Creating a Safe and Secure Network Society Using Digital Certificates and PKI Technology

Hiroshi Masamoto, Yoshihiro Yoshida, Shoichi Hashimoto, Rie Otsubo, and Yoshiaki Nakajima

Abstract

This article gives an overview of public key infrastructure (PKI) technology, which uses digital certificates, and some usage models and it introduces some important system-design considerations for building safe and secure services on networks using PKI. Although PKI is a common security technology, the concepts and considerations required when applying it to practical systems are not widely understood.

1. Risks and countermeasures in a network society

Security measures such as anti-virus software and firewalls have become commonplace with the development of a network society. However, use of these measures cannot necessarily prevent all of the most recent attacks, like spoofing or unauthorized access. When handling digital information within our network society, almost everyone has experienced the insecurity of wondering who the other person is or whether the data they are receiving is really authentic. It is a fundamental characteristic of the network society that we cannot directly confirm the identity of other parties or the authenticity of information. This leads to the inherent risks of impersonation, falsification, and denial.

Digital certificates and digital signatures have been implemented using the public key infrastructure (PKI) scheme to eliminate these risks and provide counterparts to the physical identification documents and seals (or seal imprints) used in real society. There are many technologies for providing authentication and for preventing falsification, as shown in **Fig. 1**, but one strength of PKI technology is that it can provide both authentication (digital certificates) and the means to prevent falsification (digital signatures) at the same time. Through the introduction of PKI, safe and secure transactions with reliable counterparts become possible even on the Internet with its numerous different types of users and huge variety of information.

2. Digital certificates and their trust model

Here, we give a broad overview of the PKI scheme, using the analogy of managing seals in Japan and leave a detailed explanation of PKI principles to other references [1]. PKI uses a pair of mathematically related keys: a private key kept secret by the user and a public key that can be looked up by anyone. In Japan, seals are widely used instead of signatures. For everyday use, a personal seal can be used. For important official documents, however, a person or corporation uses a registered seal to stamp a name in ink onto the document. Private keys and digital certificates correspond, respectively, to the registered seal held exclusively by the owner and the seal registration certificate stating that the seal has been registered at a government office that proves ownership of the

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

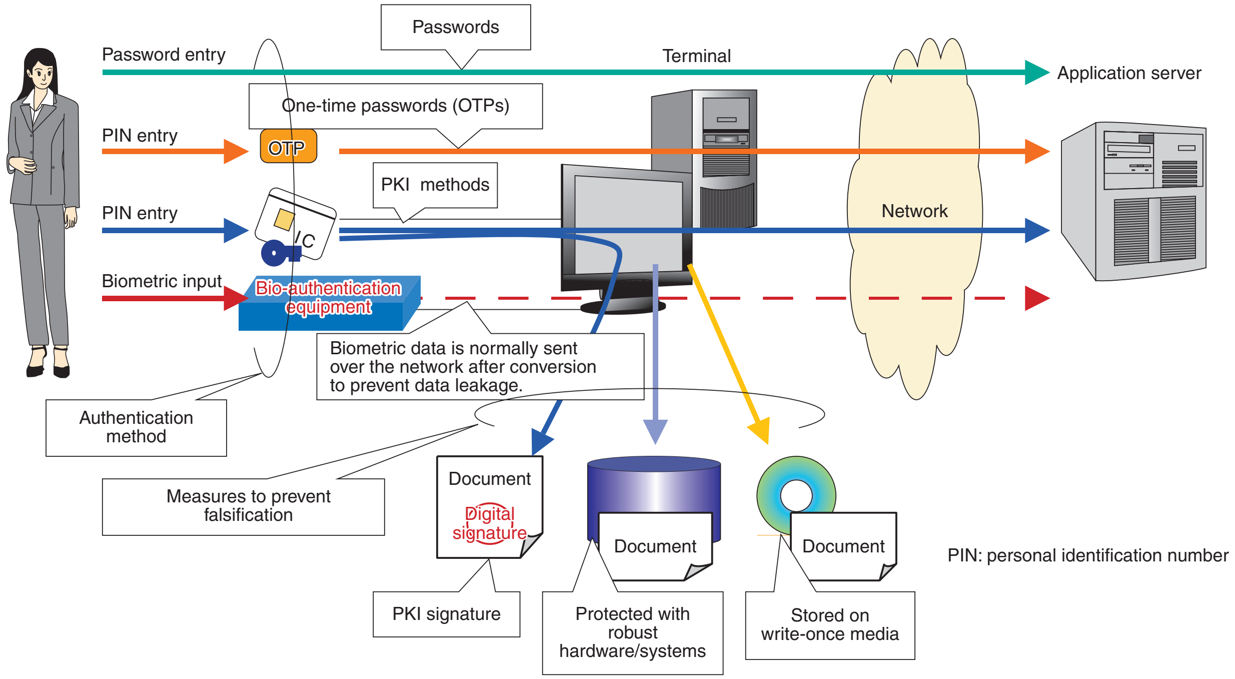
Passwords
Password entry
Terminal
Application server
One-time passwords (OTPs)
PIN entry
OTP
PKI methods
PIN entry
IC
Network
Biometric input
Bio-authentication equipment
Biometric data is normally sent over the network after conversion to prevent data leakage.
Authentication method
Measures to prevent falsification
Document
Digital signature
Document
Document
PIN: personal identification number
PKI signature
Protected with robust hardware/systems
Stored on write-once media

Fig. 1. Major security technologies for authentication and prevention of falsification.

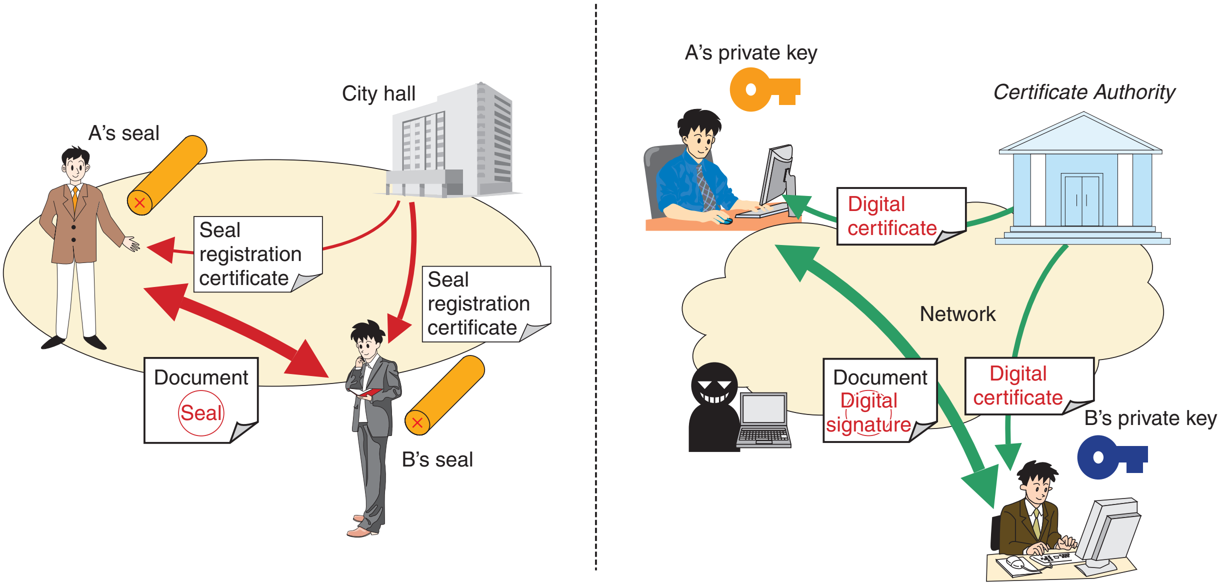

Fig. 2. Real society (in Japan) compared with the network society.

seal. Digital signatures created using a private key correspond to impressions made by applying the seal (**Fig. 2**).

It is important to note that possession of a digital certificate does not necessarily verify the identity of the party. In contrast to paper documents (such as banknotes and documents with signatures, which are hard to copy identically), digital data can be duplicated easily, so simply possessing the data cannot prove identity. To verify that the party (performing the action) is authentic, one must see both the digital certificate and a signature created using the private key.

The digital certificate is equivalent to a document

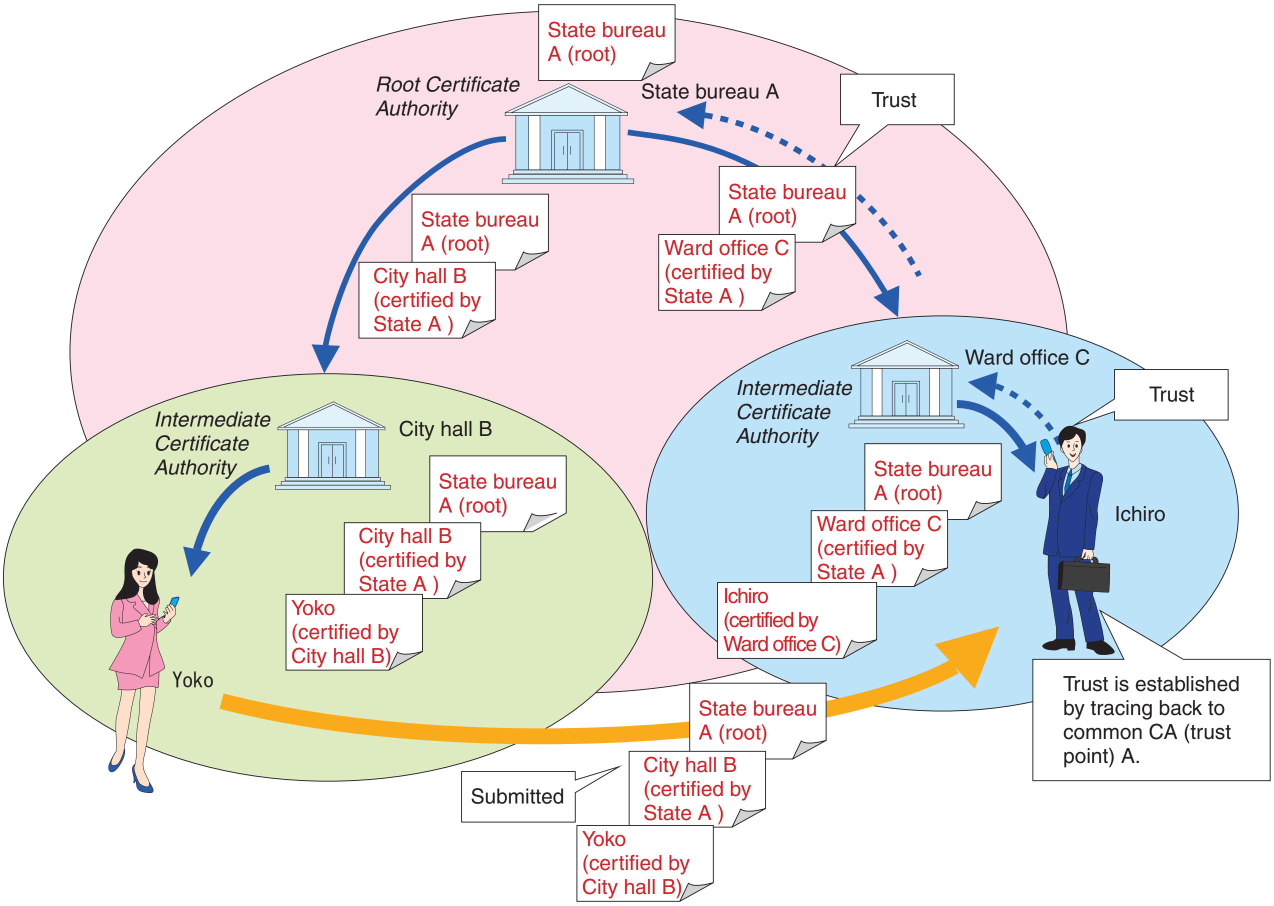
Root Certificate Authority
State bureau A (root)
State bureau A
Trust
State bureau A (root)
City hall B (certified by State A)
State bureau A (root)
Ward office C (certified by State A)
Intermediate Certificate Authority
City hall B
State bureau A (root)
City hall B (certified by State A)
Yoko (certified by City hall B)
Yoko
Intermediate Certificate Authority
Ward office C
Trust
State bureau A (root)
Ward office C (certified by State A)
Ichiro (certified by Ward office C)
Ichiro
Trust is established by tracing back to common CA (trust point) A.
State bureau A (root)
City hall B (certified by State A)
Yoko (certified by City hall B)
Submitted

Fig. 3. Digital certificates and a trust model.

that certifies the relationship between the public key (which is related to the private key) and its owner. In the case of a seal, it is the proof of the relationship between the seal itself (or the impression made by the seal) and its owner. A fundamental point here is whether or not this certificate is reliable. Certificates are issued by a *trusted third party* called a Certificate Authority (CA), which can be trusted because it is recognized by both the parties involved in a transaction. It is very difficult to find or create a third-party organization (CA) that will be trusted by all parties in the open environment of the Internet, so a scheme has been established that allows the construction of a linked-trust model through CAs (**Fig. 3**). It is a model in which trust is established by following common guarantors (trust points). Because of the difficulty of creating and verifying these links, the web model (**Fig. 4**), which simplifies this processing, is applied when a Web browser is used. Within this scheme, a number of root CA certificates that have already cleared certain fixed reliability requirements are preinstalled in the browser. Then, if the Web server being accessed is certified by one of these root CAs, the site is considered trustworthy (if it is not certified by one of these CAs, the browser will display a warning message). Note that these trusted CAs are decided regardless of the intentions of end-users, so users must understand that they should not place excessive trust in them.

3. Effects of implementing PKI

The following direct results can be expected from implementing a PKI solution:

- The ability to verify the identity of the other party over the network.
- The ability to verify the authenticity of data (that it has not been falsified).

Despite these benefits, the rate of adoption is still quite low. Some of the reasons suggested for this include the operating costs and the difficulty in understanding the technology, quantifying the bene-

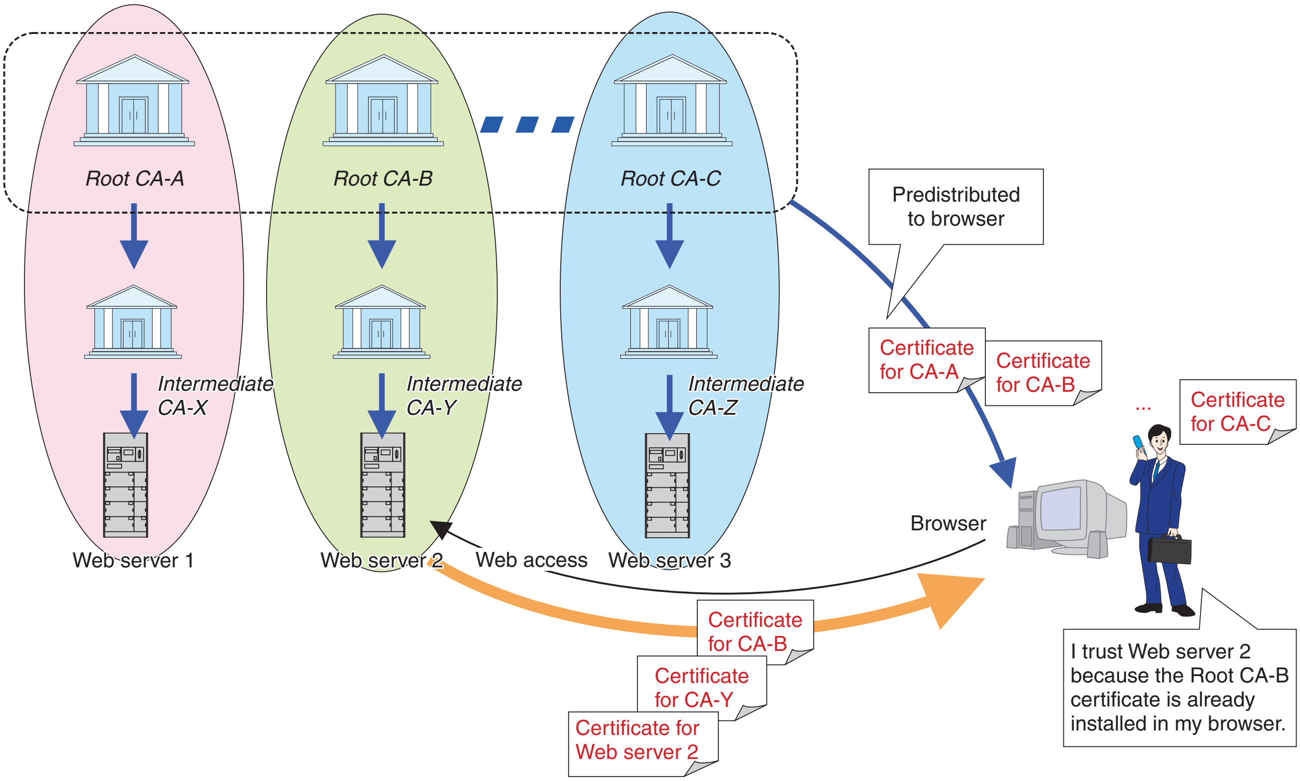

Fig. 4. Web trust model.

fits, and making the required investment decisions (it is difficult to motivate adoption of the technology) [2], [3].

However, from a different perspective, the following secondary benefits can also be achieved:

- The intentions of the party producing the information can be verified.
- The safety of the data can be guaranteed (falsification can be detected) over long periods after the fact.

With the former, responsibility for the content of messages or digital information on the network can be clearly established through signing, which addresses the need to assign social responsibility (for governments, financial institutions, industry, politicians, doctors, architects, etc.) or responsibility in trade or for making particular statements (auctions, social networking services, etc.). In addition to preventing unauthorized activity, PKI has the added benefit of clarifying responsibility in this way. In fact, some financial institutions have actually begun the practice of signing transmitted information (email messages).

The latter refers not only to demonstrating the authenticity of information at the time, but also to preventing falsification at any later date. The need for digital signing, and corresponding timestamp technology, is expected to increase as digitization progresses and the amount of digital data that must be safely maintained and stored over longer periods of time increases. The signing of documents and logs is one possible method of providing the evidence required to implement internal controls based on the Japanese version of SOX legislation*.

Finally, if the safety and security of services offered can be demonstrated by having each element in the network (users, servers, nodes, terminals, mobile phones, information appliances, etc.) certified, this should be a factor in attracting users to these services.

4. Areas of usage and application

Next, we discuss the areas of usage and application of this technology. Applications can be broadly

* SOX: The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox, is a US federal law enacted in response to a number of major corporate and accounting scandals such as those affecting Enron and World Com.

Table 1. Major systems and technologies using PKI.

Categories	Names	Overview and main applications
Communications	IPSec	IP-level data encryption
	EAP-TLS	Wireless local area network authentication protocol
	SSL	Encryption and authentication between Web browser and servers (mainly server authentication)
	S/MIME	Encryption and signing of email
Terminal management	Desktop security	Access control of user authentication/files
Document management	Authoring of applications	Signatures on text and tables
	Filing clerk system	Safe storage of documents etc. for a long time
Specialized technologies	Signing of program code	Certification of the authenticity of a program with the program's author.
	Timestamps	Certification of the existence of data at a given time and that it has not been falsified since that time.
	Grid computing	Authentication of personal computers participating in the grid
	DRM	Authentication of contents users
Administrative systems	e-bidding	Authentication of bidders, certification of documentation (e.g., use of a certificate from a recognized Certificate Authority)
	Electronic submissions	Authentication of submitters (e.g., use of an individual's public certificate for e-tax submission)
	Electronic contracts	Authentication and certification of contracts
	Electronic medical charts	Authentication of people writing on medical charts and protection against fabrication.

IPSec:	Internet protocol security
EAP-TTL:	extensible authentication protocol – time to live
SSL:	secure sockets layer
S/MIME:	secure multipurpose Internet mail extensions
DRM:	digital rights management

divided into two types. The first includes independently developed systems with PKI built in, and the second includes systems that make use of an existing protocol or product that already has PKI built in.

With the first approach, the applicability of PKI varies based on the purpose or placement of the application or system being developed. For many small-scale, closed systems, there is no need for PKI. Conversely, in the completely open world, where the chain of trust does not reach, there may be no point in using PKI. PKI is most easily applied to organizations where there is some form of loose community, or where multiple management units are linked. Examples include groups or organizations in business or industry or user groups for specific services. In Japan, public implementations like the Government Public Key Infrastructure (GPKI) are currently leading the way, but consideration of private-sector systems like the Healthcare PKI (HPKI) and the University PKI (UPKI) is progressing. There are also examples outside Japan where certificates are issued to all citizens of the country [4].

There are an increasing number of cases where PKI is used through communications methods and other tools without any particular awareness of it, as in the second approach (**Table 1**). A combination of these types of products makes possible independently designed and developed systems that make effective use of CAs or certificates.

5. PKI application model

Next, we discuss the architecture of systems incorporating PKI. As shown in **Fig. 5**, the general structure (whether in a client-server or a peer-to-peer model) can have a third-party facility that issues the digital certificates, in addition to the parties of the transaction (trusted-third party (TTP) model), or the service provider can also act as the issuer (two-party model) [4]. The main structural elements are the issuer, certificate holder, and verifier, but the CA associated with the issuer may also make use of other existing services or products. The holder and verifier may also swap roles when mutual authentication is required, for example. **Figure 6** shows some actual examples in Japan, with specially authorized CAs, vendors, and municipalities for electronic bidding, or server-certificate issuers, servers, and browser users

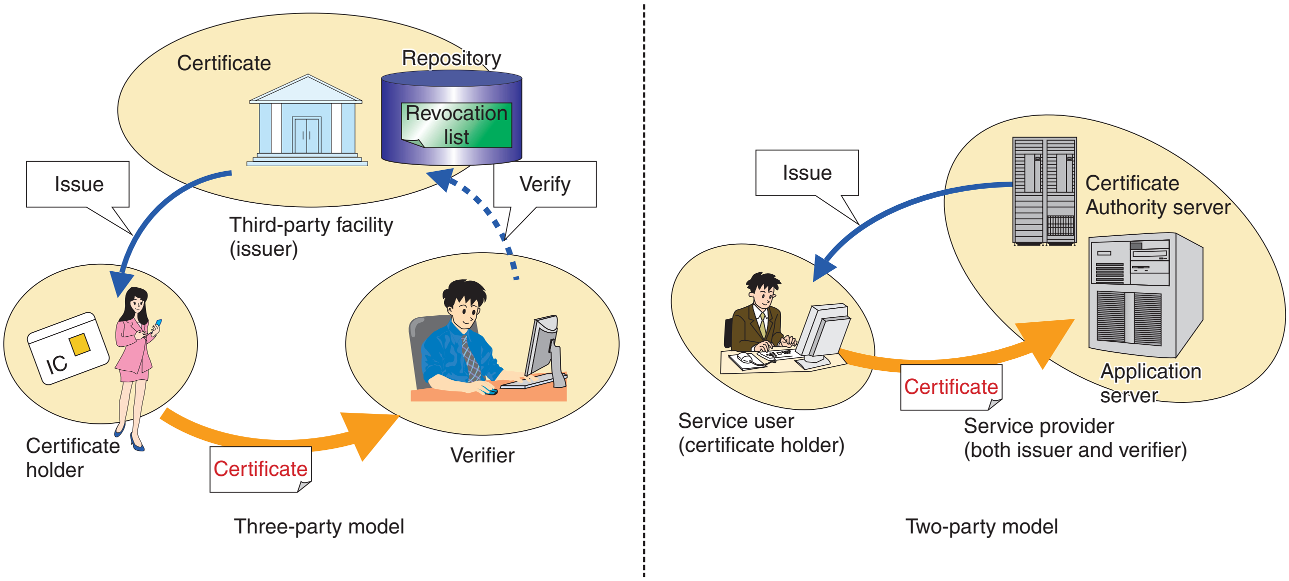

Fig. 5. PKI application model.

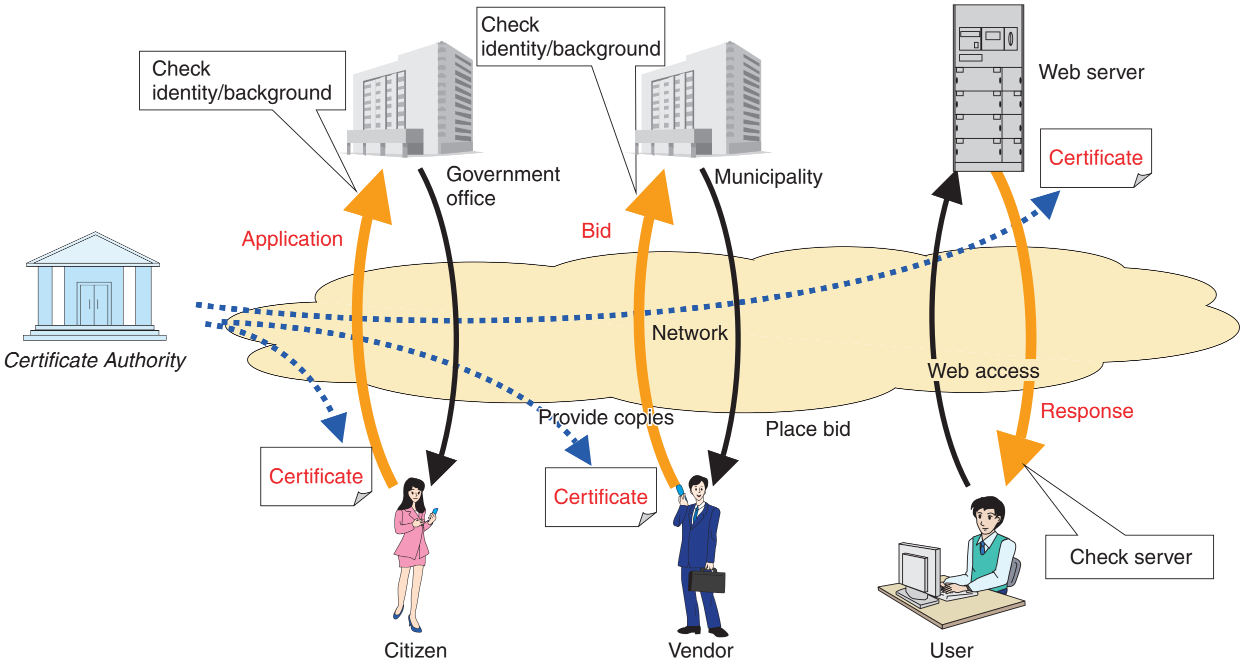

Fig. 6. Examples of certificate holders and verifiers.

for SSL (secure sockets layer) authentication when using the Web.

However, the demand for certificates is still small, and established businesses based on trusted-third-party models are limited to those mentioned above at this time. One of the reasons digital certificates are not more widely used is that in these structures, the holder of the certificate is not a beneficiary. The holder must submit the certificate or perform the signing in order to take the service, but the verifier receives all of the benefits, like protection against impersonation (unless there is a paradigm shift to where holding a certificate itself is thought to be a benefit). Accordingly, the introduction of digital certificates would likely proceed more smoothly if the cost were borne by the verifiers. Typical examples of

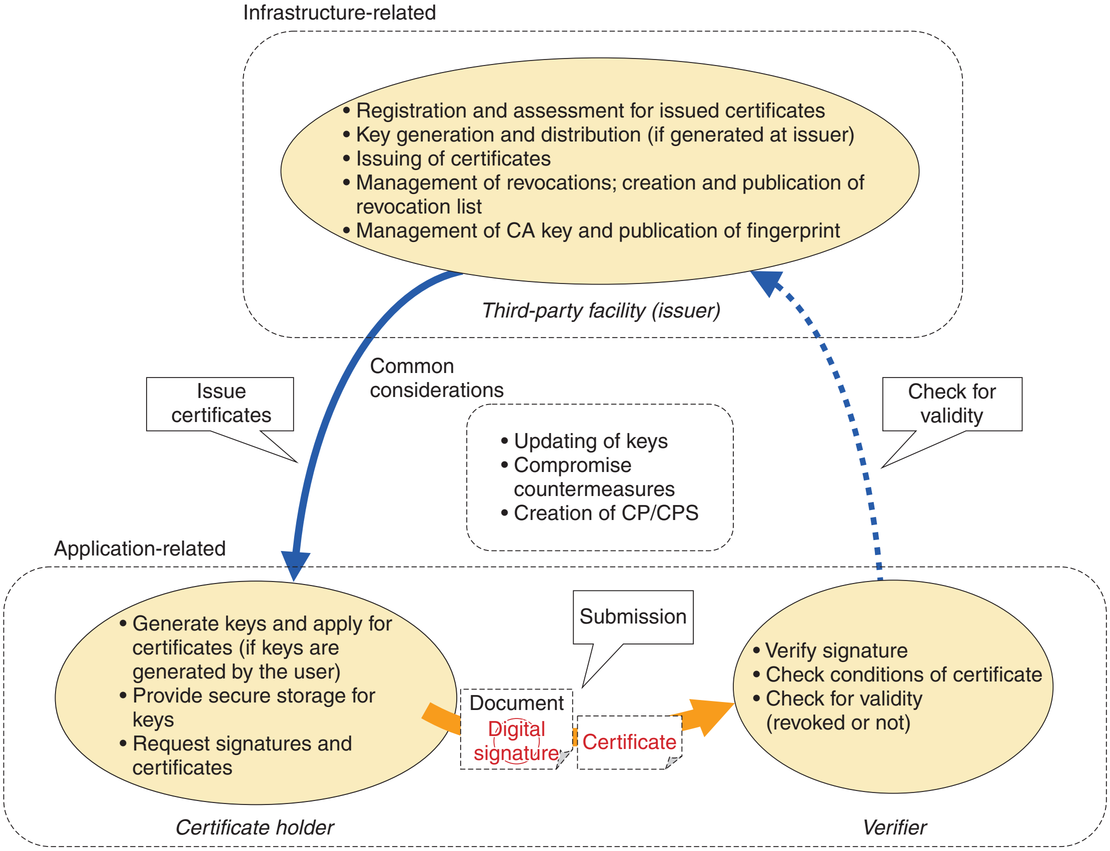
Infrastructure-related
• Registration and assessment for issued certificates
• Key generation and distribution (if generated at issuer)
• Issuing of certificates
• Management of revocations; creation and publication of revocation list
• Management of CA key and publication of fingerprint
Third-party facility (issuer)
Issue certificates
Common considerations
• Updating of keys
• Compromise countermeasures
• Creation of CP/CPS
Check for validity
Application-related
• Generate keys and apply for certificates (if keys are generated by the user)
• Provide secure storage for keys
• Request signatures and certificates
Submission
Document
Digital signature
Certificate
• Verify signature
• Check conditions of certificate
• Check for validity (revoked or not)
Certificate holder
Verifier

Fig. 7. Roles and considerations for PKI architectural elements.

this can be found in corporate or electronic procurement systems, where the service provider (corporation or procuring company) issues and distributes certificates to the service user (employee or vendor). This is the two-party model, where the verifier is also the issuer. Among these cases, the service user may also be asked to bear the burden of issuing the certificate if the service provider is in a stronger position than the user.

6. System design considerations

In this section, we discuss the roles and operating requirements of each structural element more specifically, along with important factors to consider when designing systems (**Fig. 7**).

The main roles of the issuer (infrastructure-related) are registration, assessment, and issuance of certificates and management of certificate revocations. In particular, registration and assessment are very important because trust will be based on the criteria used when issuing certificates (the strictness of the assessment must be decided based on the certificate's purpose). It is also important to reflect the current status of certificate holders promptly (e.g., status changes like hiring, firing, or position changes must be handled for employee certificates), so operational procedures for obtaining and updating this information must be established. This could be handled, for example, by the company's human resources department or by creating a link to the employee database.

Keys can be generated by the user and then registered with the CA, or generated by the issuer. The requirements for these two methods differ greatly. Ideally, holders should generate their own keys and then register only the public key without disclosing the private key to anyone. In some cases, though, the issuer generates the keys to reduce the burden on users. In these cases, it is very important to have a way to deliver the private keys to the holders safely and to ensure that the issuer does not retain them (although some issuers retain them for backup purposes). Root CAs are the final point of trust, guaranteed by no other party, so they often publish a fingerprint (a hash value) for the certificate that allows verifiers to check the validity of the certificate.

Management of revocations is related to the overall architecture, so it will be discussed later.

Certificate holders and verifiers depend on the type of application through which the service is used and provided, and the following must be considered when implementing a PKI system. A fundamental assumption of PKI is that the private key is held only by the holder, so tamper-proof storage methods (preventing unauthorized access) and safe delivery methods are very important. As described above, the safest approach is if the holder generates the key within a tamper-proof piece of equipment (like a smart card) and sends only the public key to the CA so the certificate can be issued (the private key never leaves the smart card). Requests for revocation must be issued immediately if the key is lost or stolen.

The verifier checks the validity of signatures and certificates, including the content of certificates (validity dates, policies, etc.). PKI includes the concept of invalidation, so the reliability of certificates is very much dependent on applying these validity checks promptly. The issuer must provide a way for holders to invalidate a certificate and must issue and publish (according to a pre-defined policy) a certificate revocation list (CRL) based on these requests. Verifiers must check that applicable certificates are not on the CRL. Since the CRL is published periodically, it must be understood that there will be a time-lag after an invalidation request until the corresponding CRL is published. More importantly, there is a gap from the event that prompted the invalidation request (e.g., theft of a private key) until the CRL is available to verifiers.

There are also several overall considerations. The keys and certificates used in the system can expire, and it is also possible that the encryption algorithm upon which the system is based could be compromised, so measures and procedures to update or change these components must be anticipated. This includes updating keys and certificates that have already been distributed, updating the keys for the CA itself, and handling existing signatures corresponding to these. As an example, long-term signature schemes have been devised for handling signed documents over long periods of time [5]. Finally, a CA must define the form of each type of certificate, depending on what it certifies, as well as operational regulations that each structural element of the PKI must keep (certificate policy and certification practices statement (CP/CPS)).

7. Future development

Regarding the problems of high operating costs for PKI, much attention has been given to optimizing the assessment process, which accounts for the majority of the cost of issuing certificates. Examples include distributing the assessment costs over the user management organization, or automating the assessment by linking to a user database. Moreover, in cases where a new system is being built, user administration (ID administration) and PKI can be linked by using an IC card for storage and distribution, together with a single-sign-on (SSO) procedure. This provides both the reliable authentication of PKI and the convenience of SSO.

The Trust-CANP certification system [6] from NTT is making advances in multiple-encryption support to guard against compromise, as well as a distributed Registration Authority (RA) function and strengthened links to user systems and IC card systems. Our objective is to provide authentication systems that can form the base for building safe and secure services over networks, whether fixed or wireless, and are even easier to use.

References

[1] C. Adams and S. Lloyd, “Understanding PKI,” Addison-Wesley, 2002.

[2] M. Sakurai and T. Kimura, “Electronic Authentication, Its Past and Present,” Journal of Information Processing Society of Japan, Vol. 46, No. 7, 2005 (in Japanese).

[3] Y. Maeda, M. Saeki, M Chiba, Y. Matsumoto, H. Takatsuka, H. Izumoto, N. Enomoto, K. Nagashima, M. Ito, S. Iwai, H. Masamoto, N. Maki, T. Sakagami, and T. Sawada, “Report on a Survey toward Wider Use of Digital Signatures,” Next Generation Electronic Commerce Promotion Council of Japan, Mar. 2006 (in Japanese).

[4] Y. Maeda, Y. Matsumoto, N. Enomoto, H. Masamoto, H. Takatsuka, N. Kobayashi, and K. Nakamura, “Report on a Survey toward Wider Use of Digital Signatures (2),” Next Generation Electronic Commerce Promotion Council of Japan, Mar. 2007 (in Japanese).

[5] M. Kimura, Y. Maeda, and K. Miyazaki, “Electronic document storage: structures and operation,” Chuo Keizai Inc., Dec. 2005 (in Japanese).

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

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.

Yoshihiro Yoshida

Chief, Innovative Financial Systems Department, NTT Communications.

He received the B.E. degree in industrial management engineering from Osaka Prefecture University, Osaka, in 1991. He joined NTT Information and Communication Systems Laboratories in 1991. He has been engaged in R&D of information and communication platforms, security platforms, and so on. He was transferred to NTT Communications in December 2007.

Shoichi Hashimoto

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

He received the B.E. and M.E. degrees in electrical engineering from Keio University, Kanagawa, in 1993 and 1995, respectively. He joined NTT Information and Communication Systems Laboratories in 1995. He has mainly been engaged in R&D of a security platform based on PKI.

Rie Otsubo

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

She received the B.E. degree in electrical engineering and M.E. degree in information engineering from Kagoshima University, Kagoshima, in 1993 and 1995, respectively. She joined NTT Information and Communication Systems Laboratories in 1995. She has been engaged in R&D of information and communication platforms, security platforms, and so on.

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.