ECOM 長期署名フォーマット

相互運用実証実験

テストケース設計書

2006 年 3 月

次世代電子商取引推進協議会(ECOM)

セキュリティ WG

長期署名フォーマット普及 SWG

長期署名フォーマット相互運用性実証実験プロジェクト

目次

1. はじめに

本仕様書は、ECOM セキュリティ WG 長期署名フォーマット普及 SWG の長期署名フォーマット相互運用性実証実験プロジェクトにおいて実施される実証実験の XAdES 長期署名フォーマットに関するテスト内容について記述したものである。

1.1. 本書における表記

本仕様書では、以下の表記を用いることとする（表 1)。

表 1：表記

表記	説明
<…>	テスト項目
<…OK>	検証結果の期待値が有効であるテスト項目
<…NG>	検証結果の期待値が無効であるテスト項目
[…]	参考文献

1.2. テストの構成

CAdES テストケース設計書に記述されたものと同様の構成とする。

2. オフライン共通データ検証テストカテゴリ

ECOM プロファイルに基づく共通の XAdES フォーマットデータを用いて、実験者のシステムや製品でそれらが正しく検証できるかどうかを確認する。テストツールより生成された XAdES フォーマットのデータ(XAdES-T、XAdES-A)、証明書、CRL、署名対象データをもとに、検証結果が期待値と一致するかどうかを確認する。

2.1. テストの準備

テスト実施する際は、以下の項目の準備が必要となる。

- CRL の設定

  証明書検証時にオンラインで CRL を取得する場合には、検証環境におけるインターネット接続環境の準備。実験期間終了後にはホスト名を同じくする HTTP リポジトリの立ち上げと設定。もしくは、ファイルによる CRL の設定。

- トラストアンカの設定

  テストスイートで配布されるオフラインテスト用の署名者用ルート証明書、TSA 用ルート証明書をトラストアンカとして設定する。

2.2. テストの実施

本節では、テストの実施時の設定や条件などを説明する。

・ 署名対象データの設定

内包型署名の場合は、署名対象文字列を”aaa”とし XML 署名の形式として enveloping 形式で署名対象文字列を指定する。ただし、XML 署名の Object 要素として格納するため、base64 で encode された値(YWFh)で格納するもとする。内包型署名の場合の XML 署名文書の例を以下に示す（リスト 1)。

リスト 1：内包型署名の場合の XML 署名文書の例

```
<?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>
```

base64でエンコードされたテキスト”aaa”

分離署名の場合には、'TARGET_BBB.bin”(ファイルの内容は、0x01-0x09,0x00 の繰り返しで 1024000 バイトのバイナリファイル)を設定する。

・ 検証時刻の設定

検証時刻はフォーマット毎に異なる。フォーマットに応じ検証時刻の設定を行う。検証可能な現在時刻の範囲は UTC2002 年 1 月 1 日 0 時 0 分 0 秒より UTC2035 年 12 月 31 日 23 時 59 分 59 秒までとし、各証明書や CRL もまたこれが可能なように設定されている。

・ 検証対象の長期署名フォーマットデータの設定

テストスィートにおいて長期署名フォーマットの検証対象テストデータは、”<テストケース名>-V131.xml”というファイル名となっており、各テスト項目ごとに別々のディレクトリに保存されている。

・ 検証の実施

実施すべき全てのテスト項目について実施する。署名対象データのハッシュ値を base64 でエンコードしたものは以下の通り。

“aaa” ：**fiQN50+x7Qj6CNOAY/amqRRiqBU=**

TARGET_BBB.bin ：**gpGOa0wroxRJGyeXw7tHFbrgtxM=**

2.3. テストデータに共通の情報

- 有効期限の時刻は、例外ケースを除き 00:00:00 から 23:59:59 に統一する。
- 署名時刻、タイムスタンプ時刻は例外ケースを除き 12:00:00 に統一する
- 時刻の表記は、特に断りのない限り、UTC 時刻とする。

2.4. XAdES-T フォーマット標準テスト

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

署名者証明書および署名タイムスタンプの TSA 証明書が有効期間内にあり共に失効しない場合、XAdES-T データが有効であることを検証する。表 2 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 2：< XAdEST -ATTACH-NORMAL-OK 10001>におけるテスト結果の期待値とテストパラメータ

期待値	有効（valid）
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.3 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.2 00:00:00～2001.1.3 23:59:59

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

署名タイムスタンプの TSA 証明書は有効であるが、署名証明書が期限切れの時点で署名タイムスタンプを付した場合、署名者証明書を検証する CRL に記載されていないとき XAdES データが無効であることを検証する。表 3 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 3：< XAdEST -ATTACH-EXPIERED-NG 10002>におけるテスト結果の期待値とテストパラメータ

期待値	無効（invalid）
署名を実施したとする時刻	2001.1.3 12:00:00

サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書の有効期限	2001.1.1 00:00:00～2001.1.1 23:59:59
署名者証明書の検証 CRL	2001.1.2 00:00:00～2000.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

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

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、サイニングタイム属性の時刻および署名タイムスタンプ時刻において、署名者証明書が失効して CRL に記載されている場合、ES-T データが無効であることを検証する。表 4 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 4：< XAdEST -ATTACH-REVOKED-NG 10003>におけるテスト結果の期待値とテストパラメータ

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.2 12:00:00
サイニングタイム属性の時刻	2001.1.2 12:00:00
署名タイムスタンプの時刻	2001.1.2 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.4 00:00:00～2001.1.4 23:59:59
署名者証明書 CRL 中の失効日時	2005.1.1 12:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.4 00:00:00～2001.1.4 23:59:59

2.4.4. < XAdEST -ATTACH-SIGTIME-REVOKED-OK 10004>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、署名タイムスタンプ時刻では失効していないが、サイニング属性の時刻において署名者証明書が失効して CRL に記載されている場合、署名時刻は無視し、署名タイムスタンプ時刻での証明書有効性を検証することにより、ES-T データが有効であることを検証する。表 5 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 5：< XAdEST -ATTACH-SIGTIME-REVOKED-OK 10004>におけるテスト結果の期待値とテストパラメータ

期待値	有効(valid)

署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	2001.1.4 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
署名者証明書 CRL 中失効日時	2005.1.2 12:00:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.3 00:00:00～2001.1.3 23:59:59

2.4.5. < XAdEST -ATTACH-SIGTS-REVOKED-NG 10005>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、SigningTime 属性の時刻では失効していないが、署名タイムスタンプ時刻において署名者証明書が失効して CRL に記載されている場合、署名時刻は無視し、署名タイムスタンプ時刻での証明書有効性を検証することにより、ES-T データが無効であることを検証する。

表 6：< XAdEST -ATTACH-SIGTS-REVOKED-NG 10005>におけるテスト結果の期待値とテストパラメータ

期待値	有効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.4 00:00:00～2001.1.4 23:59:59
署名者証明書 CRL 中失効日時	2005.1.2 12:00:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.4 00:00:00～2001.1.4 23:59:59

2.4.6. < XAdEST -ATTACH-ES-SIG-REVOKED-NG 10006>

ES-T フォーマットの CMS SignedData の SIgnerInfo において signature フィールドにある署名値が改ざんされていた場合に無効であることを検証する。

表 7：< XAdEST -ATTACH-EE-SIG-FORGED-NG 10006>におけるテスト結果の期待値とテストパラメータ

期待値	有効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00

サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2002.1.4 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.4.7. < XAdEST -ATTACH-SIGTS-SIG-FORGED-NG 10007>

ES-T フォーマットの SignatureTimeStamp 属性中の TimeStampToken の CMS SignedData 構造の SignerInfo において signature フィールドにある署名値が改ざんされていた場合に無効であることを検証する。

表 8：< XAdEST -ATTACH-SIGTS-SIG-FORGED-NG 10007>におけるテスト結果の期待値とテストパラメータ

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.4.8. < XAdEST -ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

ES-T フォーマットの CMS SignedData の signedAttributes の中の MessageDigest 属性の値が改ざんされていた場合に無効であることを検証する。

表 9：< XAdEST -ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>におけるテスト結果の期待値とテストパラメータ

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.4.9. < XAdEST -ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

ES-T フォーマットの SignatureTimeStamp 属性に含まれるタイムスタンプトークンの signedAttributes の中の MessageDigest 属性の値が改ざんされていた場合に無効であることを検証する。

表 10：< XAdEST -ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>におけるテスト結果の期待値とテストパラメータ

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

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

署名対象文書に対して分離署名を行った ES-T フォーマットにおいてデータが有効であることを検証する。

表 11：< XAdEST -DETACH-NORMAL-OK 10010>におけるテスト結果の期待値とテストパラメータ

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.1 00:00:00～2001.1.2 23:59:59

2.5. ES-A フォーマット標準テスト

2.5.1. < XAdESA1-ATTACH-NORMAL-OK 70001>

ECOM XAdES 長期署名フォーマットプロファイルに基づくアーカイブタイムスタンプを一つ付与された ES-A フォーマットが有効であることを検証する。

表 12：< XAdESA 1-ATTACH-NORMAL-OK 70001>におけるテスト結果の期待値とテストパラメータ

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archiveタイムスタンプ1の時刻	2001.1.3 12:00
Archiveタイムスタンプ1のTSA証明書	2001.1.1 ～ 2035.12.31
Archive TS TSA 証明書検証CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.5.2. < XAdESA1-DETACH-NORMAL-OK 70002>

DETACHED 形式の署名を行った XML 署名に対し ECOM XAdES 長期署名フォーマットプロファイルに基づくアーカイブタイムスタンプを一つ付与された ES-A フォーマットが有効であることを検証する。

表 13：< XAdESA 1-DETACH-NORMAL-OK 70002>におけるテスト結果の期待値とテストパラメータ

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名TS TSA 証明書検証CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archiveタイムスタンプ1の時刻	2001.1.3 12:00
Archiveタイムスタンプ1のTSA証明書	2001.1.1 ～ 2035.12.31
Archive TS TSA 証明書検証CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.6. XAdES-T 標準テストケース

本節では XAdES-T フォーマットを扱う実装が満足すべきテストケースを示す。

2.6.1. <OFF-T-1>

テストケース名	OFF-T-1
一般的な内包署名の ES-T フォーマットを読み込むことができる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK

2.6.2. <OFF-T-2>

テストケース名	OFF-T-2
XAdES-T フォーマットの署名者証明書の期限切れを扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10002	XAdEST-ATTACH-EXPIRED-NG

2.6.3. <OFF-T-3>

テストケース名	OFF-T-3
XAdES-T フォーマットの署名者証明書の失効を扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10003	XAdEST-ATTACH-REVOKED-NG

2.6.4. <OFF-T-4>

テストケース名	OFF-T-4
XAdES-T フォーマットの署名者証明書の認証パス検証を正しく扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10002	XAdEST-ATTACH-EXPIRED-NG
10003	XAdEST-ATTACH-REVOKED-NG

2.6.5. <OFF-T-5>

テストケース名	OFF-T-5
XAdES-T フォーマットでサイニングタイムに関係なく署名タイムスタンプの時刻により署名者証明書の失効検証ができる。	

成功条件：以下テスト項目が全て期待値通りになること。	
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>

テストケース名	OFF-T-6
XAdES-T フォーマットの Signature 要素内の署名値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10006	XAdEST-ATTACH-ES-SIG-FORGED-NG

2.6.7. <OFF-T-7>

テストケース名	OFF-T-7
XAdES-T フォーマットの署名タイムスタンプトークンの SignerInfo の署名値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10007	XAdEST-ATTACH-SIGTS-FORGED-NG

2.6.8. <OFF-T-8>

テストケース名	OFF-T-8
XAdES-T フォーマットの DigestValue 要素のハッシュ値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK
10008	XAdEST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG

2.6.9. <OFF-T-9>

テストケース名	OFF-T-9
XAdES-T フォーマットの署名タイムスタンプトークンの MessageDigest のハッシュ値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	XAdEST-ATTACH-NORMAL-OK

10009	XAdEST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG

2.6.10. <OFF-T-10>

テストケース名	OFF-T-10
分離署名の XAdES-T のフォーマットを扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10010	XAdEST-DETACH-NORMAL-OK

2.7. XAdES-A 標準テストケース

2.7.1. <OFF-A-1>

テストケース名	OFF-A-1
ECOM プロファイルに基づく内包署名の第一世代の ES-A フォーマットを扱うことができる。	
成功条件：以下テスト項目が全て期待値通りになること。	
70001	XAdESA1-ATTACH-NORMAL-OK

2.7.2. <OFF-A-2>

テストケース名	OFF-A-2
ECOM プロファイルに基づく分離署名の第一世代の ES-A フォーマットを扱うことができる。	
成功条件：以下テスト項目が全て期待値通りになること。	
70001	XAdESA1-DETACH-NORMAL-OK

3. オンライン マトリックス生成・相互検証テストカテゴリ

長期署名フォーマットを扱う製品を持つ実証実験参加組織が、指定されたレギュレーションに基づく長期書名データファイルをそれぞれ生成し、このデータが有効であることを各製品が検証できることを確認するテストである。

3.1. 生成するデータ

署名対象となるデータは小さいサイズのテキストデータを 1MB のバイナリデータを用意する。小さいサイズのテキストデータを Enveloping 形式、1MB 程度のバイナリデータファイルを Detached 形式として XML 署名を生成し、それぞれ ES-T フォーマット、第一世代とその次の世代の ES-A フォーマットを生成する。

タイムスタンプトークンの取得は今回のテスト用に提供されたタイムスタンプ局を使用することとする。失効情報の取得は証明書の cRLDistributionPoints 拡張に記載された

URL より取得してもよいし、テストデータに含まれるファイルを使用してもよい。

3.2. テストの準備

テスト実施する際は、以下の項目の準備が必要となる。

・ CRL の設定

CRL を取得するために、検証環境におけるインターネット接続環境の準備を行う。署名用認証局とタイムスタンプ局用認証局の CRL 発行間隔は 1 日となっている。

・ トラストアンカの設定

テストスイートで配布されるオフラインテスト用の署名者用ルート証明書、TSA 用ルート証明書をトラストアンカとして設定する。

3.3. テストの実施（生成）

本節では、テストの実施時の署名データ生成側の設定や条件などを説明する。

・ 署名対象データの設定

内包型署名の場合は、署名対象文字列を”aaa”とし XML 署名の形式として enveloping 形式で署名対象文字列を指定する。ただし、XML 署名の Object 要素として格納するため、base64 で encode された値(YWFh)で格納するもとする。内包型署名の場合の XML 署名文書の例を以下に示す（リスト 2)。

リスト 2：内包型署名の場合の XML 署名文書の例

```
<?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>
```

base64でエンコードされたテキスト”aaa”

分離署名の場合には、'TARGET_BBB.bin”(ファイルの内容は、0x01-0x09,0x00 の繰り返しで 1024000 バイトのバイナリファイル)を設定する。

・ データ生成の実施
・ 生成したデータを全てアーカイブし、参加企業の検証者に送信する。

3.4. テストの実施（検証）

・ 署名対象データの設定

内包型署名の場合は、署名対象文字列を”aaa”とし XML 署名の形式として enveloping 形式で署名対象文字列を指定されている。したがって、XML 署名の仕様に従い検証できれば良い。分離署名の場合には、'TARGET_BBB.bin”(ファイルの内容は、0x01-0x09,0x00 の繰り返しで 1024000 バイトのバイナリファイル)が署名対象となる。署名対象ファイルの指定方法として以下の 2 通りが考えられるので両社とも検証できる必要がある。

✧ Reference 要素の URI 属性で明示的に署名対象要素を参照している場合

✧ Reference 要素では、明示的に署名対象要素が指定されておらず、別途署名対象ファイルを指定する必要がある場合。

・ 検証時刻の設定

検証時刻はフォーマット毎に異なる。フォーマットに応じ検証時刻の設定を行う。検証可能な現在時刻の範囲は UTC2002 年 1 月 1 日 0 時 0 分 0 秒より UTC2035 年 12 月 31 日 23 時 59 分 59 秒までとし、各証明書や CRL もまたこれが可能なように設定されている。

・ 検証対象の長期署名フォーマットデータの設定

データ生成より受け取った長期署名フォーマットの検証対象テストデータを検証する。

・ 検証の実施

実施すべき全てのテスト項目について実施する。署名対象データのハッシュ値を base64 でエンコードしたものは以下の通り。

“aaa” ：**fiQN50+x7Qj6CNOAY/amqRRiqBU=**

TARGET_BBB.bin ：**gpGOa0wroxRJGyeXw7tHFbrgtxM=**

3.5. テストケース

以下のレギュレーションに関する記述で「◎」印は必ず満足しなければならないルール

とし、それ以外は可能ならば準拠しなければならないルールとする。

3.5.1. <ON-T-1>Enveloped 形式 XAdES-T 生成・相互検証テストケース

以下のレギュレーションで各製品やサービスの XAdES-T データを生成する。

- ◎署名対象文字列 “aaa”
- ◎内包証明とする。（XML 内部に aaa を含みそれを署名対象とする。）
- DigestMethod は SHA1
- 署名アルゴリズムは SHA1withRSA
- XAdES-BES フォーマットより XAdES-T を生成

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

3.5.2. <ON-T-2>Detached 形式 XAdES-T 生成・相互検証テストケース

テストケース<ON-T-1>をベースに以下のレギュレーションを加えたもので各製品やシステムで XAdES-T データを生成する。

- ◎署名対象が 1MB のデータファイル
- ◎分離署名とする。XML 署名文書に署名対象を含まない。

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

3.5.3. <ON-A1-1>Enveloped 形式 第 1 世代 XAdES-A 生成・相互検証テストケース

以下のレギュレーションで各製品やシステムで XAdES-A データを生成する。

- ◎<ON-T-1>で生成された XAdES-T データを対象として XAdES-A データを生成。
- 署名、およびアーカイブタイムスタンプ属性の証明書検証情報の格納内容、方法は ECOM プロファイルに基づく

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

3.5.4. <ON-A1-2>Detached 形式 第 1 世代 XAdES-A 生成・相互検証テストケース

以下のレギュレーションで各製品やシステムで XAdES-A データを生成する。

- ◎<ON-T-2>で生成された XAdES-T データを対象として XAdES-A を生成する。
- 署名、およびアーカイブタイムスタンプ属性の証明書検証情報の格納内容、方法は ECOM プロファイルに基づく

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

3.5.5. <ON-A2-1>Enveloped 形式 第 2 世代 XAdES-A 生成・相互検証テストケース

以下のレギュレーションで各製品やシステムで XAdES-A を生成する。

- ◎<ON-A1-1>で生成された XAdES-A を対象とし生成する（署名延長）
- 署名、およびアーカイブタイムスタンプ属性の証明書検証情報の格納内容、方法は ECOM プロファイルに基づく

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

3.5.6. <ON-A2-2>Detached 形式 第 2 世代 XAdES-A 生成・相互検証テストケース

以下のレギュレーションで各製品やシステムで XAdES-A を生成する。

- ◎<ON-A1-２>で生成された XAdES-A を対象とし生成する（署名延長）
- 署名、およびアーカイブタイムスタンプ属性の証明書検証情報の格納内容、方法は ECOM プロファイルに基づく

各製品やシステムは、これらの条件で生成されたデータが有効であることを検証する。

4. 付録：実験データ用プロファイル

本節では実証実験で用いられるデータのプロファイルを示す。なお、証明書およびタイムスタンプトークンのプロファイルは CAdES の実験に利用したものを用いる。

4.1. 実験用長期署名フォーマットデータプロファイル

長期署名フォーマットのデータは、全て XAdES の仕様に基づいている。

4.1.1. XAdES-BES

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はdetached形式とする）
ds:Transforms	署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	ECOMプロファイルに従う。
ds:Object	有り(SingingCertificateの有無に依存する)
QualifyingProperties	有り(SingingCertificateの有無に依存する)
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	ECOMプロファイルに従う（発行者名、シリアル番号、SHA1フィンガープリント）

※：テスト項目により値は変化するがデータ共通の値はこの値となる。

4.1.2. XAdES-T

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はdetached形式とする）
ds:Transforms	署名対象文書のフォーマットに依存する。 署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	ECOMプロファイルに従う。
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	ECOMプロファイルに従う（発行者名、シリアル番号、SHA1フィンガープリント）
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う

4.1.3. XAdES-A(第一世代)

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	/xmldsig#rsa-sha1)
ds:Reference	detached形式とする)
ds:Transforms	署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	ECOMプロファイルに従う。
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	ECOMプロファイルに従う(発行者名、シリアル番号、SHA1フィンガープリント)
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う
CompleteCertificateRefs	ECOMプロファイルに従う
s	ECOMプロファイルに従う
CertificateValues	ECOMプロファイルに従う
RevocationValues	ECOMプロファイルに従う
ArchiveTimeStamp	トークンは実験用データプロファイルに従う

※:テスト項目により値は変化するがデータ共通の値はこの値となる。

4.1.4. XAdES-A(第 2 世代)

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する(署名形式はdetached形式とする)
ds:Transforms	署名対象文書のフォーマットに依存する。 署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	ECOMプロファイルに従う。
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り
SignedSignatureProperties	有り
SigningCertificate	ECOMプロファイルに従う(発行者名、シリアル番号、SHA1フィンガープリント)
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う
CompleteCertificateRefs	ECOMプロファイルに従う
CompleteRevocationRefs	ECOMプロファイルに従う
CertificateValues	ECOMプロファイルに従う
RevocationValues	ECOMプロファイルに従う
ArchiveTimeStamp	トークンは実験用データプロファイルに従う
ArchiveTimeStamp	トークンは実験用データプロファイルに従う

※:テスト項目により値は変化するがデータ共通の値はこの値となる。