# ECOM CAdES/XAdES Plugtest 2007<br>XAdES Test Specification

October 2007
V1.2

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

# Contents

# 1. Introduction

This document describes the details of tests on the XAdES long-term signature format conducted in relation to the long-term signature format interoperability test project carried out by the Electronic Signature Promotion Working Group of the Security Working Group of ECOM.

## 1.1. Conventions used in this document

The typographic and usage conventions for this document are displayed below (Table 1).

Table 1: Typographic and usage conventions

| Text | Description |
|---|---|
| <...> | Text item |
| <...OK> | Text item for which the expected test result is "valid" |
| <...NG> | Text item for which the expected test result is "invalid" |
| [...] | Reference materials |

## 1.2. Test structure

The test structure used is the same as that detailed in the CAdES Test Case Specification.

# 2. Offline common data verification test category

Using common XAdES format data based on the ECOM profile, we test whether it is correctly verified on the tester's system and products. Using XAdES format data (XAdES-T, XAdES-A), certificates, CRLs, and signed data generated by test tools, we check whether test results conform to expected test values.

## 2.1. Test preparation

The following preparations are necessary when performing the tests:

- CRL settings
  When obtaining a CRL online at the time of certificate verification, the Internet connection environment for the verification 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

This section describes the settings and conditions in place at the time of implementing the tests.

- Signed data settings
  For the internal signature type, the signed data was set to the character string, "aaa", and the signed data was specified using the enveloping XML signature form. However, since it is encapsulated in the XML signature's Object element, the test string is base64 encoded (YWFh). List 1 shows an example of an XML document when the internal signature type is used.

List 1: Example of an XML document when the internal signature type is used

```
<?xml version="1.0" encoding="UTF-8" ?>
<ds:Signature Id="Signature-ID1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>......</ds:SignedInfo>
  <ds:SignatureValue>......</ds:SignatureValue>
  <ds:KeyInfo>......</ds:KeyInfo>
  <ds:Object Encoding="http://www.w3.org/2000/09/xmldsig#base64"
               Id="signdata">YWFh</ds:Object>
  <ds:Object xmlns:xa="http://uri.etsi.org/01903/v1.3.1#">......</ds:Object>
</ds:Signature>
```

The "aaa" character string, base64 encoded

For detached signatures, a file named 'TARGET_BBB.bin' is set (this is a binary file with the sequence 0x01-0x09, 0x00 repeated up to 1024000 bytes).

- Verification time settings
  Verification time is different for each format. Verification time is set in accordance with the format. The range of current times for which verification is possible is from UTC 1.1.2002 00:00:00 to UTC 2035.12.31 23:59:59, and each certificate and CRL is set so that verification over this range is possible.

- Set up of the long-term signature format data to be verified
  In the test suite, the long-term signature format test data to be verified is stored in a file named "<test_case_name>-V131.xml", and files are stored in a separate directory for each test item.

- Verification
  This was implemented for all test items. The base64 encoded hash values of the signed data are as follows:

| | |
|---|---|
| "aaa": | **fiQN50+x7Qj6CNOAY/amqRRiqBU=** |
| TARGET_BBB.bin: | **gpGOa0wroxRJGyeXw7tHFbrgtxM=** |

## 2.3. Test data conformance

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

## 2.4. XAdES-T format standard tests

### 2.4.1. <XAdEST-ATTACH-NORMAL-OK 10001>

If the signing certificate and the TSA certificate of the signature time-stamp are within the validity period and have not been revoked, then the XAdES-T data is verified as being valid. Table 2 shows the expected test value, and test parameters for time, certificates, and CRLs used when testing.

Table 2: Expected test value and test parameters for
< XAdEST -ATTACH-NORMAL-OK 10001>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.3 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.2 00:00:00 - 2001.1.3 23:59:59 |

### 2.4.2. < XAdEST -ATTACH-EXPIERED-NG 10002>

If the TSA certificate of the signature time-stamp is valid, but the signature time-stamp was attached when the signature certificate had expired, and the signing certificate is not listed on the CRL used for verification, then the XAdES data is verified as invalid. Table 3 shows the expected test value, and test parameters for time, certificates, and CRLs used when testing.

Table 3: Expected test value and test parameters for
< XAdEST -ATTACH-EXPIERED-NG 10002>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.3 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.3 12:00:00 |
| Validity period of signing certificate | 2001.1.1 00:00:00 - 2001.1.1 23:59:59 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2000.1.2 23:59:59 |

| Expected value | Invalid |
|---|---|
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.1 00:00:00 - 2035.12.31 23:59:59 |

### 2.4.3. < XAdEST -ATTACH-REVOKED-NG 10003>

If the signing certificate and the TSA certificate of the signature time-stamp are within the period of validity, and the signing certificate is revoked and listed on the CRL based on the time of the signing time attribute and the signature time-stamp, the ES-T data is verified as invalid. Table 4 shows the expected test value, and test parameters for time, certificates, and CRLs used when testing.

Table 4: Expected test value and test parameters for
< XAdEST -ATTACH-REVOKED-NG 10003>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.2 12:00:00 |
| Value of signing time property | 2001.1.2 12:00:00 |
| Signature time-stamp | 2001.1.2 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.4 00:00:00 - 2001.1.4 23:59:59 |
| Revocation time on the signing certificate CRL | 2005.1.1 12:00 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2001.1.4 23:59:59 |
| 2.4.4. Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |

### 2.4.4. < XAdEST -ATTACH-SIGTS-REVOKED-NG 10005>

If the signing certificate and the TSA certificate of the signature time-stamp are within the period of validity, and the signing certificate is not revoked based on the time of the signing time attribute, but is revoked and listed on the CRL based on the signature time-stamp, then the signing time is ignored, and certificate validity is determined based on the signature time-stamp. The ES-T data is therefore verified as invalid.

Table 5: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTS-REVOKED-NG 10005>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.3 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.4 00:00:00 - 2001.1.4 23:59:59 |

| Expected value | Invalid |
|---|---|
| Revocation time on the signing certificate CRL | 2005.1.2 12:00:00 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2001.1.4 23:59:59 |

### 2.4.5. < XAdEST -ATTACH-ES-SIG-REVOKED-NG 10006>

If the signature value in the signature field of the SignerInfo in the ES-T format CMS SignedData has been forged, then the certificate is verified as invalid.

Table 6: Expected test value and test parameters for
< XAdEST -ATTACH-EE-SIG-FORGED-NG 10006>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 1.4.2002 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |

### 2.4.6. < XAdEST -ATTACH-SIGTS-SIG-FORGED-NG 10007>

If the signature value in the signature field of the SignerInfo in the CMS SignedData strucutre of the TimeStampToken given in the ES-T format SignatureTimeStamp attribute has been forged, then the signature is verified as invalid.

Table 7: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTS-SIG-FORGED-NG 10007>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |

### 2.4.7. < XAdEST -ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

If the value of the MessageDigest attribute within the signedAttributes of the ES-T format CMS SignedData has been forged, then the signature is verified as invalid.

Table 8: Expected test value and test parameters for
< XAdEST -ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |

### 2.4.8. < XAdEST -ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

If the value of the MessageDigest attribute within the signedAttributes of the time-stamp token contained in the ES-T format SignatureTimeStamp attribute has been forged, then the certificate is verified as invalid.

Table 9: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |

### 2.4.9. < XAdEST -DETACH-NORMAL-OK 10010>

ES-T format data in a document signed by a detached signature is verified as valid.

Table 10: Expected test value and test parameters for
< XAdEST -DETACH-NORMAL-OK 10010>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | Property not present |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |

| Expected value | Valid |
|---|---|
| Signature time-stamp TSA certificate verification CRL | 2001.1.1 00:00:00 - 2001.1.2 23:59:59 |

## 2.5 ES-T format optional test

### 2.5.1 < XAdEST -ATTACH-SIGTIME-REVOKED-OK 10004>

If the signing certificate and the TSA certificate of the signature time-stamp are within the period of validity, and the signing certificate is not revoked based on the time of the signature time-stamp, but is revoked and listed on the CRL at the time given in the signing time attribute, then the signing time is ignored and validity is determined based on the signature time-stamp. The ES-T data is therefore verified as valid. Table 11 shows the expected test value, and test parameters for time, certificates, and CRLs used when testing.

Table 11: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTIME-REVOKED-OK 10004>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Value of signing time property | 2001.1.4 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Revocation time on the signing certificate CRL | 2005.1.2 12:00:00 |

## 2.6 ES-A format standard tests

### 2.6.1. < XAdESA1-ATTACH-NORMAL-OK 70001>

An ES-A format with one archive time-stamp based on the ECOM XAdES long-term signature format profile is verified as valid.

Table 12: Expected test value and test parameters for
< XAdESA 1-ATTACH-NORMAL-OK 70001>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |

| Expected value | Valid |
|---|---|
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp 1 | 2001.1.3 12:00 |
| TSA certificate for archive time-stamp 1 | 2001.1.1 - 2035.12.31 |
| Archive time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.2. < XAdESA1-DETACH-NORMAL-OK 70002>

An ES-A format with one archive time-stamp based on the ECOM XAdES long-term signature format profile for a detached XML signature is verified as valid.

Table 13: Expected test value and test parameters for
< XAdESA 1-DETACH-NORMAL-OK 70002>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| Signature time-stamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp 1 | 2001.1.3 12:00 |
| TSA certificate for archive time-stamp 1 | 2001.1.1 - 2035.12.31 |
| Archive time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.3. <XAdESA1-ATTACH-ATS-MI-UNMATCH-NG 70011>

If the value of the MessageDigest attribute within the archive timestamp has been forged, then the XAdES-A data (attached) is verified as invalid.

Table 14: Expected test value and test parameters for
< XAdESA1-ATTACH-ATS-MI-UNMATCH-NG 70011>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.4 < XAdESA1-DETACH-ATS-MI-UNMATCH-NG 70012>

If the value of the MessageDigest attribute within the archive timestamp has been forged, then the XAdES-A data (detached) is verified as invalid.

Table 15: Expected test value and test parameters for
< XAdESA1-DETACH-ATS-MI-UNMATCH-NG 70012>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.5 < XAdESA2-ATTACH-ATS-NORMAL-OK 70013>

An ES-A format with two archive time-stamp based on the ECOM XAdES long-term signature format profile for an attached XML signature is verified as valid.

Table 16: Expected test value and test parameters for
< XAdESA2-ATTACH-ATS-NORMAL-OK 70013>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Archive time-stamp 2 | 2001.1.4 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp 1 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2002.1.3 23:59:59 |
| Archive time-stamp 2 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.6 < XAdESA2-ATTACH-ATS-MI-UNMATCH-NG 70014>

An ES-A format with two archive time-stamp based on the ECOM XAdES long-term signature format profile for an attached XML signature is verified as invalid. MessageImprint of the 2nd archive time-stamp has been forged.

Table 17: Expected test value and test parameters for
< XAdESA2-ATTACH-ATS-MI-UNMATCH-NG 70014>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Archive time-stamp 2 | 2001.1.4 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp 1 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2002.1.3 23:59:59 |

| | |
|---|---|
| Archive time-stamp 2 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.7 < XAdESA2-DETACH-NORMAL-OK 70015>

An ES-A format with two archive time-stamp based on the ECOM XAdES long-term signature format profile for a detached XML signature is verified as valid.

Table 18: Expected test value and test parameters for
< XAdESA2-DETACH-NORMAL-OK 70015>

| Expected value | Valid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Archive time-stamp 2 | 2001.1.4 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |
| Archive time-stamp 1 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2002.1.3 23:59:59 |
| Archive time-stamp 2 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

### 2.6.8 < XAdESA2-DETACH-ATS-MI-UNMATCH-NG 70016>

An ES-A format with two archive time-stamp based on the ECOM XAdES long-term signature format profile for a detached XML signature is verified as invalid. MessageImprint of the 2nd archive time-stamp has been forged.

Table 19: Expected test value and test parameters for
< XAdESA2-DETACH-ATS-MI-UNMATCH-NG 70016>

| Expected value | Invalid |
|---|---|
| Signing time used | 2001.1.1 12:00:00 |
| Signature time-stamp | 2001.1.1 12:00:00 |
| Archive time-stamp 1 | 2001.1.3 12:00:00 |
| Archive time-stamp 2 | 2001.1.4 12:00:00 |
| Validity period of signing certificate | 2001.1.1 - 2035.12.31 |
| Verification CRL for the signing certificate | 2001.1.2 00:00:00 - 2001.1.2 23:59:59 |
| timestamp TSA certificate | 2001.1.1 - 2035.12.31 |
| Signature time-stamp TSA certificate verification CRL | 2001.1.3 00:00:00 - 2001.1.3 23:59:59 |

| | |
|---|---|
| Archive time-stamp 1 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2002.1.3 23:59:59 |
| Archive time-stamp 2 TSA certificate verification CRL | 2001.1.4 00:00:00 - 2035.12.31 23:59:59 |

## 2.7. XAdES-T standard test case

In this section, the test case that should be satisfied by an implementation of the XAdES-T format are shown.

### 2.7.1. <OFF-T-1>

| Test case name | OFF-T-1 |
|---|---|
| Basic ES-T format of an attached signature read-in properly. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |

### 2.7.2. <OFF-T-2>

| Test case name | OFF-T-2 |
|---|---|
| Expiry of a XAdES-T format signing certificate properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10002 | XAdEST-ATTACH-EXPIRED-NG |

### 2.7.3. <OFF-T-3>

| Test case name | OFF-T-3 |
|---|---|
| Revocation of a XAdES-T format signing certificate properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10003 | XAdEST-ATTACH-REVOKED-NG |

### 2.7.4. <OFF-T-4>

| Test case name | OFF-T-4 |
|---|---|
| Verification of the certification path of a XAdES-T format signing certificate properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10002 | XAdEST-ATTACH-EXPIRED-NG |
| 10003 | XAdEST-ATTACH-REVOKED-NG |

### 2.7.5. <OFF-T-5>

| Test case name | OFF-T-5 |
|---|---|
| Regardless of the signing time on a XAdES-T format signing certificate, revocation is verified based on the signature time-stamp. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |

| | |
|---|---|
| 10002 | XAdEST-ATTACH-EXPIRED-NG |
| 10003 | XAdEST-ATTACH-REVOKED-NG |
| 10004 | XAdEST-ATTACH-SIGTIME-REVOKED-OK |
| 10005 | XAdEST-ATTACH-SIGTS-REVOKED-NG |

### 2.7.6. <OFF-T-6>

| Test case name | OFF-T-6 |
|---|---|
| Forgery of signature values in the Signature element for the XAdES-T format detected. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10006 | XAdEST-ATTACH-ES-SIG-FORGED-NG |

### 2.7.7. <OFF-T-7>

| Test case name | OFF-T-7 |
|---|---|
| Forgery of signature values in the SignerInfo of a signature time-stamp for the XAdES-T format detected. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10007 | XAdEST-ATTACH-SIGTS-FORGED-NG |

### 2.7.8. <OFF-T-8>

| Test case name | OFF-T-8 |
|---|---|
| Forgery of the hash value in the DigestValue element for the XAdES-T format detected. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10008 | XAdEST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG |

### 2.7.9. <OFF-T-9>

| Test case name | OFF-T-9 |
|---|---|
| Forgery of the hash value in the MessageDigest of a signature time-stamp token for the XAdES-T format detected. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10001 | XAdEST-ATTACH-NORMAL-OK |
| 10009 | XAdEST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG |

### 2.7.10. <OFF-T-10>

| Test case name | OFF-T-10 |
|---|---|
| Detached signatures for the XAdES-T format properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 10010 | XAdEST-DETACH-NORMAL-OK |

## 2.8. XAdES-A standard test case

### 2.8.1. <OFF-A-1>

| Test case name | OFF-A-1 |
|---|---|
| 1st generation ES-A format with attached signature based on the ECOM profile properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 70001 | XAdESA1-ATTACH-NORMAL-OK |

### 2.8.2. <OFF-A-2>

| Test case name | OFF-A-2 |
|---|---|
| 1st generation ES-A format with detached signature based on the ECOM profile properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 70002 | XAdESA1-DETACH-NORMAL-OK |
| 70012 | XAdESA1-DETACH-ATS-MI-UNMATCH-NG |

### 2.8.3. <OFF-A-3>

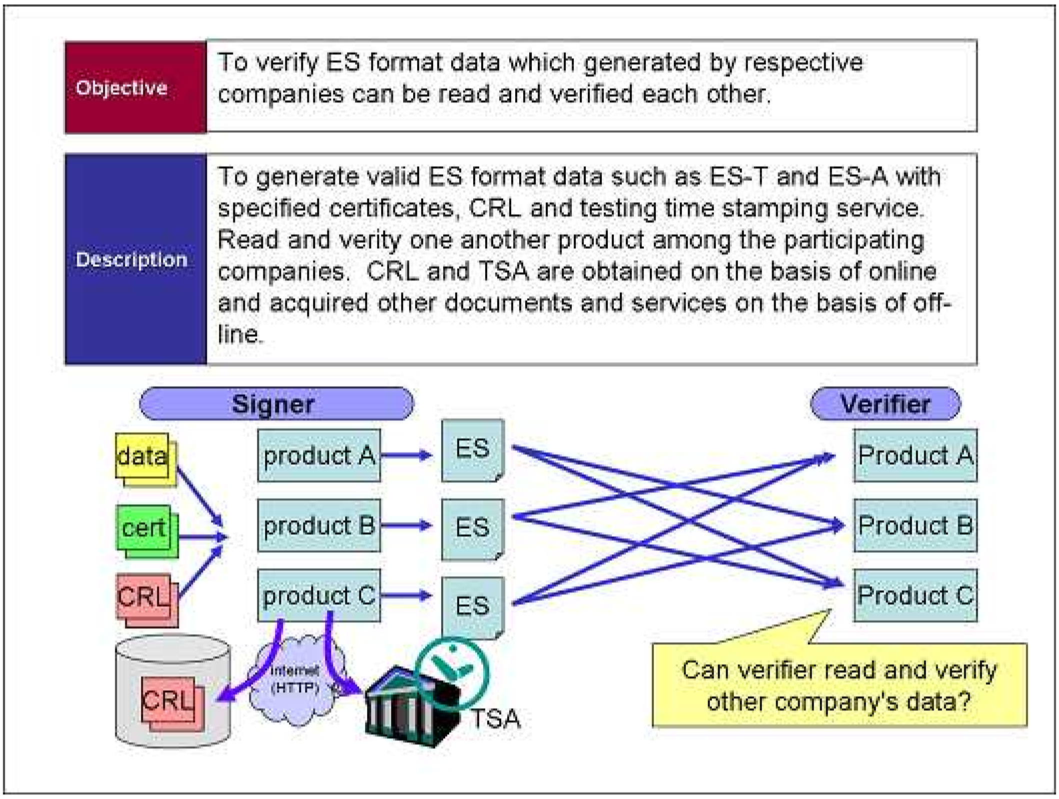
| Test case name | OFF-A-3 |
|---|---|
| 2nd generation ES-A format with attached signature based on the ECOM profile properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 70013 | XAdESA2-ATTACH-NORMAL-OK |
| 70014 | XAdESA2-ATTACH-ATS-MI-UNMATCH-NG |

### 2.8.4. <OFF-A-4>

| Test case name | OFF-A-3 |
|---|---|
| 2nd generation ES-A format with detached signature based on the ECOM profile properly handled. | |
| Conditions of success: All of the following test items return the expected values. | |
| 70015 | XAdESA2-DETACH-NORMAL-OK |
| 70016 | XAdESA2-DETACH-ATS-MI-UNMATCH-NG |

# 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 (XAdES-T, XAdES-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 XAdES-T and XAdES-A that are requirement for JIS and has been broadly exchanged.



Objective: To verify ES format data which generated by respective companies can be read and verified each other.

Description: To generate valid ES format data such as ES-T and ES-A with specified certificates, CRL and testing time stamping service. Read and verity one another product among the participating companies. CRL and TSA are obtained on the basis of online and acquired other documents and services on the basis of off-line.

Figure 3-1: Online matrix generation/verification test

## 3.1. Outline of test case

The test item is classified into 5 test case.

- XAdES-T Basic test case
  Enveloping, Enveloped, Detached signature with signature timestamp.

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

- XAdES-T Optional property test case
  This application should validate successfully the QualifyingProperty which can be stored in XAdES-T.

- XAdES-A Basic test case
  This is a basic archive signature test, and the application should validate successfully the attached signature and archivetimestamp which is more than one generation.

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

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

Table 20: Test items of Signed data generation/validation interoperability test

| | |
|---|---|
| XAdES-T Basic test case(ON-T-BASIC) | |
| ON-T-BASIC-ENVELOPING | Enveloping XML signature with signature timestamp |
| ON-T-BASIC-DETACHED | Detached XML signature with signature timestamp |
| ON-T-BASIC-ENVELOPED | Enveloped XML signature with signature timestamp |
| XAdES-T Timestamp auhtority testc cases (ON-T-TSA) | |
| ON-T-TSA-AMANO-ENVELOPING | Use AMANO TSA |
| ON-T-TSA-PFU-ENVELOPING | Use PFU TSA |
| ON-T-TSA-SEIKO-ENVELOPING | Use SEIKO TSA |
| XAdES-T Optional property test case (ON-T-PROP) | |
| ON-T-PROP-SIGNINGTIME | Use SigningTime |
| ON-T-PROP-EPES-FREEXML | Use SignaturePolicyIdentifierand and XML free format policy file |
| ON-T-PROP-EPES-TR102038-V111 | Use SignaturePolicyIdentifier and XML Signature Policy based on the ETSI TR 102 038 v1.1.1. |
| ON-T-PROP-SIGNATUREPRODUCTIONPLACE | Use SignatureProductionPlace. |
| ON-T-PROP-SIGNERROLE-CLAIMED | Use SignerRolewhich has ClaimedRole. |
| ON-T-PROP-DATAOBJECTFORMAT | Use DataObjectFormat. |
| ON-T-PROP-COMMITMENTTYPEINDICATION | Use CommitmentTypeIndication. |
| ON-T-PROP-ALLDATATS-CLAIMEDTIME | Use AllDataObjectsTimeStamp and SigningTime. |
| ON-T-PROP-INDVDATATS-CLAIMEDTIME | Use IndividualDataObjectsTimeStamp and SigningTime |
| ON-T-PROP-COUNTERSIGNATURE | Use CounterSignature |
| ON-T-PROP-SIGNINGCERTIFICATE | Use SigningCertificate |
| XAdES-A Basic test case (ON-A-BASIC) | |

| | |
|---|---|
| ON-A-BASIC-A1-ENVELOPING | Enveloping signature without Refs and one ArchiveTimeStamp is appended. |
| ON-A-BASIC-A1-DETACHED | Detached signature without Refs and one ArchiveTimeStamp is appended. |
| ON-A-BASIC-A1-ENVELOPED | Enveloped signature without Refs and one ArchiveTimeStamp is appended. |
| ON-A-BASIC-A2-ENVELOPING | Append two ArchiveTimeStamps |
| ON-A-BASIC-A3-ENVELOPING | Append three ArchiveTimeStamps |
| XAdES-A Optional property test case (ON-A-PROP) | |
| ON-A-PROP-A1-REFS | Append Refs, ArchiveTimeStamp |
| ON-A-PROP-A1-REFS-REFSONLYTS | Append Refs, RefsOnlyTimeStamp, ArchivfeTimeStamp. |
| ON-A-PROP-A1-REFS-SIGANDREFSTS | Append Refs, SigAndRefsTimeStamp, ArchiveTimeStamp |

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

Table 21: List of test items of signed data generation/verification interoperability test

| TEST CASE ID | | ON-T-BASIC ENVELOPING | ON-T-BASIC DETACHED | ON-T-BASIC ENVELOPED | ON-T-TSA AMANO-ENVELOPING | ON-T-TSA PFU-ENVELOPING | ON-T-TSA SEIKO-ENVELOPING | ON-T-PROP SIGNINGTIME | ON-T-PROP EPES-FREEXML | ON-T-PROP EPES-TR102038-V111 | ON-T-PROP SIGNATUREPRODUCTIONPLACE | ON-T-PROP SIGNERROLE-CLAIMED | ON-T-PROP DATAOBJECTFORMAT | ON-T-PROP COMMITMENTTYPEINDICATION | ON-T-PROP ALLDATATS-CLAIMEDTIME | ON-T-PROP INDVDATATS-CLAIMEDTIME | ON-T-PROP COUNTERSIGNATURE | ON-T-PROP SIGNINGCERTIFICATE | ON-A-BASIC A1-ENVELOPING | ON-A-BASIC A1-DETACHED | ON-A-BASIC A1-ENVELOPED | ON-A-BASIC A2-ENVELOPING | ON-A-BASIC A3-ENVELOPING | ON-A-PROP A1-REFS | ON-A-PROP A1-REFS-REFSONLYTS | ON-A-PROP A1-REFS-SIGANDREFSTS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Signed Signature Properties | SigningTime | | | | | | | ✓ | | | | | | | ✓ | ✓ | | | | | | | | | | |
| | SigningCertificate | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | ✓ | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 |
| | KeyInfo.X509Data.X509Cert with Ref | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 | | C1 | C1 | C1 | C1 | C1 | C1 | C1 | C1 |
| | SignaturePolicyIdentifier | | | | | | | | ✓ | ✓ | | | | | | | | | | | | | | | | |
| | SignatureProductionPlace | | | | | | | | | | ✓ | | | | | | | | | | | | | | | |
| | SignerRole | | | | | | | | | | | ✓ | | | | | | | | | | | | | | |
| Signed Data Object Properties | DataObjectFormat | | | | | | | | | | | | ✓ | | | | | | | | | | | | | |
| | CommitmentTypeIndication | | | | | | | | | | | | | ✓ | | | | | | | | | | | | |
| | AllDataObjectsTimeStamp | | | | | | | | | | | | | | ✓ | | | | | | | | | | | |
| | IndividualDataObjectsTimeStamp | | | | | | | | | | | | | | | ✓ | | | | | | | | | | |
| Unsigned Signature Properties | CounterSignature | | | | | | | | | | | | | | | | ✓ | | | | | | | | | |
| | SignatureTimeStamp | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | CompleteCertificateRefs | | | | | | | | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ |
| | CompleteRevocationRefs | | | | | | | | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ |
| | AttributeCertificateRefs | | | | | | | | | | | | | | | | | | | | | | | | | |
| | AttributeRevocationRefs | | | | | | | | | | | | | | | | | | | | | | | | | |
| | SigAndRefsTimeStamp | | | | | | | | | | | | | | | | | | | | | | | | | ✓ |
| | RefsOnlyTimeStamp | | | | | | | | | | | | | | | | | | | | | | | | ✓ | |
| | CertificateValues | | | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | RevocationValues | | | | | | | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | AttrAuthoritiesCertValues | | | | | | | | | | | | | | | | | | | | | | | | | |
| | AttributeRevocationValues | | | | | | | | | | | | | | | | | | | | | | | | | |
| | ArchiveTimeStamp | | | | | | | | | | | | | | | | | | 1 | 1 | 1 | 2 | 3 | 1 | 1 | 1 |
| Unsigned Data Object Property | | | | | | | | | | | | | | | | | | | | | | | | | | |

C?: Choice

## 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 use 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 should 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 should 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 XAdES format based on ETSI TS 101 903 v1.3.2. | | Mandatory |
| | The application must generate successfully the XAdES format in cases where signer should use distributed test key and certificate for signature. | | Mandatory |
| | Property in QualifyingProperties | | |
| | | SignatureTimeStamp must be included. | Mandatory |
| | | SigningCertificate or X509Data.X509Certificate in KeyInfo must be included. The KeyInfo must be referred by SignedInfo.Reference. | Mandatory |
| | | Other properties may be included.(*1) | Option |
| | The application may choose TSA voluntarily from 3 test use TSA . | | Option |
| Validation requirement | | | |
| | The application should validate successfully the XAdES format based on ETSI TS 101 903 v1.3.2.. | | Mandatory |
| | The application should validate successfully the XAdES format based on the XML signature except for certificate path validation. | | Mandatory |
| | The application should validate timestamp token except for certificate path validation. | | Mandatory |
| | The application should validate successfully the signature certificate at the time when SignatureTimeStamp was generated | | Mandatory |

(*1)Note: In the other test items you can add other property as long as the provision requirements are fulfilled. For example, a generated signed data which is designed to include more than one property

## 3.4. XAdES-T Signature basic test case (ON-T-BASIC)

### 3.4.1 <ON-T-BASIC-ENVELOPING>

The application should successfully generate and validate enveloping signature XAdES-T format with text file.

| | | |
|---|---|---|
| Based on the common requirement | | |
| Generation requirement | | |
| | The application must generate enveloping signature. | Mandatory |
| | Target data must be "./TARGET_AAA.txt" | Mandatory |
| | SignedInfo.Reference | |

| | | | |
|---|---|---|---|
| | | The target data must be de:Object. | Mandatory |
| | Transform of Reference in the target data is recommended to be Base64. | | Recommended |

### 3.4.2 <ON-T-BASIC-DETACHED>

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

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirements | | | |
| Generation requirement | | | |
| | The application must generate detached signature. | | Mandatory |
| | Target data must be<br>http://ecom-es-test.ath.cx/repository/TARGET_CCC.bin | | Mandatory |
| | SignedInfo.Reference | | |
| | | Reference URL of the target data must be above URI. | Mandatory |

### 3.4.3<ON-T-BASIC-ENVELOPED>

The application should successfully generate and validate enveloped signature XAdES-T format with binary data file.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | The application must generate enveloped signature. | | Mandatory |
| | Target data must be “./TARGET_DDD.xml” | | Mandatory |
| | SignedInfo.Reference | | |
| | | URI of Reference in target signature must be blank. | Mandatory |

## 3.5. XAdES 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-ENVELOPING>

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

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

### 3.5.2<ON-T-TSA-PFU-ENVELOPING>

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

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

### 3.5.3<ON-T-TSA-SEIKO-ENVELOPING>

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

| | | |
|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING> | | |
| Generation requirement | | |
| | The application must use SEIKO Precision TSA. | Mandatory |

## 3.6 XAdES-T Optional property test case (ON-T-PROP)

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

### 3.6.1 <ON-T-PROP-SIGNINGTIME>

The application should generate/validate the XAdES-T format in cases where it has the common SigningTime property.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>requirement. | | | |
| Generation requirement | | | |
| | property in the QualifyingProperties | | |
| | | The application must generate XAdES-T data which includes SigningTime | Mandatory |
| | | The application must generate SigningTime and timestamp based on the time order of ETSI TS 101 903 v1.3.2 G.2.2.16. | Mandatory |
| Vallidation requirement | | | |
| | The application must validate successfully the attached signature CAdES format based on the time order of ETSI TS 101 903 v1.3.2 G.2.2.16. | | Mandatory |
| | It is recommended to indicate the generation time of timestamp and SigningTime in some way. | | Recommended |

### 3.6.2<ON-T-PROP-EPES-FREEXML>

The application should generate/validate successfully the XAdES-T format (XAdES-EPES) with SignaturePolicyIdentifier property referring to a free format XML document.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING> | | | |
| Generation requirement | | | |
| | Property in the Qualifying Properties | | |
| | | SignaturePolicyIdentifer must be included | Mandatory |
| | | The OID of the policy must be uri:oid:1.2.3.4.5 | Mandatory |
| | | XML Signature policy file must be http://ecom-es-test.ath.cx/repository/TARGET-SIGPOL-XMLFREE.xml. | Mandatory |
| Validation requirement | | | |

| | | |
|---|---|---|
| | The existence of SignaturePolicyIdentifier and the description of policy 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.

### 3.6.3<ON-T-PROP-EPES-TR102038-V111>

The application should generate/validate successfully the XAdES-T format (XAdES-EPES) with SignaturePolicyIdentifier property referring to a XML signature policy based on ETSI TR 102 038 v1.1.1.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | | | |
| Generation Requirement | | | |
| | Property in Qualifying Properties | | |
| | | SignaturePolicyIdentifier must be included. | Mandatory |
| | | The OID of the policy must be uri:oid:1.2.3.4.5 | Mandatory |
| | | The target XML signature policy file must be http://ecom-es-test.ath.cx/repository/TARGET-SIGPOL-XML2038.xml. | Mandatory |
| Validation Requirement | | | |
| | The existence of SignaturePolicyIdentifier and the information of signature policy must be visually verified in some way. | | Mandatory |

### 3.6.4<ON-T-PROP-SIGNATUREPRODUCTIONPLACE>

The applications generate/validate successfully the XAdES-T format in cases where it has Signature ProductionPlace property.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING> Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | SignatureProductionPlace must be included. | Mandatory |
| Validation information | | | |
| | The existence of SignatureProductionPlace and the description must be visually verified in some way. | | Mandatory |

### 3.6.5<ON-T-PROP-SIGNERROLE-CLAIMED>

The application should successfully generate/validate the XAdES-T format in case where it has ClaimedRole.

| |
|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement |

| | | | |
|---|---|---|---|
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | SignerRole which has ClaimedRole.must be included. | Mandatory |
| Validation requrement | | | |
| | The existence of SignerRole and the description must be visually verified in some way. | | Mandatory |

### 3.6.6<ON-T-PROP-DATAOBJECTFORMAT>

The application should successfully generate/validate the XAdES-T format in cases where it has DataObjectFormat property.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING> | | | |
| Generation requirement | | | |
| | property in the QualifyingProperties | | |
| | | DataObjectFormat which has "text/plain" MimeType must be included. | Mandatory |
| Validation Requirement | | | |
| | The existence of DataObjectFormat and the information must be visually verified by person, or the appropriate viewer software for MimeType must be used. | | Mandatory |

### 3.6.7<ON-T-PROP-COMMITMENTTYPEINDICATION>

The application should generate/validate successfully in cases where the XAdES-T format which has CommitmentTypeIndication.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | CommitmentTypeIndication must be included. | Mandatory |
| Validation Requirement | | | |
| | The existance of CommitmentTypeIndication and the information must be visually verified in some way. | | Mandatory |

### 3.6.8<ON-T-PROP-ALLDATATS-CLAIMEDTIME>

The application should successfully generate/validate the XAdES-T format in cases where it has AllDataObjectsTimeStamp and SigningTime property.

| | | |
|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING> | | |
| Generation requirement | | |
| | property in the QualifyingProperties | |

| | | | |
|---|---|---|---|
| | | AllDataObjectsTimeStamp and SigningTime must be included. | Mandatory |
| | | The application must generate SigningTime and Timestamp based on the time order of ETSI TS 101 903 v1.3.2 G.2.2.16. | Mandatory |
| Validation information | | | |
| | The application must validate successfully the attached signature XAdES-T format based on the time order of ETSI TS 101 903 v1.3.2 G.2.2.16 | | Mandatory |
| | It is recommended to indicate the time of timestamp and SigningTime. | | Recommended |

### 3.6.9<ON-T-PROP-INDVDATATS-CLAIMEDTIME>

The application should generate/validate successfully the XAdES-T format in cases where it has IndividualDataObjectsTimeStamp and SigningTime property.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | property in the QualifyingProperties | | |
| | | IndividualDataObjectsTimeStamp and SigningTime.must be included. | Mandatory |
| | | The application must generate SigningTime and timestamp bases on the methodical relationship of ETSI TS 101 903 v1.3.2 G.2.2.16. | Mandatory |
| Validation information | | | |
| | The application must validate the methodical relationship of ETSI TS 101 903 v1.3.2 G.2.2.16. | | Mandatory |
| | Time of the timestamp and SigningTime are recommended to be expressed in some way. | | Recommended |

### 3.6.10<ON-T-PROP-COUNTERSIGNATURE>

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

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | The application must generate XAdES-T data which includes CounterSignature provided by<br>Signer (EE-ON-SIG-ECOMSAMPLE-OK). | Mandatory |
| | | The CounterSignature must include SignatureTimeStamp. | Mandatory |
| Validation information | | | |
| | The application should validate CounterSignature the same as “common requirement” mentioned above. | | Mandatory |

### 3.6.11<ON-T-PROP-SIGNINGCERTIFICATE>

The application should generate/validate successfully the XAdES-T format in cases where it has SigningCertificate property.

| | |
|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | |
| Generation requirement | |
| Property in QualifyingProperties | |
| SigningCertificate.must be included. | Mandatory |
| Validation information | |
| The application must validate the XAdES-T format in cases where SigningCertificate information is in conformance with signer certificate. | Mandatory |

## 3.7 XAdES-A Basic test case (ON-A-BASIC)

### 3.7.1 <ON-A-BASIC-A1-ENVELOPING>

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

| | |
|---|---|
| Based on <ON-T-BASIC-ENVELOPING>Requirement | |
| Generation requirement | |
| property in the QualifyingProperties | |
| CertificateValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| RevocationValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| An ArchiveTimeStamp which is based on ETSI TS 101 903 v1.3.2. 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 information | |
| 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 the 1st generation detached signature XAdES-A format.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-DETACHED>Requirement | | | |
| Generation requirement | | | |
| | property in the QualifyingProperties | | |
| | | CertificateValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| | | RevocationValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| | | An ArchiveTimeStamp which is based on ETSI TS 101 903 v1.3.2. 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 information | | | |
| | 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-A1-ENVELOPED>

The application should validate successfully the 1st generation attached signature XAdES-A format.

| | | | |
|---|---|---|---|
| Based on <ON-T-BASIC-ENVELPED>Requirement | | | |
| Generation requirement | | | |
| | property in the QualifyingProperties | | |
| | | CertificateValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| | | RevocationValues which have necessary information for validation of signer certificate must be included. | Mandatory |
| | | An ArchiveTimeStamp which is based on ETSI TS 101 903 v1.3.2. 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 | Mandatory |

| | | | |
|---|---|---|---|
| | | signed data of generation result if validation information of TSA certificate is not included into timestamp token fields. | |
| Validation information | | | |
| | 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 |

### 3.7.4 <ON-A-BASIC-A2-ENVELOPING>

The application should generate/validate successfully the 2nd generation attached signature XAdES-A format.

| | | | |
|---|---|---|---|
| Based on <ON-A-BASIC-A1-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | 2 ArchiveTimeStamps which is based on ETSI TS 101 903 v1.3.2. must be included. | Mandatory |
| | | Interval to the ArchiveTimestamp recommended to be more than one day. | Recommended |

### 3.7.5 <ON-A-BASIC-A3-ENVELOPING>

The application should generate/validate successfully the 3rd generation attached signature XAdES-A format.

| | | | |
|---|---|---|---|
| Based on <ON-A-BASIC-A2-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | 3 ArchiveTimeStamps which is based on ETSI TS 101 903 v1.3.2. must be included. | Mandatory |

## 3.8 XAdES-A Optional property test case (ON-A-PROP)

### 3.8.1 <ON-A-PROP-A1-REFS>

The application should generate/validate successfully the XAdES-A format in cases where it has CompleteCertificateRefs and CompleteRevocationRefs.

| | | | |
|---|---|---|---|
| Based on <ON-A-BASIC-A1-ENVELOPING>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | CompleteCertifiacteRefs and CompleteRevocationRefs must be included. | Mandatory |
| Validation requirement | | | |
| | When the application validates signer certificate, Refs must be in conformance with validation information. | | Mandatory |

### 3.8.2 <ON-A-PROP-A1-REFS-REFSONLYTS>

The application should generate/validate successfully the XAdES-A format in cases where it has RefsOnlyTimeStamp property.

| | | | |
|---|---|---|---|
| Based on <ON-A-PROP-A1-REFS>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | RefsOnlyTimeStamp must be included. | Mandatory |

### 3.8.3 <ON-A-PROP-A1-REFS-SIGANDREFSTS>

The application should generate/validate successfully the XAdES-A format in cases where it has SigAndRefsTimeStamp property.

| | | | |
|---|---|---|---|
| Based on <ON-A-PROP-A1-REFS>Requirement | | | |
| Generation requirement | | | |
| | Property in QualifyingProperties | | |
| | | SigAndRefsTimeStamp must be included. | 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

The section provides a profile of the data used for the tests. Note that the profile used in the CAdES tests is utilized for the certificates and time-stamp tokens used here.

## 4.1. Profile of the long-term signature format data used for the tests

All long-term signature format data is based on the XAdES specification.

### 4.1.1. XAdES-BES

| Element | Content |
|---|---|
| ds:Signature | |
| ds:SignedInfo | Present |
| ds:CanonicalizationMethod | Canonical XML (REC-xml-c14n-20010315) |
| ds:SignatureMethod | RSA with SHA1 (http://www.w3.org/2000/09/xmldsig#rsa- |
| ds:Reference | Consider that several are possible (signinging is by the detached method) |
| ds:Transforms | Depends on the format of the signed document.<br>If the data to be signed is XML, use canonical XML. |
| ds:DigestMethod | http://www.w3.org/2000/09/xmldsig#sha1 |
| ds:DigestValue | Digest value of the signed document |
| ds:SignatureValue | Signature value |
| ds:KeyInfo | According to the ECOM profile. |
| ds:Object | Present (depends on the existence or not of |
| QualifyingProperties | Present (depends on the existence or not of |
| SignedProperties | Present (depends on the existence or not of |
| SignedSignatureProperties | Present (depends on the existence or not of |
| SigningCertificate | According the the ECOM profile (issuer, serial number, SHA1 fingerprint) |

*Values will differ depending on the test item, but these are the values for data conformance.

### 4.1.2. XAdES-T

| Element | Content |
|---|---|
| ds:Signature | |
| ds:SignedInfo | Present |
| ds:CanonicalizationMethod | Canonical XML (REC-xml-c14n-20010315) |
| ds:SignatureMethod | RSA with SHA1 (http://www.w3.org/2000/09/xmldsig#rsa- |
| ds:Reference | Consider that several are possible (signinging is by the detached method) |
| ds:Transforms | Depends on the format of the signed document.<br>If the data to be signed is XML, use canonical XML. |
| ds:DigestMethod | http://www.w3.org/2000/09/xmldsig#sha1 |
| ds:DigestValue | Digest value of the signed document |
| ds:SignatureValue | Signature value |
| ds:KeyInfo | According to the ECOM profile. |
| ds:Object | Present |
| QualifyingProperties | Present |
| SignedProperties | Present (depends on the existence or not of |
| SignedSignatureProperties | Present (depends on the existence or not of |
| SigningCertificate | According the the ECOM profile (issuer, serial number, SHA1 fingerprint) |
| UnSignedProperties | Present |
| UnSignedSignaturePropertie | Present |
| SignatureTimeStamp | Token should conform with the test data profile. |

*Values will differ depending on the test item, but these are the values for data conformance.

### 4.1.3. XAdES-A (1st generation)

| Element | Content |
|---|---|
| ds:Signature | |
| ds:SignedInfo | Present |
| ds:CanonicalizationMethod | Canonical XML (REC-xml-c14n-20010315) |
| ds:SignatureMethod | RSA with SHA1 (http://www.w3.org/2000/09/xmldsig#rsa-sha1) |
| ds:Reference | Consider that several are possible (signinging is by the detached method) |
| ds:Transforms | Depends on the format of the signed document.<br>If the data to be signed is XML, use canonical XML. |
| ds:DigestMethod | http://www.w3.org/2000/09/xmldsig#sha1 |
| ds:DigestValue | Digest value of the signed document |
| ds:SignatureValue | Signature value |
| ds:KeyInfo | According to the ECOM profile. |
| ds:Object | Present |
| QualifyingProperties | Present |
| SignedProperties | Present (depends on the existence or not of SigningCertificate) |
| SignedSignatureProperties | Present (depends on the existence or not of SigningCertificate) |
| SigningCertificate | According the the ECOM profile (issuer, serial number, SHA1 fingerprint) |
| UnSignedProperties | Present |
| UnSignedSignatureProperties | Present |
| SignatureTimeStamp | Token should conform with the test data profile. |
| CompleteCertificateRefs | According to the ECOM profile. |
| CompleteRevocationRef | According to the ECOM profile. |
| CertificateValues | According to the ECOM profile. |
| RevocationValues | According to the ECOM profile. |
| ArchiveTimeStamp | Token should conform with the test data profile. |

*Values will differ depending on the test item, but these are the values for data conformance.

### 4.1.4. XAdES-A (2nd generation)

| Element | Content |
|---|---|
| ds:Signature | |
| ds:SignedInfo | Present |
| ds:CanonicalizationMethod | Canonical XML (REC-xml-c14n-20010315) |
| ds:SignatureMethod | RSA with SHA1 (http://www.w3.org/2000/09/xmldsig#rsa-sha1) |
| ds:Reference | Consider that several are possible (signinging is by the detached method) |
| ds:Transforms | Depends on the format of the signed document.<br>If the data to be signed is XML, use canonical XML. |
| ds:DigestMethod | http://www.w3.org/2000/09/xmldsig#sha1 |
| ds:DigestValue | Digest value of the signed document |
| ds:SignatureValue | Signature value |
| ds:KeyInfo | According to the ECOM profile. |
| ds:Object | Present |
| QualifyingProperties | Present |
| SignedProperties | Present |
| SignedSignatureProperties | Present |
| SigningCertificate | According the the ECOM profile (issuer, serial number, SHA1 fingerprint) |
| UnSignedProperties | Present |
| UnSignedSignatureProperties | Present |
| SignatureTimeStamp | Token should conform with the test data profile. |
| CompleteCertificateRefs | According to the ECOM profile. |
| CompleteRevocationRef | According to the ECOM profile. |
| CertificateValues | According to the ECOM profile. |
| RevocationValues | According to the ECOM profile. |
| ArchiveTimeStamp | Token should conform with the test data profile. |
| ArchiveTimeStamp | Token should conform with the test data profile. |

*Values will differ depending on the test item, but these are the values for data conformance.

## 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 |
| 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 |
|---|---|---|
| vesion | 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 |
|---|---|---|
| vesion | 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 |
| authorityKeyIdentifier | Present | FALSE |
| keyIdentifier | Present SHA1-160bit | - |
| basicConstraints | Present | TRUE |
| CA flag | TRUE | - |
| cRLDistributionPoints | Present | FALSE |
| DistPt.fullName.UR | http://distribution host/**/*crl | - |

### 4.3.4 Profile of End Entity certificate for the signer

| Field | Value | Critical |
|---|---|---|
| vesion | 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 |
|---|---|---|
| vesion | 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 common 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 |