ECOM CAdES/XAdES Plugtest 2007 CAdES Test Specification

October 2007
V1.2

ECOM CAdES/XAdES Plugtest 2007 Project
Next Generation Electronic Commerce Promotion Council of Japan
(ECOM)

Contents

List of Figures

1 Introduction

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

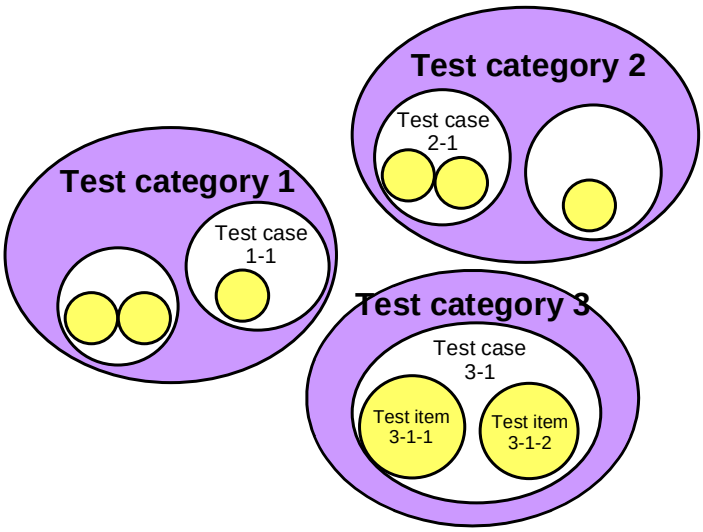

Figure 1-1: Test structure

2 Offline common data verification test category

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

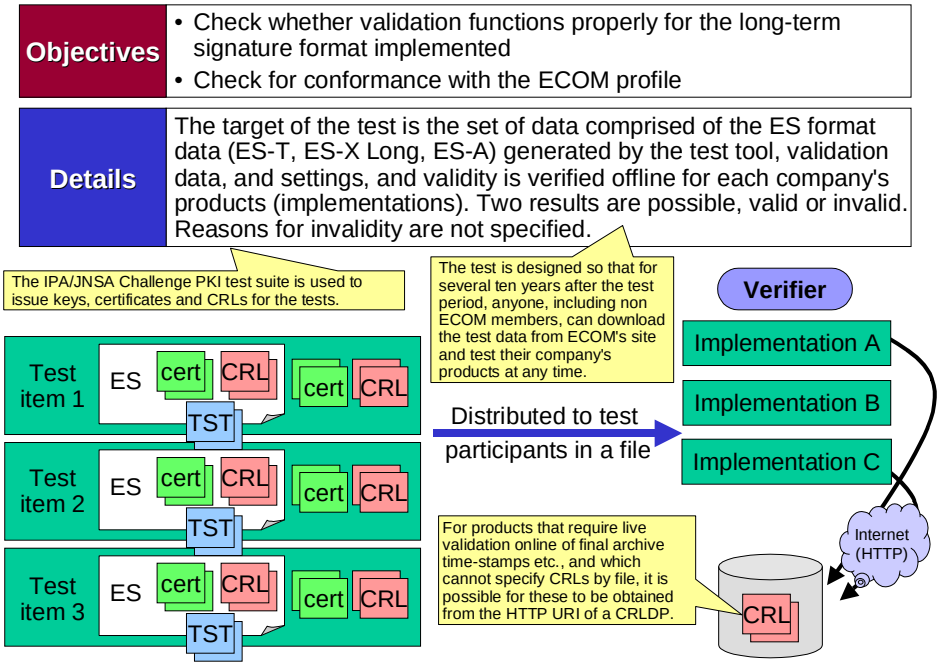

Figure 2-1: Offline validation test

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 00:000:00 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 CAdES-T, CAdES-C, CAdES-X Long, and CAdES-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/v1.6.3 and v1.7.3
- Verification of revocation or expiry based on times provided by SigningTime, and SignatureTimeStampv
- Checks for forgery of each of the hash values
- Content time-stamp
- Parallel signatures (= independent signatures)
- Validation in accordance with signature policy files
- Countersignature

- ESS SigningCertificate V2

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 Signature TimeStamp.		
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.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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.		
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.		
20012	EST-ESSCERTV2-SHA256-OK	VALID
The ES-T format should be successfully validated if the ESSSigningCertificate attribute and the SHA256 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.		
20013	EST-ESSCERTV2-SHA256-FORGED-NG	INVALID
The ES-T format should NOT be validated if the ESSSigningCertificate attribute and the SHA256 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.		
20014	EST-ESSCERTV2-SHA512-OK	VALID
The ES-T format should be successfully validated if the ESSSigningCertificate attribute and the SHA512 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.		
20015	EST-ESSCERTV2-SHA512-FORGED-NG	INVALID
The ES-T format should NOT be validated if the ESSSigningCertificate attribute and the SHA512 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.		
20016	EST-COUNTER-SIGNATURE1-OK	VALID
The EST-format data should be successfully validated in cases where the counter signature from one signer with a valid signature timestamp, have been applied. Certificate of signer and counter signer should be issed from the same sub CA.		
20017	EST-COUNTER-SIGNATURE1-FORGED-NG	INVALID
The ES-T format data should NOT be validated in cases where the field of the counter signature from one signer, each with a valid signature timestamp, have been applied. Certificate of signer, and counter signer are from the same sub CA.		
20018	EST-COUNTER-SIGNATURE2-OK	VALID
The EST-format data should be successfully validated in cases where the parallel signatures from two signers, each with a valid signature timestamp, have been applied. Certificate of signer and counter signer should be issed from the same sub CA.		
20019	EST-COUNTER-SIGNATURE2-FORGED-NG	INVALID
The ES-T format data should be successfully validated in cases where the field of the counter signature from one signer, each with a valid signature timestamp, have been applied. Certificate of signer, and counter signer are from the same sub CA.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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 and it will provided by out-of-bound methods such as files.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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.)		
70003	ESA1-V173-ATTACH-NORMAL-OK	VALID
Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by an attached signature.		
70004	ESA1-V173-DETACH-NORMAL-OK	VALID
Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by an attached signature.		
70005	ESA1-V173-ATTACH-ATS-FORGED-NG	INVALID
Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp V2(ETSI TS 10The CAdES-A with an attached signature should NOT be validated if the messageImprint value of archive timestamp V2 was forged.		
70006	ESA1-V173-DETACH-ATS-FORGED-NG	INVALID
The CAdES-A with a detached signature should NOT be validated if the messageImprint value of archive timestamp V2 was forged.		
70007	ESA2-V173-ATTACH-NORMAL-OK	VALID
Data should be successfully validated for CAdES-A formats that contain 2nd ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by an attached signature.		
70008	ESA2-V173-DETACH-NORMAL-OK	VALID
Data should be successfully validated for CAdES-A formats that contain 2nd ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by a detached signature.		
70009	ESA2-V173-ATTACH-ATS-FORGED-NG	INVALID
The CAdES-A that contains 2nd ArchieTimeStamp V2 with an attached signature should NOT be validated if the messageImprint value of archive timestamp was forged.		
70010	ESA2-ETSI173-DETACH-ATS-FORGED-NG	INVALID
The CAdES-A that contains 2nd ArchieTimeStamp V2 with a detached signature should NOT be validated if the messageImprint value of archive timestamp was forged.		

ITEM-ID	TEST-ITEM-NAME	EXPECTED VALUE
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 - 2001.1.1 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 23:5959
CRL used for validating signer's certificate	2001.1.2 00:00:00 - 2001.1.1 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.

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	1.2.3.4.5.20000
Signature policy SHA1 hash value	90490e8e411bd495415988298d07ab45922e8bff
Hash value of CMS signature policy identifier attribute	1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f

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 manadatedSignedAttr 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	5a6c1d137ca139771adbd8d41c868d682dd8b20
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

2.6.12 < EST-ESSCERTV2-SHA256-OK 20012>

The ES-T format should be successfully validated if the ESSSigningCertificate attribute and the SHA256 hashing algorithm is used to identify the signer’s certificate and the certificate hash value is in conformance.

EXPECTED VALUE	VALID
Signing time used e	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	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.13 < EST-ESSCERTV2-SHA256-FORGED-NG 20013>

The ES-T format should NOT be validated if the ESSSigningCertificate attribute and the SHA256 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.

EXPECTED VALUE	INVALID
Signing time used e	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	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.14 < EST-ESSCERTV2-SHA512-OK 20014>

The ES-T format should be successfully validated if the ESSSigningCertificate attribute and the SHA512 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.

EXPECTED VALUE	VALID
Signing time used e	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	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.15 < EST-ESSCERTV2-SHA512-FORGED-NG 20015>

The ES-T format should NOT be validated if the ESSSigningCertificate attribute and the SHA512 hashing algorithm is used to identify the signer's certificate and the certificate hash value is in conformance.

EXPECTED VALUE	INVALID
Signing time used e	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	2001.1.1 00:00:00 - 2035.12.31 23:59:59

2.6.16 < EST-COUNTER-SIGNATURE1-OK 20016>

The EST-format data should be successfully validated in cases where the counter signature from one signer with a valid signature timestamp, have been applied. Certificate of signer and counter signer should be issued from the same sub CA.

EXPECTED VALUE	VALID
Time in signature time stamp for sign(0)	2001.1.1 12:00:00
Signer(0) certificate	2001.1.1 - 2035.12.31
Time in signature time stamp for countersignature(1)	2001.1.1 13:00:00
Signer(1) certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificates	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

2.6.17 < EST-COUNTER-SIGNATURE1-FORGED-NG 20017>

The ES-T format data should NOT be validated in cases where the field of the counter signature from one signer, each with a valid signature timestamp, have been applied. Certificate of signer, and counter signer are from the same sub CA.

EXPECTED VALUE	INVALID
Time in signature time stamp for sign(0)	2001.1.1 12:00:00
Signer(0) certificate	2001.1.1 - 2035.12.31
Time in signature time stamp for countersignature(1)	2001.1.1 13:00:00
Signer(1) certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificates	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

2.6.18 < EST-COUNTER-SIGNATURE2-OK 20018>

The EST-format data should be successfully validated in cases where the countersignatures from two signers, each with a valid signature timestamp, have been applied. Certificate of signer and counter signer should be issued from the same sub CA.

EXPECTED VALUE	VALID
Time in signature time stamp for sign(0)	2001.1.1 12:00:00
Signer(0) certificate	2001.1.1 - 2035.12.31
Time in signature time stamp for countersignature(1)	2001.1.1 13:00:00
Time in signature time stamp for countersignature(2)	2001.1.1 14:00:00
Signer(1) certificate	2001.1.1 - 2035.12.31
Signer(2) certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificates	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

2.6.19 < EST-COUNTER-SIGNATURE2-FORGED-NG 20019>

The ES-T format data should be successfully validated in cases where the field of the counter signature from one signer, each with a valid signature timestamp, have been applied. Certificate of signer, and counter signer are from the same sub CA.

EXPECTED VALUE	INVALID
Time in signature time stamp for sign(0)	2001.1.1 12:00:00
Signer(0) certificate	2001.1.1 - 2035.12.31
Time in signature time stamp for countersignature(1)	2001.1.1 13:00:00
Time in signature time stamp for countersignature(2)	2001.1.1 14:00:00
Signer(1) certificate	2001.1.1 - 2035.12.31
Signer(2) certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificates	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

2.7 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

2.11.3 < ESA1-V173-ATTACH-NORMAL-OK 70003>

Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by an attached signature.

EXPECTED VALUE	VALID

Time in signature time-stamp	2001.1.1 12:00:00
Time in archive time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 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
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

2.11.4 < ESA1-V173-DETACH-NORMAL-OK 70004>

Data should be successfully validated for ES-A formats that contain only one 1st generation ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in archive time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 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
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

2.11.5 < ESA1-V173-ATTACH-ATS-FORGED-NG 70005>

The CAdES-A with an attached signature should NOT be validated if the messageImprint value of archive timestamp V2 was forged.

EXPECTED VALUE	INVALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in archive time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 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

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

2.11.6 < ESA1-ETSI173-DETACH-ATS-FORGED-NG 70006>

The CAdES-A with a detached signature should NOT be validated if the messageImprint value of archive timestamp V2 was forged.

EXPECTED VALUE	INVALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in archive time-stamp	2001.1.3 12:00:00
Signer's certificate	2001.1.1 - 2035.12.31
CRL used for validating signer's certificate	2001.1.2 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
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

2.11.7 < ESA2-V173-ATTACH-NORMAL-OK 70007>

Data should be successfully validated for CAdES-A formats that contain 2nd ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by an attached signature.

EXPECTED VALUE	VALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in 1st archive time-stamp	2001.1.3 12:00:00
Time in 2nd archive time-stamp	2001.1.4 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
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for 1st archive time-stamp	2001.1.4 00:00:00 - 2002.1.3 23:59:59
CRL used for validating the TSA certificate for 2nd archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.11.8 < ESA2-V173-DETACH-NORMAL-OK 70008>

Data should be successfully validated for CAdES-A formats that contain 2nd ArchiveTimeStamp V2(ETSI TS 101 733 v1.7.3), and when the signed document has been signed by a detached signature.

EXPECTED VALUE	VALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in 1st archive time-stamp	2001.1.3 12:00:00
Time in 2nd archive time-stamp	2001.1.4 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
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for 1st archive time-stamp	2001.1.4 00:00:00 - 2002.1.3 23:59:59
CRL used for validating the TSA certificate for 2nd archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.11.9 < ESA2-V173-ATTACH-ATS-FORGED-NG 70009>

The CAdES-A that contains 2nd ArchieTimeStamp V2 with an attached signature should NOT be validated if the messageImprint value of archive timestamp was forged.

EXPECTED VALUE	INVALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in 1st archive time-stamp	2001.1.3 12:00:00
Time in 2nd archive time-stamp	2001.1.4 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
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for 1st archive time-stamp	2001.1.4 00:00:00 - 2002.1.3 23:59:59
CRL used for validating the TSA certificate for 2nd archive time-stamp	2001.1.4 00:00:00 - 2035.12.31 23:59:59

2.11.10 < ESA2-V173-DETACH-ATS-FORGED-NG 70009>

The CAdES-A that contains 2nd ArchieTimeStamp V2 with a detached signature should NOT be validated if the messageImprint value of archive timestamp was forged.

EXPECTED VALUE	INVALID
Time in signature time-stamp	2001.1.1 12:00:00
Time in 1st archive time-stamp	2001.1.3 12:00:00
Time in 2nd archive time-stamp	2001.1.4 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
TSA certificate for archive time-stamp 1	2001.1.1 - 2035.12.31
CRL used for validating the TSA certificate for 1st archive time-stamp	2001.1.4 00:00:00 - 2002.1.3 23:59:59
CRL used for validating the TSA certificate for 2nd 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 case

This section provides the test case 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 case 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 case

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 case

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 case

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 case

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

2.18.3 <OFF-A-3>

Test case name	OFF-A-3
Attached signature type 1st generation ES-A format based on ETSI TS 10 733 v1.7.3 properly handled.	
Conditions for success: All test items below return the expected value.	
70003	ESA1-V173-ATTACH-NORMAL-OK
70005	ESA1-V173-ATTACH-ATS-FORGED-NG

2.18.4 <OFF-A-4>

Test case name	OFF-A-4
Detached signature type 1st generation ES-A format based on ETSI TS 10 733 v1.7.3 properly handled.	
Conditions for success: All test items below return the expected value.	
70004	ESA1-V173-DETACH-NORMAL-OK
70006	ESA1-V173-DETACH-ATS-FORGED-NG

2.18.5 <OFF-A-5>

Test case name	OFF-A-5
Attached signature type 2ndt generation ES-A format based on ETSI TS 10 733 v1.7.3 properly handled.	
Conditions for success: All test items below return the expected value.	
70007	ESA2-V173-ATTACH-NORMAL-OK
70009	ESA2-V173-ATTACH-ATS-FORGED-NG

2.18.6 <OFF-A-6>

Test case name	OFF-A-6
Detached signature type 2nd generation ES-A format based on ETSI TS 10 733 v1.7.3 properly handled.	
Conditions for success: All test items below return the expected value.	
70008	ESA2-V173-DETACH-NORMAL-OK
70010	ESA2-V173-DETACH-ATS-FORGED-NG

2.19 ES-A optional test case

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 (CAdES-T, CAdES-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.Long-term format data such as CAdES-T and CAdES-A that are requirement for JIS and has been broadly circulated..

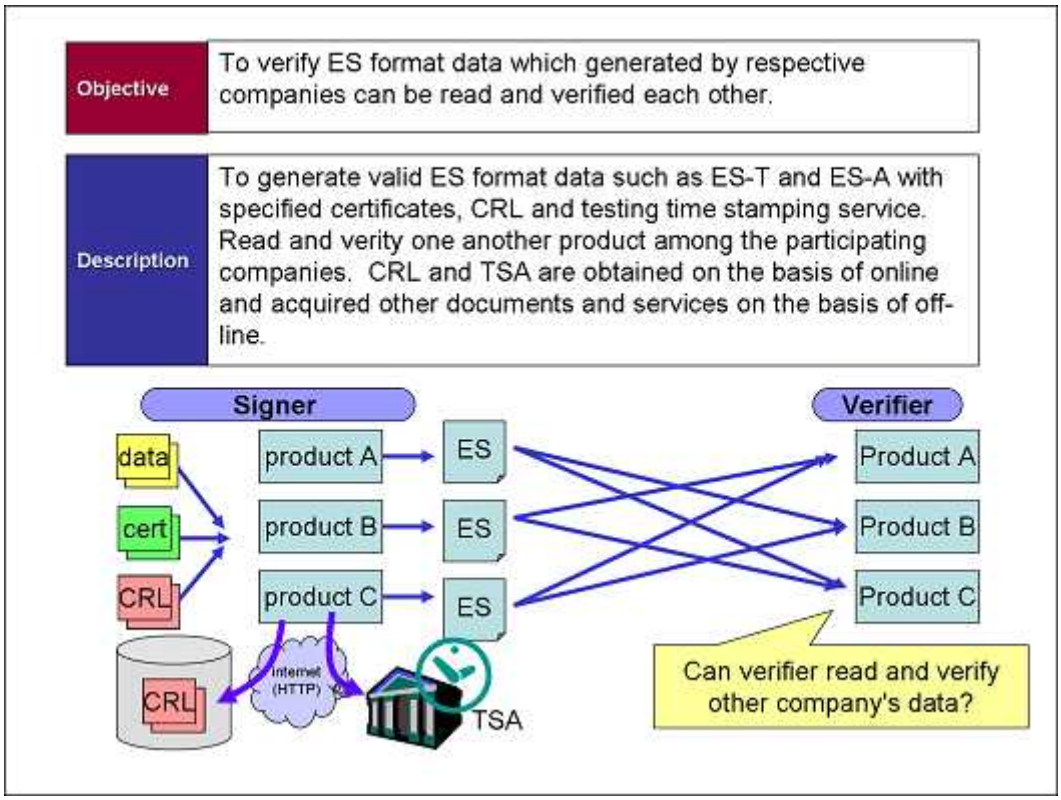

Figure 3-1: Online matrix generation/verification test

3.1 Outline of test case

A test case has 5 items.

- CAdES-T Basic test case
  Attached/Detached signature with signature timestamp.

- CAdES-T Timestamp authority test case
  This test will confirm if CAdES-T correspond to 3 timestamp authorities which has cooperated with the test.

- CAdES-T Optional attribute test case
  This application should successfully validate the CAdES-T format in cases where it support signed and unsigned attributes that can be included in CAdES-T.

- CAdES-A Basic test case
  Attached/Detached signature with archive timestamps.

- CAdES-A Optional attributes test case
  This application should successfully validate the CAdES-A format in cases where it support signed and unsigned attributes that can be included in CAdES-A.

Test cases include test items that create signed data based on the provided requirements. Test items can be implemented where the implementation can be supported by the participating organizations.

The followings are the summerized test items which constitute each test case.

CAdES-T Basic test case (ON-T-BASIC)	
ON-T-BASIC-ATTACHED	CMS attached case signature with signature timestamp
ON-T-BASIC-DETACHED	CMS detached case signature with signature timestamp
CAdES-T Timestamp authority test case (ON-T-TSA)	
ON-T-TSA-AMANO-ATTACHED	Use AMANO TSA
ON-T-TSA-PFU-ATTACHED	Use PFU TSA
ON-T-TSA-SEIKO-ATTACHED	ON-T-TSA-SEIKO-ATTACHED
CAdES-T Optional attribute test case (ON-T-ATTR)	
ON-T-ATTR-SIGNINGTIME	Use SigningTime
ON-T-ATTR-EPES-RFC3125	Use SignaturePolicyIdentifier. Use ASN.1 format signature policy file based on RFC 3125.
ON-T-ATTR-SIGNERLOCATION	Use SignerLocation
ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	Use Signature Attributes that contains ClaimedAttributes
ON-T-ATTR-CONTENTHINTS	Use ContentHints
ON-T-ATTR-COMMITMENTTYPEINDICATION	Use CommitmentTypeIndication
ON-T-ATTR-CONTENTTS-CLAIMEDTIME	Use ContentTimeStamp and SigningTime
ON-T-ATTR-CONTENTREFERENCE	Use ContentReference
ON-T-ATTR-CONTENTIDENTIFIER	Use ContentIdentifier
ON-T-ATTR-COUNTERSIGNATURE	Use CounterSignature
ON-T-ATTR-ESSCERTV2	Use ESSCertV2
CAdES-A Basic test case	
ON-A-BASIC-A1-ATTACHED	Attached case signature with 1 archiveTimeStampV2
ON-A-BASIC-A1-DETACHED	Detached case signature with 1 ArchiveTimeStampV2
ON-A-BASIC-A2-ATTACHED	Attached signature with two ArchiveTimeStamps(V2)
ON-A-BASIC-A3-ATTACHED	Attached signature with three ArchiveTimeStamps(V2)
CAdES-A Optional attributes test case	
ON-A-ATTR-A1-ARCTSV1-ATTACHED	Attached signature with one ArchiveTimeStampV1
ON-A-ATTR-A1-	Append TimestampedCertsCRLs

TIMESTAMPEDCERTSCRLS	
ON-A-ATTR-A1-ESCTIMESTAMP	Append ESCTimeStamp

The following table encapsulated CAdES property which is required by each test items.

TEST CASE ID		ON-T-BASIC-ATTACHED	ON-T-BASIC-DETACHED	ON-T-TSA-AMANO-ATTACHED	ON-T-TSA-PFU-ATTACHED	ON-T-TSA-SEIKO-ATTACHED	ON-T-ATTR-SIGNINGTIME	ON-T-ATTR-EPES-RFC3125	ON-T-ATTR-SIGNERLOCATION	ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	ON-T-ATTR-CONTENTHINTS	ON-T-ATTR-COMMITMENTTYPEINDICATION	ON-T-ATTR-CONTENTS-CLAIMEDTIME	ON-T-ATTR-CONTENTREFERENCE	ON-T-ATTR-CONTENTIDENTIFIER	ON-T-ATTR-COUNTERSIGNATURE	ON-T-ATTR-ESSCERTV2	ON-A-BASIC-A1-ATTACHED	ON-A-BASIC-A1-DETACHED	ON-A-BASIC-A2-ATTACHED	ON-A-BASIC-A3-ATTACHED	ON-A-ATTR-A1-ARCTS1-ATTACHED	ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS	ON-A-ATTR-A1-ESCTIMESTAMP
Signed Attributes	ContentType	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	MessageDigest	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ESSSigningCertificate	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1		C1	C1	C1	C1	C1	C1	C1
	ESSSigningCertificateV2	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	✓	C1	C1	C1	C1	C1	C1	C1
	OtherSigningCertificate	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1		C1	C1	C1	C1	C1	C1	C1
	SigningTime						✓						✓											
	SignaturePolicyIdentifier							✓														✓		
	SignerLocation								✓															
	SignerAttributes									✓														
	ContentHints										✓													
	CommitmentTypeIndication											✓												
	ContentTimeStamp												✓											
	ContentReference													✓										
	ContentIdentifier														✓									
Unsigned Attributes	CounterSignature															✓								
	SignatureTimeStamp	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CompleteCertificateRefs																	✓	✓	✓	✓	✓	✓	✓
	CompleteRevocationRefs																	✓	✓	✓	✓	✓	✓	✓
	AttributeCertificateRefs																							
	AttributeRevocationRefs																							
	ESCTimeStamp																							✓
	TimestampedCertsCRLs																						✓	
	CertificateValues																	✓	✓	✓	✓	✓	✓	✓
	RevocationValues																	✓	✓	✓	✓	✓	✓	✓
	ArchiveTimeStampV1																					1		
	ArchiveTimeStampV2																	1	1	2	3		1	1

BLANK: Option ✓ :Mandatory 123: Number of ArcTS

C1: Choice however ESSSigningCertificate is recommended

3.2 Procedures of Test

- Test Preparation
  - Confirm connectivity of timestamp authority.

- Confirm connectivity of CRL repository.

♦ Signed data generation

- Download signature key (PKCS#12 or JKS) and set up for signed data generation application.
- Download data generation template archive (includes component of data result folder, input data and required information)
- Create copies and links of necessary data for validation.
- Generate data which corresponds to the each test requirements.
- Save hash target, used certificates and CRL for reference if necessary.
- Necessary data for validation should be saved under the test item directory.
- Create a set of compressed archive file for generated data.
- Upload generated data into common space (ECOM file share server).
- Generated data can be uploaded again within the valid period of time if the data had a problem.

♦ Validation of signed data

- Download all data which are generated in the common space (ECOM file share server).
- Open data archive into the appropriate directory.
- Set up certificate path validation
- Keep record of verification result in the Excel sheet. (make note for cause of the failure)
- Update verification results in the common space (ECOM file share server Web site).
- Repeat the above procedures in cases of unsatisfied results or when new archive is uploaded.

3.2.1 Download and unpack of template archive

Template archive is a compressed archive of certificate, input data and test items that are necessary for test data generation. Below is the directory structure of unpacked archive.

02_ONLINE/ Folder for generation/interoperability test.

01_CADES/ CAdES Folder for CAdES generation test --- Copy this to submit as a result.

ON-T-BASIC-ATTACHED/ Folder for each test item --- Store CAdES signature result here.

:

02_XADES/ XAdES Folder for XAdES generation test --- Copy this to submit as a result.

ON-T-BASIC-ENVELOPING/ Folder for each test items --- Store XAdES signature result here.

:

03_CERTS/ Certificates and PKCS#12 keys for Signature

99_WORK/ Directory that used as scope of validation--- Validate signature of other organization.

CADES_1_*company name_generation date*/ The directory should be emptied before the test.

CADES_2_*company name_generation date*/

XADES_1_*company name_generation date*/

3.2.2 Input file name

Input file names for signing should be used shown below.

- TARGET_AAA.txt
  This file contains "aaa" ascii text. It is used for an attached signature.

- TARGET_BBB.bin
  This file is 1MB binary file. It is used for a detached signature.

- TARGET-SIGPOL-RFC3125.der
  This file is signature policy file in the form of ASN.1 DER based on ETSI TR 101 272 v1.1.1 or RFC3125. The policy OID is 1.2.3.4.5.1.

3.2.3 Generation of signature

Create signed data according to generation requirement of test design in the folder of each item under 01_CADES or 02 XADES

3.2.4 Requirement for file names of generated signature

File names in the test item directory should be used shown below.

- Generated signature file should be "sig.der" or "sig.xml".
- Necessary certificate and CRL for validation should be included in the each test item directory.
- It is recommended to save hash target, certificate and CRL under Data/ folder for reference, even they are not necessary for data validation.
- Record of file generation should be kept by updating ChangeLog.en.txt file for English and ChangeLog.ja.txt(SJIS coding) for Japanese.

3.2.5 Certificate that included in generation archive and name of CRL file

Generator should give verifier a guideline to accelerate automatic process with name of file which contains necessary data for validation of certificate.

Certificate of signer and counter signer shoud have the file name shown below.

CERT-SIG-EE.cer --- Signer Certificate (It varies from each companies)
CERT-SIG-EE-CS1.cer --- Counter signer certificate (common)
CERT-SIG-SUB1.cer --- sub CA certificate for signer certificate (common)
CERT-SIG-ROOT.cer --- root CA certificate for signer certificate (common)

CRL file is necessary for validation of signer certificate and counter signer certificate, should follow as shown below. The file should be created by generator of the signature.

CRLs for verifying end entity certificate are available online.
If CRLs are used offline, use files below.
CERT-SIG-SUB1.x.crl --- CRL that specifies issue time for signer
CERT-SIG-SUB1-CS1.x.crl --- CRL that specifies issue time for counter signer
(note) Do the same for other CA issued CRL such as root CA
(note) Use ".x.crl"extension for CRL that has issued in the past.

Name of the TSA certificate file should be shown below. It varies among the timestamp authorities to be used for the test. Also, it is available to make a copy from test item folder included in "ON-T-TSA" test case.

CERT-TSA-EE.cer	--- TSA certificate (depending on TSA)
CERT-TSA-SUB1.cer	--- sub CA certificate (depending on TSA)
CERT-TSA-ROOT.cer	--- root CA certificate (depending on TSA)

Following guideline shows name of files which is necessary for TSA certificate validation.

CERT-TSA-SUB1-ST1.x.crl	CRL to verify TSA used for signature timestamp
CERT-TSA-SUB1-ST1-CS1.x.crl	CRL to verify TSA used for signature timestamp of countersignature
CERT-TSA-SUB1-CT1.x.crl	CRL to verify TSA used for content timestamp
CERT-TSA-SUB1-DT1.x.crl	CRL to verify TSA used for AllDataObjectsTimeStamp
CERT-TSA-SUB1-IT1.x.crl	CRL to verify TSA used for IndividSualDataObjectsTimeStamp
CERT-TSA-SUB1-ROT1.x.crl	CRL to verify TSA used for RefsOnlyTimestamp or TimestampedCertsCRLs
CERT-TSA-SUB1-RST1.x.crl	CRL to verify TSA used for SigAndRefsTimestamp or ESCTimeStamp
CERT-TSA-SUB1-AT1.x.crl	CRL to verify TSA used for 1st ArchiveTimeStamp
CERT-TSA-SUB1-AT2.x.crl	CRL to verify TSA used for 2nd ArchiveTimeStamp
CERT-TSA-SUB1-AT3.x.crl	CRL to verify TSA used for 3rd ArchiveTimeStamp

Validation information of a signer certificate is recommended to store in Revocation Values. In that case, unnecessary certificates and CRL file for validation shoud not be included in test item directory.

3.2.6 Create compressed archive for generation result.

Create ZIP compressed archive with signatures and memos of the generation result and its procedures are shown below.

Record of file generation or modification should be kept by updating ChangeLog.en.txt file for English and ChangeLog.ja.txt(Japanese SJIS coding) placed under 01_CADES or 02_XADES directory.

Make copies of generated directory of 01_CADES or 02_XADES and apply the following name for the new directory.

[CADES or XADES]_[put into groups (1 or 2)]_[company name]_[Date of generation] (Example) CADES_1_ENTRUST_20071024

Create compressed archive of directory which was created with the procedures mentioned above.

Upload the archive file on ECOM electronic conference room.

3.2.7 Validate signature

Download the signature which has been generated by other participating companies. Validate the signature after being unpacked with 99_WORK.

3.3 Common requirements

At generation/validation interoperability test for signed data, indicates requirement in relation with generation of common signed data as well as validation.

Generation requirement			
	The application must generate successfully the CAdES format based on ETSI TS 101 733 or RFC3126.		Mandatory
	The application must generate successfully the CAdES format in cases where signer should use distributed test key and certificate for signature.		Mandatory
	Signature atributes, Non-signature attributes		
		Must include ContentType, MessageDigest	Mandatory
		Must include either ESSSigningCertificate or ESSSigningCertificateV2 or OtherSigningCertificate.	Mandatory
		Must include SignatureTimeStamp	Mandatory
		Other attributes may be included.	Option
	The application may choose voluntarily from 3 test use TSA .		Option
Validation requirement			
	The application should validate successfully the CAdES format based on ETSI TS 101 733 or RFC 3126.		Mandatory
	The application should validate successfully the CAdES format based on the CMS signature except for certification.		Mandatory
	The application should validate successfully the timestamp token except for signature validation.		Mandatory
	The application should validate successfully the signer certificate at the time when SignatureTimeStamp was generated		Mandatory

3.4 CAdES-T Signature basic test case (ON-T-BASIC)

3.4.1<ON-T-BASIC-ATTACHED>

The application should successfully generate and validate attached signature CAdES-T format with text file.

Based on common requirement		
Generation requirement		
	The application must generate successfully the CAdES-T which includes target data for signing into eContent field of encapContentInfo.	Mandatory
	Target data must be "./TARGET_AAA.txt"	Mandatory

3.4.2<ON-T-BASIC-DETACHED>

The application should successfully generate and validate detached signature CAdES-T with binary data file.

Based on <ON-T-BASIC-ATTACHED> requirement		
Generation requirement		
	The application must generate successfully the CAdES-T in cases where it generate detached signature which excludes target data for signing.	Mandatory
	Target data must be "./TARGET_BBB.bin".	Mandatory

3.5 CAdES-T Timestamp authority test case (ON-T-TSA)

3 timestamp services are available for the signature generation/interoperability test and each of them are provided by companies cooperated in the test. Choices of TSA are optional in the other tests. However, each TSA should be used for validation in this test case.

3.5.1 <ON-T-TSA-AMANO-ATTACHED>

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

The application should successfully generate and validate attached signature CAdES-T format in cases where using Amano Time Business test TSA.

Based on <ON-T-BASIC-ATTACHED>requirement.		
Generation requirement		
	The application must use Amano Time Business TSA.	Mandatory

3.5.2 <ON-T-TSA-PFU-ATTACHED>

The application should successfully generate and validate attached signature CAdES-T format in cases where using PFU test TSA.

Based on <ON-T-BASIC-ATTACHED>requirement		
Generation requirement		
	The application must use PFU TSA.	Mandatory

3.5.3 <ON-T-TSA-SEIKO-ATTACHED>

The application should successfully generate and validate attached signature CAdES-T format in cases where using SEIKO Precision test TSA.

Based on <ON-T-BASIC-ATTACHED>requirement.		
Generation requirement		
	The application must use SEIKO precision TSA.	Mandatory

3.6 CAdES-T Optional attribute test case (ON-T-ATTR)

In this test case, the application should validate successfully the CAdES-T format in cases where it has optional attribute in which can append to the format.

3.6.1 <ON-T-ATTR-SIGNINGTIME>

The application should generate/validate the CAdES-T format in cases where it has SigningTime attribute.

Based on <ON-T-BASIC-ATTACHED>requirement.			
Generation requirement			
	signed attribute		
		The application must generate CAdES-T data which includes SigningTime	Mandatory
		The application must generate SigningTime and timestamp based on the time order of ETSI TS 101 733 v1.7.3 C.3.6.	Mandatory
Vallidation requirement			
	The application must validate successfully the attached signature CAdES format based on the the time order of ETSI TS 101 733 v1.7.3 C.3.6.		Mandatory
	It is recommended to indicate the generation time of timestamp and SigningTime in some way.		Recoomended

3.6.2 <ON-T-ATTR-EPES-RFC3125>

The application should generate/validate successfully CAdES-T in cases where it has SignaturePolicyIdentifier which has conformance with ETSI TR 101 272 v1.1.1 or RFC3125

Based on <ON-T-BASIC-ATTACHED>requirement.			
Generation requirement			
	signed attribute		
		The application must generate CAdES-T data which includes SignaturePolicyIdentifier	Mandatory
		Signature policy must use “./TARGET-SIGPOL-RFC3125.der”	Mandatory
Validation requirement			
	The application must be validated based on “./TARGET-SIGPOL-RFC3125.der”.		Mandatory

3.6.3 <ON-T-ATTR-SIGNERLOCATION>

The application should generate/validate successfully CAdES-T in cases where it has SignerLocation.

Based on <ON-T-BASIC-ATTACHED>requirement		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes SignerLocation	Mandatory
Validation requirement		
	Existence of SignerLocation and description must be visually verified in some way.(*1)	Mandatory

(*1) Indication method could be any form such as log, dialog, window, etc.It applies to further instruction of the test in cases the "visual verification" is mentioned in the procedure.

3.6.4 <ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED>

The application should generate/validate successfully the CAdES-T format in cases where it has SignerAttributes include ClaimedAttributes.

Based on the <ON-T-BASIC-ATTACHED>Requirement		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes SignerAttributes which has Claimed Attribute.	Mandatory
	The application may generate CAdES-T data which includes SignerAttributes which has ClaimedAttributes.	Optional
Validation requirement		
	Existence of SignerAttributes and ClaimedAttributes as well as the description must be visually verified in some way.	Mandatory
	The application may omit CertifiedAttributes.	Optional

3.6.5 <ON-T-ATTR-CONTENTHINTS>

The application should generate/validate successfully the CAdES-T in cases where it has ContentHints.

Based on <ON-T-BASIC-ATTACHED>requirement.		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes content hints	Mandatory

Validation requirement		
	Existence of ContentHints and the description must be visually verified in some way.	Mandatory

3.6.6 <ON-T-ATTR-COMMITMENTTYPEINDICATION>

The application should generate/validate the CAdES-T in cases where it has CommitmentTypeIndication.

Based on <ON-T-BASIC-ATTACHED>reauirement		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes CommitmentTypeIndication.	Mandatory
Validation requirement		
	Existence of CommitmentTypeIndication and the description must be visually verified in some way.	Mandatory

3.6.7 <ON-T-ATTR-CONTENTTS-CLAIMEDTIME>

The application should generate/validate successfully the CAdES-T in cases where it has ContentTimeStamp and SigningTime property.

Based on <ON-T-BASIC-ATTACHED>requirement		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes ContentTimeStamp and SigningTime.	Mandatory
	The application must generate SigningTime and timestamp bases on the methodical relationship of ETSI TS 101 733 v1.7.3 C.3.6.	Mandatory
Validation requirement		
	The application must validate the methodical relationship of ETSI TS 101 733 v1.7.3C.3.6.	Mandatory
	Time of the timestamp and SigningTime are recommended to be expressed in some way.	Recommended

3.6.8 <ON-T-ATTR-CONTENTREFERENCE>

The application should generate/validate successfully the CAdES-T format in cases where it has contentReference.

Based on <ON-T-BASIC-ATTACHED>
Generation requirement

	signed attribute	
	The application must generate CAdES-T data which includes ContentReference.	Mandatory
Validation requirement		
	The application must verify consistency with signature referred by ContentReference, or visually verify the existence of ContentRefence and the referred content in some way.	Mandatory

3.6.9 <ON-T-ATTR-CONTENTIDENTIFIER>

The application should generate/validate the CAdES-T format in cases where it has ContentIdentifier.

Based on <ON-T-BASIC-ATTACHED>		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes ContentIdentifier.	Mandatory
Validation requirement		
	Existence of ContentIdentifier and the description must be visually verified in some way.	Mandatory

3.6.10 <ON-T-ATTR-COUNTERSIGNATURE>

The application should generate/validate successfully the CAdES-T format in cases where it has CounterSignature.

Based on <ON-T-BASIC-ATTACHED>requirement		
Generation requirement		
	signed attribute	
	The application must generate CAdES-T data which includes CounterSignature provided by Signer (EE-ON-SIG-ECOMSAMPLE-OK).	Mandatory
	The CounterSignature must include SignatureTimeStamp.	Mandatory
Validation requirement		
	CounterSignature must be verified as same as "Common requirements".	Mandatory

3.6.11 <ON-T-ATTR-ESSCERTV2>

The application should generate/validate successfully the CAdES-T in cases where it has ESSSigningCerftificateV2 attribute instead of other Signing Certificate attribute.

Based on <ON-T-BASIC-ATTACHED>requirement		
Generation requirement		
	signed attribute	

		ESSSigningCertificateV2 must be included	Mandatory
		The hash argorithm used in ESSSigningCertificateV2 must be stronger than SHA1.	Mandatory
		SHA-256 or SHA-512 is recommended for hash algorithm used in ESSSigningCertificateV2.	Recommended
Validation requirement			
	Signer certificate must be in accordance with ESSSigningCertificateV2.		Mandatory

3.7 CAdES-A Basic test case (ON-A-BASIC)

In this test case, the application should validate the CAdES-A format.

Test items in this test are shown below.

3.7.1 <ON-A-BASIC-A1-ATTACHED>

The application should generate/validate successfully the 1st generation attached signature CAdES-A format.

Based on <ON-T-BASIC-ATTACHED>			
Generation requirement			
	unsigned attribute		
		CertificateValues and CompleteCertificateRefs that have necessary information for validation of signature certificate must be included.	Mandatory
		One ArchiveTimeStamp whose calculation method is based on ETSI TS 101 733 v1.7.3 must be included.	Mandatory
		It is recommended that the validation information (certificates, CRLs) archives for TSA certificates are included in the "certificates" and "crls" field of timestamp token.	Recommended
		Validation information must be saved in the same directory with signed data of generation result if validation information of TSA certificate is not included into timestamp token fields.	Mandatory
Validation requirement			
	The signer certificate must be validated by using validation information such as CertificateValues,RevocationValues, CompleteCertificateRefs and CompleteRevocationRefs at the point in time that indicated by SignatureTimeStamp.		Mandatory
	It is recommended to use the validation information if it was in the timestamp token.		Recommended

3.7.2 <ON-A-BASIC-A1-DETACHED>

The application should generate/validate successfully CAdES-A format which has one archive timestamp based on ETSI TS 101 733 v1.7.3 with detached signature.

Based on <ON-T-BASIC-DETACHED>			
Generation requirement			
	unsigned attribute		
		CertificateValues and CompleteCertificateRefs that have necessary information for validation of signature certificate must be included.	Mandatory
		One ArchiveTimeStamp whose calculation method is based on ETSI TS 101 733 v1.7.3 must be included.	Mandatory
		It is recommended that the validation information (certificates, CRLs) archives for TSA certificates are included in the "certificates" and "crls" field of timestamp token.	Recommended
		Validation information must be saved in the same directory with signed data of generation result if validation information of TSA certificate is not included into timestamp token fields.	Mandatory
Validation requirement			
	The signer certificate must be validated by using validation information such as CertificateValues,RevocationValues, CompleteCertificateRefs and CompleteRevocationRefs at the point in time that indicated by SignatureTimeStamp.		Mandatory
	It is recommended to use the validation information if it was in the timestamp token.		Recommended

3.7.3 <ON-A-BASIC-A2-ATTACHED>

The application should generate/validate successfully CAdES-A format which has two archive timestamps based on ETSI TS 101 733 v1.7.3 with attached signature.

..

Based on ON-A-BASIC-A1-ATTACHED			
Generation requirement			
	unsigned attribute		
		The application must generate CAdES-A data which includes two ArchiveTimeStamps which have hash calculation method based on ETSI TS 101 733 v1.7.3.	Mandatory
		It is recommended that the interval between timestamps should be more than one day.	Recommended

3.7.4 <ON-A-BASIC-A3-ATTACHED>

The application should generate/validate successfully CAdES-A format which has 3 archive timestamps based on ETSI TS 101 733 v1.7.3 with attached signature.

Based on< ON-A-BASIC-A2-ATTACHED>		
Generation requirement		
	unsigned attribute	

		The application must include 3 ArchiveTimeStamps which has hash calculated method based on ETSI TS 101 733v1.7.3.	Mandatory

3.8 CAdES-A Optional attributes test case (ON-A-ATTR)

3.8.1 <ON-A-ATTR-A1-ARCTSV1-ATTACHED>

The application should generate/validate successfully CAdES-A format which has one archive timestamp based on RFC 3126 or ETSI TS 101 733 v1.4.0.

Based on <ON-A-BASIC-A1-ATTACHED>			
Generation requirement			
	unsigned attribute		
		ArchiveTimeStamp of old version which was regulated in the ETSI TS 101 733v1.4.0 must be included instead of ETSI TS 101 733 v1.7.3 ArchiveTimeStampV2.	Mandatory
		SignaturePolicyIdentifier. must be included.	Mandatory
		The application must use “/TARGET-SIGPOL-RFC3125.der” for signature policy.	Mandatory
Validation requirement			
	The application must validate ArchiveTimeStamp of old version which is based on RFC 3126 or ETSI TS 101 733 v1.4.0.		Mandatory
	The application must validate based on signature policy "./TARGET-SIGPOL-RFC3125.der".		Mandatory

3.8.2 <ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS>

The application should generate/validate successfully CAdES-A format which has TimestampedCertsCRLs.

Based on <ON-A-BASIC-A1-ATTACHED>			
Generation requirement			
	unsigned attribute		
		TimestampedCertsCRLs which is based on ETSI TS 101 733 v1.7.3 must be included.	Mandatory
Validation requirement			
	The application must validate TimestampedCertsCRLs based on ETSI TS 101 733 v1.7.3.		Mandatory

3.8.3 <ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS>

The application should generate/validate successfully CAdES-A format which has ESCTimeStamp.

Based on <ON-A-BASIC-A1-ATTACHED>		
Generation requirement		
	Unsigned attribute	
	ESCTimeStamp which is based on ETSI TS 101 733 v1.7.3 must be included.	Mandatory
Validation requirement		
	The application must validate ESCTimeStamp which is based on ETSI TS 101 733 v1.7.3.	Mandatory

3.9 In case the participants do not have internet connection environment for validation.

You may download the file in the http//ecom-es-test.ath.cx/repository/ for validation whenever possible, if unable to access the internet with HTTP(TCP/80) during the test.

4 Appendix: Test data profile

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

4.1 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.

4.1.1 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier 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, SHA-1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

4.1.2 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier of the signer's certificate
digestAlgorithm	SHA1
signedAttrs	Present
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	Present
sigPolicyId	Present(SHA-1fingerprint)
eSSSigningCertificate	Present (issuer name, serial number, SHA-1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

4.1.3 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier 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, SHA-1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile.

4.1.4 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier 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, SHA-1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile.(including validation data)
completeCertificateRef	According to the ECOM profile
completeRevocationRe	According to the ECOM profile
certificateValues	According to the ECOM profile
revocationValues	According to the ECOM profile

4.1.5 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier 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, SHA-1 fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	Present
signatureTimeStamp	The token is according to the test data profile.(including validation data)
completeCertificateRef	According to the ECOM profile
completeRevocationRe	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.

4.1.6 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	160bit
version	v3(3)
sid	Same as the value of the subjectKeyIdentifier 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, SHA-1 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
completeRevocationRef	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.

4.2 Profile of timestamp tokens used for the tests

4.2.1 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 defined below.
certificates	TSA cetificate and path may be included as validation data in accordance with the ECOM profile
crls	All CRLs may be included as vlaidation data in accordance with the ECOM profile
signerInfos	Present (number of elements = 1)
signerInfo	160bit
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, SHA-1fingerprint)
signatureAlgorithm	SHA1withRSA
signature	Signature value
unsignedAttrs	None

4.2.2 TSTInfo

Field	Value
version	v1(1)
policy	TSAPolicyId=0.1.2.3.4.5
messageImprint	Present
hashAlgorithm	SHA1
hashedMessage	160bit
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(fiexed)
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.

4.3 Profile of certificates used in the tests

4.3.1 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 0:00:00 and 2035.12.31 23:59:59)
subject DN	PrintableString
public key information	Present
X.509 extension	Present
keyUsage	Present

4.3.2 RootCA certificate profile

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

4.3.3 SubCA certificate profile

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

4.3.4 Profile of End Entity certificate for the signer

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

4.3.5 TSA certificate profile

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

4.3.6 Profile of RootCA certificate for the online TSA

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

4.3.7 Online TSA certificate profile

Field	Value	Critical
version	V3	
serial number	Present	
signature algorithm	SHA1withRSA	
issuerDN	PrintableString	
validity period	UTCTime	
subject DN	PrintableString	
public key information	1024bit	
X.509 extension	Present	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	Present SHA1-160bit	FALSE
authorityKeyIdentifier	Present	FALSE
keyIdentifier	Present SHA1-160bit	-
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	-

4.3.8 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

4.4 Profile of signature profile used for the offline test.

Field	Value
signPolicyHashAlg	SHA1
signPolicyInfo	Present
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c
fieldOfApplication	"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]	
ttsCertificateTrustTrees[0]?	CA certificate for TSA
ttsRevReq[1]?	EE=crlCheck(0), CA=crlCheck(0)
attributeTrustCondition[3]	None
algorithmConstraintSet[4]	None
commitmentRules	Empty Sequence
signPolExtensions	None
signPolExtensions	None
signPolicyHash	None

4.5 Profile of signature profile used for the online test.

Field	Value
signPolicyHashAlg	SHA1
signPolicyInfo	Present
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c
fieldOfApplication	"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=eitherCheck(3), CA=eitherCheck(3)
timeStampTrustCondition[2]	None
attributeTrustCondition[3]	None
algorithmConstraintSet[4]	None
commitmentRules	Empty Sequence
signPolExtensions	None
signPolExtensions	None
signPolicyHash	None