

Long-Term Signature Format ECOM Interoperability Plug Test CAdES Test Case Specifications

March 2006

Next Generation Electronic Commerce Promotion Council of Japan
(ECOM)

Security Working Group

Long-Term Signature Diffusion Sub Working Group

Electronic Signature Format ECOM Interoperability Plug Test Project

Contents

1	Introduction	1
1.1	Conventions used in this document	1
1.2	Test structure.....	1
2	Offline common data verification test category	2
2.1	Test preparation	2
2.2	Test implementation	2
2.3	Test data conformance	3
2.4	Outline of test items for offline tests	3
2.5	ES-T format standard test items	6
2.5.1	<EST-ATTACH-NORMAL-OK 10001>	6
2.5.2	<EST-ATTACH-EXPIRED-NG 10002>	6
2.5.3	<EST-ATTACH-REVOKED-NG 10003>	6
2.5.4	<EST-ATTACH-SIGTIME-REVOKED-OK 10004>	7
2.5.5	<EST-ATTACH-SIGTS-REVOKED-NG 10005>	7
2.5.6	<EST-ATTACH-ES-SIG-FORGED-NG 10006>	7
2.5.7	<EST-ATTACH-SIGTS-SIG-FORGED-NG 10007>	8
2.5.8	<EST-ATTACH-ES-MESSAGE-DIGEST-FORGED-NG 10008>	8
2.5.9	<EST-ATTACH-SIGTSTST-MESSAGE-DIGEST-FORGED-NG 10009>	8
2.5.10	<EST-DETACH-NORMAL-OK 10010>	9
2.6	ES-T format optional test items	9
2.6.1	<EST-OTHERCERT-SHA256-OK 20001>	9
2.6.2	<EST-SIGTS-SHA256-OK 20002>	9
2.6.3	<EST-SIGTS-SHA512-OK 20003>	10
2.6.4	<EST-CONTENT-TIMESTAMP-OK 20004>	10
2.6.5	<EST-INDEPENDENT-SIGNATURES-OK 20005>	11
2.6.6	<EST-EPES-WITHOUT-HASHCHECK-OK 20006>	11
2.6.7	<EST-EPES-NORMAL-OK 20007>	11
2.6.8	<EST-EPES-POLICY-HASH-NOT-MATCH-NG 20008>	12
2.6.9	<EST-EPES-NOT-BEFORE-VIOLATION-NG 20009>	12
2.6.10	<EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG 20010>	13
2.6.11	<EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG 20011>	13
2.7	ES-C format standard test items	14
2.8	ES-C format optional test items	14

2.8.1	<ESC-ATTACH-NORMAL-OK 40001>	14
2.8.2	<ESC-DETACH-NORMAL-OK 40002>	14
2.9	ES-X Long format standard test items	15
2.9.1	<ESXL-ATTACH-NORMAL-OK 50001>	15
2.9.2	<ESXL-DETACH-NORMAL-OK 50002>	15
2.10	ES-X Long format optional test items	15
2.10.1	<ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK 60001>	15
2.11	ES-A format standard test items	16
2.11.1	<ESA1-ATTACH-NORMAL-OK 70001>	16
2.11.2	<ESA1-DETACH-NORMAL-OK 70002>	16
2.12	ES-A format optional test items	17
2.12.1	<ESA1-ATTACH-ETSI151-OK 80001>	17
2.12.2	<ESA1-DETACH-ETSI151-OK 80002>	17
2.13	ES-T standard test cases	17
2.13.1	<OFF-T-1>	18
2.13.2	<OFF-T-2>	18
2.13.3	<OFF-T-3>	18
2.13.4	<OFF-T-4>	18
2.13.5	<OFF-T-5>	18
2.13.6	<OFF-T-6>	18
2.13.7	<OFF-T-7>	19
2.13.8	<OFF-T-8>	19
2.13.9	<OFF-T-9>	19
2.13.10	<OFF-T-10>	19
2.14	ES-T optional cases	19
2.14.1	<OFF-T-OP-1>	19
2.14.2	<OFF-T-OP-2>	20
2.14.3	<OFF-T-OP-3>	20
2.14.4	<OFF-T-OP-4>	20
2.14.5	<OFF-T-OP-5>	20
2.14.6	<OFF-T-OP-6>	20
2.14.7	<OFF-T-OP-7>	21
2.14.8	<OFF-T-OP-8>	21
2.14.9	<OFF-T-OP-9>	21
2.14.10	<OFF-T-OP-11>	21
2.15	ES-C optional test cases	21
2.15.1	<OFF-C-OP-1>	21
2.15.2	<OFF-C-OP-2>	22
2.16	ES-X Long standard test cases	22

2.16.1	<OFF-X-1>	22
2.16.2	<OFF-X-2>	22
2.17	ES-X Long optional test cases	22
2.17.1	<OFF-X-OP-1>	22
2.18	ES-A standard test cases	22
2.18.1	<OFF-A-1>	22
2.18.2	<OFF-A-2>	23
2.19	ES-A optional test cases	23
2.19.1	<OFF-A-OP-1>	23
2.19.2	<OFF-A-OP-2>	23
3	Online matrix generation/validation test category	24
3.1	Data generated	24
3.2	Test preparation	25
3.3	Test implementation (data generation)	25
3.4	Test implementation (validation)	26
3.5	Test cases	26
3.5.1	<ON-T-1> Attached type ES-T generation/mutual verification test case	26
3.5.2	<ON-T-2> Detached form ES-T generation/mutual verification test case	26
3.5.3	<ON-X-1> Attached form ES-X Long generation/mutual verification test case	26
3.5.4	<ON-X-2> Detached form ES-X Long generation/mutual verification test case	27
3.5.5	<ON-A1-1> Attached form 1st generation ES-A generation/mutual verification test case	27
3.5.6	<ON-A1-2> Detached form 1st generation ES-A generation/mutual verification test case	27
3.5.7	<ON-A1-3> Attached form 1st generation new algorithm ES-A generation/mutual verification test case (optional)	28
3.5.8	<ON-A2-1> Attached form 2nd generation ES-A generation/mutual verification test case	28
3.5.9	<ON-A2-2> Detached form 2nd generation ES-A generation/mutual verification test case	28
3.5.10	<ON-A2-3> Attached form 2nd generation new algorithm ES-A generation/mutual verification test case (optional)	29
4	Reference material	29
4.1	Archive hash calculation method based on ETSI TS 101 733 v1.5.1 and later versions and used in the optional ECOM tests	29

5	Appendix: Test data profile.....	32
5.1	Profile of long-term signature format data used for the tests	32
5.1.1	BES (Basic Electronic Signature).....	32
5.1.2	EPES (Explicit Policy-based Electronic Signature)	32
5.1.3	ES-T	33
5.1.4	ES-X Long.....	33
5.1.5	ES-A (1st generation)	34
5.1.6	ES-A (2nd and later generations).....	34
5.2	Profile of timestamp tokens used for the tests.....	35
5.2.1	TimeStampToken.....	35
5.2.2	TSTInfo	35
5.3	Profile of certificates used in the tests	36
5.3.1	Profile of common aspects of certificates used in the tests	36
5.3.2	RootCA certificate profile.....	36
5.3.3	SubCA certificate profile	36
5.3.4	Profile of End Entity certificate for the signer.....	37
5.3.5	TSA certificate profile	37
5.3.6	Profile of RootCA certificate for the online TSA	38
5.3.7	Online TSA certificate profile	38
5.3.8	Profile of common online/offline/signer/TSA CRL	38
5.4	Profile of signature profile used for the tests.....	39

List of Figures

Figure 1-1: Test structure.....	1
Figure 2-1: Offline validation test	2
Figure 3-1: Online matrix generation/verification test.....	24
Figure 4-1: Items included in the archive hash according to ETSI TS 101 733 v1.5.1 and later versions	30
Figure 4-2: Hash calculation method based on v1.5.1 used for these tests	30

1 Introduction

This document provides test case specifications that give details on testing for conformance with the long-term signature format and the ECOM profile.

1.1 Conventions used in this document

The typographic and usage conventions for this document are displayed below.

Text	Description
<...>	Test item
<...-OK>	Test item for which the expected test result is "valid"
<...-NG>	Test item for which the expected test result is "invalid"
<... 00000>	The 5 digits at the end of the test item name correspond to the test item number.
[...]	References

1.2 Test structure

- Test category (test categories here are broadly broken into the offline test category, and the online test category.)
- Test cases (individual test cases that provide a means for evaluating functionality. They consist of several test items.)
- Test items (the smallest component of the tests, results of verification are expressed as success or failure depending on whether they meet the expected value or not.)

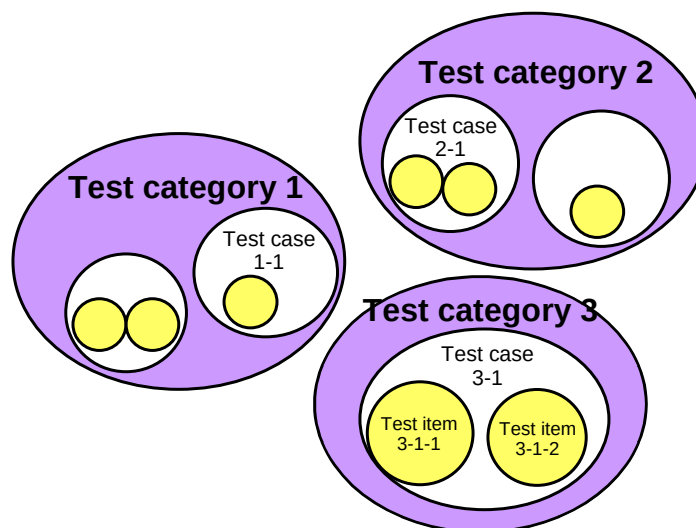


Figure 1-1: Test structure

2 Offline common data verification test category

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 ES format data (ES, ES-T, ES-C, ES-X Long, ES-A) generated with the test tool, certificates, CRL, and signature target data.

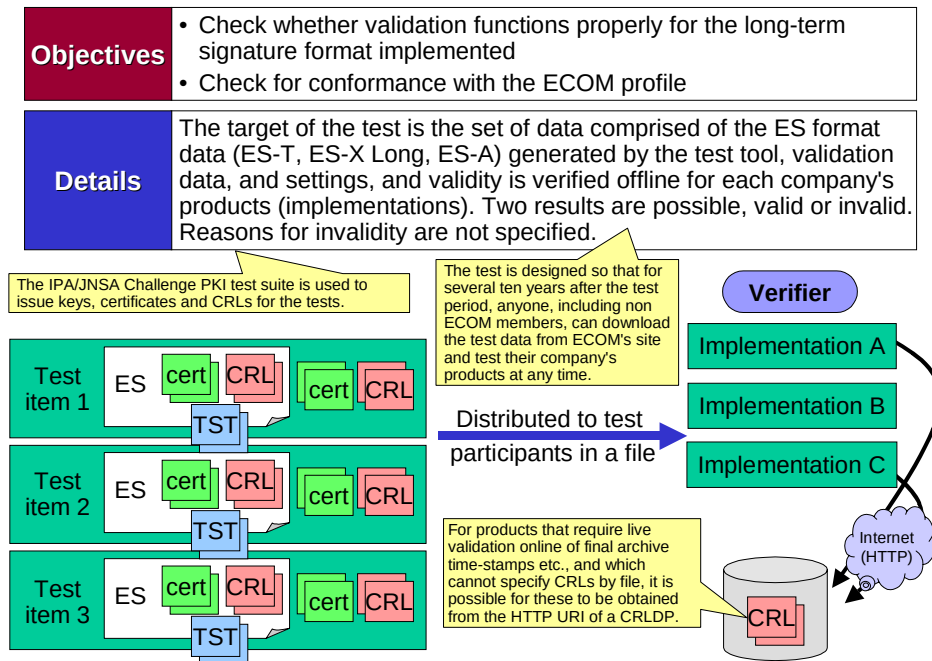


Figure 2-1: Offline validation test

2.1 Test preparation

- **CRL settings**
For online acquisition of CRLs the Internet connection environment of the validation environment must be set up. Following the testing period, an HTTP repository is set up with the same hostname. A file may also be used for the CRL.
- **Trust anchor settings**
Set as a trust anchor, the signer's root certificate and the TSA's root certificate distributed in the test suite for offline testing.

2.2 Test implementation

- **Signature target data set up and settings**
For attached signatures a file named 'TARGET_AAA.txt' (containing only the 3 byte 3 character string, "aaa") is set up, and for detached signatures a file named 'TARGET_BBB.bin' (containing the sequence 0x01-0x09, 0x00 repeated up to a total of 1024000 bytes) is set up.

- **Validation time settings**
Validation time is different for each format. Validation time is set in accordance with the format. The range of current times for which verification is possible is from 2002.1.1 00:00:00 UTC to 2035.12.31 23:59:59 UTC, and each certificate and CRL is set so that verification over this range is possible.
- **Set up of the long-term signature format validation target data**
In the test suite, the long-term signature format validation target data is stored in a file named 'data.der', and files are stored in a separate directory for each test item.
- **Execution of tests**
This is implemented for all test items.

SHA1 hash values of the signature target data are as follows:

- TARGET_AAA.txt
SHA-1: 7e240de74fb1ed08fa08d38063f6a6a91462a815
- TARGET_BBB.bin
SHA-1: 82918e6b4c2ba314491b2797c3bb4715bae0b713

2.3 Test data conformance

- The validity period, excluding exceptional cases, is from 00:00:00 to 23:59:59 for all cases.
- The signing time and time-stamp are set to 12:00:00 for all cases, excluding exceptional cases.
- Time is expressed in UTC time, unless there is a compelling reason to do otherwise.

2.4 Outline of test items for offline tests

Test cases for the offline tests involve the following:

- Validation of ES-T, ES-C, ES-X Long, and ES-A formats
- Attached and detached signatures
- Hashing algorithms (SHA-1, SHA-256, SHA-512)
- BES and EPES
- Archive hashes for RFC3126 and ETSI TS 101733 v1.5.1 and later versions
- Verification of revocation or expiry based on times provided by SigningTime, and SignatureTimeStamp
- Checks for forgery of each of the hash values
- Content time-stamp
- Parallel signatures (= independent signatures)
- Validation in accordance with signature policy files

All 30 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 signer's certificate has expired.		
10003	EST-ATTACH-REVOKED-NG	INVALID
The application should NOT validate the ES-T format in cases where its signer's certificate has not expired but was revoked before the time in the genTime field of the SignatureTimeStamp.		
10004	EST-ATTACH-SIGTIME-REVOKED-OK	VALID
The application should ignore the SigningTime attribute and validate successfully the ES-T format in cases where it is revoked at the time in the SigningTime attribute, but NOT revoked according to the time in signature time-stamp.		
10005	EST-ATTACH-SIGTS-REVOKED-NG	INVALID
The application should NOT validate the ES-T format in cases where it is revoked at the time of the signature time-stamp even though it is NOT revoked at the time of the SigningTime attribute in consideration with the signature time-stamp.		
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 CMS attribute in the signedAttrs field 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 cases where the OtherSigningCertificate CMS attribute indicates the SHA256 algorithm.		
20002	EST-SIGTS-SHA256-OK	VALID
The application should validate successfully the ES-T format in cases where it has a SignatureTimeStamp in which the hash algorithm of MessageImprint of TSTInfo and the DigestAlgorithm field in SignerInfo are both SHA256 and the signatureAlgorithm is SHA256withRSA.		
20003	EST-SIGTS-SHA512-OK	VALID
The application should validate successfully the ES-T format in cases where it has a SignatureTimeStamp in which the hash algorithm of MessageImprint of TSTInfo and the DigestAlgorithm field of SignerInfo are both SHA512 and the signatureAlgorithm is SHA512withRSA.		
20004	EST-CONTENT-TIMESTAMP-OK	VALID
The application should validate successfully the ES-T format in cases where it has the ContentTimeStamp CMS attribute in its signedAttributes field.		
20005	EST-INDEPENDENT-SIGNATURES-OK	VALID
The application should validate successfully the ES-T format in cases where it has independent signatures with two signerInfos.		
20006	EST-EPES-WITHOUT-HASHCHECK-OK	VALID
The application should validate successfully the ES-T format based on an EPES with a signaturePolicyIdentifier CMS attribute.		
20007	EST-EPES-NORMAL-OK	VALID
With reference to the signature policy file, the application should validate successfully the ES-T format based on an EPES with a signaturePolicyIdentifier CMS attribute.		
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG	INVALID
The application should NOT validate the ES-T format in cases where the hash value of the signaturePolicyIdentifier CMS attribute is not in conformance with the signature policy.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG	INVALID
The application should NOT validate the ES-T format at the current time if the notBefore field of the signingPeriod in the signature policy file gives a time that is far into the future and not yet within the validity period since this means that the signature policy is currently invalid.		
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG	INVALID
The application should NOT validate the ES-T format if the MANDATORY SigningTime attribute is not present in the mandatedSignedAttr field in the signature policy file.		
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG	INVALID
The application should NOT validate the ES-T format if the signature is an attached signature regardless of the fact that the value of externalSignedData is TRUE in the signature policy file, meaning that a detached signature is actually requested.		
40001	ESC-ATTACH-NORMAL-OK	VALID
The application should validate successfully ES-C format data based on the attached signature BES format.		
40002	ESC-DETACH-NORMAL-OK	VALID
The application should validate successfully ES-C format data based on the detached signature BES format.		
50001	ESXL-ATTACH-NORMAL-OK	VALID
The application should validate successfully ES-X Long format data based on the attached signature BES format.		
50002	ESXL-DETACH-NORMAL-OK	VALID
The application should validate successfully ES-X Long format based on the detached signature BES format.		
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK	VALID
The application should validate successfully the ES-X Long format in cases where the validation information of the TSA certificate in the SignatureTimeStamp was not included in the token, but it will be provided by out-of-bound methods such as files.		
70001	ESA1-ATTACH-NORMAL-OK	VALID
The application should validate successfully the 1st generation attached signature ES-A format (i.e. has only one ArchiveTimeStamp CMS attribute.)		
70002	ESA1-DETACH-NORMAL-OK	VALID
The application should validate successfully the 1st generation detached signature ES-A format (i.e. has only one ArchiveTimeStamp CMS attribute.)		
80001	ESA1-ATTACH-ETSI151-OK	VALID
The application should validate successfully the 1st generation attached signature ES-A format in cases where the 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 cases where the ArchiveTimeStamp hash calculation method is based on ESTI TS 101 733 v1.5.1 or later.		

2.5 ES-T format standard test items

2.5.1 <EST-ATTACH-NORMAL-OK 10001>

The signer's certificate and the TSA certificate in the signature timestamp are both within the validity period, and not revoked. The ES-T data should be successfully validated. This is the standard ES-T format test for this test case.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.5.2 <EST-ATTACH-EXPIRED-NG 10002>

The ES-T data should NOT be validated if the TSA certificate in the signature timestamp is valid, and the signing certificate is not listed on the CRL used for validation for the signer's certificate, but the signature timestamp was attached at a time when the signature certificate had expired.

EXPECTED VALUE	INVALID
Signing time used	2001.1.3 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 00:00:00 - 2001.1.1 23:59:59
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.5.3 <EST-ATTACH-REVOKED-NG 10003>

The ES-T data should NOT be validated if the TSA certificate in the signature timestamp and the signer's certificate are within the validity period, but the signer's certificate is revoked and listed on the CRL at the times given in the signing time attribute and the signature timestamp.

EXPECTED VALUE	INVALID
Signing time used	2001.1.2 12:00:00
Time in signing time attribute	2001.1.2 12:00:00
Time in signature time-stamp	2001.1.2 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.4 00:00:00-2001.1.4 23:59:59
Signer's certificate revocation time on CRL	2005.1.1 12:00

TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.4 00:00:00-2001.1.4 23:59:59

2.5.4 <EST-ATTACH-SIGTIME-REVOKED-OK 10004>

The ES-T data should be validated based on the signature timestamp, and the signing time should be ignored, if the signer's certificate and the TSA certificate in the signature timestamp are within the validity period, and the signer's certificate is revoked and listed on the CRL at the time given in the signing attribute, but not at the time given in the signature timestamp.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00 (=SignatureTS)
Time in signing time attribute	2001.1.4 12:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.3 00:00:00-2001.1.3 23:59:59
Signer's certificate revocation time on CRL	2005.1.2 12:00:00
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.3 00:00:00-2001.1.3 23:59:59

2.5.5 <EST-ATTACH-SIGTS-REVOKED-NG 10005>

The ES-T data should NOT be validated, and this decision should be based on the validation of the certificate at the time of the signature timestamp, with the signing time being ignored, if the signer's certificate and TSA certificate in the signature timestamp are within the validity period, and the signer's certificate is not revoked at the time of the SigningTime attribute, but is revoked and listed on the CRL at the time of the signature timestamp.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	2001.1.1 12:00:00
Time in signature time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.4 00:00:00-2001.1.4 23:59:59
Signer's certificate revocation time on CRL	2005.1.2 12:00:00
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.4 00:00:00-2001.1.4 23:59:59

2.5.6 <EST-ATTACH-ES-SIG-FORGED-NG 10006>

The data should NOT be validated if the signature value in the signature field within SignerInfo in the ES-T format CMS SignedData has been forged.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00

Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.5.7 <EST-ATTACH-SIGTS-SIG-FORGED-NG 10007>

The data should NOT be validated if the signature value in the signature field in SignerInfo in the CMS SignedData structure of the TimeStampToken present within the ES-T format SignatureTimeStamp attributes has been forged.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.5.8 <EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

The data should NOT be validated if the value of the MessageDigest attribute within signedAttributes of the ES-T format CMS SignedData has been forged.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.5.9 <EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

The data should NOT be validated if the value of the MessageDigest attribute within signedAttributes of the timestamp token contained in the ES-T format SignatureTimeStamp attribute has been forged.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00

Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.5.10 <EST-DETACH-NORMAL-OK 10010>

ES-T format data should be successfully validated where the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6 ES-T format optional test items

2.6.1 <EST-OTHERCERT-SHA256-OK 20001>

The ES-T format should be successfully validated if the SHA256 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance. This can be compared to the <EST-ATTACH-NORMAL-OK> test item, except that the ESSSigningCertificate attribute is not used to specify the signer's certificate.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.2 <EST-SIGTS-SHA256-OK 20002>

The ES-T format should be successfully validated in cases where the hashing algorithm for the signature timestamp's timestamp token is SHA256, and the signature algorithm is SHA256withRSA.

- MessageImprint in TSTInfo in the TimeStampToken is SHA256
- DigestAlgorithm in SignerInfo in the TimeStampToken is SHA256

- SignatureAlgorithm is SignerInfo in the TimeStampToken is SHA256withRSA

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.3 <EST-SIGTS-SHA512-OK 20003>

The ES-T format should be successfully validated in cases where the hashing algorithm for the signature timestamp's timestamp token is SHA512, and the signature algorithm is SHA512withRSA.

- MessageImprint in TSTInfo in the TimeStampToken is SHA512
- DigestAlgorithm in SignerInfo in the TimeStampToken is SHA512
- SignatureAlgorithm is SignerInfo in the TimeStampToken is SHA512withRSA

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.4 <EST-CONTENT-TIMESTAMP-OK 20004>

The ES-T format should be successfully validated in cases where a valid ContentTimeStamp is present in the CMS signed attributes.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in the ContentTimeStamp	2001.1.1 09:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.5 <EST-INDEPENDENT-SIGNATURES-OK 20005>

The ES-T format data should be successfully validated in cases where parallel signatures (also known as independent signatures) from two signers, each with a valid signature timestamp, have been applied.

Certificates for both signers are taken as having been issued from the same sub CA.

EXPECTED VALUE	VALID
Signing time used for signature 1	2001.1.1 12:00:00
Time in signing time attribute 1	Attribute not present
Time in signature time-stamp 1	2001.1.1 12:00:00
Validity period for signer's certificate 1	2001.1.1 - 2035.12.31
Signing time used for signature 2	2001.1.1 13:00:00
Time in signing time attribute 2	Attribute not present
Time in signature time-stamp 2	2001.1.1 13:00:00
Validity period for signer's certificate 2	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.6 <EST-EPES-WITHOUT-HASHCHECK-OK 20006>

In cases where a signature timestamp has been applied to an EPES (Explicit Policy Electronic Signatures) format that has an explicit signature policy identifier in the signedAttributes field, the ES-T data should be read-in without error.

In implementations that handle signature policies strictly, this is used to verify the signature policy file distributed as test data.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59
OID of signature policy	1.2.3.4.5
Signature policy SHA1 hash value	af1d3ea7aef706a898191dd257218f5e9acafaa1

2.6.7 <EST-EPES-NORMAL-OK 20007>

ES-T data for which a signature timestamp has been applied to an EPES format that has an explicit signature policy identifier in the signedAttributes field, and ES-T data generated according to the EPES format with a signature policy file read-in should be successfully validated.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59
OID of signature policy	1.2.3.4.5.20000
Signature policy SHA1 hash value	90490e8e411bd495415988298d07ab45922e8bff

2.6.8 <EST-EPES-POLICY-HASH-NOT-MATCH-NG 20008>

For ES-T format data generated according to EPES, if the hash value in the SignaturePolicyIdentifier CMS signed attribute does not correspond to the hash value of the signature policy file, then the ES-T data should NOT be validated.

[illegible]

2.6.9 <EST-EPES-NOT-BEFORE-VIOLATION-NG 20009>

For the signature policy data used by ES-T format data generated according to EPES, if the value of the notBefore field in signingPeriod is set to a value that would normally be invalid (December 31, 2035), the signature policy is not within the validity period, and therefore the associated ES-T data should NOT be validated.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31

CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59
OID of signature policy	1.2.3.4.5.20009
Signature policy SHA1 hash value	eab88babb6ffc05343fc8ef0ca6a7dd4920b7e02
signingPeriod.notBefore field in signature policy	2035.12.31 23:59:59

2.6.10 <EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG 20010>

For the signature policy data associated with ES-T format data generated according to EPES, if a signingTime CMS attribute does not appear in the ES-T format data despite the fact that a signingTime OID is contained in mandatedSignedAttr in signerRules within signerAndVerifierValue in commonRules, the ES-T data should NOT be validated since this is a violation of the signature policy.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59
OID of signature policy	1.2.3.4.5.20010
Signature policy SHA1 hash value	5a6c1d137ca139771adbd8d41c868d682ded8b20
mandatedSignedAttr	1.2.840.113549.1.9.4 1.2.840.113549.1.9.5 (signingTime) 1.2.840.113549.1.9.16.2.15

2.6.11 <EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG 20011>

For the signature policy data associated with ES-T format data generated according to EPES, if the ES-T format data is in attached signature form despite the fact that the value of the externalSignedData field in signerRules within signerAndVerifierValue in commonRules is TRUE, so that the signature policy requires a detached signature, the ES-T data should NOT be validated since this is a violation of the signature policy.

EXPECTED VALUE	INVALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.1 00:00:00 - 2035.12.31 23:59:59
OID of signature policy	1.2.3.4.5.20011

Signature policy SHA1 hash value	b363f51a65438136d26ce87f3078657df52b5dc4
externalSignedData	TRUE

2.7 ES-C format standard test items

The ECOM profile designates the ES-C format as optional, and there are therefore no standard test items specified.

2.8 ES-C format optional test items

2.8.1 <ESC-ATTACH-NORMAL-OK 40001>

If the TSA certificate of the signature timestamp and the signer's certificate are both within the validity period, and not revoked, the ES-C data should be successfully validated. This is the standard ES-C format test for this test case.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.8.2 <ESC-DETACH-NORMAL-OK 40002>

ES-C format data should be successfully validated where the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.9 ES-X Long format standard test items

2.9.1 <ESXL-ATTACH-NORMAL-OK 50001>

In cases where the TSA certificate of the signature timestamp and the signer's certificate are within the validity period, and not revoked, ES-X Long data that contains this validation information should be successfully validated. This is the standard ES-X Long format test for this test case.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.9.2 <ESXL-DETACH-NORMAL-OK 50002>

ES-X Long format data should be successfully validated where the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.10 ES-X Long format optional test items

2.10.1 <ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK 60001>

When validating the ES-X Long format, in cases where the validation information of the TSA certificate in the SignatureTimeStamp is not included in the token, but provided by out-of-bound methods, the ES-X format should be successfully validated.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signing time attribute	Attribute not present
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31

CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.2 00:00:00 - 2001.1.2 23:59:59

2.11 ES-A format standard test items

2.11.1 <ESA1-ATTACH-NORMAL-OK 70001>

An ES-A format should be successfully validated when it contains one archive timestamp attribute that was provided by the archive timestamp hash calculation method based on RFC3126 and defined in the 2005 ECOM Long-Term Signature Format Profile.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.3 00:00:00 - 2001.1.3 23:59:59
Time in archive time-stamp 1	2001.1.3 12:00:00
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.11.2 <ESA1-DETACH-NORMAL-OK 70002>

Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp, and when the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.3 00:00:00 - 2001.1.3 23:59:59
Time in archive time-stamp 1	2001.1.3 12:00:00
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.12 ES-A format optional test items

2.12.1 <ESA1-ATTACH-ETSI151-OK 80001>

Although outside the scope of the ECOM Long-Term Signature Format Profile, an ES-A format should be successfully validated where it has one archive timestamp attribute, and the canonicalization method shown in the appendix of this specification has been applied to the new archive hash calculation method defined in ETSI TS 101 733 v1.5.1 and later versions.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.3 00:00:00 - 2001.1.3 23:59:59
Time in archive time-stamp 1	2001.1.3 12:00:00
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.12.2 <ESA1-DETACH-ETSI151-OK 80002>

An ES-A format should be successfully validated where a detached signature has been used under the same conditions as in the <ESA1-ATTACH-ETSI151-OK> test item. The first hashing target, encapContentInfo must have content, and all of it must be DER canonicalized. The signature target data is the same data as used in <ESA1-ATTACH-ETSI151-OK>, and the signature target for other detached signatures is different.

EXPECTED VALUE	VALID
Signing time used	2001.1.1 12:00:00
Time in signature time-stamp	2001.1.1 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.2 23:59:59
TSA certificate in signature time-stamp	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate in the signature time-stamp	2001.1.3 00:00:00 - 2001.1.3 23:59:59
Time in archive time-stamp 1	2001.1.3 12:00:00
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.13 ES-T standard test cases

This section provides the test cases that should be satisfied by implementations that handle the ES-T format.

2.13.1 <OFF-T-1>

Test case name	OFF-T-1
Basic attached signature type ES-T format successfully read-in.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK

2.13.2 <OFF-T-2>

Test case name	OFF-T-2
Expiry of ES-T format signer's certificate handled properly.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG

2.13.3 <OFF-T-3>

Test case name	OFF-T-3
Revocation of ES-T format signer's certificate handled properly.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG

2.13.4 <OFF-T-4>

Test case name	OFF-T-4
Certification path properly verified for ES-T format signer's certificate.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG
10003	EST-ATTACH-REVOKED-NG

2.13.5 <OFF-T-5>

Test case name	OFF-T-5
Revocation of ES-T format signer's certificate successfully verified based on signature timestamp, regardless of the signing time.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG
10004	EST-ATTACH-SIGTIME-REVOKED-OK
10005	EST-ATTACH-SIGTS-REVOKED-NG

2.13.6 <OFF-T-6>

Test case name	OFF-T-6
Forged signature value in SignerInfo successfully detected for the ES-T format.	
Conditions for success: All test items below return the expected value.	

10001	EST-ATTACH-NORMAL-OK
10006	EST-ATTACH-ES-SIG-FORGED-NG

2.13.7 <OFF-T-7>

Test case name	OFF-T-7
Forged signature value in SignerInfo in timestamp token of ES-T format signature timestamp successfully detected.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10007	EST-ATTACH-SIGTS-SIG-FORGED-NG

2.13.8 <OFF-T-8>

Test case name	OFF-T-8
Forged hash value in ES-T format MessageDigest successfully detected.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG

2.13.9 <OFF-T-9>

Test case name	OFF-T-9
Forged hash value in MessageDigest in timestamp token of ES-T format signature timestamp successfully detected.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG

2.13.10 <OFF-T-10>

Test case name	OFF-T-10
Detached signature type ES-T format properly handled.	
Conditions for success: All test items below return the expected value.	
10010	EST-DETACH-NORMAL-OK

2.14 ES-T optional cases

This section gives the optional test cases for testing the functionality of implementations that handle the ES-T format.

2.14.1 <OFF-T-OP-1>

Test case name	OFF-T-OP-1
ES-T format where OtherSigningCertificate attribute indicates SHA256 properly handled.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20001	EST-OTHERCERT-SHA256-OK

2.14.2 <OFF-T-OP-2>

Test case name	OFF-T-OP-2
ES-T format properly handled where the SHA256 algorithm is used for hashes and signatures in timestamp tokens of signature timestamps.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20002	EST-SIGTS-SHA256-OK

2.14.3 <OFF-T-OP-3>

Test case name	OFF-T-OP-3
ES-T format properly handled where the SHA512 algorithm is used for hashes and signatures in timestamp tokens of signature timestamps.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20003	EST-SIGTS-SHA512-OK

2.14.4 <OFF-T-OP-4>

Test case name	OFF-T-OP-4
ES-T format correctly verified where a content timestamp attribute is present in the CMS signed attributes.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20004	EST-CONTENT-TIMESTAMP-OK

2.14.5 <OFF-T-OP-5>

Test case name	OFF-T-OP-5
ES-T format correctly verified where independent signatures (parallel signatures) are used (i.e. there are 2 signerInfos) and the signer's certificates used to sign form a single point of trust.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20005	EST-INDEPENDENT-SIGNATURES-OK

2.14.6 <OFF-T-OP-6>

Test case name	OFF-T-OP-6
ES-T format based on the EPES format verified that should not produce an error when reading in.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20006	EST-EPES-WITHOUT-HASHCHECK-OK

Note: Implementations that correctly handle signature policies should validate based on the signature policy included in the test data. Implementations that do not process signature policies only need to be checked to see that errors are not produced.

2.14.7 <OFF-T-OP-7>

Test case name	OFF-T-OP-7
Hash value conformance correctly checked, and signature policy properly handled for an ES-T format based on the EPES format.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG

2.14.8 <OFF-T-OP-8>

Test case name	OFF-T-OP-8
notBefore in the signature policy correctly handled for an ES-T format based on the EPES format.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG

2.14.9 <OFF-T-OP-9>

Test case name	OFF-T-OP-9
mandatedSignedAttrs in signerRules of the signature policy correctly handled for an ES-T format based on the EPES format.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG

2.14.10 <OFF-T-OP-11>

Test case name	OFF-T-OP-10
ES-T data of the ES-T format based on the EPES format correctly handled when the signature is attached even though value of externalSignedData in the signature policy is TRUE, so that detached signatures are actually required.	
Conditions for success: All test items below return the expected value.	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG

2.15 ES-C optional test cases

2.15.1 <OFF-C-OP-1>

Test case name	OFF-C-OP-1
Basic attached signature type ES-C format successfully read-in.	
Conditions for success: All test items below return the expected value.	

40001	ESC-ATTACH-NORMAL-OK
-------	----------------------

2.15.2 <OFF-C-OP-2>

Test case name	OFF-C-OP-2
Detached signature type ES-C format properly handled.	
Conditions for success: All test items below return the expected value.	
40001	ESC-ATTACH-NORMAL-OK
40002	ESC-DETACH-NORMAL-OK

2.16 ES-X Long standard test cases

2.16.1 <OFF-X-1>

Test case name	OFF-X-1
Basic attached signature type ES-X Long format successfully read-in.	
Conditions for success: All test items below return the expected value.	
50001	ESXL-ATTACH-NORMAL-OK

2.16.2 <OFF-X-2>

Test case name	OFF-X-2
Detached signature type ES-X Long format properly handled.	
Conditions for success: All test items below return the expected value.	
50002	ESXL-DETACH-NORMAL-OK

2.17 ES-X Long optional test cases

2.17.1 <OFF-X-OP-1>

Test case name	OFF-X-OP-1
Validation properly performed on the basis of separately attached validation data when signature timestamp validation data is not included in the timestamp token for the ES-X Long format.	
Conditions for success: All test items below return the expected value.	
50001	ESXL-ATTACH-NORMAL-OK
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK

2.18 ES-A standard test cases

2.18.1 <OFF-A-1>

Test case name	OFF-A-1
Attached signature type 1st generation ES-A format based on the ECOM profile properly handled.	

Conditions for success: All test items below return the expected value.	
70001	ESA1-ATTACH-NORMAL-OK

2.18.2 <OFF-A-2>

Test case name	OFF-A-2
Detached signature type 1st generation ES-A format based on the ECOM profile properly handled.	
Conditions for success: All test items below return the expected value.	
70002	ESA1-DETACH-NORMAL-OK

2.19 ES-A optional test cases

2.19.1 <OFF-A-OP-1>

Test case name	OFF-A-OP-1
Attached signature type 1st generation ES-A format based on the hash calculation method in ETSI TS 101 733 v1.5.1 and later versions properly handled.	
Conditions for success: All test items below return the expected value.	
80001	ESA1-ATTACH-ETSI151-OK

2.19.2 <OFF-A-OP-2>

Test case name	OFF-A-OP-2
Detached signature type 1st generation ES-A format based on the hash calculation method in ETSI TS 101 733 v1.5.1 and later versions properly handled.	
Conditions for success: All test items below return the expected value.	
80002	ESA1-DETACH-ETSI151-OK

3 Online matrix generation/validation test category

This test is performed to check that valid Long-term Electronic Signature Format data generated by a particular implementation can be interoperably read and verified. Signature target data specified in advance, certificates, CRLs and timestamp services are used to generate Long-term Electronic Signature Format data (ES-T, ES-X Long, ES-A) from products of all participating companies. Data generated from one company's products is checked to see if it is validated by products of other participating companies. CRLs and timestamp tokens are acquired online.

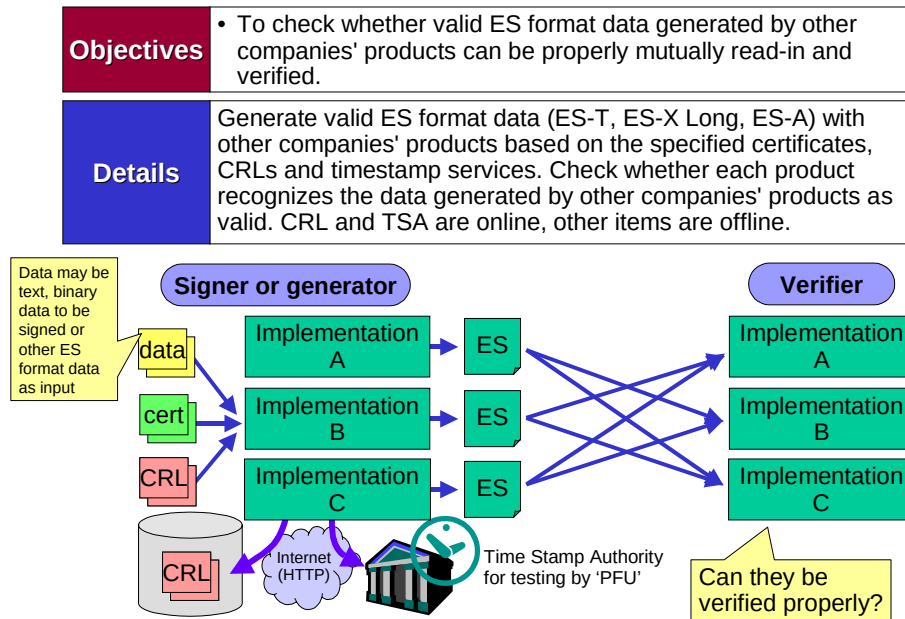


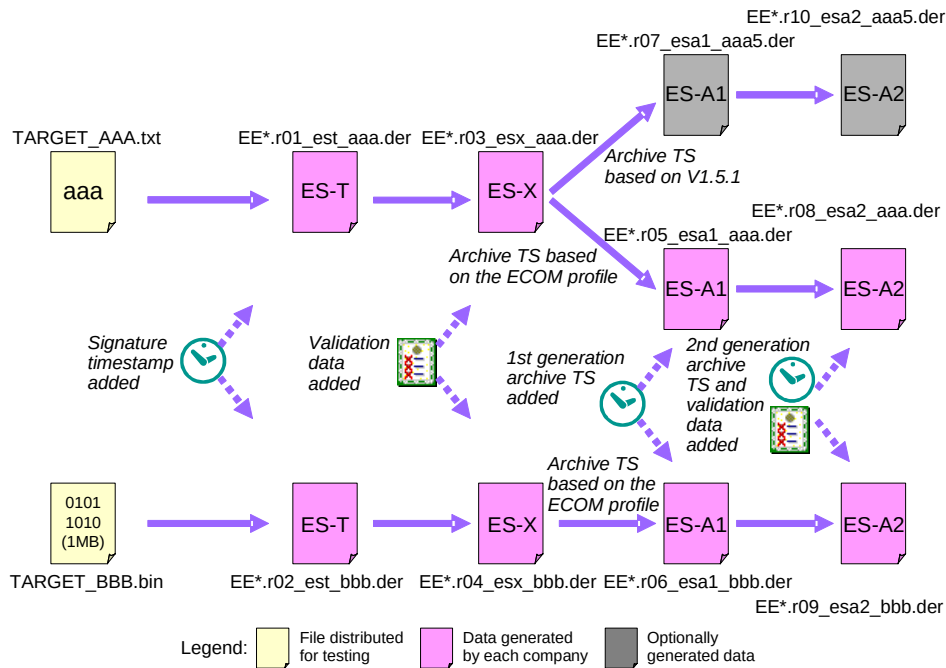
Figure 3-1: Online matrix generation/verification test

A test case has ten items. Some optional tests are also performed using the new archive timestamp hash value calculation method based on ETSI TS 101 733 v1.5.1.

Among the implementations of participating companies, there are very few products that are able to output ES-C format data, and the ES-C format has therefore been removed from test objectives. There are also document management products that implement ES-X Long but use secure archiving measures other than ES-A, and for this reason ES-X Long has been added to test objectives.

3.1 Data generated

A small amount of text data is used for attached signatures, and a 1MB binary file is used for detached signatures, and for each an ES-T format, ES-X Long format and a 1st generation ES-A format and the corresponding next generation ES-A formats are generated. Optional tests may also be performed with data generated using the archive timestamp hash calculation method in ETSI TS 101 733 v1.5.1 and later versions (refer to section 4.1).



The Time Stamp Authority provided for these tests is used for timestamp token acquisition. Revocation data may be acquired from the URL appearing in the certificate's cRLDistributionPoints extension, or the file included with the test data may also be used.

3.2 Test preparation

- **CRL settings**
In order to obtain the CRL, the Internet connection environment of the verification environment must be set up. The CRL issuance period for the signature certifying authority and the timestamp certifying authority is 1 day.
- **Trust anchor settings**
Set as a trust anchor, the signer's root certificate and the TSA's root certificate distributed in the test suite for offline testing.

3.3 Test implementation (data generation)

- **Set up of signature target data**
For attached signatures a file named 'TARGET_AAA.txt' (containing only the 3 byte 3 character string, "aaa") is set up, and for detached signatures a file named 'TARGET_BBB.bin' (containing the sequence 0x01-0x09, 0x00 repeated up to a total of 1024000 bytes) is set up.
- **Data generated**
- **All generated data archived, and transmitted to verifiers at each participating company**

3.4 Test implementation (validation)

- Set up of signature target data
For attached signatures a file named 'TARGET_AAA.txt' (containing only the 3 byte 3 character string, "aaa") is set up, and for detached signatures a file named 'TARGET_BBB.bin' (containing the sequence 0x01-0x09, 0x00 repeated up to a total of 1024000 bytes) is set up.
- Validation time settings
Validation time is different for each format. Validation time is set in accordance with the format. The range of current times for which verification is possible is from 2002.1.1 00:00:00 UTC to 2035.12.31 23:59:59 UTC, and each certificate and CRL is set so that verification over this range is possible.
- Set up of long-term signature format data to be validated
- Validation carried out

3.5 Test cases

The following test regulations with a "#" recorded next to them are rules that must be satisfied, and other items are rules that must be conformed with if possible.

3.5.1 <ON-T-1> Attached type ES-T generation/mutual verification test case

ES-T data is generated by each product according to the following test regulations:

- # The signature target data is the text string "aaa" (x61 x61 x61)
- # Attached signature used. ("aaa" appears in EncapContentInfo)
- MessageDigest is SHA1
- The signing algorithm is SHA1withRSA
- ES-T generated according to the BES format

Test each product for successful validation of this data.

3.5.2 <ON-T-2> Detached form ES-T generation/mutual verification test case

With the <ON-T-1> test case as a base, ES-T data is generated by each product according to the following additional test regulations.

- # The signed object is a 1MB data file
- # Detached signature used. (Signature target data does not appear in EncapContentInfo)

3.5.3 <ON-X-1> Attached form ES-X Long generation/mutual verification test case

ES-X Long data is generated by each company's products according to the following test regulations:

- # Generated with the ES-T data generated in <ON-T-1> as the target
- ES-X Long generated after 48 hours have passed following the generation of the ES-T in <ON-T-1>
- The content and encapsulation method of the signature and the certificate verification data of the signature timestamp are based on the ECOM profile.

Test each product for successful validation of this data.

3.5.4 <ON-X-2> Detached form ES-X Long generation/mutual verification test case

With the <ON-X-1> test case as a base, ES-X Long data is generated by each product according to the following additional test regulations.

- # Generated with the ES-T data generated in <ON-T-2> as the target
- # The signed object is a 1MB data file
- # Detached signature used. (Signature target data does not appear in EncapContentInfo)

Test each product for successful validation of this data.

3.5.5 <ON-A1-1> Attached form 1st generation ES-A generation/mutual verification test case

ES-A data is generated by each product according to the following test regulations:

- # Generated with the ES-X Long data generated in <ON-X-1> as the target, or if the product does not support this, with the ES-T data generated in <ON-T-1> as the target
- Archive timestamp generation and validation method based on the ECOM profile (RFC3126 or ESTI TS 101 733 v1.4.0 and prior versions)
- The content and encapsulation method of the signature and the certificate verification data of the signature timestamp are based on the ECOM profile.

Test each product for successful validation of this data.

3.5.6 <ON-A1-2> Detached form 1st generation ES-A generation/mutual verification test case

With the <ON-A1-1> test case as a base, ES-A data is generated by each product according to the following additional test regulations.

- # Generated with the ES-X Long data generated in <ON-X-2> as the target, or if the product does not support this, with the ES-T data generated in <ON-T-2> as the target
- # The signed object is a 1MB data file
- # Detached signature used. (Signature target data does not appear in EncapContentInfo)

Test each product for successful validation of this data.

3.5.7 <ON-A1-3> Attached form 1st generation new algorithm ES-A generation/mutual verification test case (optional)

This test case is optional. ES-A data is generated by each product according to the following test regulations:

- # Generated with the ES-X Long data generated in <ON-X-1> as the target
- # The archive timestamp generation and validation method is based on ESTI TS 101 733 v1.5.1, with a calculation method applied that utilizes a canonicalization method agreed upon in the ECOM Long-Term Signature Format SWG.
- The content and encapsulation method of the signature and the certificate verification data of the signature timestamp are based on the ECOM profile.

Test each product for successful validation of this data.

3.5.8 <ON-A2-1> Attached form 2nd generation ES-A generation/mutual verification test case

ES-A data is generated by each product according to the following test regulations:

- # Generated (signature extended) with the ES-A generated in <ON-A1-1> as the target
- # Archive timestamp generation and validation method based on the ECOM profile (RFC3126 or ESTI TS 101 733 v1.4.0 and prior versions)
- The content and encapsulation method of the signature and the certificate verification data of the archive timestamp are based on the ECOM profile.

Test each product for successful validation of this data.

3.5.9 <ON-A2-2> Detached form 2nd generation ES-A generation/mutual verification test case

With the <ON-A2-1> test case as a base, ES-A data is generated by each product according to the following additional test regulations.

- # Generated (signature extended) with the ES-A data generated in <ON-A1-2> as the target
- # The signed object is a 1MB data file
- # Detached signature used. (Signature target data does not appear in EncapContentInfo)

Test each product for successful validation of this data.

3.5.10 <ON-A2-3> Attached form 2nd generation new algorithm ES-A generation/mutual verification test case (optional)

This test case is optional. ES-A data is generated by each product according to the following test regulations:

- # Generated with the ES-A data generated in <ON-A1-3> as the target
- # The archive timestamp generation and validation method is based on ETSI TS 101 733 v1.5.1, with a calculation method applied that utilizes a canonicalization method agreed upon in the ECOM Long-Term Signature Format SWG.
- The content and encapsulation method of the signature and the certificate verification data of the signature timestamp are based on the ECOM profile.

Test each product for successful validation of this data.

4 Reference material

4.1 Archive hash calculation method based on ETSI TS 101 733 v1.5.1 and later versions and used in the optional ECOM tests

The CADES format profile formulated by the ECOM Long-Term Signature Format SWG in 2005 utilizes the archive timestamp hash calculation method used in RFC3126 and ETSI TS 101 733 v1.4.2. This is because there is nothing in ETSI TS 101 733 v1.5.1 regarding the data canonicalization method or processing method for when other CMS unsigned attributes are added to the signature extension, and there is nothing regarding how to deal with CounterSignatures. This information would be useful for achieving interoperation between the methods mentioned in v1.5.1. As the first Japanese profile, it was decided that coordination with ETSI would be necessary, and we therefore utilize the traditional method.

For these test we have decided on a tentative calculation method based on v1.5.1, the version applicable at this time. Some optional v1.5.1 based test cases that utilize this method have been created. Of course, this will not have a direct effect on newer versions based on the v1.5.1 standard or on the modification of profiles, it simply provides an impetus for discussion and debate.

According to the standard, the hash is calculated on items as shown in the figure below.

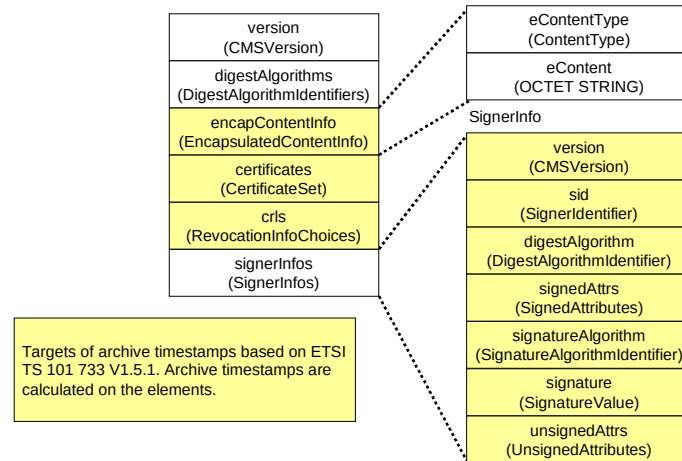


Figure 4-1: Items included in the archive hash according to ETSI TS 101 733 v1.5.1 and later versions

The calculation method is as follows:

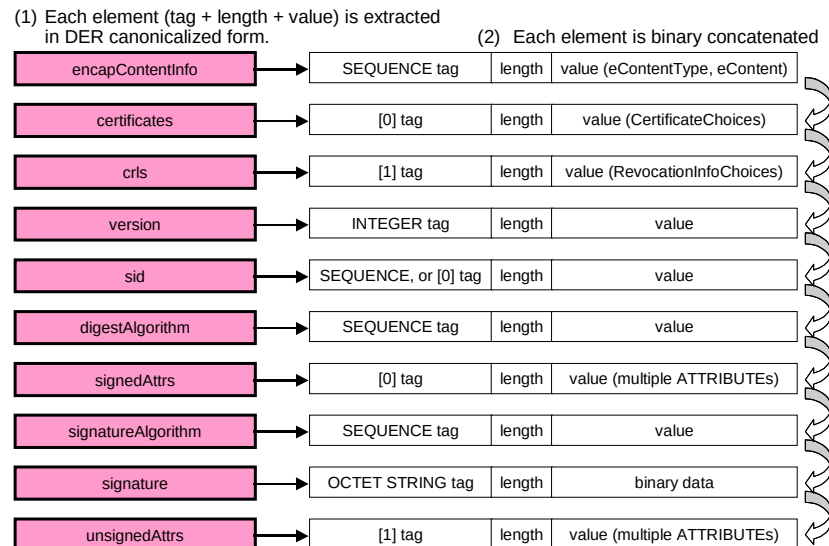
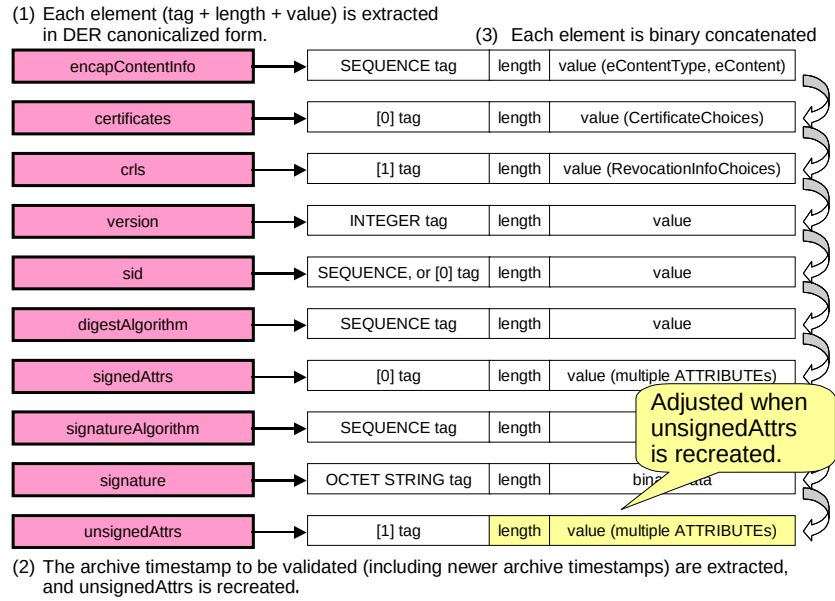


Figure 4-2: Hash calculation method based on v1.5.1 used for these tests

Attention must be paid to the fact that the hash is calculated on ASN.1 TLV (tag, length, value) structure tags and the length part as well. Context specific tags ([0], [1] etc.) are not canonicalized into a SET or SEQUENCE, but just included as is.

The hash input is generated according to the procedure displayed in the figure below when each archive timestamp is verified. Particular attention must be paid to the recalculation of CMS unsigned attributes. For example, say that a CMS unsigned attribute contains n archive timestamps. When validating archive timestamp i (between the 1st and nth archive timestamps), a new ContextSpecific [1] ASN.1 SET structure CMS unsigned attribute is regenerated with the archive timestamps in the CMS unsigned attributes from the 1st one up until the one before the ith timestamp as the elements, and the length byte of the resulting ASN.1 TLV structure is also recalculated, and this must be used as hash input.



5 Appendix: Test data profile

This section provides a profile of the data used for the tests.

5.1 Profile of long-term signature format data used for the tests

All long-term signature format data is based on the CMS SignedData formats, and the required CMS attributes for the signedAttributes field and the unsignedAttributes field are different for each format.

5.1.1 BES (Basic Electronic Signature)

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

5.1.2 EPES (Explicit Policy-based Electronic Signature)

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
sigPolicyId	Present (SHA1 fingerprint)
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

5.1.3 ES-T

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile

5.1.4 ES-X Long

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile (including validation data)
completeCertificateRefs	According to the ECOM profile
completeRevocationRefs	According to the ECOM profile
certificateValues	According to the ECOM profile
revocationValues	According to the ECOM profile

5.1.5 ES-A (1st generation)

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile (including validation data)
completeCertificateRefs	According to the ECOM profile
completeRevocationRefs	According to the ECOM profile
certificateValues	According to the ECOM profile
revocationValues	According to the ECOM profile
archiveTimeStamp	The token is according to the test data profile

5.1.6 ES-A (2nd and later generations)

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	Attached/detached depending on the test item
certificates	Signer's certificate only
crls	None
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier extension of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data (1.2.840.113549.1.7.1)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile (including validation data)
completeCertificateRefs	According to the ECOM profile
completeRevocationRefs	According to the ECOM profile
certificateValues	According to the ECOM profile
revocationValues	According to the ECOM profile
archiveTimeStamp1	The token is according to the test data profile (including validation data)
archiveTimeStamp2 ...	The token is according to the test data profile (Signature extension)

5.2 Profile of timestamp tokens used for the tests

5.2.1 TimeStampToken

TimeStampToken has the CMS SignedData structure. The certificates and crls fields may contain validation data in accordance with the ES-X Long and ES-A validation data encapsulation method defined in the ECOM profile.

Field	Value
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	According to the TSTInfo profile detailed above.
certificates	TSA certificate and path may be included as validation data in accordance with the ECOM profile
crls	All CRLs may be included as validation data in accordance with the ECOM profile
signerInfos	Present (number of elements = 1)
signerInfo	160 bit
version	v1(1)
sid	IssuerAndSerialNumber of the TSA certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=tSTInfo (1.2.840.113549.1.9.16.1.4)
messageDigest	Present
eSSSigningCertificate	Present (issuer name, serial number, SHA1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

5.2.2 TSTInfo

Field	Value
version	v1(1)
policy	TSAPolicyId=0.1.2.3.4.5
messageImprint	Present
hashAlgorithm	SHA1
hashedMessage	160 bit
serialNumber	Value is the same as the serial number of the TSA certificate (*1)
genTime	GeneralizedTime (including at most 3 decimal places)
accuracy	500 milliseconds
ordering	TRUE
nonce	0x1234567890 (fixed)
tsa	directoryName = TSA certificate subject name
extensions	None

*1: This is essentially the serial number of the token issued by the relevant TSA, but only 1 token is issued from the TSA in test situations, so for convenience the same serial number as that of the TSA certificate is used which makes it easy to determine the test item number.

5.3 Profile of certificates used in the tests

5.3.1 Profile of common aspects of certificates used in the tests

Field	Value
version	V3
serial number	5 byte ASN.1 INTEGER (*1)
signature algorithm	SHA1withRSA
issuer DN	PrintableString (All DN are PrintableString)
validity period	UTCTime (times used are between 2000/1/1 00:00:00 and 2035/12/31 23:59:59)
subject DN	PrintableString
public key information	Present
X.509 extension	Present
keyUsage	Present

5.3.2 RootCA certificate profile

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	2048 bit	
X.509 extension	Present	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
basicConstraints	Present	TRUE
CA flag	TRUE	-

5.3.3 SubCA certificate profile

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	1024 bit	
X.509 extension	Present	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160 bit	-
basicConstraints	Present	TRUE
CA flag	TRUE	-
cRLDistributionPoints	Present	FALSE
DistPt.fullName.URI	http://distribution_host/**/*.*.crl	-

5.3.4 Profile of End Entity certificate for the signer

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	1024 bit	
X.509 extension	Present	
keyUsage	digitalSignature, nonRepudiation	TRUE
basicConstraints	Present (empty sequence)	FALSE
CA flag	Present	-
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160 bit	-
cRLDistributionPoints	Present	FALSE
DistPt.fullName.URI	http://distribution_host/**/*.*.crl	-

5.3.5 TSA certificate profile

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	1024 bit	
X.509 extension	Present	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160 bit	-
extKeyUsage	1.3.6.1.5.5.7.3.8 (timeStamping)	TRUE
cRLDistributionPoints	Present	FALSE
DistPt.fullName.URI	http://distribution_host/**/*.*.crl	-

5.3.6 Profile of RootCA certificate for the online TSA

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	2048 bit	
X.509 extension	Present	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160 bit	-
authorityCertIssuer	directoryName (PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	Present	FALSE
CA flag	TRUE	-

5.3.7 Online TSA certificate profile

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	1024 bit	
X.509 extension	Present	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	Present SHA1-160 bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160 bit	-
authorityCertIssuer	directoryName (PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	Present (empty sequence)	FALSE
CA flag	None	-
extKeyUsage	1.3.6.1.5.5.7.3.8 (timeStamping)	TRUE
cRLDistributionPoints	Present	FALSE
DistPt.fullName.URI	http://distribution_host/**/*.*.crl	-

5.3.8 Profile of common online/offline/signer/TSA CRL

Field	Value	Critical
version	V2(1)	
signature algorithm	SHA1withRSA	
issuer DN	PrintableString	
thisUpdate	UTCTime	
nextUpdate	UTCTime	
revokedCertificate		
userCertificate	Serial number of revoked certificate	
revocationDate	UTCTime	
crlEntryExtensions		
cRLReason		FALSE
X.509 extension	Present	
cRLNumber		FALSE

5.4 Profile of signature profile used for the tests

Field	Value
signPolicyHashAlg	SHA1
signPolicyInfo	Present
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c=JP
fieldOfApplication	A "for ..." memo for the test policy
signatureValidationPolicy	
signingPeriod	
notBefore	Present
notAfter	None
commonRules	
signerAndVerifierRules[0]	
signerRules	
externalSignedData?	None
mandatedSignedAttr	messageDigest, sigPolicyId
mandatedUnsignedAttr	signatureTimeStamp
mandatedCertificateRef?	None
mandatedCertificateInfo?	None
signPolExtensions?	None
verifierRules	
mandatedUnsignedAttr	Empty sequence
signPolExtensions?	None
signingCertTrustCondition[1]	
signerTrustTrees	CA certificate for signer
signerRevReq	EE=crlCheck(0), CA=crlCheck(0)
timeStampTrustCondition[2]	
tsCertificateTrustTrees[0]?	CA certificate for TSA
tsRevReq[1]?	EE=crlCheck(0), CA=crlCheck(0)
attributeTrustCondition[3]	None
algorithmConstraintSet[4]	None
commitmentRules	Empty sequence
signPolExtensions	None
signPolExtensions	None
signPolicyHash	None