

Our Efforts in PKI Technologies

Authors: Satoshi Takeda*, Tadakazu Yamanaka* and Hideyuki Miyohara**

1. Introduction

A digital signature is an effective means of authenticating the identity of an electronic document's author or preventing the illegal alteration of an electronic document. The digital signature can be verified through a digital certificate, which is valid for a maximum period of five years, as defined by the law. However, many electronic documents must be stored for longer than 5 years, as in the case of receipts and financial statements that have a legally required retention period of 7 years. As a consequence, an issue arises when the 5-year validity period for a digital certificate has expired, and the digital signature cannot be verified.

Long-term signature technology ensures the validity of a digital signature even after the certificate's period of validity. This technology is standardized by the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI). The Next Generation Electronic Commerce Promotion Council of Japan (ECOM) proposed the standardization of long-term signature formats under the Japanese Industrial Standards (JIS), and it was officially announced as a JIS standard in March 2008. ECOM formulated a long-term signature profile and conducted interoperability tests based on the formulated profile and involving multiple vendors. Meanwhile, the Japanese Association of Healthcare Information Systems Industry (JAHIS) is developing a guideline and working on the standardization of electronic archiving and digital signatures for healthcare documents to ensure the interoperability of healthcare information systems.

Mitsubishi Electric has been participating in the ECOM and JAHIS committees and is actively involved in the formulation of a long-term signature profile and interoperability tests. This paper presents the details and development status of some of Mitsubishi Electric's efforts in Public Key Infrastructure (PKI) technologies,

including standardization activities at ECOM and JAHIS.

2. Trend of Standardization

2.1 Long-term signature format

Digital signature technology allows authentication of a signer's document, where a digital signature is generated using a digital certificate and corresponding private key issued by the user's trusted Certificate Authority (CA), and verification is performed using the digital certificate and public key. The digital signature can be verified by confirming that it is within the valid period of the digital certificate and has not been invalidated. To ensure the validity of a digital signature, it is necessary to prove that it existed when the signer's document was created. The creation time of a digital signature can be set as one of the attributes of the signature. However, the time set will be the time information provided by the equipment that generates the electronic signature, which may create a reliability issue. It is also necessary to be able to check the validity of the signature even after the certificate expires or is invalidated. To deal with these issues, the following requirements must be satisfied:

- Identify the time when the signature was applied.
- Identify the evidence information required for re-verification.
- Enable the detection of illegal alteration of electronically signed document and information required for re-verification.
- Retain electronically signed document and information required for re-verification, with the detection of illegal alteration enabled.

The long-term signature format satisfies the above requirements, and ensures the validity of a digital signature "even after the digital certificate has expired, or even if the old encryption algorithm has been compro-

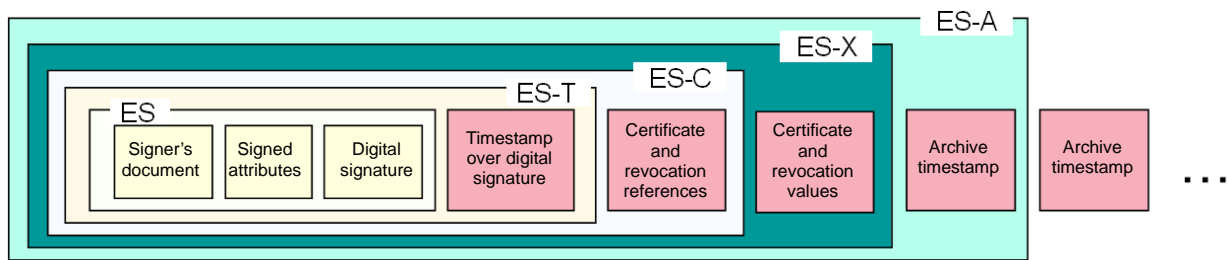


Fig. 1 Long-term signature format

mised." As shown in Fig. 1, in addition to the signer's document and digital signature (ES), the long-term signature format data includes a timestamp over the digital signature that indicates the signing time (ES-T), certificate and revocation references for the digital certificate and revocation information (ES-C), certificate and revocation values used as verification information for the digital signature and the timestamp over the digital signature (ES-X), and an archive timestamp (ES-A). The timestamp data proves "when" the signer's document was signed; and the issuing agency in Japan secures the reliability of timestamps using the certification system. As long as an archive timestamp is affixed using an uncompromised encryption algorithm, the validity period of the digital signature can be extended. The authenticity of the data can be proven for a long term by verifying the consistency of the digital signature, timestamp over the digital signature, and digital certificate and revocation data included in the long-term signature format.

The long-term signature uses the advanced format of either Cryptographic Message Syntax (CMS) or Extensible Markup Language (XML), referred to as CAdES (CMS Advanced Electronic Signatures) or XAdES (XML Advanced Electronic Signatures), respectively, and published as standards RFC 5126^[1], ETSI TS 101 733^[2], and ETSI TS 101 903^[3].

2.2 JIS Standards for long-term signature profile

ECOM has been working on standardizing the profile for the long-term signature format as described in the previous section. During their activities, ECOM exchanged information and opinions with ETSI to establish consistency between the profiles developed by ECOM and the profiles specified by ETSI, and then developed JIS drafts for the long-term signature profiles, which were eventually published as JIS X 5092^[4] and JIS X 5093^[5].

2.3 Activities by JAHIS

JAHIS is working to promote standardization in the field of healthcare systems, including the standardization of electronic archiving and digital signatures to ensure the interoperability of healthcare information systems.

In the guideline developed by JAHIS, the digital certificate for Healthcare PKI (HPKI), developed by the Ministry of Health, Labour and Welfare, is recommended as the digital certificate to be used for digital signatures on electronically archived medical records. According to the policy for the HPKI certificate, since the qualification data is described in the digital certificate, the hcRole attribute can be used as an extended certificate field. An important feature of this certificate is that the person who is verifying the certificate can use

hcRole to determine if the signer is a licensed medical doctor or a management representative of a medical institution, such as a hospital director.

With regard to the validity of a certificate, in order to indicate that the digital signature was valid at the time that it was timestamped, it is specified that the authenticity of the information required to verify the certificate, such as the certificate and revocation values on a certificate 'pass' (CRL/ARL), must be maintained during the certificate retention period; and the recommended format to be used is the long-term signature format specified in the previously mentioned JIS standards. It is also specified that the signer prepares the ES-A format for documents to be personally retained, and the ES-T format for documents to be externally submitted.

3. Our Efforts

3.1 Interoperability tests according to the JIS draft for ECOM long-term signature profile

From 2006 to 2007, ECOM conducted "Interoperability tests according to the JIS draft for long-term signature profiles." Eighteen companies including Mitsubishi Electric participated in the tests, in cooperation with three companies that offer the service of issuing timestamps. The interoperability tests consist of the following two kinds of tests:

(1) Off-line test to verify long-term signature format

ECOM prepared the long-term signature data, verification data, and set-up data conforming to the JIS draft for long-term signature profiles. Products or prototypes of participating companies performed off-line verification of the validity of the long-term signature data. The verification results were checked to determine if they matched ECOM's assumptions.

(2) Product matrix interoperability test

Data prepared by the products (prototypes) of participating companies was verified using other companies' products, and the implementation of data generation functions and verification functions was checked to determine if they were in conformance with the JIS draft for long-term signature profiles. ECOM prepared the verification data and set-up data, and timestamps were provided using the timestamp agencies of the three cooperating companies.

Mitsubishi Electric participated in the interoperability tests to confirm that both of our proprietary CAdES and XAdES libraries were in conformance with the JIS draft for long-term signature profiles. As the first step in the test, conformity of the long-term signature format data prepared by other companies was checked using Mitsubishi's libraries. In parallel, we also prepared long-term signature format data, and confirmed that our

data was properly verified using the other companies' verification mechanisms. With these results, both our CAdES and XAdES libraries were confirmed to be in conformance with the JIS draft for long-term signature profiles.

3.2 Office add-on: long-term signature application

For the purpose of creating long-term signatures directly from an application program for preparing electronic documents, we used our long-term signature libraries to develop an Office Add-on for long-term signature application for Microsoft Office® (Note 1) 2007.

The Office Add-on for long-term signature application has the capability to construct and verify ES-T format data that is recommended in the JAHIS guideline for application to documents for external submission. It can create CAdES data as a PDF document and XAdES data as an OpenXML document. These functions are used to create a PDF document, generate a signature for the PDF document, and affix a timestamp in the case of CAdES data; they also generate a signature for an OpenXML document created using the Office application, and affix a timestamp in the case of XAdES data; and create ES-T format data for either CAdES or XAdES data.

Until now, a document prepared using an Office application was printed out on paper, and then the paper document was sealed and stored. In contrast, by using the Office Add-on for long-term signature application, a long-term signature format can be constructed and verified on the Office application, allowing preparation and storage of electronic documents having legal force equivalent to the paper document. As a result, a reduction in paper consumption and administrative costs, as well as time costs, is expected by using emails and file servers for real-time data communications and data sharing.

4. Conclusion

The Office Add-on for long-term signature application has wide-ranging relevance including in the healthcare field and for digital signatures on mandatory archive documents. We will further strive to integrate the long-term signature library into existing applications, enabling long-term signature generation on various products.

References

- (1) RFC 5126: CMS Advanced Electronic Signatures (CAdES) (2008)

- (2) ETSI TS 101 733 V1.7.4: CMS Advanced Electronic Signatures (CAdES) (2008)
- (3) ETSI TS 101 903 V1.3.2: XML Advanced Electronic Signatures (XAdES) (2006)
- (4) JIS X 5092: Long term signature profiles for CMS advanced electronic signatures (CAdES) (2008)
- (5) JIS X 5093: Long term signature profiles for XML advanced electronic signatures (XAdES) (2008)

Note 1: The Microsoft and Microsoft Office logo are registered trademarks of Microsoft Corporation in the United States and other countries.