

# EVERSIGN: Preserving the Long-Term Authenticity of Electronic Records

Authors: Kazuya Miyazaki\* and Manabu Tanaka\*\*

## 1. Introduction

Abiding by the e-Document Law and J-SOX Law (Japanese SOX law: Financial Products Dealings Act of 2006) requires that the authenticity of electronic records can be maintained for an extended period of time. In order to meet this requirement, a technology for securing the long-term validity of digital signatures is necessary. The EVERSIGN system mechanically constructs data complying with the long-term signature format, which is a standard format for this purpose, according to a predetermined schedule.

## 2. Mechanism of Signature Validity Extension

A digital signature is used to secure the authenticity of an electronic record. A digital signature refers to an electronic signature based on Public Key Infrastructure (PKI), and bases its trust on a public key certificate issued by the certification authority. The public key certificate contains mechanisms for the validity period and revocation, and the validity of the digital signature depends on the validity period and revocation of the public key certificate (Fig. 1). In other words, if the public key certificate exceeds the validity period or is revoked, the validity of the digital signature is also lost.

This is because a signature could be forged due to leakage of the signature key or vulnerability of algorithms if the public key certificate were allowed to exceed the validity period. This is also true of revocation because a signature could be forged using the leaked key.

A digital signature can contain time information, which is usually based on the system clock of the personal computer used to generate the digital signature. Since this time can be freely changed by the personal computer manager, it cannot generally be considered to be a reliable time. Thus, when a signature is re-verified, it is impossible to distinguish whether it is an authentic signature created within the validity period or a forged signature created after the validity period. If revocation takes place, it is also impossible to distinguish whether it is a signature before or after revocation. In addition, since even revocation information is not issued after the validity period, it will be impossible to confirm even whether or not revocation takes place.

Therefore, since the validity of a digital signature is usually lost in about one to three years, it is impossible to retain healthcare records for five years, tax documents for seven years and other documents that must be retained for 30 years or longer while maintaining their authenticity.

Signature validity extension is a technology that overcomes the validity period and revocation of public key certificates and vulnerability of cryptographic technology used for digital signatures in order to maintain the long-term validity of digital signatures. The requirements<sup>(1)</sup> for signature validity extension are shown below (Fig. 2).

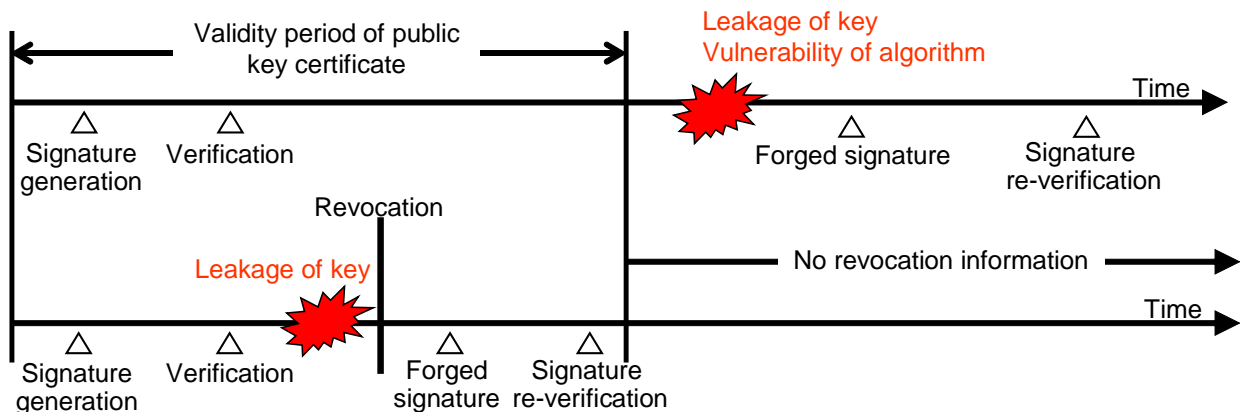


Fig. 1 Limit of digital signature

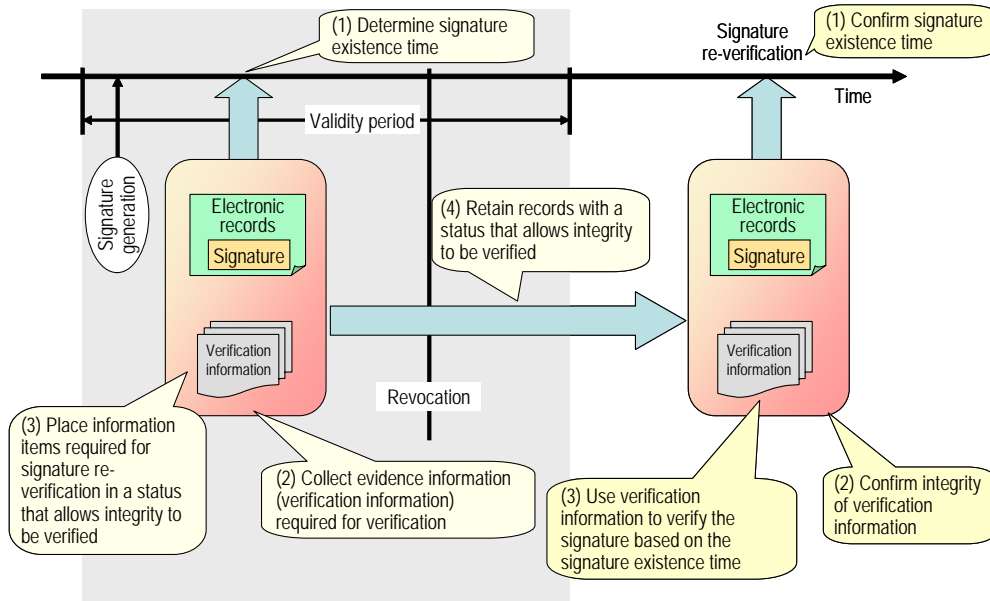


Fig. 2 Requirements for signature validity extension

Requirement (1): Determine digital signature existence time: Assign a reliable time to a digital signature to enable confirmation of the relationship between the digital signature and its validity period and revocation.

Requirement (2): Collect evidence information (verification information) required for verification of a digital signature: Collect revocation information items such as the sets of public key certificates from the signer to the route certification authority and CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol)<sup>(2)</sup> responses for those public key certificates.

Requirement (3): Place information items required for digital signature re-verification in a status that allows integrity to be verified: Place the original electronic records and verification information in a status that allows integrity to be verified.

Requirement (4): Retain records with a status that allows integrity to be verified as indicated in (3) above: Maintain the status in which integrity of records can be verified as indicated in (3) over the required retention period.

If requirements (1) to (4) are satisfied, then the following confirmation steps (1) to (3) can be used to distinguish whether the original signature is true or

false:

Confirmation (1): Confirm the signature existence time.

Confirmation (2): Confirm that electronic records attached their signatures and verification information have not been tampered with.

Confirmation (3): Use verification information to perform verification based on the signature existence time.

### 3. Long-term Signature Format

One way of satisfying the requirements described in the previous chapter is to use the long-term signature format (Fig. 3). The long-term signature format is a global standard as RFC3126<sup>(3)</sup>, etc. This method satisfies the requirements as follows:

Requirement (1): Assign a standard time stamp to a signature value (ES-T signature time-stamp).

Requirement (2): Store verification information items such as the set of public key certificates and CRL and OCSP responses (ES-C and ES-X verification information references and verification information).

Requirement (3): Assign a time stamp to electronic records with signature (ES), signature time stamp, verification information reference, and the entire verifi-

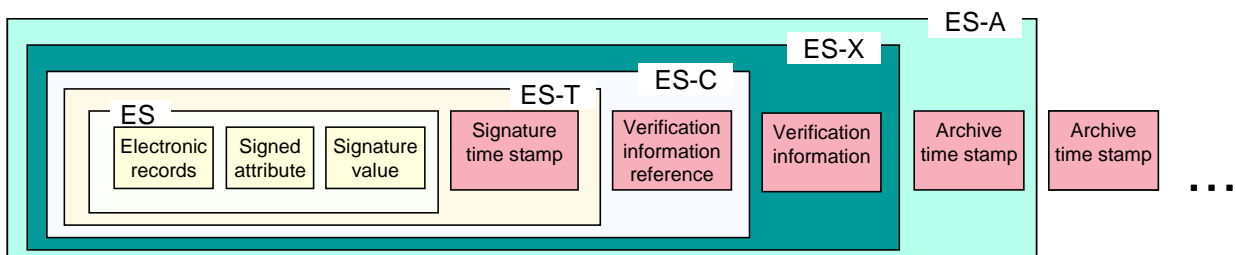


Fig. 3 Long-term signature format

cation information (ES-A archive time stamp).

Requirement (4): Overlap a time stamp on the entirety in order to maintain long-term tamper-resistance (outside archive time stamp).

The method that uses the long-term signature format with a time stamp to meet requirements (3) and (4) has the following features that make it superior to the method that assumes the safety of the system and operation to obtain the same effect (e.g., electronic original management system):

- (1) Standard PKI technology allows anyone to verify the validity.
- (2) Processing to construct and extend a long-term signature can be performed by anyone and can be taken over by others in the middle of processing.
- (3) Trust is based on only the trust point in standard PKI without needing to consider the safety of the system and operation, which are currently difficult to confirm.
- (4) Since time stamp services are always provided using the cryptographic technology whose safety has been confirmed at the relevant point of time, obsolescence of the technology is not a concern.

#### 4. Signature Validity Extension System MistyGuard "EVERSIGN"

Constructing the long-term signature format requires that the signature time stamp, verification information including revocation information and archive time stamp be collected at their respective appropriate timings and be appropriately stored in the long-term signature format. Management of the timings is extremely complex, and so cannot be left to individual users.

When the constructed long-term signature is to be verified, it is also necessary to verify the original signature, signature time stamp, verification information, archive time stamp, etc. respectively after assuming the fixed time (e.g., time indicated by each time stamp) and to determine whether the signature is true or false after confirming the consistency between the time indicated by the time stamp and validity period and revocation information.

The Mitsubishi signature validity extension system MistyGuard "EVERSIGN" is a server-type system that automatically constructs the long-term signature format by only registering a document with signature according to a fixed protocol. Such operation is achieved by the EVERSIGN server that contains a scheduler to automatically execute processing based on the settings regarding various timings and where various data items on time stamp services, etc. are collected. The constructed long-term signature data can also be collected by the user according to the fixed protocol.

A report on the results of long-term signature veri-

fication can also be obtained by using the verification protocol to issue the request to the EVERSIGN server.

The EVERSIGN client library can be used to incorporate the exchange of requests and responses with the EVERSIGN server in various applications. Normally, the structure is such that the long-term retention function is expanded by interfacing with various document management systems and record management systems instead of using EVERSIGN on a standalone basis.

#### 5. Long-term Signature Format Interoperability Test

From October to December 2005, the long-term signature format interoperability test was performed by ECOM<sup>(4)</sup>. This test aims to confirm the conformance to the "long-term signature profile" established by ECOM and the interoperability between products of companies. This profile was established to minimize the redundancy and ambiguity of the standard long-term signature format. By complying with this profile, it is possible to construct and verify a long-term signature with the objective of long-term retention.

A total of 13 companies participated in the test with their products or prototypes including the prototype from Mitsubishi Electric Information Technology R&D Center and the product EVERSIGN from Mitsubishi Electric Information Systems.

The following two types of tests were performed:

- (1) Offline validation test: Conduct tests on the prepared sets of ES format data (ES-T, ES-X Long, ES-A), verification information and setting information to verify the validity using the actual products of the companies.
- (2) Online matrix generation and validation test: Confirm whether long-term signature test data generated by the actual products of the companies can be read normally and verified correctly by the actual products of other companies.

The actual products of the companies including two Mitsubishi Electric-related actual products passed the test and were confirmed to comply with the long-term signature profile established by ECOM.

#### 6. Application Example

EVERSIGN has been incorporated and used in the electronic record management system of a certain social infrastructure system company since May 2006. This system provides a retention management function for the workflow and electronic records and computerized documents to make electronic contracts between the company that has installed the system and the company that conducts transactions with it. EVERSIGN has functions for generating the long-term signature format, extending the validity and verifying the validity

of the electronically signed contracts and other transaction records between the companies conducting transactions from the document storage server at the heart of the system. To comply with the revised Electronic Ledger Preservation Law of the e-Document Law, this system uses the certificate of specified certification operation and the PFU time stamp service certified by the Nippon Information Communications Association. As of June 2006, which was immediately after operation started when the number of initial companies using the system was limited, the system was used about 3,000 times per month on the basis of registered documents. However, the number of companies using the system will increase in future and the scope of application of the system is expected to expand significantly.

From this fall, the system will also be used for a nationwide electronic contract document retention service provided by a financial institution. Both the number of companies using this system and the number of documents handled are expected to exceed those for the system that is currently in use. The system has the same basic configuration as that mentioned earlier, but will be provided as an ASP (Application Service Provider) service that can be used among multiple companies. The OCSP-based revocation verification system will be used as the mechanism of public key certificate verification.

## 7. Conclusion

In future, enforcement of J-SOX Law (Japanese SOX law: Financial Products Dealings Act of 2006) will raise the importance of securing the authenticity and adequacy of documents and records and their retention. Mitsubishi Electric technology and products are expected to make a significant contribution.

## References

- (1) Kazuya Miyazaki et al.: Mechanism and Practice of Electronic Record Retention, CHUOKEI-ZAI-SHA (2005)
- (2) RFC2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP (1999)
- (3) RFC3126: Electronic Signature Formats for Long-term Electronic Signatures (2001)
- (4) Next-Generation Electronic Commerce Promotion Council of Japan: Long-term Signature Format Interoperability Test Report (2006)