Electronic Signature Format

ECOM Interoperability Plug Test 2005

Final Report Executive Summary

January 2006

Next Generation Electronic Commerce Promotion Council of Japan (ECOM)

Security Working Group

Electronic Signature Format ECOM Interoperability Plug Test Project

www.ecom.jp

1. Introduction

The Next Generation Electronic Commerce Promotion Council of Japan (ECOM http://www.ecom.jp/) has been carrying out research and promoting activities related to long-term storage of electronic documents since 2000. As an activity of ECOM for this fiscal year, the Electronic Signature Format profile was formulated in June based on CAdES [6] and XAdES [9]. In this autumn, a plug test was performed to check products for this profile, compliance of the products, and interoperability between the products. Fourteen IT vendors in Japan took part in this plug test. This paper not only reports the overview and results of this plug test, but also describes issues on interoperation uncovered by the test.

2. Background

To promote the adoption of computerized documents instead of documents stored on paper, the Electronic Signature Law [13] was enforced in April 2001, and the e-Document Law [14] was enforced in April 2005 in Japan. Documents legally obliged to be saved include documents that are obliged to be saved for more than ten years. To save such documents in digital format, the e-Document Law essentially requires the addition of a digital signature and timestamp.

Since the time to be used for a digital signature indicates only the local time, ensuring “when the data was signed” needs a timestamp provided by reliable third party organization (i.e. TimeStamp Authority). As of January 2006 in Japan, three accredited commercial TimeStamp Authority services are provided, and all of them supports the international standard RFC 3161 as its communication protocol.[2].

The electronic document storage method currently considered the most effective is an electronic signature format of CMS [3] or XML format defined in the international standard and European standard, such as RFC 3126 [1] and ETSI. Even if the expiration date of a timestamp is exceeded or an encryption algorithm becomes doubtful in the future, the extension by the latest algorithm with high strength can assure that original documents will not be falsified over spans of several decades, and verification by a third party can be conducted at any time. This means that migration of document management systems in the future and migration of certificate authority and timestamp services can be implemented, and an important merit is also found in providing service for a long time.

3. ECOM Electronic Signature Format Profile

In July 2005, ECOM formulated profiles based on the following international standards and European standards to improve and diffuse the interoperability of Electronic Signature Formats in Japan.

- ECOM CAdES Electronic Signature Format Profile
- ECOM XAdES Electronic Signature Format Profile

Features of each profile are as shown below.

- ECOM CAdES Electronic Signature Format Profile
    - Based on ETSI TS 101 733 v1.5.1 Electronic Signature Format
    - Only ES, ES-T, ES-C, ES-X long, and ES-A are handled. ES-X type 1/2 and ES-X long type 1/2 are excluded.
    - The method defined by RFC 3126 and ETSI TS 101 733 v1.4.0 is used for the hash calculation method of archive timestamp.
    - For ES-A and ES-X Long, TSA certificate of signature timestamp, and verification information of TSA certificate of archive timestamp, i.e., certificate chain and CRL, are stored in the certificates of timestamp token CMS SignedData structure and crls field.
    - Invalid information is CRL only. OCSP and others are excluded.
    - CMS version 3 is not required. The IssuerAndSerial format is also available for the SignerIdentifier field of SignerInfo.
- ECOM XAdES Electronic Signature Format Profile
    - Based on ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) v.1.3.1 (DRAFT)
    - Only ES, ES-T, ES-X long and ES-A are handled.

4. Participating Companies

Fourteen companies in total participated in the tests: ten companies participated in the CAdES plug test, and three companies participated in the XAdES plug test, and one company provided the test case design and test environment.

	Perticipant	Type
CAdES	RSA Security	Product
	NTT Data	Prototype
	SECOM	Product
	J-Notary	Product
	NTT	Prototype
	HYPER GEAR	Product
	PFU	Prototype
	Hitachi	Prototype
	Mitsubishi Electric	Prototype
	MDIS	Product
XAdES	KS Solutions	Product
	NEC	Prototype
	Fuji Xerox	Product

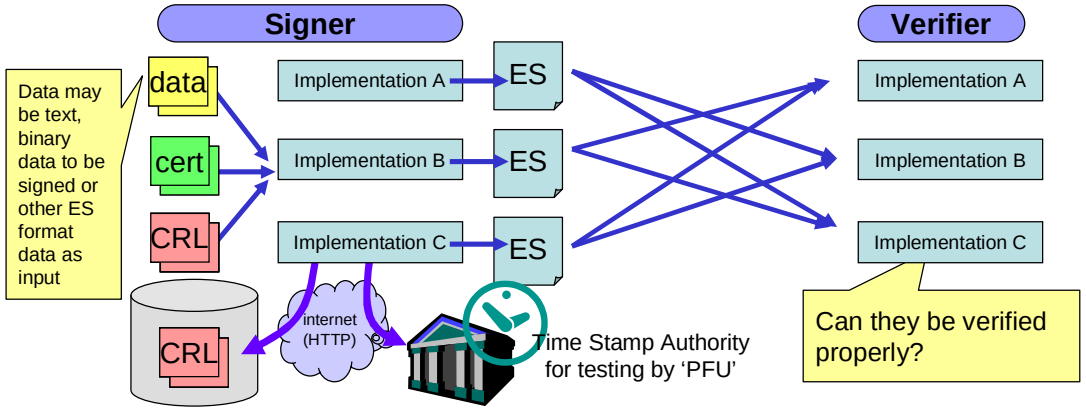
Entrust Japan Co., Ltd. carried out the test case design and construction of certificate authority for test. In addition, PFU Limited provided test Timestamp Authority services for an online test.

5. Contents of Plug Test

The plug tests performed were divided into two types: online matrix generation/validation test and offline validation test.

5.1. Online Matrix Generation/Validation Test

This test is performed to check that data given in the valid Electronic Signature Format generated in an implementation can interoperably be read and verified. Signature target data specified in advance, certificate, CRL and timestamp service are used to generate Electronic Signature Format data (ES-T, ES-X Long, ES-A) from products of all participating companies. In products of participating companies, data generated from products of other companies is checked for validation. CRL and timestamp token are acquired online.

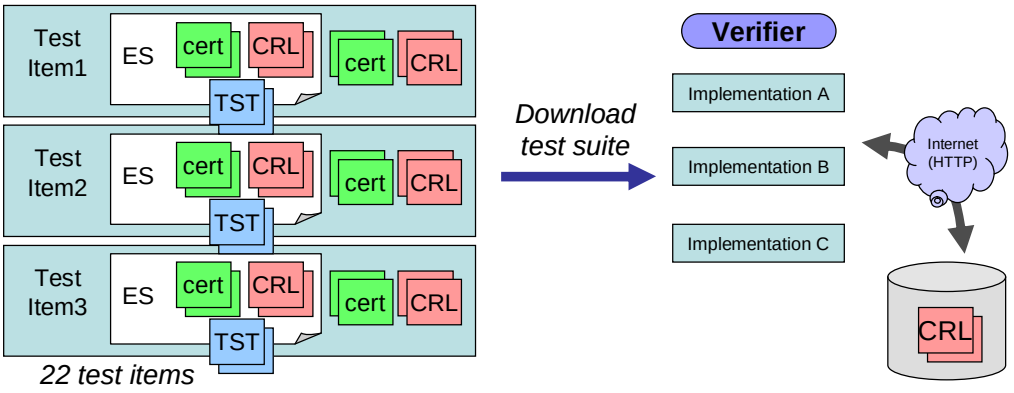


A test case has ten items. As optional tests, some tests are to be performed using a hash value calculation method of a new archive timestamp based on ETSI TS 101 733 v1.5.1.

Format	Testcase	Description
ES-T	ON-T-1	Generation and verification of attached signature ES-T data
	ON-T-2	Generation and verification of detached signature ES-T data
ES-XL	ON-X-1	Generation and verification of attached signature ES-X long data
	ON-X-2	Generation and verification of detached signature ES-X long data
ES-A	ON-A1-1	Generation and verification of 1st generation attached signature ES-A data
	ON-A1-2	Generation and verification of 1st generation detached signature ES-A data
	ON-A1-3	Generation and verification of 1st generation attached signature ES-A data with v1.5.1 hash method
	ON-A2-1	Generation and verification of 2nd generation attached signature ES-A data
	ON-A2-2	Generation and verification of 2nd generation detached signature ES-A data
	ON-A2-3	Generation and verification of 2nd generation attached signature ES-A data with v1.5.1 hash method

5.2. Offline Validation Test

Common ES format data is used based on the ECOM profile to check for correct validation. The validation result is checked for a match with the expected value based on the data (ES, ES-T, ES-C, ES-X long, ES-A) of the ES format generated with the test tool, certificates, CRL, and signature target data.



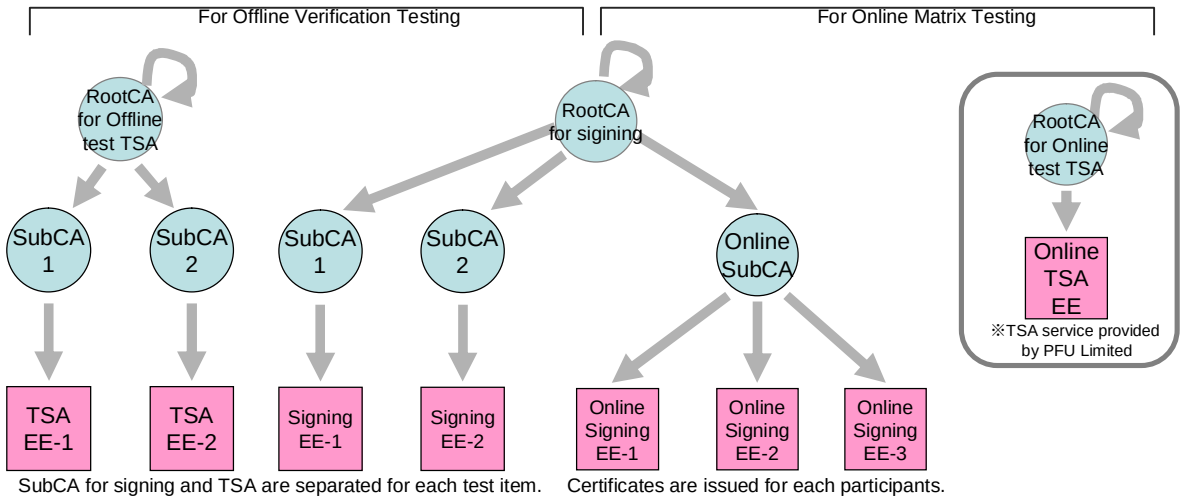
There are 30 test items in total. Some of the test items are shown below.

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
10001	EST-ATTACH-NORMAL-OK	VALID
The application should validate successfully the ES-T format based on attached signature BES format.		
10002	EST-ATTACH-EXPIRED-NG	INVALID
The application should NOT validate the ES-T format when its signing certificate has been expired.		
10003	EST-ATTACH-REVOKED-NG	INVALID
The application should NOT validate the ES-T format in case that it's not expired however it was revoked before the time which described in genTime field of the Signature TimeStamp.		
10004	EST-ATTACH-SIGTIME-REVOKED-OK	VALID
The application should validate successfully the ES-T format in case that it is revoked at the time of SigningTime attribute however it is NOT revoked at the time of Signature TimeStamp.		
10005	EST-ATTACH-SIGTS-REVOKED-NG	INVALID
The application should NOT validate the ES-T format in case that it is revoked at the time of Signature Time however it is NOT revoked at the time of SigningTime attribute.		
10006	EST-ATTACH-ES-SIG-FORGED-NG	INVALID
The application should NOT validate the ES-T format when the signature field of the signerInfo was forged.		
10007	EST-ATTACH-ES-SIGTS-SIG-FORGED-NG	INVALID
The application should NOT validate the ES-T format when the signature field of the SignatureTimeStamp TimeStampToken was forged.		
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG	INVALID
The application should NOT validate the ES-T format when the MessageDigest attribute in the signedAttributes was forged.		
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG	INVALID
The application should NOT validate the ES-T format when the MessageDigest attribute of the SignatureTimeStamp TimeStampToken was forged.		
10010	EST-DETACH-NORMAL-OK	VALID
The application should validate successfully the ES-T format based on detached signature BES format.		
20001	EST-OTHERCERT-SHA256-OK	VALID
The application should validate successfully the ES-T format in case that it has OtherSigningCertificate attribute of SHA256 algorithm.		
20002	EST-SIGTS-SHA256-OK	VALID
The application should validate successfully the ES-T format in case that it has SignatureTimeStamp in which the hash algorithm of MessageImprint of TSTInfo and DigestAlgorithm of SignerInfo are SHA256 and the signatureAlgorithm is SHA256withRSA.		
20003	EST-SIGTS-SHA512-OK	VALID
The application should validate successfully the ES-T format in case that it has SignatureTimeStamp in which the hash algorithm of MessageImprint of TSTInfo and DigestAlgorithm of SignerInfo are SHA512 and the signatureAlgorithm is SHA512withRSA.		
20004	EST-CONTENT-TIMESTAMP-OK	VALID
The application should validate successfully the ES-T format in case that it has ContentTimeStamp attribute in in its signedAttributes field.		

20005	EST-INDEPENDENT-SIGNATURES-OK	VALID
The application should validate successfully the ES-T format in case that it has independent signatures with two signerInfos.		
20006	EST-EPES-WITHOUT-HASHCHECK-OK	VALID
The application should validate successfully the ES-T format generated from EPES format.		
20007	EST-EPES-NORMAL-OK	VALID
The application should validate successfully the ES-T format generated from EPES format with signature policy checking.		
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG	INVALID
The application should NOT validate EPES based ES-T data in which the hash value of signaturePolicyIdentifier does not match with signature policy file.		
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG	INVALID
The application should NOT validate EPES based ES-T data in case notBefore field of signingPeriod in the corresponding signature policy is too far from current time.		
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG	INVALID
The application should NOT validate EPES based ES-T without SigningTime which is mandatedSignedAttr as described in signature policy.		
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG	INVALID
The application should NOT validate attached signature EPES based ES-T in case corresponding signature policy mandates the data to be signed should be external. (i.e. externalSignData field is TRUE.)		
40001	ESC-ATTACH-NORMAL-OK	VALID
The application should validate successfully the ES-C format consists of attached signature BES format.		
40002	ESC-DETACH-NORMAL-OK	VALID
The application should validate successfully the ES-C format consists of detached signature BES format.		
50001	ESXL-ATTACH-NORMAL-OK	VALID
The application should validate successfully the ES-X long format consists of attached signature BES format.		
50002	ESXL-DETACH-NORMAL-OK	VALID
The application should validate successfully the ES-X long format consists of detached signature BES format.		
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK	VALID
The application should validate successfully the ES-X long format in case that the validation information of the TSA certificate int the SignatureTimeStamp was not included in it and it will provided by out-of-bound method such as files.		
70001	ESA1-ATTACH-NORMAL-OK	VALID
The application should validate successfully the 1st generation attached signature ES-A format. i.e. it has only one ArchiveTimeStamp attribute.		
70002	ESA1-DETACH-NORMAL-OK	VALID
The application should validate successfully the 1st generation detached signature ES-A format.		
80001	ESA1-ATTACH-ETSI151-OK	VALID
The application should validate successfully the attached signature ES-A format in case that ArchiveTimeStamp hash calculation method is based on ESTI TS 101 733 v1.5.1 or later.		
80002	ESA1-DETACH-ETSI151-OK	VALID
The application should validate successfully the detached signature ES-A format in case that ArchiveTimeStamp hash calculation method is based on ESTI TS 101 733 v1.5.1 or later.		

All of offline test data is available from 2001 to 2035.

5.3. Trust Model of Plug Test



All certificates and CRLs except for online TSA are issued by 'Challenge PKI Test Suite' [12]. Since validity period of certificates are very long and some of them are in the past time for testing purpose.

6. Plug Test Results

ECOM Plug Test results are described as follows.

	Participant	Type	Offline Verification Test					Online Matrix Test							
								Data Generation				Data Verification			
			ES-T	ES-C	ES-X	ES-A	ES-A 1.5.1	ES-T	ES-X	ES-A	ES-A 1.5.1	ES-T	ES-X	ES-A	ES-A 1.5.1
CAdES	RSA Security	Product	✓	-	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-
	NTT Data	Prototype	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	SECOM	Product	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	J-Notary	Product	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-
	NTT	Prototype	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-
	HYPER GEAR	Product	✓	-	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-
	PFU	Prototype	-	-	-	-	-	✓	✓	✓	-	-	-	-	-
	Hitachi	Prototype	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Mitsubishi Electric	Prototype	✓	-	✓	✓	-	✓	✓	✓	-	✓	✓	✓	-
	MDIS	Product	✓	-	-	✓	-	✓	-	✓	-	✓	✓	✓	-
XAdES	KS Solutions	Product	✓	-	-	✓	-	✓	-	✓	-	✓	-	✓	-
	NEC	Prototype	✓	-	-	✓	-	✓	-	✓	-	✓	-	✓	-
	Fuji Xerox	Product	✓	-	-	✓	-	✓	-	✓	-	✓	-	✓	-

LEGEND: "✓" passed "-" not supported

Some implementations had interoperability issues however they are fixed during the plug test. Half of the implementations doesn't support detached signature yet.

7. Interoperability Issue

7.1. Common Issue

Problems shown below are common to the CAdES format and XAdES format.

- In each of the ES-T, ES-C, ES-X long, and ES-A formats, some products make an incorrect interpretation as to when signing certificate and TSA certificate should be checked for validity. The ECOM profile to be revised in the future must clarify this point.

- Some implementations accurately consider the Grace Period to collect revocation information, others do not consider it exactly. The exactness raises a problem that ES data cannot be generated.

7.2. CAdES Issue

- Problem on DER normalization of ASN.1 BER encoding data
  ES format and timestamp token are expressed as ASN.1 BER encoded. This means that addition to CMS SignedData signature target or hash target of archive timestamp requires normalization to DER.
  However, since some implementation has not been normalized as shown below, hash value or signature value of the implementation is different.

- Sorting of elements of SET OF structure

- DER normalization of undefined length expression of BER
  During normalization, a problem was found as to whether or not normalization is needed for the internal structure of BER.

- Problem on hash target of archive timestamp
  When there are many implementations, and UnsignedAttributes element of SignerInfo of CMS SignedData is added to the hash target of the archive timestamp, some implementations adopt not the attributes themselves but attributeValues as the targets.

- Problem on the hash calculation method of archive timestamp of ETSI TS 101 733 v1.5.1
  Two companies performed both the online test and offline test by using the calculation method of archive timestamp based on the new CAdES Internet Draft proposed in ETSI TS 101 733 v1.5.1 or later, or IETF. Since the standard specification describes little about the normalization method of the hash target, we had to define many prerequisites in order to perform hash calculation method test.

- All elements targeted for hash are to include not only values but also byte arrays of tag, length and value of ASN.1 construction.

- The SET OFF structure of the unsignedAttrs field is normalized with DER, but the internal structure is not normalized.

- The normalization does not put Implicit Context-specific tags of certificates, crls, signedAttr and unsignedAttrs fields back into the Explicit format but adds them to hash targets as they are.

This means that, in the current standardization specification, implementations without interoperability may appear more often than use of the old hash calculation method. It is considered necessary that the knowledge acquired through this test be reflected in cooperation with standardization organizations such as ETSI and IETF.

7.3. XAdES Issue

- Problems on version compatibility
  The ECOM XAdES format profile is based on version 1.3.1, or a draft version of ETSI TS 101 903. However, some companies that participated in the XAdES test adopt implementation based on v1.2.2, and others adopt implementation based on v1.3.1, or a draft version. The compatibility between them causes a problem. Even if a version was to be generated in the implementation, the implementation performed could support the validation of both v1.2.2 base and v1.3.1 base.

- Method of saving certificate validation information
  Some implementations of the method of saving certificate validation information including certificate chain and CRL do not follow the profile. Embedding validation information in the timestamp token, or CMS SignedData format, seemed to be a heavy burden for XAdES implementers.

8. Downloading Test Suite

The test suite of this plug test including test case document and test data will be made available at the ECOM site ‘http://ww.ecom.jp/’, allowing anyone to validate their products. Since private keys of certificate authority and timestamp authority used for the plug test are also included as PKCS#12 files in the suite, new test cases to be designed and added. However, there are some limitations after the plug test as follows:

- Online retrieval of CRL will not be available since HTTP repository will not be provided.

- TimeStamping with the timestamp Authority which was provided by PFU LIMITED for testing purpose will not be available. However online test output from participants will be included to the test suite for your validation test.

9. Contact Information

Any your comments, proposals and questions will be appreciated. Please write to following address.

EMAIL: pubcom@ecom.jp

10. Reference

[1] RFC 3126 Electronic Signature Formats for long term electronic signatures, Sep 2001, D.Pinkas et. al, http://www.ietf.org/rfc/rfc3126.txt
[2] RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Aug 2001, C.Adams et al, http://www.ietf.org/rfc/rfc3126.txt
[3] RFC 3369 Cryptographic Message Syntax (CMS), Aug 2002, R.Housley, http://www.ietf.org/rfc/rfc3369.txt
[4] Internet Draft CMS Advanced Electronic Signatures (CAdES), J.Ross, et al., Dec 2005, http://www.ietf.org/internet-drafts/draft-ietf-smime-cades-00.txt
[5] ETSI TS 101 733 V1.4.0 (2002-09) Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, Sep 2002, ETSI
[6] ETSI TS 101 733 V1.5.1 (2003-12) Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, Sep 2002, ETSI
[7] ETSI TS 101 733 V1.6.3 (2005-09) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), Sep 2005, ETSI
[8] ETSI TS 101 903 V1.2.2 (2004-04) XML Advanced Electronic Signatures (XAdES), Apr 2004, ETSI
[9] ETSI TS 101 903 V1.3.1 (DRAFT) XML Advanced Electronic Signatures (XAdES), DRAFT, ETSI
[10] ITU-T X.680 Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation, Jul 2002, ITU-T

[11] ITU-T X.690 Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), Jul 2002, ITU-T
[12] Challenge PKI Test Suite, NPO Japan Network Security Association, http://www.jnsa.org/mpki/index.html
[13] Electronic Signature Law (in Japanese), 2001, http://www.meti.go.jp/policy/netsecurity/digitalsign.htm
[14] e-Document Law (in Japanese), 2005, http://www.kantei.go.jp/jp/singi/it2/hourei/16-149gou/honbun.html