CLIP: An Online PKI Management Function

Yoshiaki Nakajima, Hiroshi Masamoto, Kunio Kobayashi, Masanobu Sakamoto, and Satoshi Arai

Abstract

CLIP is a new function of Trust-CANP, which is a PKI-based electronic certification system available from NTT. It is designed to reduce operating costs, one of the barriers to widespread adoption of the public key infrastructure (PKI) scheme, by providing services online to both end users and operators, while also making it more convenient for these users.

1. Authentication technology and PKI

In order for the Internet to be used as part of the social infrastructure, it is very important to have technology that can conclusively confirm with whom we are communicating, or who created any particular digital data. The public key infrastructure (PKI) scheme is one such type of authentication technology. PKI provides an infrastructure for authentication using public-key cryptography. With PKI, a trusted third-party authority issues a public key certificate that verifies the relationship between the key and its holder. Authentication can be carried out by verifying the public key certificate and a digital signature created by the other party. In Japan, this operation can be easily understood by regarding a public key certificate as the counterpart of a registered seal in the real world and by regarding a digital signature as the impression of a seal.

2. Certificate Authority system

A Certificate Authority (CA) is an entity that issues public key certificates. The CA is composed of the Issuing Authority (IA), which has the role of issuing and revoking public key certificates and issuing a list of revoked certificates, and the Registration Authority (RA), which accepts applications, verifies the identities of end-users, and manages end-user information, as shown in **Fig. 1**. The IA generally issues public key certificates in the standard format specified in RFC 3280, but the RA functions vary according to the individual product or system.

NTT Information Sharing Platform Laboratories is developing Trust-CANP [1], [2] as a CA product. Its RA function uses an issuing method that accepts only off-line constituents and is limited to handling fixed combinations of user data. Most of the applications of this product so far have been in the public-sector field.

3. Difficulties with PKI

With the RA function of most traditional CAs, such as Trust-CANP, aspects like the user data and application procedure are fixed, so these CAs are difficult to use when there is wider variation in the type of user data or a variety of application procedures for issuing public key certificates. Traditional RAs have not been suited to private services because the level of requirements in these areas tends to be high.

Moreover, operational costs tend to increase for systems operating off-line, which is also not always compatible with cost-conscious private services, and the extra burden on users of acquiring a public key certificate through an off-line process can be a reason

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Contact: ninkou-info@lab.ntt.co.jp

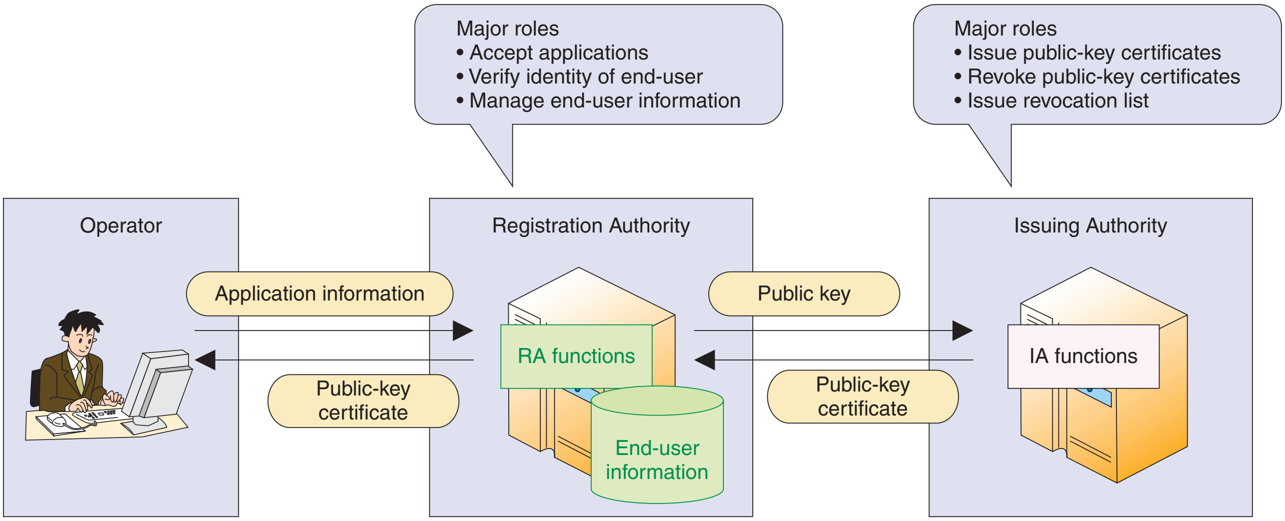


Fig. 1. RA and IA functions.

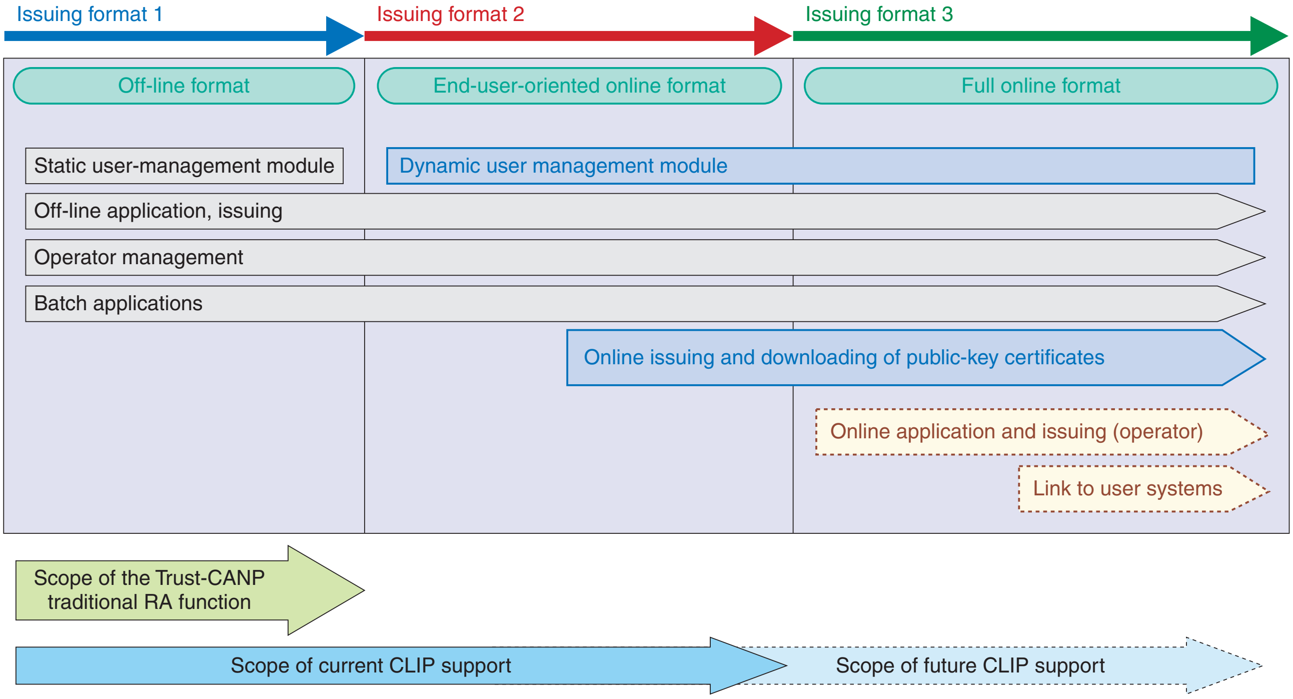

Issuing format 1
Issuing format 2
Issuing format 3
Off-line format
End-user-oriented online format
Full online format
Static user-management module
Dynamic user management module
Off-line application, issuing
Operator management
Batch applications
Online issuing and downloading of public-key certificates
Online application and issuing (operator)
Link to user systems
Scope of the Trust-CANP traditional RA function
Scope of current CLIP support
Scope of future CLIP support

Fig. 2. Directions for the extension of RA issuing functions and the state of CLIP support.

for avoiding PKI.

In particular, a significant obstruction to the adoption of PKI is the increase in the variety of applications and devices providing PKI functions, such as Web browsers, email programs, and network routers along with the variety of public key certificates required for each of them. This is adding another layer of burden to the acquisition of public key certificates.

4. Implementing an online CA with CLIP

NTT Information Sharing Platform Laboratories believes that extending the functions of the RA in the ways shown in **Fig. 2** will be an effective way to resolve the issues discussed in Section 3. Based on the above-mentioned ideas, it is developing CLIP (customizable lightweight identity profiler) as a new function of Trust-CANP. A comparison of traditional

Table 1. Comparison of traditional RA functions and CLIP.

	Traditional function	CLIP
Certificate distribution method	Off-line (face-to-face, by email, etc.)	Online (download using a Web browser)
Assumed user	Operator	End user or operator
Assumed network	Authenticated internal network	Internet
Dedicated client software	Installation required	No installation required
User management module	Fixed for system	Can be defined at point of use

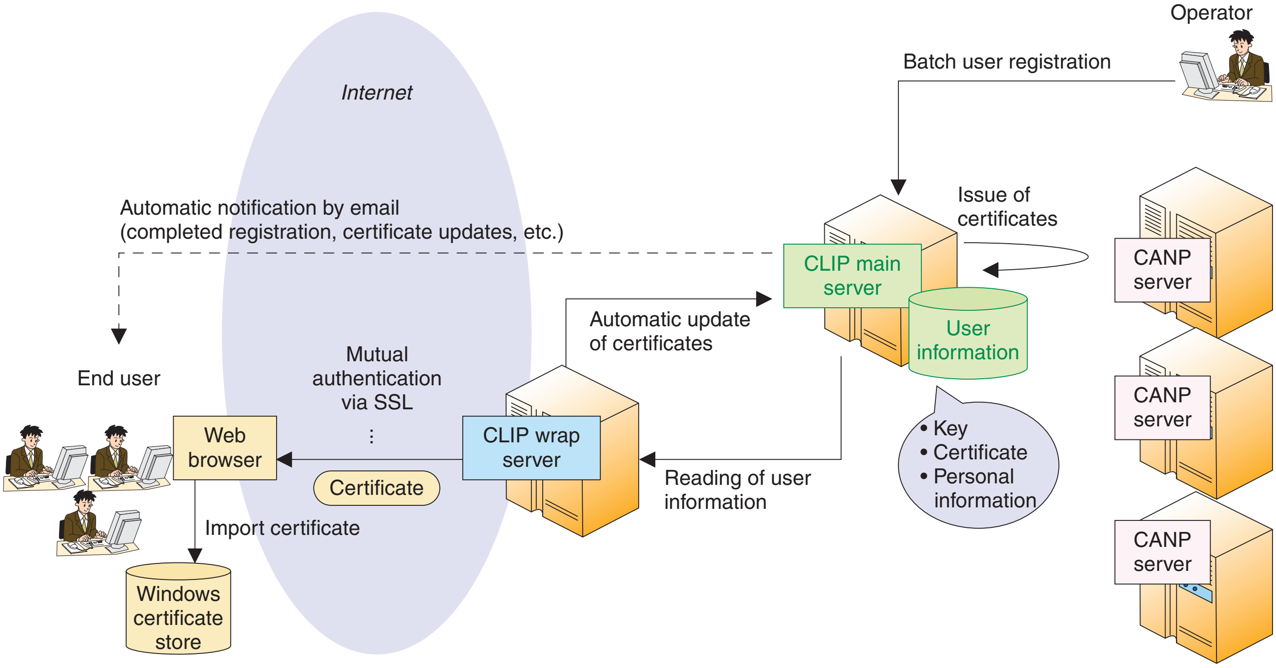


Fig. 3. Example of CLIP system configuration.

RA functions and CLIP is given in **Table 1**.

CLIP differs from traditional RAs by enabling online operation via the Internet instead of requiring off-line procedures for the initial contact. It can issue various types of public key certificates effectively with various combinations of user information because it manages the user data required for the certificates flexibly, according to the requirements where the certificate is to be used. These characteristics satisfy the direction of *end-user-oriented online support* shown in Fig. 2. Extending it further to provide full online support will make possible an online CA system yielding improvements in both convenience and operational efficiency.

5. Architecture and characteristics of CLIP

An example of a typical system architecture using CLIP is shown in **Fig. 3**. The role of CLIP is to provide the RA function for Trust-CANP. The CLIP main server manages user information and processes the issuing and revoking of public key certificates through its link to the CANP server, which provides the IA function. The CLIP wrap server provides user access as well as functions for issuing and downloading public key certificates. The main features of CLIP are as follows:

(1) It handles a variety of types of user data used to issue public key certificates.
(2) It can link to multiple CAs.
(3) It can verify requirements for issuing a certificate based on a public key certificate.
(4) It can issue multiple and various types of public

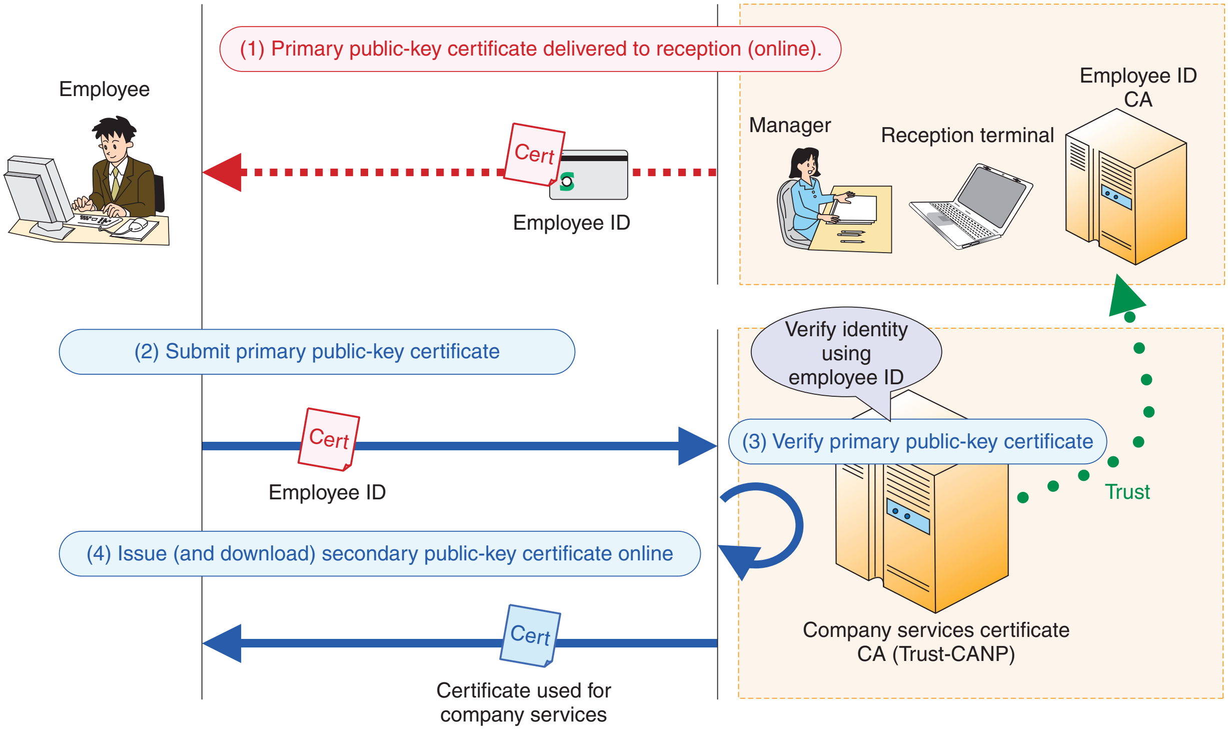

(1) Primary public-key certificate delivered to reception (online).
Employee
Cert
Employee ID
Manager
Reception terminal
Employee ID CA
(2) Submit primary public-key certificate
Verify identity using employee ID
Cert
Employee ID
(3) Verify primary public-key certificate
Trust
(4) Issue (and download) secondary public-key certificate online
Cert
Certificate used for company services
Company services certificate CA (Trust-CANP)

Fig. 4. Linked issuing of public-key certificates.

key certificates online.

(5) Certificates can be distributed to users and imported into terminals automatically.

CLIP handles user data including the key, public key certificate, and personal data as generalized attribute data. In so doing, it can handle information that will not all be stored in the public key certificate (like user classification or contract information) more flexibly, providing specialized functionality that can meet the various needs of private-sector services.

As shown in Fig. 3, users can use multiple CAs in a centralized way through CLIP, so multiple certificates can be managed together, and certificates can be issued based on verification using other, already-existing public key certificates. In addition to this feature being used for renewing a public key certificate, it can also be applied to the process of issuing new, different certificates in a linked fashion. An existing public key certificate (the primary certificate) would be used to verify the requirements for issuing the new certificate (the secondary certificate), as shown in **Fig. 4**. For example, this will allow modes of operation, using PKI, much like when a membership certificate ("Employee ID" in Fig. 4) is issued based on verification of a person's identity using more-widely used means such as a driver's license ("Certificate used for company services" in Fig. 4).

Public key certificates can also be automatically imported into a terminal's certificate store (or the Windows* certificate store) when they are downloaded by the user. Users do not need to install any additional software on their terminal in order to use this function. If this function is combined with a public-key-certificate-issuing portal service, users can be provided with the public key certificates they need in an online, low-cost, and timely manner.

CLIP also provides practical functions for issuing X.509-attribute certificates and for sending email notifications to users for new registrations and when certificates need to be renewed.

6. Example of a CLIP Installation

NTT is using CLIP in a trial operation (**Fig. 5**) to provide a public key certificate issuing service for certifying users of other in-house services. For this service, all employee user accounts were created in CLIP at once, based on data already in the employee database.

Employees can easily download public key certifi-

* Windows is a registered trademark of Microsoft Corporation in the U.S.A. and other countries.

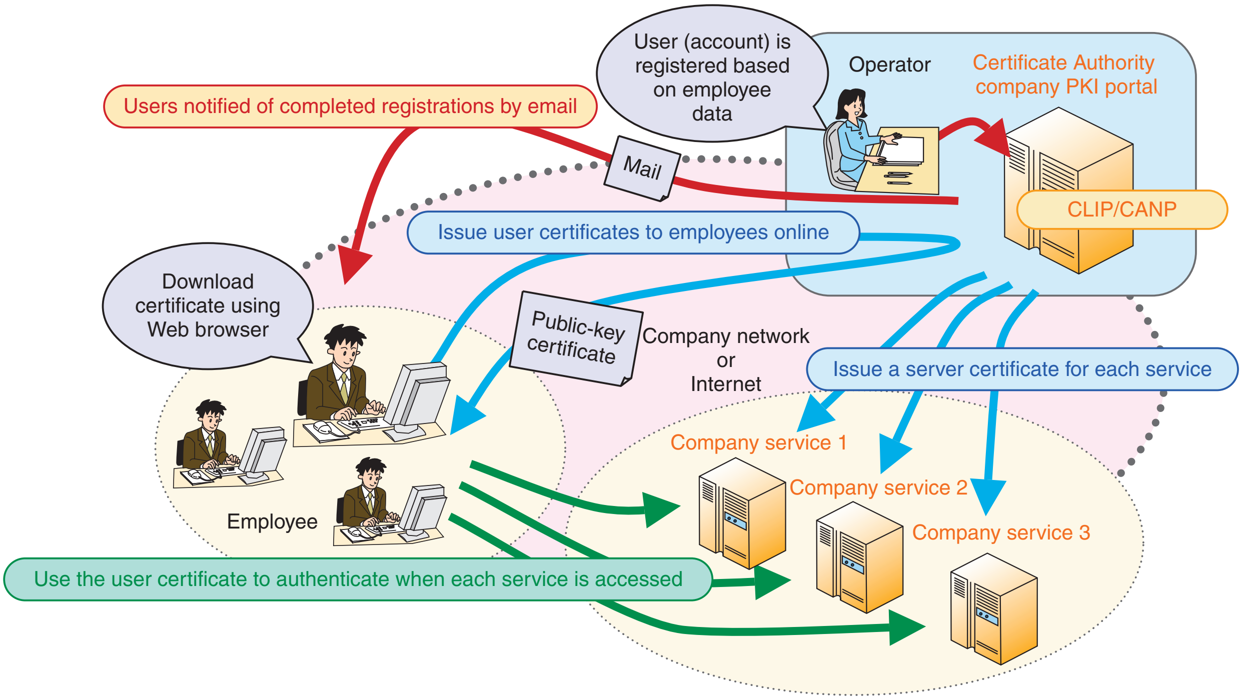
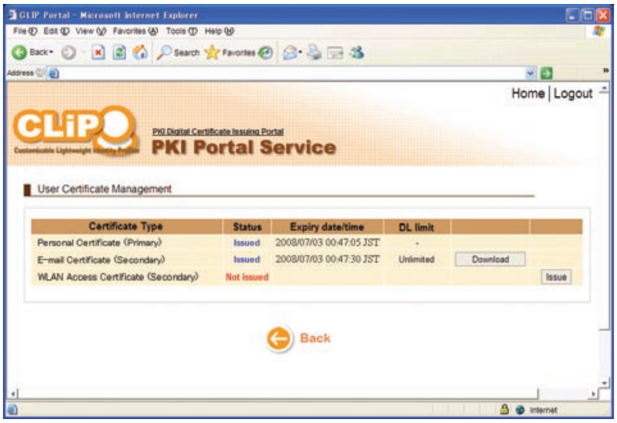

User (account) is registered based on employee data
Operator
Certificate Authority company PKI portal
Users notified of completed registrations by email
Mail
CLIP/CANP
Issue user certificates to employees online
Download certificate using Web browser
Public-key certificate
Company network or Internet
Issue a server certificate for each service
Company service 1
Company service 2
Company service 3
Employee
Use the user certificate to authenticate when each service is accessed

Fig. 5. Example of a CLIP installation.


CLIP Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Home | Logout
CLiP
Customizable Lightweight Identity Profiler
PKI Digital Certificate Issuing Portal
PKI Portal Service

User Certificate Management

Certificate Type	Status	Expiry date/time	DL limit		
Personal Certificate (Primary)	Issued	2008/07/03 00:47:05 JST	-		
E-mail Certificate (Secondary)	Issued	2008/07/03 00:47:30 JST	Unlimited	Download	
WLAN Access Certificate (Secondary)	Not issued				Issue

Fig. 6. User-operation screen when issuing a public-key certificate.

cates using only a Web browser, as shown in the screen-shot in **Fig. 6**. The certificate is automatically stored in the certificate store of the user's terminal when it is downloaded, so compared with conventional procedures in which the user first downloads the file containing the public key certificate and then manually imports it, this system is extremely simple to use. Moreover, users are automatically notified by email when the certificates need to be renewed, and they can perform the update online by themselves, so no operator intervention is required.

At this time, the number of services using public key certificates to verify users is quite limited, and services supporting PKI are not advancing due to the cost barriers of issuing public key certificates. However, if procedures are established within the system to distribute and renew public key certificates at a low cost, this situation will be improved, which should stimulate the appearance of more services using public key certificates.

7. Future developments

To further encourage the spread of PKI in the private sector, it will be necessary to address demands for even greater cost reductions. In particular, one approach that could effectively provide further cost reductions by centralizing facilities and operations is to create an outsourced CA, by contracting out the system operation in an application service provider (ASP) format. Then, by providing an online interface for operators together with end-users, we hope to provide an even more enhanced online CA. Of the main functions of the CA authority, only the application-handling functions will remain in the organization; the rest will be concentrated at the outsourcer. Application handling depends heavily on the structure and operational policies of the organization, but we plan to include functions for a variety of application procedures and ways of allocating roles.

Furthermore, information specific to the issuee (e.g., name and address) is part of what is certified by the public key certificate, so this information is required by both the applicant and the person assessing an application. Thus, there is a need in various circumstances to reference and verify user data that is specific to the organization where the system is being used. Because of this, we are also considering further facilitating the adoption of PKI by expanding functions that link to the organizations' systems, allowing management of issuee data and automatic assessment of applications to be done based on existing user databases.

References

[1] H. Masamoto, S. Arai, T. Matsumura, and J. Kikuchi, "Obtaining ISO 15408 Certification for the Trust-CANP V8.0i Electronic Certification System," NTT Technical Journal, Vol. 17, No. 10, pp. 54–57, 2005 (in Japanese).

[2] Y. Yoshida and H. Masamoto, "Electronic Certification Systems for More Secure Ciphers," NTT Technical Review, Vol. 4, No. 2, pp. 43–48, 2006.

Yoshiaki Nakajima

Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in information science and the M.S. degree in mathematical and computing science from Tokyo Institute of Technology, Tokyo, in 1995 and 1997, respectively. He joined NTT Information and Communication Systems Laboratories in 1997. He has been engaged in R&D of information and communication platforms, security platforms, and so on.

Hiroshi Masamoto

Senior Research Engineer, Supervisor, Application Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in electrical engineering and the M.E. degree in electronics engineering from Kobe University, Hyogo, in 1981 and 1983, respectively. He joined Yokosuka Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT) in 1983. He has been engaged in R&D of data communication protocols, information and communication platforms, security platforms, and so on.

Kunio Kobayashi

Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees from Waseda University, Tokyo, in 1995 and 1997, respectively. He joined NTT Information and Communication Systems Laboratories in 1997. He has been engaged in R&D of cryptography and information security. He received the SCIS '97 Paper Prize in 1997. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan. He is a Certified Information Systems Security Professional.

Masanobu Sakamoto

Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in physics and the M.S. degree in information science from Yamaguchi University, Yamaguchi, in 1996 and 1998, respectively. He joined NTT Human Interface Laboratories in 1998. He has been engaged in research on digital watermarking technology, development of systems to which that technology applied, and so on.

Satoshi Arai

Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in electrical and computer engineering and the M.E. degree in electronics and computer engineering from Toyama University, Toyama, in 1997 and 1999, respectively. He joined NTT Toyama Branch in 1999. He moved to NTT Yokosuka Electrical Communication Laboratories in 2002. He has been engaged in R&D of data communication protocols, information and communication platforms, security platforms, and so on. He is a member of the Information Processing Society of Japan.