ECOM Long-Term Signature Format Interoperability Test Test Case Specification

Maech, 2006

Next Generation Electronic Commerce Promotion Council of Japan (ECOM)

Security Working Group

Long Term Signature Diffusion Sub Working Group

Long-Term Signature Format Interoperability Test Project

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 Long Term Signature Diffusion Sub Working Group of the Security Working Group at 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 strucutre

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 12.31.2035 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	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.3.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.2.2001 00:00:00~1.3.2001 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	1.3.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.3.2001 12:00:00
Validity period of signing certificate	1.1.2001 00:00:00~1.1.2001 23:59:59

Expected value	Invalid
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2000 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.1.2001 00:00:00~12.31.2035 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	1.2.2001 12:00:00
Value of signing time attribute	1.2.2001 12:00:00
Signature time-stamp	1.2.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.4.2001 00:00:00~1.4.2001 23:59:59
Revocation time on the signing certificate CRL	1.1.2005 12:00
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.4.2001 00:00:00~1.4.2001 23:59:59

2.4.4. < 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 5 shows the expected test value, and test parameters for time, certificates, and CRLs used when testing.

Table 5: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTIME-REVOKED-OK 10004>

Expected value	Valid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	1.4.2001 12:00:00
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.3.2001 00:00:00~1.3.2001 23:59:59

Expected value	Valid
Revocation time on the signing certificate CRL	1.2.2005 12:00:00
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.3.2001 00:00:00~1.3.2001 23:59:59

2.4.5. < 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 6: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTS-REVOKED-NG 10005>

Expected value	Invalid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	1.1.2001 12:00:00
Signature time-stamp	1.3.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.4.2001 00:00:00~1.4.2001 23:59:59
Revocation time on the signing certificate CRL	1.2.2005 12:00:00
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.4.2001 00:00:00~1.4.2001 23:59:59

2.4.6. < 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 7: Expected test value and test parameters for
< XAdEST -ATTACH-EE-SIG-FORGED-NG 10006>

Expected value	Invalid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.4.2002 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.2.2001 00:00:00~1.2.2001 23:59:59

2.4.7. < 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 certificate is verified as invalid.

Table 8: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTS-SIG-FORGED-NG 10007>

Expected value	Invalid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.2.2001 00:00:00~1.2.2001 23:59:59

2.4.8. < 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 certificate is verified as invalid.

Table 9: Expected test value and test parameters for
< XAdEST -ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

Expected value	Invalid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.2.2001 00:00:00~1.2.2001 23:59:59

2.4.9. < 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 10: Expected test value and test parameters for
< XAdEST -ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

Expected value	Invalid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.2.2001 00:00:00~1.2.2001 23:59:59

2.4.10. < XAdEST -DETACH-NORMAL-OK 10010>

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

Table 11: Expected test value and test parameters for
< XAdEST -DETACH-NORMAL-OK 10010>

Expected value	Valid
Signing time used	1.1.2001 12:00:00
Value of signing time attribute	Attribute not present
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.1.2001 00:00:00~1.2.2001 23:59:59

2.5. ES-A format standard tests

2.5.1. < 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	1.1.2001 12:00:00
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035

Expected value	Valid
Signature time-stamp TSA certificate verification CRL	1.3.2001 00:00:00~1.3.2001 23:59:59
Archive time-stamp 1	1.3.2001 12:00
TSA certificate for archive time-stamp 1	1.1.2001 ~ 12.31.2035
Archive time-stamp TSA certificate verification CRL	1.4.2001 00:00:00~12.31.2035 23:59:59

2.5.2. < 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 signed by 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	1.1.2001 12:00:00
Signature time-stamp	1.1.2001 12:00:00
Validity period of signing certificate	1.1.2001~12.31.2035
Verification CRL for the signing certificate	1.2.2001 00:00:00~1.2.2001 23:59:59
Signature time-stamp TSA certificate	1.1.2001~12.31.2035
Signature time-stamp TSA certificate verification CRL	1.3.2001 00:00:00~1.3.2001 23:59:59
Archive time-stamp 1	1.3.2001 12:00
TSA certificate for archive time-stamp 1	1.1.2001 ~ 12.31.2035
Archive time-stamp TSA certificate verification CRL	1.4.2001 00:00:00~12.31.2035 23:59:59

2.6. XAdES-T standard test cases

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

2.6.1. <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

2.6.2. <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

2.6.3. <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

2.6.4. <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

2.6.5. <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

2.6.6. <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

2.6.7. <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

2.6.8. <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

2.6.9. <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

2.6.10. <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

2.7. XAdES-A standard test cases

2.7.1. <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

2.7.2. <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.	
70001	XAdESA1-DETACH-NORMAL-OK

3. Online matrix generation and mutual verification test categories

These proving tests allows participating organizations that have products that handle the long-term signature format to generate long-term signature data files based on each set of specified test regulations, and to check whether each product verifies this data as valid.

3.1. Generated data

The data to be signed is prepared in the form of a small amount of text data, and a 1 MB binary file. An XML signature for the small amount of text data is generated used the enveloping method, and one is generated for the binary file using the detached method. An ES-T format, and a first generation, and next generation ES-A format signature is generated for each.

For time-stamp token acquisition, the time-stamp authority provided for these tests will be used. Revocation data may be obtained from the URI specified in the certificate's cRLDistributionPoints extension, or the file included with the test data may be used.

3.2. Test preparation

The following preparations are necessary when performing the tests:

- CRL settings
  In order to obtain the CRL, the Internet connection environment of the verification environment must be set up. The CRL issuance period for the signature certifying authority and the time-stamp certifying authority is 1 day.

- Trust anchor settings
  Set as a trust anchor, the signer's root certificate and the TSA's root certificate distributed in the test suite for offline testing.

3.3. Test implementation (data generation)

This section describes the settings and conditions on the signature data generation side at the time of test implementation.

- 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 2 shows an example of an XML document when the internal signature type is used.

List 2: 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">YWEh</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).

- Data generation

- All generated data is archived, and sent to the person in charge of verification at the participating company.

3.4. Test implementation (verification)

- Signed data settings
  For the internal signature type, the signed data is set to the character string, "aaa", and the signed data is specified using the enveloping XML signature form. Therefore, it is sufficient if verification is achieved according to the XML signature specification. For detached signatures, the signed data is a file named 'TARGET_BBB.bin' (this is a binary file with the sequence 0x01-0x09, 0x00 repeated up to 1024000 bytes). The following two methods of specifying the signed file are possible, so it is essential that both can be verified.

  ✧ The signed element is explicitly referred by the URI attribute on the Reference element.

  ✧ The signed element is not explicitly specified in the Reference element, so that a separate signature file must be specified.

- 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 12.31.2035 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
  The long-term signature format test data to be verified is obtained from the data generation steps and verified.

- 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=**

3.5. Test cases

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

3.5.1. <ON-T-1>: Enveloped form XAdES-T generation/mutual verification test case

The XAdES-T data for each product and service is generated according to the following test regulations:

- # The signed character string is "aaa"
- # Internal certification is used. ("aaa" is included within the XML document and used as the signed data.)
- DigestMethod is SHA1
- The signing algorithm is SHA1withRSA
- The XAdES-T is generated based on the XAdES-BES format

Each product and system should verify data generated under these conditions as valid.

3.5.2. <ON-T-2>: Detached form XAdES-T generation/mutual verification test case

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

- # The signed object is a 1 MB data file
- # Detached signing is used. The signed data is not included within the XML document.

Each product and system should verify data generated under these conditions as valid.

3.5.3. <ON-A1-1>: Enveloped form 1st generation XAdES-A generation/mutual verification test case

The XAdES-A data for each product and system is generated according to the following test regulations:

- # XAdES-A data is generated using the XAdES-T data generated in the <ON-T-1> test case as the target.
- The content and encapsulation method of the signature and the certificate verification data for the archive time-stamp attribute are based on the ECOM profile.

Each product and system should verify data generated under these conditions as valid.

3.5.4. <ON-A1-2>: Detached form 1st generation XAdES-A generation/mutual verification test case

The XAdES-A data for each product and system is generated according to the following test regulations:

- # XAdES-A data is generated using the XAdES-T data generated in the <ON-T-2> test case as the target.
- The content and encapsulation method of the signature and the certificate verification data for the archive time-stamp attribute are based on the ECOM profile.

Each product and system should verify data generated under these conditions as valid.

3.5.5. <ON-A2-1>: Enveloped form 2nd generation XAdES-A generation/mutual verification test case

The XAdES-A data for each product and system is generated according to the following test regulations:

- # Generated with the XAdES-A generated in the <ON-A1-1> test case used as the target. (signature extension)
- The content and encapsulation method of the signature and the certificate verification data for the archive time-stamp attribute are based on the ECOM profile.

Each product and system should verify data generated under these conditions as valid.

3.5.6. <ON-A2-2>: Detached form 2nd generation XAdES-A generation/mutual verification test case

The XAdES-A data for each product and system is generated according to the following test regulations:

- # Generated with the XAdES-A generated in the <ON-A1-2> test case used as the target. (signature extension)
- The content and encapsulation method of the signature and the certificate verification data for the archive time-stamp attribute are based on the ECOM profile.

Each product and system should verify data generated under these conditions as valid.

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. 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. 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. 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. 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.