication key and the user key encrypted with public-key of *Attribute Certificate* owner which are encrypted with public-key of *Service Provider*. Hash of *AuthInfo* is set in objectDigestInfo of the holder field of *Attribute Certificate*.

There is a possibility to be traced from service usage information when same *Attribute Certificate* is used. So, we decided to make *Attribute Certificate* disposable to preclude the possibility of it. Basically, *Attribute Certificate* is set to one certificate per one session. Therefore, the validity period of *Attribute Certificate* can be set very short. Thus, *Attribute Certificate* revocation and CRL (Certificate Revocation List) or OCSP (Online Certificate Status Protocol) might be unnecessary by this setting.

C. Procedure

User operates as follows to take the services of *Service Provider* and the system flow is shown in Figure 3.

Issuing Attribute Certificate:

1) *User* pushes *PKC* to *AA*.
2) *AA* verifies *PKC* validity. Moreover, *AA* verifies whether *User* has private-key which is another of a pair of *PKC*.
3) *AA* generates *AuthInfo* as follows. First, *AA* generates two random numbers. One is the authentication key between *User* and *SP*, and the other is the

TABLE III.
PROFILE OF HOLDER FIELD OPTIONS

Options Name	Definition
baseCertificateID	the holder's PKC serialNumber and issuer
entityName	the holder's PKC subject or subjectAltName
objectDigestInfo	a hash of the target object

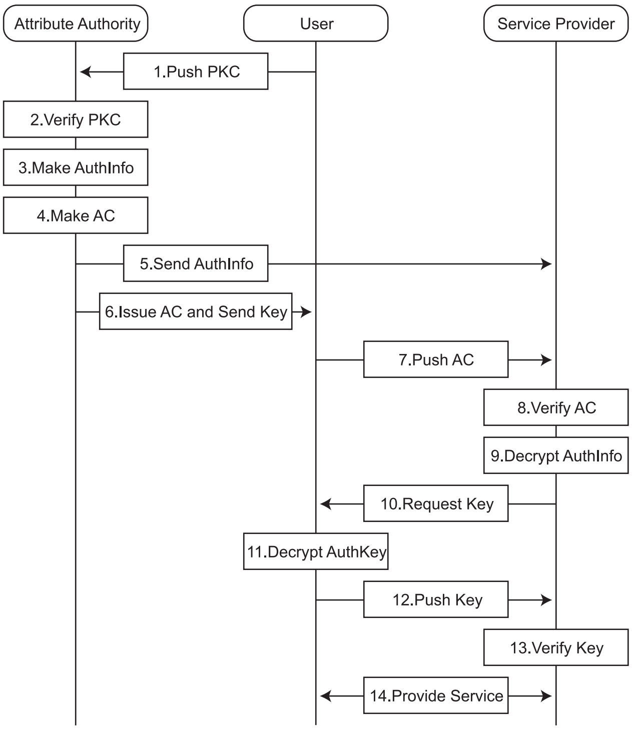

Figure 3. The Flow of Our Method

session key for *User*. The user key is calculated with XOR of the authentication key and the session key. *AuthInfo* is made from the authentication key and the user key encrypted with public-key of *AC* owner which are encrypted with public-key of *SP*.

4) *AA* calculates a hash of the object that is *AuthInfo*, it is written into objectDigestInfo of *AC*.holder. Moreover, *User*'s attributes are written into attributes field of *AC*, and *AA* makes *AC*.
5) *AA* sends *AuthInfo* to *SP*.
6) *AA* issues *AC* to *User*. And *AA* sends the session key to *User*.

Pushing Attribute Certificate:

7) *User* pushes *AC* issued by *AA* to *SP*.
8) *SP* verifies digital signature of *AC* is correct, and confirms *AC* issuer is assigned privilege *AA*. Moreover, *SP* confirms the modification and the forgery, and confirms validity period.
9) *SP* verifies *AC.holder* with hash of *AuthInfo* that is from *AA*. *AuthInfo* is decrypted by private-key, and the authentication key and *AuthKey* are taken out.
10) *SP* sends the user key which is encrypted by public-key of *AC* owner to *User* for confirming *User* is a regular user.

TABLE IV.
NOTATION

Symbol	Meaning
$E(M, A)$	encrypt M by A's public-key
$D(M, A)$	decrypt M by A's private-key
$H(M)$	hash of M
$AC.holder$	holder field of AC
KEY	as random integer
$AuthKey$	as a key for the authentication
$AuthInfo$	authentication information
SP	Service Provider
U	User
$A \overset{sendto}{\longrightarrow} B$	A is sent to B
$A \overset{?}{=} B$	comparison whether A is equal to B

Authorization:

11) *User* decrypts *AuthKey* which is from *SP* with private-key of *User*. And the authentication key is calculated with XOR of the user key and the session key.
12) *User* pushes the authentication key to *SP*.
13) *SP* judges that *User* is correct owner of *AC* if the authentication key from *User* is equal to the key which is taken out of *AuthInfo*.
14) *SP* provides the service based on authority of *AC*.

D. Effectiveness

The effectiveness of privacy protection and safe use of our method are explained with the notation of Table IV.

Attribute Authority:

$$\begin{aligned}
&\text{Generate } KEY_A, KEY_S \text{ as random integer}\\
&KEY_U = KEY_A \oplus KEY_S\\
&AuthKey = E(KEY_U, U)\\
&AuthInfo = E((KEY_A, AuthKey), SP)\\
&AC.holder = H(AuthInfo)\\
&AuthInfo \overset{sendto}{\longrightarrow} SP\\
&KEY_S \overset{sendto}{\longrightarrow} U
\end{aligned}$$

Service Provider:

$$\begin{aligned}
&H(AuthInfo) \overset{?}{=} AC.holder\\
&KEY_A, AuthKey = D(AuthInfo, SP)\\
&AuthKey \overset{sendto}{\longrightarrow} U
\end{aligned}$$

User:

$$\begin{aligned}
&KEY_U = D(AuthKey, U)\\
&KEY_A = KEY_U \oplus KEY_S\\
&KEY_A \overset{sendto}{\longrightarrow} SP
\end{aligned}$$

Service Provider:

$$KEY_A \text{ from } AuthInfo \overset{?}{=} KEY_A \text{ from } U$$

AA has *User*'s identity and authority information, and issues *AC* for the service, though *AA* cannot know what services *User* actually used. *AA* issues *AC* including the authority information and *AuthInfo* including the authentication information. *AA* generates KEY_A, KEY_S and KEY_U for the authentication information.

$$KEY_A = KEY_U \oplus KEY_S$$

and

$$KEY_S = KEY_U \oplus KEY_A$$

though *User* has KEY_S and KEY_U encrypted by *User*'s public-key. *User* can obtain KEY_A from KEY_S and decrypted KEY_U. Therefore, *AC* can be used when both KEY_S is issued from *AA* and the private-key corresponding to *AC* owner's public-key.

AuthInfo includes the confirmation information which is the *AC* user is regular, but it cannot identify who the *AC* user is. Therefore, *AC* verifier cannot confirm who the *AC* user is.

AuthInfo does not include who the *AC* user is although it includes the confirmation information that is the *AC* user is regular. Therefore, *SP* knows what services *User* actually used, but cannot identify who the *AC* user is.

Thus, privacy information can be protected because it is distributed with *SP* and *AA*.

IV. Development

A. Application Scope

We separate authentication and authorization with identity information and attribute information respectively. Herewith, the method makes it possible that the user take the service without identifying by service provider, and it achieves privacy protection by hiding the service usage information. The method is useful under the following conditions.

- The service that is not including privacy information
- Two or more services must exist
- No meter rate service

At the service that is including privacy information, Privacy information can be specified from the service used. As an example of this problem is healthcare information service. Healthcare information is attribute information extremely near privacy information, and the demand of user who wants to be protecting it is strong. However, both identity information and attribute information are needed in the greater part of services of healthcare field. Thus, the method is not useful in such a scene.

At just single service, the user's purpose is to use the only service. Therefore, there is no point in hiding the service usage information.

At meter rate service, the content of service used can be guessed according to the charge of service, because the charge of service is different depending on the content of service or the amount used. Therefore, it is difficult to protect privacy information only by hiding the service usage information.

B. Operative Example

E-learning, the books browsing service, and the video delivery service, etc. are thought as an example of applying our method.

We assume e-learning: the user can freely attend the class which is providing, as long as the user pays the tuition. The user does not want the service provider to ever know what class the user attends. Service provider does not mind as long as the user has regular authority even if the user attends which class. Moreover, service provider can know the popularity of each class although it cannot know who to which class is attending.

The user registers to service provider that provides e-learning. Service provider assigns privilege to attribute authority for issuing attribute certificate that is necessary of the service use. Attribute authority issues attribute certificate and the authentication key to the user. The user pushes attribute certificate to service provider, proves the regular user by the authentication key, and takes e-learning.

Attribute authority cannot know which class the user attended although it knows which class can be attended and who is the user. Service provider cannot know who the user is although it can confirm which class the user can attend and can know the popularity of each class. As mentioned above, service provider and attribute authority never know who to which class is attending.

In the same way, we assume the books browsing service: a free member can browse only for a free member's although the dues-paying member can browse all books. The user does not want the service provider to ever know what books the user browses. Service provider does not mind as long as the user has regular authority even if the user browses which books.

Last, we assume the video delivery service: there are many genres such as the movie, sports, and dramas, and the user who has contracted the genre can freely watch contents in the genre. The user does not want the service provider to ever know what contents the user watches. Service provider does not mind as long as the user has regular authority even if the user watches which contents. Moreover, service provider can know the popularity of each content.

Thus, the user can freely use the services; howbeit service provider does not record the service usage information. It is possible to protect the service usage information that is privacy information.

V. Discussion

A. Advantage

Our method makes it possible to take the services without identifying and to protect user's privacy. *Attribute Authority* can know who is user and what authority user has, although it cannot know what services user used actually. *Service Provider* can know what services are used and what authority user has, although it cannot know who is user. Nobody can know what services are used and who is user. The method has the advantage that user's privacy information is protected and the authority can be managed efficiently.

The method has adaptability with PKIX because it uses the *Public-key Certificate* and *Attribute Certificate*. Many PKI applications such as SSL and S/MIME use X.509 certificate. PKIX is in widespread than SPKI. Therefore, our method achieved on PKIX has more adaptability to current infrastructure than the method achieved on SPKI [3], [4].

Attribute Certificate is made to be disposable to prevent the traceability from service usage information. However, it is preferable to be able to recycle *Attribute Certificate* as long as attribute does not change. Especially, there is the problem that the issuing cost of *Attribute Certificate* becomes high in case of the service frequently used. Even if *Attribute Certificate* is recycled several times, it might be safe enough. However, the possibility that an individual is specified increases by using same *Attribute Certificate*. Therefore, the level of privacy protection and the issuing cost of *Attribute Certificate* are trade-offs.

B. Security

1) Modification and Forgery: *Attribute Certificate* is X.509 certificate. *Attribute Certificate* is signed by *Attribute Authority* which is *Attribute Certificate* issuer. The modification and forgery can be detected by verifying digital signature. The security level of this certificate is equal to others of PKI.

2) Reusing: The lifetime of *Attribute Certificate* is very short, because of one certificate per one session. In addition, *Service Provider* records the serialNumber of *Attribute Certificate* which is used. Thus, *Attribute Certificate* cannot be reused.

The reason why our method does not permit reusing *Attribute Certificate* is that an individual is specified by reusing, and privacy protection becomes difficult. If *Attribute Certificate* is reused, it is a pseudonyms method because the serialNumber can be assumed the fake name. Oppositely, if *Attribute Certificate* is made disposable, it is an anonymous method. Our goal is privacy protection by anonymous. Therefore, there was a necessity for making *Attribute Certificate* disposable because we had to have employed an anonymous method.

3) Fraud and Spoofing: We discuss the case that malicious user gets *Attribute Certificate* by the fraud method. Malicious user pushes *Attribute Certificate* to *Service Provider*. To confirm the *Attribute Certificate* user is correct, *Service Provider* sends *AuthKey* which is encrypted by *Attribute Certificate* owner's public-key to *Attribute Certificate* user who is malicious user. At this time, the malicious user cannot decrypt *AuthKey* because malicious user is not regular *Attribute Certificate* owner. Malicious user does not have private-key of regular *Attribute Certificate* owner. Therefore, even if malicious user illegally gets *Attribute Certificate*, one cannot use it. Furthermore, regular user is not permitted to take the services by the illegal authority, too.

Even if it does not know KEY_S or KEY_U, KEY_A can be estimated. However, if the authentication is failed at one trial, service provider rejects the session because it is easy to calculate KEY_A from KEY_S and KEY_U. New *Attribute Certificate* is needed for re-authentication because *Attribute Certificate* is disposable. Therefore, it is difficult for malicious user to attack it.

C. Untraceability

Identity information is not contained in *Attribute Certificate* which is necessary in the services. *Attribute Certificate* verifier cannot identify user from *Attribute Certificate* directly. However, user activity can be traced by service usage information. For instance, user who uses same *Attribute Certificate* can identify that one is same user. Moreover, there is a possibility that an individual can be identified in the some situations. There is the problem that is the traceability from service usage information from the side of privacy protection. Therefore, we propose the method that *Attribute Certificate* cannot reuse to prevent it.

VI. Conclusion

In this paper, we propose the authentication method that achieves privacy protection by using services based on user's authority without identifying. Our method makes it possible to protect user's privacy information when the services, such as Web service etc., are used.

Identity information that identifies an individual is not contained in attribute certificate. And only attribute information for authorization is contained in it. However its holder is bound in the holder field. Attribute certificate verifier can confirm that attribute certificate owner is a regular user although it cannot identify attribute certificate owner directly. Thus, the user can take the services without identifying an individual, and the service provider can provide the services only for a regular user. Our method makes it possible to protect user's privacy because service provider cannot identify user.

We discuss the security of the attacks that are modification, forgery, fraud and spoofing, and the untraceability from attribute information to user's usage information and identity information. Thereby we show the effectiveness of our method.

References

[1] G. of Japan, *Act for Protection of Computer Processed Personal Data held by Administrative Organs*, 2005. [Online]. Available: www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

[2] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, *SPKI Certificate Theory*, 1999, RFC2693.

[3] T. Saito, K. Umesawa, T. Kito, and H. Okuno, "Privacy-Enhanced SPKI Access Control on PKIX and Its Application to Web Server," in *AINA2003*, 2003, pp. 696–703.

[4] T. Saito, K. Umesawa, and H. Okuno, “A Privacy-Enhanced Access Control,” *IEICE Transactions*, vol. J84-D1, no. 11, pp. 1553–1562, 2001.

[5] L. Nguyen and R. Safavi-Naini, “Dynamic k-Times Anonymous Authentication,” in *ACNS 2005*, vol. 3531 of LNCS, 2005, pp. 318–333.

[6] I. Teranishi, J. Furukawa, and K. Sako, “k-Times Anonymous Authentication,” in *ASIACRYPT 2004*, vol. 3329 of LNCS, 2004, pp. 308–322.

[7] S. Farrell and R. Housley, *An Internet Attribute Certificate Profile for Authorization*, 2002, RFC3281.

[8] M. Chiba, K. Urushima, and Y. Maeda, “Personal Attribute Provider: A Secure Framework for Personal Attribute Exchange on the Internet,” *IPSJ Journal*, vol. 47, no. 3, pp. 676–685, 2006.

[9] N. Imaeda, H. Odahara, and H. Masamoto, “A consideration to tie PKCs to ACs at using ACs,” IEICE, Tech. Rep., 2003, ISEC2002-106.

[10] T. Nakanishi and Y. Sugiyama, “Anonymous Statistical Survey of Attributes,” in *ACISP2001*, vol. 2119 of LNCS, 2001, pp. 460–473.

[11] J. S. Park, R. Sandhu, and G. Ahn, “Role-Based Access Control on the Web,” *ACM Transactions on Information and System Security*, vol. 4, no. 1, pp. 37–71, 2001.

[12] V. Benjumea, J. Lopez, J. A. Montenegro, and J. M. Troya, “A First Approach to Provide Anonymity in Attribute Certificates,” in *PKC 2004*, vol. 2947 of LNCS, 2004, pp. 402–415.

[13] N. Sato and H. Suzuki, “An Authentication System that Can Verify an Anonymous Person’s Rights,” *IPSJ Journal*, vol. 41, no. 8, pp. 2138–2147, 2000.

[14] Y. Kakizaki, H. Yamamoto, and H. Tsuji, “A Proposal of An Anonymous Authentication Method For Flat-rate Service,” in *ARES 2006*, 2006, pp. 551–557.

Yoshio KAKIZAKI is currently a Ph.D. candidate at Tokai University, Japan. He received his MS and BS degrees in engineering from Tokai University, Japan, in 2005 and 2003, respectively. His research interests include information security and network communication.

Hiroshi YAMAMOTO was born in Osaka, Japan. He received his PhD degree in engineering from Osaka University in 1996, his MS degree in engineering from Osaka University 1993, and his BS degree in engineering from Osaka University 1991. He is currently an Associate Professor of School of Information Science and Technology, Tokai University, Japan. His current research interests include coding theory and information security. He is a member ofthe Institute of Electronics, Information and Communication Engineers, Engineering Sciences Society.

Hidekazu TSUJI received the BS, MS and Ph.D degree in electrical engineering from Osaka University, in 1969, 1971 and 1974, respectively. He is currently a professor, head in the Dept. of Information Media Technology, School of Information Science and Technology, Tokai University, in Kanagawa, Japan. He joined the Mitsubishi Electric Corporation in 1974. He researched and developed the human-interface system, knowledge information system, and agent software. He studied e-commerce and information security in the ECOM(Electronic Commerce Promotion Council of JAPAN) from 1997 to 1999. He has joined Tokai University in 2000.