ECOM 長期署名フォーマット
相互運用実証実験
CAdES 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

図表番号

1 はじめに

本書では、長期署名フォーマットおよび ECOM プロファイルへの準拠性を確認するためのテストの内容を示したテストケース設計書である。

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。

表記	説明
<…>	テスト項目
<…-OK>	検証結果の期待値が有効のテスト項目
<…-NG>	検証結果の期待値が無効のテスト項目
<… 00000>	テスト項目名の末尾の 5 桁の数字はテスト項目番号
[…]	参考文献

1.2 テストの構成

・テストカテゴリ（今回のテストではオフラインテストカテゴリとオンラインテストカテゴリに大別される）
・テストケース（個々のテストケースであり機能評価判定の単位となる。複数のテスト項目を含む）
・テスト項目（テストの最小単位であり、検証の結果として期待値通りかそうでないかを成功・失敗として表現する。）

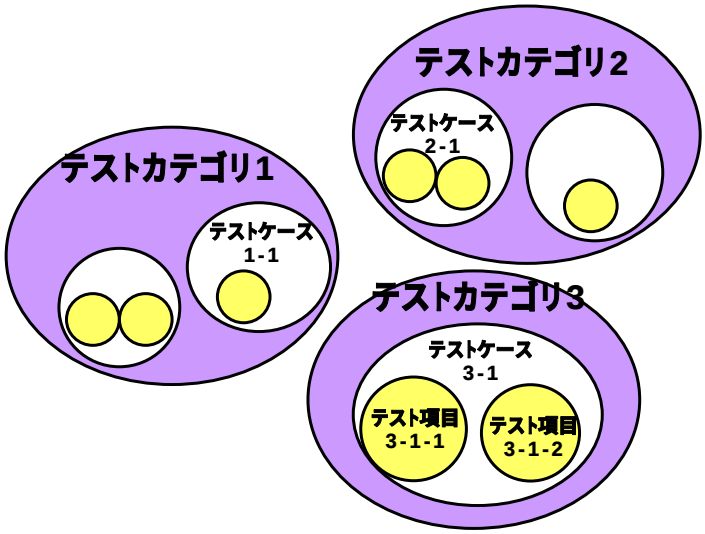


図 1-1 テストの構成

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 ES フォーマットデータを用いて正しく検証することができるかを確認する。テストツールにより生成された ES フォーマットのデータ(ES, ES-T, ES-C, ES-X long, ES-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。

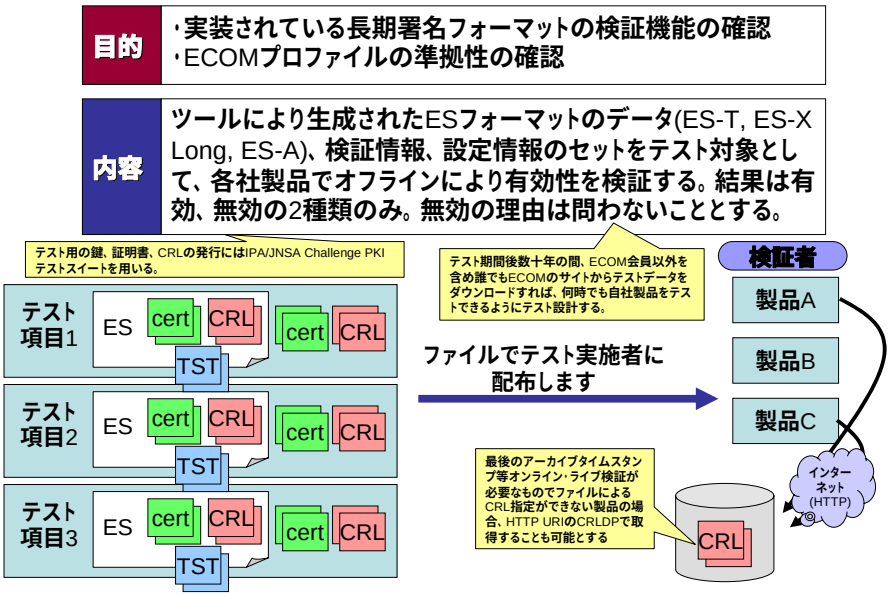


図 2-1 オフライン検証テスト

2.1 テストの準備

- **CRL のための設定**

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

- **署名対象データの設定**

内包署名の場合にはファイル'TARGET_AAA.txt'(ファイルの内容は"aaa"という 3 文字 3 バイトの文字列のみ)、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 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、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**

テストスイ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'data.der'というファイル名となっており、各テスト項目毎に別々のディレクトリに保存されている。

- **検証の実施**

これを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 SHA1 ハッシュ値は以下の通り。

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

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**
- **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**
- **時刻の表記は特に断りの無い限り、**UTC **時刻であるとする。**

2.4 オフライン検証テストのテスト項目の概要

オフライン検証テストのテストケースは以下の内容を含んでいる。

- ES-T, ES-C, ES-X Long, ES-A **フォーマットの検証**
- **内包署名と分離署名**
- **ハッシュアルゴリズム** (SHA-1, SHA-256, SHA-512)
- BES **と** EPES
- RFC3126 **と** ETSI TS 101733 v1.5.1 **以降のアーカイブハッシュ**
- SigningTime, SignatureTimeStamp **時刻による失効、期限切れ検証**
- **各種ハッシュ値の改竄の検証**
- **コンテンツタイムスタンプ**

- **並列署名(=独立署名)**
- **署名ポリシーファイルを考慮した検証**

全 30 テスト項目のリストを以下に示す。

番号	テスト項目名	期待値
10001	EST-ATTACH-NORMAL-OK	有効
BES 内包署名による ES-T フォーマットのデータが有効となることを検証する。		
10002	EST-ATTACH-EXPIRED-NG	無効
ES-T フォーマットで署名者証明書が期限切れの場合、無効となることを検証する。		
10003	EST-ATTACH-REVOKED-NG	無効
期限切れではないが署名タイムスタンプの genTime の値よりも前に署名者証明書が失効している場合に ES-T データが無効であることを検証する。		
10004	EST-ATTACH-SIGTIME-REVOKED-OK	有効
SigingTime 属性の値の時点では失効しているが、署名タイムスタンプの時点では失効していない場合に、SigningTime 属性の値に関わらず ES-T データが有効であることを検証する。		
10005	EST-ATTACH-SIGTS-REVOKED-NG	無効
SigningTime 属性の値の時点では失効してないが、署名タイムスタンプの時点で失効している場合に、署名タイムスタンプを考慮して ES-T データが無効であることを検証する。		
10006	EST-ATTACH-ES-SIG-FORGED-NG	無効
signerInfo の signature フィールドが改竄されている場合に ES-T データが無効であることを検証する。		
10007	EST-ATTACH-ES-SIGTS-SIG-FORGED-NG	無効
署名タイムスタンプのタイムスタンプトークンの signature フィールドが改竄されている場合に、ES-T データが無効であることを検証する。		
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG	無効
signedAttrs フィールド中の MessageDigest CMS 属性の値が改竄されている場合に、ES-T データが無効であることを検証する。		
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG	無効
署名タイムスタンプのタイムスタンプトークンの MessageDigest CMS 属性が改竄されている場合に、ES-T データが無効であることを検証する。		
10010	EST-DETACH-NORMAL-OK	有効
BES 分離署名による ES-T フォーマットのデータが有効であることを検証する。		
20001	EST-OTHERCERT-SHA256-OK	有効
SHA-256 アルゴリズムによる OtherSigningCertificate CMS 属性がある場合に、ES-T フォーマットのデータが有効であることを検証する。		
20002	EST-SIGTS-SHA256-OK	有効
TSTInfo の MessageImprint および SignerInfo の DigestAlgorithm フィールドが SHA-256 アルゴリズムであり、signatureAlgorithm が SHA256withRSA であるようなタイムスタンプトークンの署名タイムスタンプである場合に、ES-T フォーマットデータが有効であることを検証する。		
20003	EST-SIGTS-SHA512-OK	有効
TSTInfo の MessageImprint および SignerInfo の DigestAlgorithm フィールドが SHA-512 アルゴリズムであり、signatureAlgorithm が SHA512withRSA であるようなタイムスタンプトークンの署名タイムスタンプである場合に、ES-T フォーマットデータが有効であることを検証する。		
20004	EST-CONTENT-TIMESTAMP-OK	有効
signedAttributes フィールドに ContentTimeStamp CMS 属性がある場合に、ES-T フォーマットデータが有効であることを検証する。		
20005	EST-INDEPENDENT-SIGNATURES-OK	有効
2 つの signerInfo を持つような並列署名(独立署名)である ES-T フォーマットデータが有効であることを検証する。		
20006	EST-EPES-WITHOUT-HASHCHECK-OK	有効

signaturePolicyIdentifier CMS 属性があるような EPES に基づく ES-T フォーマットデータが有効であることを検証する。		
20007	EST-EPES-NORMAL-OK	有効
signaturePolicyIdentifier CMS 属性がある EPES に基づく ES-T フォーマットデータにおいて、署名ポリシーファイルを参照しながら有効であることを検証する。		
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG	無効
signaturePolicyIdentifier CMS 属性のハッシュ値が署名ポリシーと一致しない場合に ES-T フォーマットが無効であることを検証する。		
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG	無効
署名ポリシーファイルの signingPeriod の notBefore フィールドの時刻が遠い将来であり、まだ有効期間内に無い場合、署名ポリシーが無効であるために ES-T フォーマットが現時点で無効であることを検証する。		
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG	無効
署名ポリシーファイルの mandatedSignedAttr フィールドで必須とされている SigningTime 属性が無い場合に、ES-T フォーマットデータが無効であることを検証する。		
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG	無効
署名ポリシーファイルにおいて externalSignedData が TRUE、即ち分離署名を要求しているにも関らず、内包署名である場合に、ES-T フォーマットデータが無効であることを検証する。		
40001	ESC-ATTACH-NORMAL-OK	有効
内包署名の BES に基づく ES-C フォーマットデータが有効であることを検証する。		
40002	ESC-DETACH-NORMAL-OK	有効
分離署名の BES に基づく ES-C フォーマットデータが有効であることを検証する。		
50001	ESXL-ATTACH-NORMAL-OK	有効
内包署名の BES に基づく ES-X Long フォーマットデータが有効であることを検証する。		
50002	ESXL-DETACH-NORMAL-OK	有効
分離署名の BES に基づく ES-X Long フォーマットデータが有効であることを検証する		
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK	有効
署名タイムスタンプの TSA 証明書のための懸賞情報がトークンに含まれず、ファイルなどの別の方法で検証情報が提供される場合に、ES-X Long フォーマットのデータが有効であることを検証する。		
70001	ESA1-ATTACH-NORMAL-OK	有効
内包署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
70002	ESA1-DETACH-NORMAL-OK	有効
分離署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
80001	ESA1-ATTACH-ETSI151-OK	有効
ESTI TS 101 733 v1.5.1 以降のアーカイブハッシュ計算方法による内包署名による第一世代の ES-A フォーマットデータが有効であることを検証する。		
80002	ESA1-DETACH-ETSI151-OK	有効
ESTI TS 101 733 v1.5.1 以降のアーカイブハッシュ計算方法による分離署名による第一世代の ES-A フォーマットデータが有効であることを検証する。		

2.5 ES-T フォーマット標準テスト項目

2.5.1 <EST-ATTACH-NORMAL-OK 10001>

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、共に失効しない場合。ES-T データが有効であることを検証する。本テストケースは ES-T フォーマットの標準テストである。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.5.2 <EST-ATTACH-EXPIRED-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 ES-T データが無効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1 00:00:00～2001.1.1 23:5959
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 00:00:00～2035.12.31 23:59:59

2.5.3 <EST-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。

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	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	2005.1.1 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

2.5.4 <EST-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。

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

2.5.5 <EST-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。

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	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	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

2.5.6 <EST-ATTACH-ES-SIG-FORGED-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竄されていた場合に無効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

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

ES-T フォーマットの SiginatureTimeStamp 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竄されていた場合に無効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

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

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

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.5.9 <EST-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 中の MessageDigest 属性の値が改竄されていた場合に無効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.5.10 <EST-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。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.6 ES-T フォーマットオプショナルテスト項目

2.6.1 <EST-OTHERCERT-SHA256-OK 20001>

テスト項目<EST-ATTACH-NORMAL-OK>と比較して、署名者証明書を特定するための情報として、ESSSigningCertificate 属性ではなく、ハッシュアルゴリズムに SHA256 を用いた場合で証明書のハッシュ値が一致している場合に、有効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.6.2 <EST-SIGTS-SHA256-OK 20002>

ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンのハッシュアルゴリズムに SHA256、署名アルゴリズムに SHA256withRSA が用いられた場合に有効であることを検証する。

- TimeStampToken の TSTInfo の MessageImprint は SHA256
- TimeStampToken の SignerInfo の DigestAlgorithm は SHA256
- TimeStampToken の SignerInfo の SignatureAlgorithm は SHA256withRSA

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.6.3 <EST-SIGTS-SHA512-OK 20003>

ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンのハッシュアルゴリズムに SHA512、署名アルゴリズムに SHA512withRSA が用いられた場合に有効であることを検証する。

- TimeStampToken の TSTInfo の MessageImprint は SHA512
- TimeStampToken の SignerInfo の DigestAlgorithm は SHA512
- TimeStampToken の SignerInfo の SignatureAlgorithm は SHA512withRSA

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.6.4 <EST-CONTENT-TIMESTAMP-OK 20004>

ES-T フォーマットのデータの CMS 署名属性に有効なコンテンツタイムスタンプが含まれている場合に有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
コンテンツタイムスタンプの時刻	2001.1.1 09:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59

2.6.5 <EST-INDEPENDENT-SIGNATURES-OK 20005>

二人の署名者による並列署名(独立署名とも言う)の双方に有効な署名タイムスタンプが付与された ES-T フォーマットのデータが有効であることを検証する。

二人の署名者用証明書は同一のサブ CA から発行されているとする。

期待値	有効(valid)
署名 1 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 1 の時刻	属性無し
署名タイムスタンプ 1 の時刻	2001.1.1 12:00:00
署名者証明書 1 の有効期限	2001.1.1～2035.12.31
署名 2 を実施したとする時刻	2001.1.1 13:00:00
サイニングタイム属性 2 の時刻	属性無し
署名タイムスタンプ 2 の時刻	2001.1.1 13:00:00
署名者証明書 2 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 00:00:00～2035.12.31 23:59:59

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

signedAttributes フィールドに署名ポリシー識別子を明示的に持つ EPES(Explicit Policy Electronic Signatures)フォーマットに対し署名タイムスタンプを付与した ES-T データを読み込みエラーとならないことを検証する。
署名ポリシーを厳密に扱う実装では、テストデータとして配布される署名ポリシーファイルを共に検証に用いる。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5
署名ポリシーSHA1 ハッシュ値	af1d3ea7aef706a898191dd257218f5e9acafaa1

2.6.7 <EST-EPES-NORMAL-OK 20007>

signedAttributes フィールドに署名ポリシー識別子を明示的に持つ EPES フォーマットに対し署名タイムスタンプを付与した ES-T データおよび署名ポリシーファイルを読み込み EPES フォーマットより生成された ES-T データが有効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5.20000
署名ポリシーSHA1 ハッシュ値	90490e8e411bd495415988298d07ab45922e8bff

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

EPES より生成された ES-T フォーマットのデータにおいて、その SignaturePolicyIdentifier CMS 署名属性の持つハッシュ値が署名ポリシーファイルのハッシュ値と一致しない場合に、その ES-T データが無効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5.20000
署名ポリシーSHA1 ハッシュ値	90490e8e411bd495415988298d07ab45922e8bff
CMS 署名ポリシー識別子属性のハッシュ値	1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f

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

EPES より生成された ES-T フォーマットのデータの使用する署名ポリシーデータにおいて、signingPeriod の notBefore フィールドの値が常に無効となるような値(2035 年 12 月 31 日)に設定されていた場合に、署名ポリシーが有効期間内に無いために、関連付けられた ES-T データが無効となることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5.20009
署名ポリシーSHA1 ハッシュ値	eab88babb6ffc05343fc8ef0ca6a7dd4920b7e02
署名ポリシーの sigingPeriod.notBefore フィールド	2035.12.31 23:59:59

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

EPES より生成された ES-T フォーマットのデータに関連付けられた署名ポリシーデータにおいて、commonRules の signerAndVerifierValue の signerRules の mandatedSigndAttr に sigingTime の OID が含まれているにもかかわらず、ES-T フォーマットのデータには signingTime CMS 属性が含まれていない場合に、署名ポリシーに違反するため ES-T データが無効となることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5.20010
署名ポリシーSHA1 ハッシュ値	5a6c1d137ca139771adbd8d41c868d682ded8b20
mandatedSignedAttr	1.2.840.113549.1.9.4 1.2.840.113549.1.9.5(signingTime)

	1.2.840.113549.1.9.16.2.15

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

EPES より生成された ES-T フォーマットのデータに関連付けられた署名ポリシーデータにおいて、commonRules の signerAndVerifierValue の signerRules の externalSignedData フィールドの値が TRUE、即ち署名ポリシーが分離署名であることを要求している場合に、ES-T フォーマットのデータが内包署名であったとき、署名ポリシーに違反するため ES-T データが無効となることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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 00:00:00～2035.12.31 23:59:59
署名ポリシーOID	1.2.3.4.5.20011
署名ポリシーSHA1 ハッシュ値	b363f51a65438136d26ce87f3078657df52b5dc4
externalSignedData	TRUE

2.7 ES-C フォーマット標準テスト項目

ES-C フォーマットは ECOM プロファイルにおいてオプショナルであるため、標準テスト項目は無しとする。

2.8 ES-C フォーマットオプショナルテスト項目

2.8.1 <ESC-ATTACH-NORMAL-OK 40001>

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、共に失効しない場合。ES-C データが有効であることを検証する。本テストケースは ES-C フォーマットの標準テストである。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

2.8.2 <ESC-DETACH-NORMAL-OK 40002>

署名対象文書に対して分離署名を行った ES-C 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。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

2.9 ES-X Long フォーマット標準テスト項目

2.9.1 <ESXL-ATTACH-NORMAL-OK 50001>

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、共に失効しておらず、これらの検証情報を含む ES-X Long データが有効であることを検証する。本テストケースは ES-X Long フォーマットの標準テストである。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

2.9.2 <ESXL-DETACH-NORMAL-OK 50002>

署名対象文書に対して分離署名を行った ES-X Long 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。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

2.10 ES-X Long フォーマットオプショナルテスト項目

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

ES-X Long フォーマットを検証する際、署名タイムスタンプ属性のタイムスタンプトークンの TSA 証明書の検証情報がトークン無いに含まれず、別の手段により渡される場合、この ES X-Long フォーマットが有効であることを検証する。

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	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	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

2.11 ES-A フォーマット標準テスト項目

2.11.1 <ESA1-ATTACH-NORMAL-OK 70001>

ECOM 長期署名フォーマットプロファイル 2005 で定めた RFC3126 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。

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	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 12:00:00
Archive タイムスタンプ 1 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

2.11.2 <ESA1-DETACH-NORMAL-OK 70002>

署名対象文書に対して分離署名を行った第一世代の ArchiveTimeStamp のみを持つ ES-A 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。

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	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 12:00:00
Archive タイムスタンプ 1 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

2.12 ES-A フォーマットオプショナルテスト項目

2.12.1 <ESA1-ATTACH-ETSI151-OK 80001>

ECOM 長期署名フォーマットプロファイルの範囲外ではあるが、ETSI TS 101 733 v1.5.1 以降で定めている新しいアーカイブハッシュ計算方法に本設計書付録で示した正規化法を用いたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。

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	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 12:00:00
Archive タイムスタンプ 1 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

2.12.2 <ESA1-DETACH-ETSI151-OK 80002>

テスト項目<ESA1-ATTACH-ETSI151-OK>と同じ条件で分離署名であった場合に ES-A フォーマットが有効であることを検証する。最初のハッシュ対象 encapContentInfo はコンテンツを含め内部まで DER 正規化されていなければならない。署名対象データは<ESA1-ATTACH-ETSI151-OK>と同じデータとし、他の分離署名の署名対象とは異なる。

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	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 12:00:00
Archive タイムスタンプ 1 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

2.13 ES-T 標準テストケース

本節では ES-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。

2.13.1 <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：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK

2.13.2 <OFF-T-2>

テストケース名	OFF-T-2
ES-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：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG

2.13.3 <OFF-T-3>

テストケース名	OFF-T-3
ES-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：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG

2.13.4 <OFF-T-4>

テストケース名	OFF-T-4

ES-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行える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG
10003	EST-ATTACH-REVOKED-NG

2.13.5 <OFF-T-5>

テストケース名	OFF-T-5
ES-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：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG
10004	EST-ATTACH-SIGTIME-REVOKED-OK
10005	EST-ATTACH-SIGTS-REVOKED-NG

2.13.6 <OFF-T-6>

テストケース名	OFF-T-6
ES-T フォーマットの SignerInfo の署名値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10006	EST-ATTACH-ES-SIG-FORGED-NG

2.13.7 <OFF-T-7>

テストケース名	OFF-T-7
ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンの SignerInfo の	

署名値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10007	EST-ATTACH-SIGTS-SIG-FORGED-NG

2.13.8 <OFF-T-8>

テストケース名	OFF-T-8
ES-T フォーマットの MessageDigest のハッシュ値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG

2.13.9 <OFF-T-9>

テストケース名	OFF-T-8
ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンの MessageDigest のハッシュ値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG

2.13.10 <OFF-T-10>

テストケース名	OFF-T-10
分離署名の ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10010	EST-DETACH-NORMAL-OK

2.14 ES-T オプショナルテストケース

本節では ES-T フォーマットを扱う実装の機能を確認するために行うことが可能はオプショナルテストケースを示す。

2.14.1 <OFF-T-OP-1>

テストケース名	OFF-T-OP-1
OtherSigningCeritificate 属性において SHA-256 である ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20001	EST-OTHERCERT-SHA256-OK

2.14.2 <OFF-T-OP-2>

テストケース名	OFF-T-OP-2
署名タイムスタンプのタイムスタンプトークンのハッシュや署名に SHA-256 アルゴリズムが使われている ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20002	EST-SIGTS-SHA256-OK

2.14.3 <OFF-T-OP-3>

テストケース名	OFF-T-OP-3
署名タイムスタンプのタイムスタンプトークンのハッシュや署名に SHA-512 アルゴリズムが使われている ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20003	EST-SIGTS-SHA512-OK

2.14.4 <OFF-T-OP-4>

テストケース名	OFF-T-OP-4
CMS 署名属性にコンテンツタイムスタンプ属性が含まれる ES-T フォーマットを正しく検証できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20004	EST-CONTENT-TIMESTAMP-OK

2.14.5 <OFF-T-OP-5>

テストケース名	OFF-T-OP-5
独立署名(並列署名)、即ち signerInfo が 2 つあり、署名に用いたそれらの署名者証明書が同一の信頼点である ES-T フォーマットを正しく検証できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20005	EST-INDEPENDENT-SIGNATURES-OK

2.14.6 <OFF-T-OP-6>

テストケース名	OFF-T-OP-6
EPES フォーマットに基づく ES-T フォーマットにおいて読み込み時エラーとならないことを検証する。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20006	EST-EPES-WITHOUT-HASHCHECK-OK

備考：署名ポリシーを正しく扱う実装は、テストデータに含まれる署名ポリシーを用いて検証を行う。署名ポリシーを処理しない実装はエラーが発生しないことのみを確認する。

2.14.7 <OFF-T-OP-7>

テストケース名	OFF-T-OP-7
EPES フォーマットに基づく ES-T フォーマットにおいて署名ポリシーのハッシュ値の一致確認を行い正しく署名ポリシーが扱えることを検証する。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG

2.14.8 <OFF-T-OP-8>

テストケース名	OFF-T-OP-8
EPES に基づく ES-T フォーマットにおいて、署名ポリシーの notBefore を正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG

2.14.9 <OFF-T-OP-9>

テストケース名	OFF-T-OP-9
EPES に基づく ES-T フォーマットにおいて、署名ポリシーの signerRules の mandatedSignedAttrs を正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG

2.14.10 <OFF-T-OP-11>

テストケース名	OFF-T-OP-10
EPES に基づく ES-T フォーマットにおいて、署名ポリシー^が externalSignedData が TRUE,即ち分離署名を要求しているのに内包署名であるような ES-T データを正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG

2.15 ES-C オプショナルテストケース

2.15.1 <OFF-C-OP-1>

テストケース名	OFF-C-OP-1
一般的な内包署名の ES-C フォーマットを読み込むことができる	
成功条件：以下のテスト項目が全て期待値通り	
40001	ESC-ATTACH-NORMAL-OK

2.15.2 <OFF-C-OP-2>

テストケース名	OFF-C-OP-2
分離署名の ES-C フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
40001	ESC-ATTACH-NORMAL-OK
40002	ESC-DETACH-NORMAL-OK

2.16 ES-X Long 標準テストケース

2.16.1 <OFF-X-1>

テストケース名	OFF-X-1
一般的な内包署名の ES-X Long フォーマットを読み込むことができる	
成功条件：以下のテスト項目が全て期待値通り	
50001	ESXL-ATTACH-NORMAL-OK

2.16.2 <OFF-X-2>

テストケース名	OFF-X-2
分離署名の ES-X Long フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
50002	ESXL-DETACH-NORMAL-OK

2.17 ES-X Long オプショナルテストケース

2.17.1 <OFF-X-OP-1>

テストケース名	OFF-X-OP-1
ES-X Long フォーマットで署名タイムスタンプの検証情報がそのタイムスタンプトークン内に含まれていない場合に別途与えられる検証情報を元に検証できる	
成功条件：以下のテスト項目が全て期待値通り	
50001	ESXL-ATTACH-NORMAL-OK
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK

2.18 ES-A 標準テストケース

2.18.1 <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：以下のテスト項目が全て期待値通り	
70001	ESA1-ATTACH-NORMAL-OK

2.18.2 <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：以下のテスト項目が全て期待値通り	
70002	ESA1-DETACH-NORMAL-OK

2.19 ES-A オプショナルテストケース

2.19.1 <OFF-A-OP-1>

テストケース名	OFF-A-OP-1
ETSI TS 101 733 v1.5.1 以降のハッシュ計算法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：以下のテスト項目が全て期待値通り	
80001	ESA1-ATTACH-ETSI151-OK

2.19.2 <OFF-A-OP-2>

テストケース名	OFF-A-OP-2
ETSI TS 101 733 v1.5.1 以降のハッシュ計算法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：以下のテスト項目が全て期待値通り	
80002	ESA1-DETACH-ETSI151-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

ある実装が生成した有効な長期署名フォーマットのデータが相互に読み込みおよび検証ができることを確認するためのテストを行う。あらかじめ指定された署名対象データ、証明書、CRL、タイムスタンプサービスを用いて参加企業全ての製品により長期署名フォーマットデータ(ES-T, ES-X Long, ES-A)を生成する。参加企業の各製品において、他社製品の生成したデータが有効であることを検証する。CRL およびタイムスタンプトークンはオンラインで取得する。

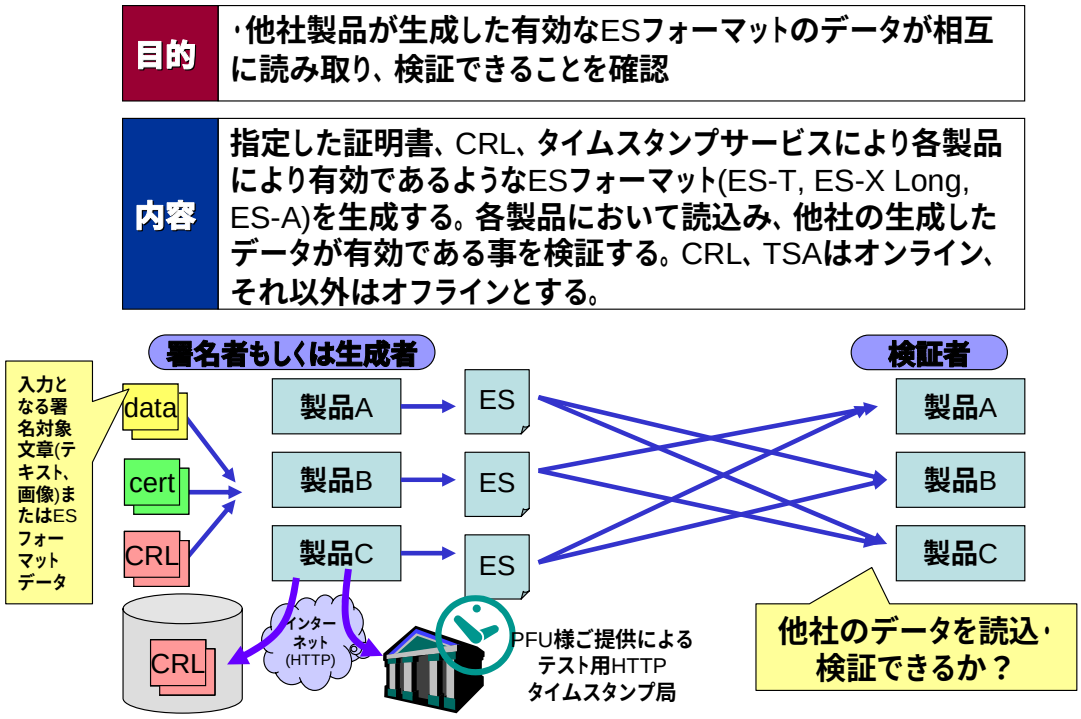


図 3-1 オンラインマトリックス生成・検証テスト

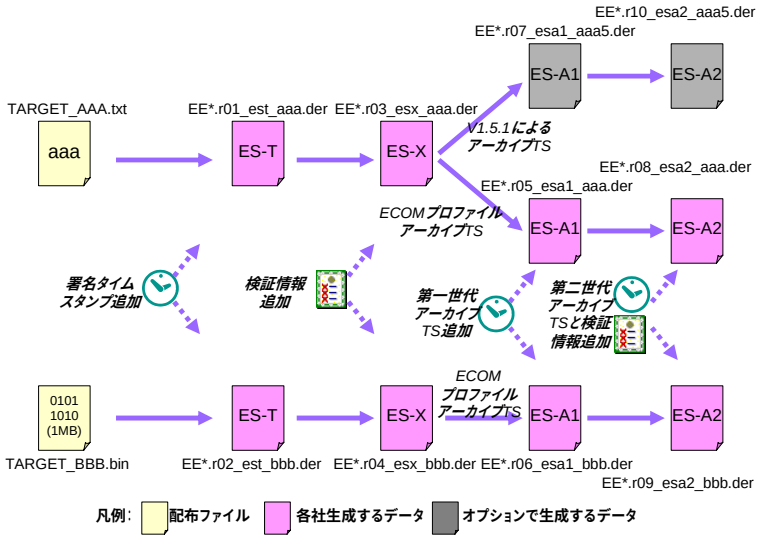
テストケースは 10 項目ある。オプショナルテストとして、ETSI TS 101 733 v1.5.1 に基づく新しいアーカイブタイムスタンプのハッシュ値の計算方法を用いたテストもある。

参加企業の実装では、ES-C フォーマットを出力できる製品が少ないために ES-C フォーマットを実験対象から外した。また、文書管理製品で ES-X Long の

状態で ES-A とは異なる別のセキュアなアーカイビング方法を採用して保存する製品もあるため、ES-X Long はテスト対象に加えた。

3.1 生成するデータ

小さいサイズのテキストデータを内包署名、1MB 程度のバイナリデータファイルを分離署名として、それぞれ ES-T フォーマット、ES-X Long 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。オプショナルテストとして ETSI TS 101 733 v1.5.1 以降のアーカイブタイムスタンプハッシュ対象計算方法(4.1 節参照)を用いたデータ生成を行ってよい。



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

- CRL のための設定

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)

- **署名対象データの設定**

内包署名の場合にはファイル'TARGET_AAA.txt'(ファイルの内容は"aaa"という 3 文字 3 バイトの文字列のみ)、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 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**

内包署名の場合にはファイル'TARGET_AAA.txt'(ファイルの内容は"aaa"という 3 文字 3 バイトの文字列のみ)、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 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、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**
- **検証の実施**

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> データ内包型 ES-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 ES-T データを生成する。

- ◎署名対象が文字列"aaa"(x61 x61 x61)
- ◎内包署名とする。(EncapContentInfo に"aaa"を含む)
- MessageDigest は SHA1
- 署名アルゴリズムは SHA1withRSA
- BES フォーマットより ES-T を生成

各製品を用いこれが有効であることを検証する。

3.5.2 <ON-T-2> データ分離型 ES-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 ES-T データを生成する。

- ◎署名対象が 1MB 程度のデータファイル
- ◎分離署名とする。(EncapContentInfo に署名対象を含まない)

3.5.3 <ON-X-1> データ内包型 ES-X Long 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社 ES-X Long データを生成する。

- ◎<ON-T-1>で生成された ES-T データを対象とし生成
- <ON-T-1>の ES-T を生成後、48 時間以降経過した後に ES-X Long を生成する
- 署名、および署名タイムスタンプ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

各製品を用いこれが有効であることを検証する。

3.5.4 <ON-X-2> データ分離型 ES-X Long 生成・相互検証テストケース

テストケース<ON-X-1>を基本に以下のレギュレーションを加えたもので各製品により ES-X Long データを生成する。

- ◎<ON-T-2>で生成された ES-T データを対象とし生成
- ◎署名対象が 1MB 程度のデータファイル
- ◎分離署名とする。(EncapContentInfo に署名対象を含まない)

各製品を用いこれが有効であることを検証する。

3.5.5 <ON-A1-1> データ内包型第一世代 ES-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により ES-A データを生成する。

- ◎<ON-X-1>で生成された ES-X Long データ、もしくは製品が未対応ならば、<ON-T-1>で生成された ES-T データを対象とし生成
- アーカイブタイムスタンプの生成・検証方法は ECOM プロファイル (RFC 3126 or ESTI TS 101 733 v1.4.0 以前の方法)に基づく
- 署名、および署名タイムスタンプの証明書検証情報情報の格納内容、方法は ECOM プロファイルに基づく

各製品を用いこれが有効であることを検証する。

3.5.6 <ON-A1-2> データ分離型第一世代 ES-A 生成・相互検証テストケース

<ON-A1-1>のレギュレーションを基本に以下のレギュレーションを加えたもので各製品により ES-A データを生成する。

- ◎<ON-X-2>で生成された ES-X Long データ、もしくはこれに製品が未対応ならば、<ON-T-2>で生成された ES-T データを対象とし生成
- ◎署名対象が 1MB 程度のデータファイル
- ◎分離署名とする。(EncapContentInfo に署名対象を含まない)

各製品を用いこれが有効であることを検証する。

3.5.7 <ON-A1-3> データ内包型第一世代新方式 ES-A 生成・相互検証テストケース(OP)

本テストケースはオプショナルである。以下のレギュレーションで各製品により ES-A データを生成する。

- ◎<ON-X-1>で生成された ES-X Long データを対象とし生成

- ◎アーカイブタイムスタンプの生成・検証方法は ESTI TS 101 733 v1.5.1 に基づき、ECOM 長期署名フォーマット SWG で合意を得た正規化方法を用いた計算方法を用いる。
- 署名、および署名タイムスタンプ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

各社製品を用いこれが有効であることを検証する。

3.5.8 <ON-A2-1> データ内包型第二世代 ES-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 ES-A データを生成する。

- ◎<ON-A1-1>で生成された ES-A を対象とし生成(署名延長)
- ◎アーカイブタイムスタンプの生成・検証方法は ECOM プロファイル (RFC 3126 or ESTI TS 101 733 v1.4.0 以前の方法)に基づく
- 署名、および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

各製品を用いこれが有効であることを検証する。

3.5.9 <ON-A2-2> データ分離型第二世代 ES-A 生成・相互検証テストケース

<ON-A2-1>のレギュレーションを基本に以下のレギュレーションを加えたもので各製品 ES-A データを生成する。

- ◎<ON-A1-2>で生成された ES-A データを対象とし生成(署名延長)
- ◎署名対象が 1MB 程度のデータファイル
- ◎分離署名とする。(EncapContentInfo に署名対象を含まない)

各社製品を用いこれが有効であることを検証する。

3.5.10 <ON-A2-3> データ内包型第二世代新方式 ES-A 生成・相互検証テストケース(OP)

本テストケースはオプショナルである。以下のレギュレーションで各社 ES-A データを生成する。

- ◎<ON-A1-3>で生成された ES-A データを対象とし生成
- ◎アーカイブタイムスタンプの生成・検証方法は ESTI TS 101 733 v1.5.1 に基づき、ECOM 長期署名フォーマット SWG で合意を得た正規化方法を用いた計算方法を用いる。
- 署名、および署名タイムスタンプ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

各社製品を用いこれが有効であることを検証する。

4 参考資料

4.1 ECOM オプショナルテストで用いられる ETSI TS 101 733 v1.5.1 以降によるアーカイブハッシュ計算法

H17 年度に ECOM 長期署名フォーマット普及 SWG が策定した CAdES フォーマットプロファイルでは、RFC 3126 や ETSI TS 101 733 v1.4.2 で用いられていたアーカイブタイムスタンプのハッシュ対象計算方法を採用している。これは、ETSI TS 101 733 v1.5.1 で記載されている方法を相互運用させるためには、データの正規化方法や署名延長中に他の CMS 非署名属性が加わった場合の処理方法、直列署名(CounterSignature)の場合の処理などが記述されておらず、日本発のプロファイルとして ETSI と調整を必要としたことから従来方法を採用している。

今回の実証実験のために、現時点で妥当と思われる v1.5.1 ベースの計算方法を仮決めし、この方法を元にオプショナルテストとして v1.5.1 ベースのテストケースを作成した。当然の事ながら、今後、調整されるであろう v1.5.1 ベースの標準やプロファイルの改変に対して直接的に影響を与えるものではなく、単に議論のきっかけを与えたに過ぎない。

標準よりハッシュ対象は下図の通りである。

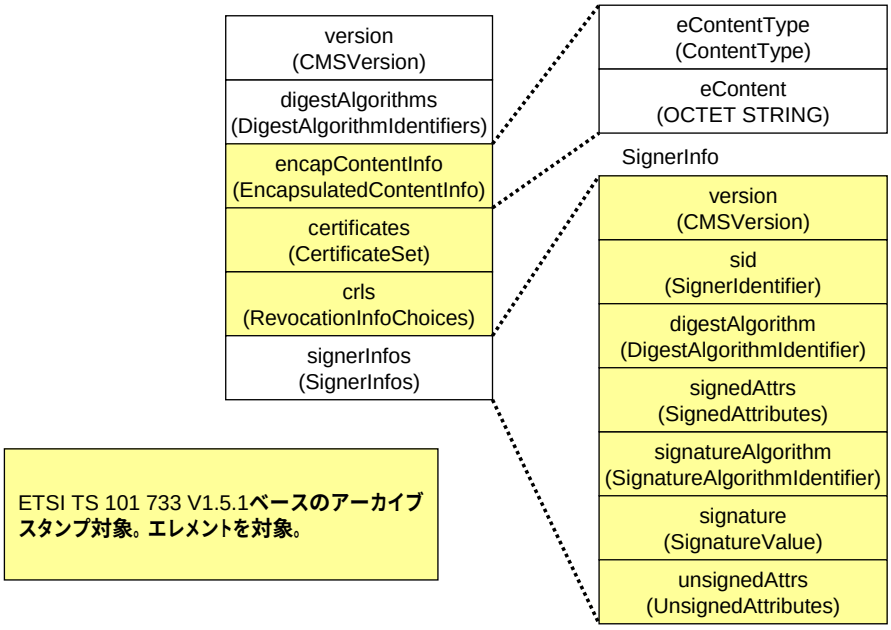


図 4-1 ETSI TS 101 733 v1.5.1 以降のアーカイブハッシュ対象

その計算方法は以下の通りとする。

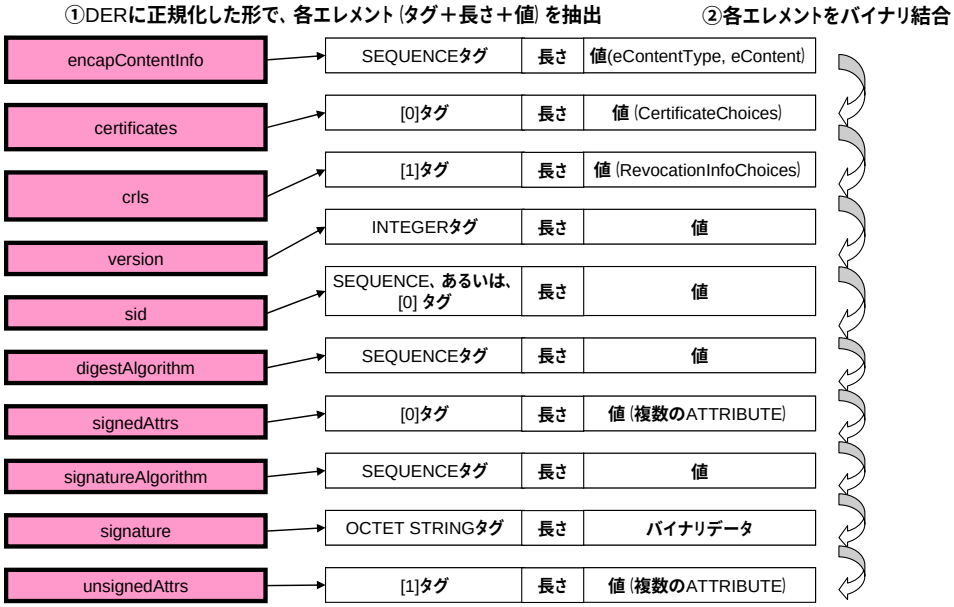
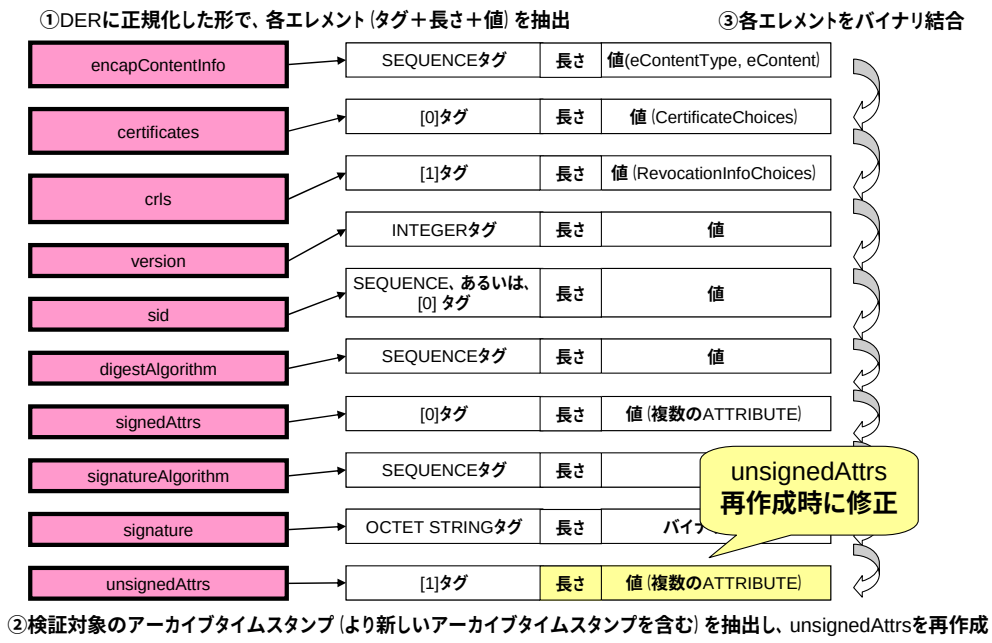


図 4-2 本実証実験のために定めた v1.5.1 ベースのハッシュ計算法

ハッシュ対象に ASN.1 TLV(タグ、長さ、値)構造のタグおよび長さ部分もハッシュ対象に含まれることに注意しなければならない。また、ContextSpecific タグ([0]や[1]など)は、SET や SEQUENCE に正規化することなく、そのままハッシュ対象として加えなければならない。

各アーカイブタイムスタンプの検証時には、下図の手順でハッシュ対象を生成する。特に注意しなければならないのは CMS 非署名属性の再計算についてである。例えば CMS 非署名属性中に n 個のアーカイブスタンプがあったとして、その途中の i 番目のアーカイブタイムスタンプを検証する際には、CMS 非署名属性において 1 番目から i 番目アーカイブタイムスタンプ属性の一つ手前の属性までを要素とする新しい CMS 非署名属性の ContextSpecific '[1]'の ASN.1 SET 構造を再生成し、その結果 ASN.1 TLV 構造の長さバイトも再計算を行い、これをハッシュ対象としなければならない。


①DERに正規化した形で、各エレメント（タグ＋長さ＋値）を抽出
③各エレメントをバイナリ結合
encapContentInfo
SEQUENCEタグ
長さ
値(eContentType, eContent)
certificates
[0]タグ
長さ
値（CertificateChoices）
crls
[1]タグ
長さ
値（RevocationInfoChoices）
version
INTEGERタグ
長さ
値
sid
SEQUENCE、あるいは、
[0] タグ
長さ
値
digestAlgorithm
SEQUENCEタグ
長さ
値
signedAttrs
[0]タグ
長さ
値（複数のATTRIBUTE）
signatureAlgorithm
SEQUENCEタグ
長さ
signature
OCTET STRINGタグ
長さ
unsignedAttrs
[1]タグ
長さ
値（複数のATTRIBUTE）
unsignedAttrs
再作成時に修正
②検証対象のアーカイブタイムスタンプ（より新しいアーカイブタイムスタンプを含む）を抽出し、unsignedAttrsを再作成

5 付録：実験用データプロファイル

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。

5.1 実験用長期署名フォーマットデータのプロファイル

長期署名フォーマットのデータは全て CMS SignedData フォーマットに基づいており、その中で各フォーマット毎に signedAttributes フィールドおよび unsignedAttributes フィールドに必要となる CMS 属性が異なる。

5.1.1 BES (Basic Electronic Signature)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

5.1.2 EPES (Explicit Policy-based Electronic Signature)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
sigPolicyId	有(SHA1フィンガープリント)
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

5.1.3 ES-T

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う

5.1.4 ES-X Long

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う(検証情報を含む)
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

5.1.5 ES-A (**第一世代**)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う(検証情報を含む)
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

5.1.6 ES-A (第二世代以降)

フィールド			値
version			v3(3)
digestAlgorithms			{ SHA1 }
encapContentInfo			内包/分離はテスト項目に依存
certificates			署名者証明書のみ
crls			無
signerInfos			有(要素数=1)
	signerInfo		160bit
		version	v3(3)
		sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
		digestAlgorithm	SHA1
		signedAttrs	有
			contentInfo =data(1.2.840.113549.1.7.1)
			messageDigest 有
			eSSSigningCertificate 有(発行者名、シリアル番号、SHA1フィンガープリント)
		signatureAlgorithm	SHA1withRSA
		signature	署名値
		unsignedAttrs	有
			signatureTimeStamp トークンは実験用データプロファイルに従う(検証情報を含む
			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
			archiveTimeStamp1 トークンは実験用データプロファイルに従う(検証情報を含む
			archiveTimeStamp2 ... トークンは実験用データプロファイルに従う(署名延長)

5.2 実験用タイムスタンプトークンのプロファイル

5.2.1 TimeStampToken

TimeStampToken は CMS SignedData の構造となっている。ECOM プロファイルの ES-X Long, ES-A の検証情報の格納方法の定義に従い、certificates, crls フィールドに検証情報を持つ場合がある。

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	前述TSTInfoプロファイルに従う
certificates	ECOMプロファイルにより検証情報としてTSA証明書およびパスを含みうる
crls	ECOMプロファイルにより検証情報として全てのCRLを含みうる
signerInfos	有(要素数=1)
signerInfo	160bit
version	v1(1)
sid	TSA証明書のIssuerAndSerialNumber
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=tSTInfo(1.2.840.113549.1.9.16.1.4)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

5.2.2 TSTInfo

フィールド	値
バージョン	v1(1)
policy	TSAPolicyId=0.1.2.3.4.5
messageImprint	有
hashAlgorithm	SHA1
hashedMessage	160bit
serialNumber	値はTSA証明書のシリアル番号と同じとする(※1)
genTime	GeneralizedTime(小数点以下最大3桁を含む)
accuracy	500ミリ秒
ordering	TRUE
nonce	0x1234567890(固定)
tsa	directoryName=TSA証明書の主体者名
extensions	無

※1：本来は該当 TSA より発行されたトークンのシリアル番号となるがテスト上 TSA からは 1 つのトークンしか発行されないので便宜上 TSA 証明書のシリアル番号と同じとし、テスト項目番号がすぐにわかるようにする。

5.3 実験用証明書のプロファイル

5.3.1 実験用証明書の共通のプロファイル

フィールド	値
バージョン	V3
シリアル番号	5バイトのASN.1 INTEGER(※1)
署名アルゴリズム	SHA1withRSA
発行者DN	PrintableString(全てのDNはPrintableStringとする)
有効期限	UTCTime(使用される時刻は2000/1/1 0:00:00～2035/12/31 23:59:59とする)
主体者DN	PrintableString
公開鍵情報	有
X.509拡張	有
keyUsage	有

5.3.2 RootCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	2048bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
basicConstraints	有	TRUE
CAフラグ	TRUE	-

5.3.3 SubCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
basicConstraints	有	TRUE
CAフラグ	TRUE	-
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

5.3.4 署名者用 End Entity 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
basicConstraints	有(空シーケンス)	FALSE
CAフラグ	無	-
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

5.3.5 TSA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
extKeyUsage	1.3.6.1.5.5.7.3.8(timeStamping)	TRUE
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

5.3.6 オンライン TSA 用 RootCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	2048bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
authorityCertIssuer	directoryName(PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	有	FALSE
CAフラグ	TRUE	-

5.3.7 オンライン TSA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
authorityCertIssuer	directoryName(PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	有(空シーケンス)	FALSE
CAフラグ	無	-
extKeyUsage	1.3.6.1.5.5.7.3.8(timeStamping)	TRUE
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	https://配布ホスト/**/*.crl	-

5.3.8 オンライン/オフライン/署名者/TSA 共通 CRL プロファイル

フィールド	値	クリティカル
バージョン	V2(1)	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
thisUpdate	UTCTime	
nextUpdate	UTCTime	
revokedCertificate		
userCertificate	失効する証明書のシリアル番号	
revocationDate	UTCTime	
crlEntryExtensions		
cRLReason		FALSE
X.509拡張	有	
cRLNumber		FALSE

5.4 実験用署名ポリシーのプロファイル

フィールド	値
signPolicyHashAlg	SHA1
signPolicyInfo	有
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c=JP
fieldOfApplication	"for …" テスト用ポリシーとしてのメモ
signatureValidationPolicy	
signingPeriod	
notBefore	有
notAfter	無
commonRules	
signerAndVerifierRules[0]	
signerRules	
externalSignedData?	無
mandatedSignedAttr	messageDigest, sigPolicyId
mandatedUnsignedAttr	signatureTimeStamp
mandatedCertificateRef?	無
mandatedCertificateInfo?	無
signPolExtensions?	無
verifierRules	
mandatedUnsignedAttr	空シーケンス
signPolExtensions?	無
signingCertTrustCondition[1]	
signerTrustTrees	署名者用CA証明書
signerRevReq	EE=crlCheck(0), CA=crlCheck(0)
timeStampTrustCondition[2]	
ttsCertificateTrustTrees[0]?	TSA用CA証明書
ttsRevReq[1]?	EE=crlCheck(0), CA=crlCheck(0)
attributeTrustCondition[3]	無
algorithmConstraintSet[4]	無
commitmentRules	空シーケンス
signPolExtensions	無
signPolExtensions	無
signPolicyHash	無