Electronic Certification Systems for More Secure Ciphers

Yoshihiro Yoshida† *and Hiroshi Masamoto*

Abstract

NTT Information Sharing Platform Laboratories is working on electronic certification systems that use cipher technology to provide a platform for safe and secure information sharing. In this article, we describe the effects of the recent problem of the increasing vulnerability of cipher algorithms and an approach for dealing with it.

1. Electronic certification systems that supports safe and secure information sharing

Safe and secure information sharing in a network society requires data encryption and digital signatures, which employ cipher technology. Digital signatures are based on a method known as public key encryption, a cryptosystem in which the original text is encrypted with one key of a pair of keys and can be decrypted only with the other key. The key used to encrypt the text is kept private, while the related key used to decrypt the text is public. Thus, this system enables anyone to be certain that the decrypted text could only have been created by the owner of the corresponding private key. This method makes it possible to authenticate not only the creator but also documents signed (encrypted) by the creator by confirming the personal identity of the signer. This scheme requires a third-party organization to issue certificates, including one that certifies the owner of the public key and the owner's identification information. The mechanism and the rules for using it are called the public key infrastructure (PKI) (**Fig. 1**).

An electronic notarization authority can conveniently serve as a third-party organization that maintains digitally signed data as evidence to prove that an electronic document or other such data exists or that data has been transferred. A time stamp authority, which issues time stamps, can verify the time of transfer.

NTT Information Sharing Platform Laboratories offers the Trust-CANP (certification authority for network policy) electronic certification system, the Trust-CYNOS (cyber notary system) electronic notarization system, and the Trust-STL (secure time long-term effectiveness) time stamp system as products for constructing an electronic certification platform. Their functions are based on cipher technology and they must always be able to accommodate newer, more secure cipher algorithms and switch over to using them.

2. Cipher technology used in the electronic certification systems

2.1 Trust-CANP electronic certification system

This is an electronic certification system that affixes its own signature to a public key certificate to prove the relationship between the public key and its owner (and the corresponding private key of the key pair). The Trust-CANP electronic certification system generates key pairs, registers public keys, and issues public key certificates, which are the basic functions of an electronic certification system (**Fig. 2**). It is used by administrative systems and so on.

2.2 Trust-CYNOS electronic notarization system

This is an electronic notarization authority that uses digital signature technology to prove relationships and to prevent after-the-fact repudiation. The Trust-CYNOS electronic notarization system can verify the fact of document delivery by verifying that a docu-

† NTT Information Sharing Platform Laboratories
Yokosuka-shi, 239-0847 Japan
E-mail: yoshida@isl.ntt.co.jp

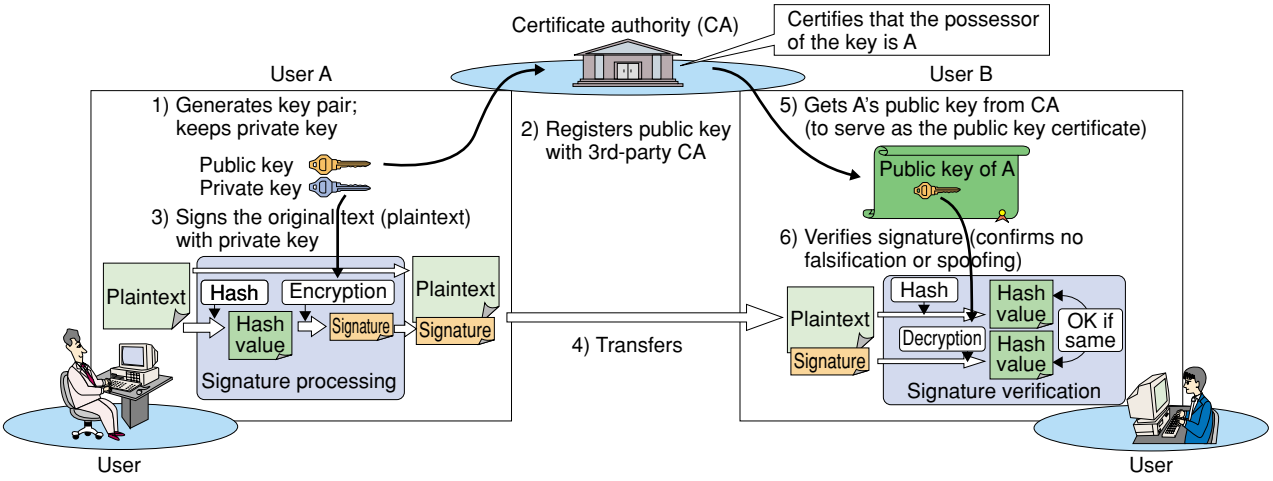

Fig. 1. Digital signature and PKI.

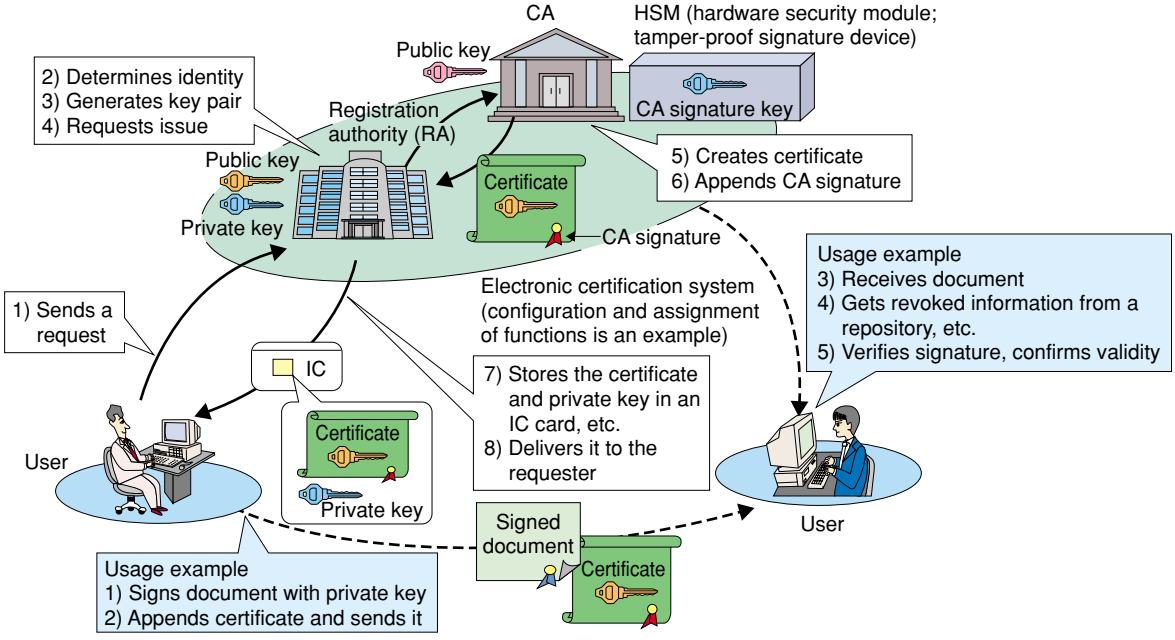

Fig. 2. Electronic certification system and usage example.

ment has been signed and signing it with information about the sender and receiver (**Fig. 3**). Common key encryption is used for communication between servers and clients. It is used in electronic bidding systems and electronic application systems.

2.3 Trust-STL time stamp system

A time stamp authority uses time stamps to guarantee the existence of data at a certain time and its subsequent integrity. The time stamp authority signs the union of a hash value of the user data and accurate time information obtained from a time authority. The Trust-STL time stamp system also uses hash technology to centralize management of the history of the issued time stamps, thus guaranteeing the validity of the time stamp over a long period of time (**Fig. 4**).

3. Effects of cipher compromise on electronic certification systems and countermeasures against them

Some possible compromises of hash functions,

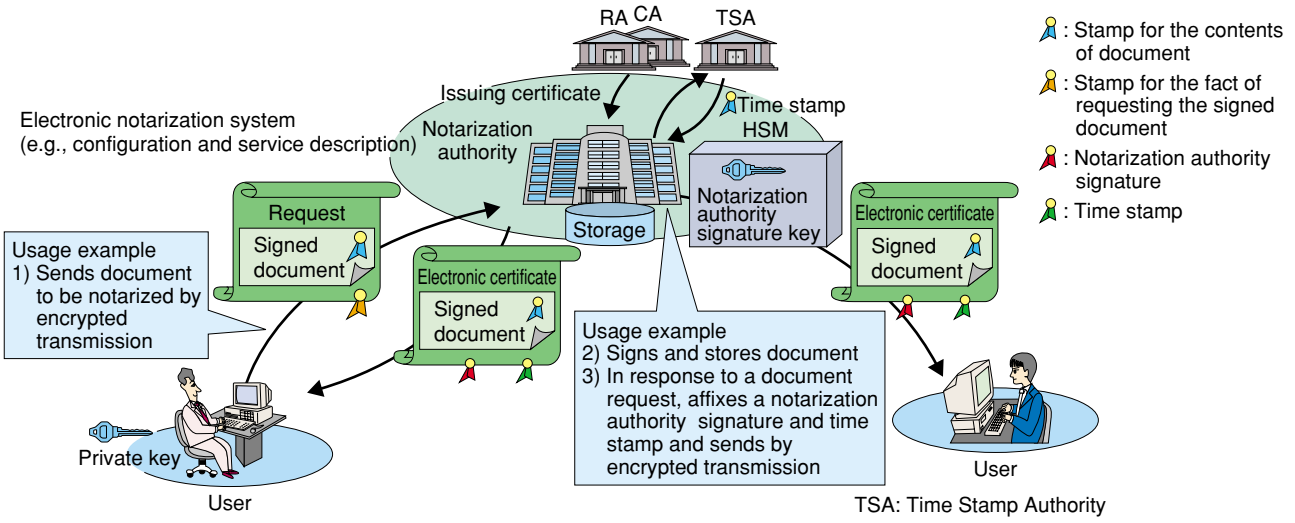

Fig. 3. Electronic notarization system and usage example.

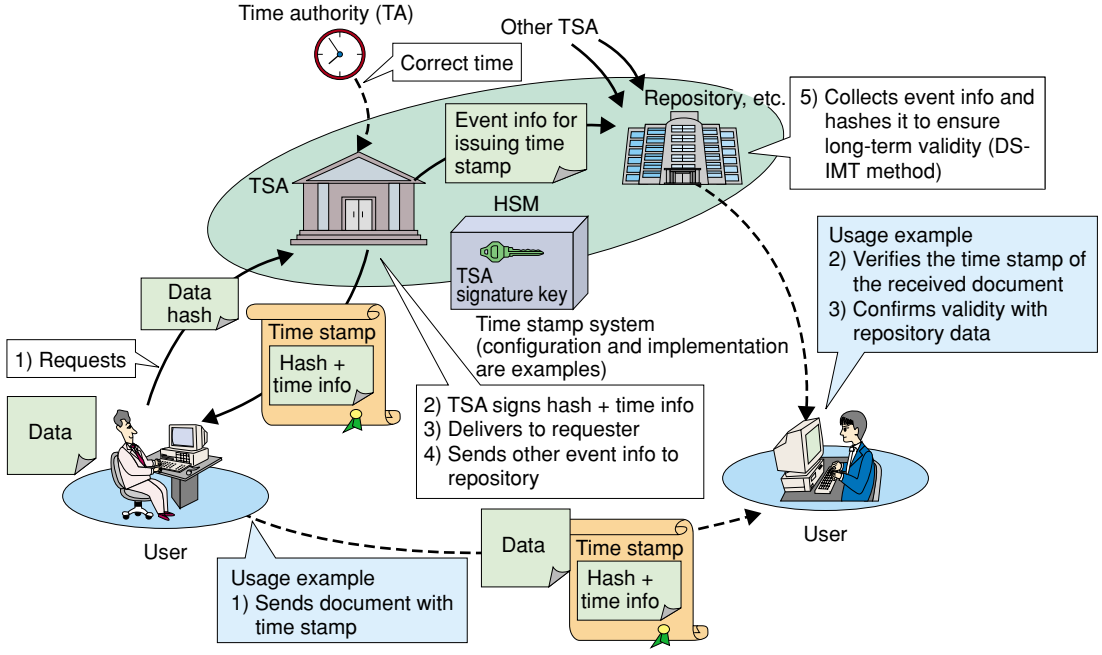

Fig. 4. Time stamp system and usage example.

public key encryption and digital signatures, and common key encryption have been identified. The National Institute of Standards and Technology (NIST) of the USA has specifically pointed out compromises in the functions listed below.

- Hash function
  SHA-1
- Public key encryption and digital signatures
  Encryption and signature functions that use RSA encryption with 1024 bits or fewer
  Signature functions that use the SHA-1 hash algorithm
- Common-key cryptosystem
  Two-key Triple DES

Compromises of these cipher algorithms have led to planned recommendations for the discontinuation

of their use in U.S. government systems and related systems by 2010. For the use of digital signatures in particular, the recommendation will be to halt the use of new signatures by 2008. Since these functions are essential technology for electronic certification systems and are used extensively in the NTT products mentioned above, any compromises would have serious effects, as listed below.

1) When data is encrypted for transmission or when encryption is used for authentication, eavesdropping or spoofing could occur.
2) The trustworthiness of the public key certificates, time stamps, and signed data to be created in future with those functions would be lost.
3) The trustworthiness of public key certificates, time stamps, and signed data already created in the past would be lost.

A digital signature is supposed to guarantee the trustworthiness of data for a certain period of time after it has been affixed. However, if the reliability of the signature (i.e., the algorithm used for the signature) is lost at a given time, previous signatures can no longer be trusted and the integrity of the data cannot be determined. Furthermore, operation logs or other important information can no longer be trusted, even if the data has been signed and stored to guarantee against falsification, because the trustworthiness as signed data is lost.

To deal with these effects, the measures listed in **Table 1** were implemented in NTT electronic certification systems. Basically, they involve the following policies.

- Change the parts that use compromised functions and use secure algorithms
- Support traditional functions only as far as necessary for compatibility and interconnectivity

However, in PKI technology, there are standard agreements and *de facto* standard agreements including old algorithms. Furthermore, electronic certification systems include commercially available peripheral devices and software, but some hardware security modules and peripheral devices such as IC (integrated circuit) cards are currently not compatible with the new algorithms. Eliminating these kinds of problems and dealing with the issue of compromisability at an early stage allows an overall response to be made immediately upon achieving compatibility with standards agreements and the products of other companies. Policies for coping with this problem are listed for each type of cipher technology in **Table 2**.

Table 1. Countermeasures against compromising of electronic certification systems.

	Main product being used	Now	After countermeasure
Hash	Trust-STL	SHA-1 or MD5 ☆80-bit security or less	SHA-256/512 ☆128-bit security or higher
Signature	Trust-CANP Trust-CYNOS Trust-STL	SHA-1 with RSASSA-PKCS1-v1.5 (max: 2048 bits) ☆Maximum: 112-bit security	SHA-256 with RSASSA-PKCS1-v1.5 (max: 3072 bits or more) ☆Maximum: 128-bit security or higher
Common key	Trust-CYNOS	Camellia/AES DES/3DES/FEAL ☆Used for 112-bit security or less	Camellia/AES ☆128-bit security

Table 2. Problems in addressing compromises and policies for countering them.

	Main problem	Countermeasures
Hash	RFC and PKCS regulations are SHA-1 and MD5, so interoperability is lost when this is changed.	Accept the NIST recommendations on security and make preparations in advance for applying secure algorithms to prepare for immediate conformance when RFC and PKCS regulations are changed and compatibility with the products of other companies is achieved.
Signature	IC cards, JCE, CryptoAPI, and other libraries of other companies are not supported, so programs that use them cannot be created.	
Common key	RFC or PKCS regulations are DES and Triple DES, so interoperability is lost when this is changed.	

4. Example transition schedule for a system that uses the electronic certification system

There is no problem in the use of encryption or the use of encryption for authentication if the encryption is secure at the time of use. However, before a digital signature becomes untrustworthy as described above, it must be changed over to a secure one. That is to say, a transition schedule must be planned with consideration given to the period of validity of the public key certificates corresponding to the private key with which the data was signed.

The transition for public key certificates involves the application of one or more of the following measures with respect to the old algorithms (**Fig. 5**).

1) Revoke certificates when the time for discontinuation of use arrives.
2) Shorten the period of certificate validity and issue only certificates that are valid up to but not after the discontinuation time.
3) Leave the validity period unchanged, but stop issuing certificates prior to the discontinuation time.

When signatures are used for digital signatures, there is a period after a signature has been generated during which it is necessary to verify its validity. However, it is important to note that revocation disables the signature validation function as well as the signature generation function. The first and second measures in the above list involve onerous changes in operation.

In practice, the transition plan will be decided with consideration given to the system specifications, the purpose for which the cipher method is used, the ease of changing the certificate's validity period, the procedure for updating certificates for users before and after the transition, relevant laws and regulations, and the conditions of connected systems. In any case, though, if the electronic certification systems are not dealt with first, they cannot be used by the higher-level systems. We are therefore giving precedence to the foundation systems in developing countermeasures.

For systems that are actually in operation, halting operation or making the transition for all of the data at once at the time of transition would be very difficult. NTT's electronic certification systems have long featured support for simultaneous use of multiple algorithms, which enables a smooth transition.

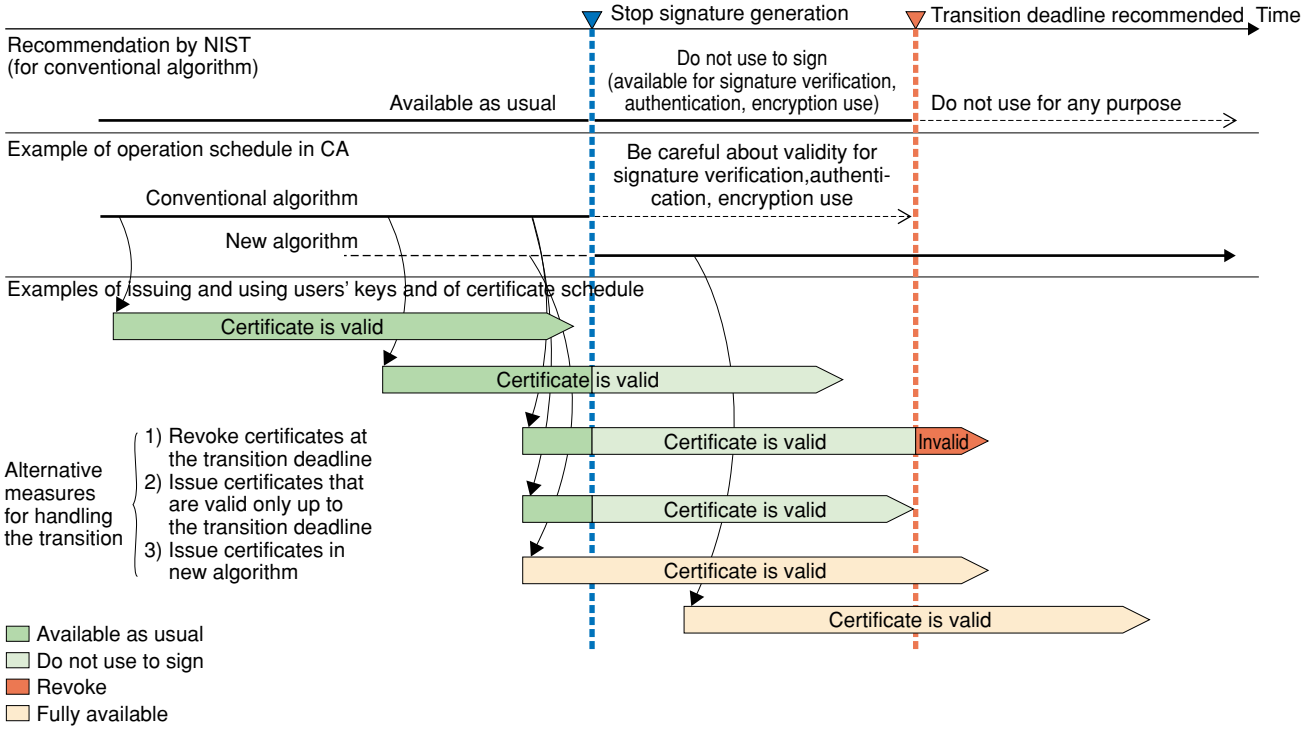

Fig. 5. Examples of possible certificate validity schemes for certificates issued before and after the transition.

5. Future developments

In addition to providing the results of current development as planned, we are dealing with the issues of compatibility with agreements and the products of other companies. We will also deal with fundamental products that are not included here (attribute certification systems, etc.) in accordance with standardization and other industry trends.

Yoshihiro Yoshida
Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He received the B.E. degree in industrial management engineering from Osaka Prefecture University, Osaka in 1991. He joined the Information and Communication Systems Laboratories, NTT, Kanagawa in 1991. 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 the Yokosuka Electrical Communication Laboratories, Nippon Telegraph and Telephone Public Corporation (now NTT), Kanagawa in 1983. He has been engaged in R&D of data communication protocols, information and communication platforms, security platforms, and so on.