PKI Day 2011

最近の欧州PKI事情

2011年9月26日
一般財団法人日本情報経済社会推進協会（JIPDEC)
主席研究員　木村　道弘

目次

1. 欧州における電子署名基盤標準
    1. 標準化マップ
    2. 署名生成/検証と長期署名
    3. 信頼サービス提供者(TSP)のステータス情報リスト
    4. 書留電子メール（REM)
2. 直近の動向
    1. EC指令460 (Mandate 460)
    2. 電子署名基盤標準の枠組み再構築
    3. AdESベースラインプロファイル
    4. 認証局の適合性評価
    5. 署名ポリシ
    6. 2011年のプラグテスト（ PAdES & ASiC ）

１．欧州における電子署名基盤標準

電子署名指令第5条

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signature

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

— in electronic form, or

— not based upon a qualified certificate, or

— not based upon a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device

電子署名基盤の標準化推進体制

- 1999年～2004年　ICTSB/EESSI

  ICTSB：ICT Standard Board；　CEN（非電気）、CENELEC（電気）、ETSI（通信）によるICT領域の仕様調整イニシアティブ

  EESSI：European Electronic Signature Standardization Initiative

  – 目的はEC電子署名指令(1999)の実装を支援する標準化の調整

- 2004年～　ETSI/ESI

  ETSI TC ESI: European Telecommunications Standards Institute/ Electronic Signatures and Infrastructures

  ETSI：参加は60ヶ国748組織、日本は、JIPDEC、NEC、NICT、NTT、東工大

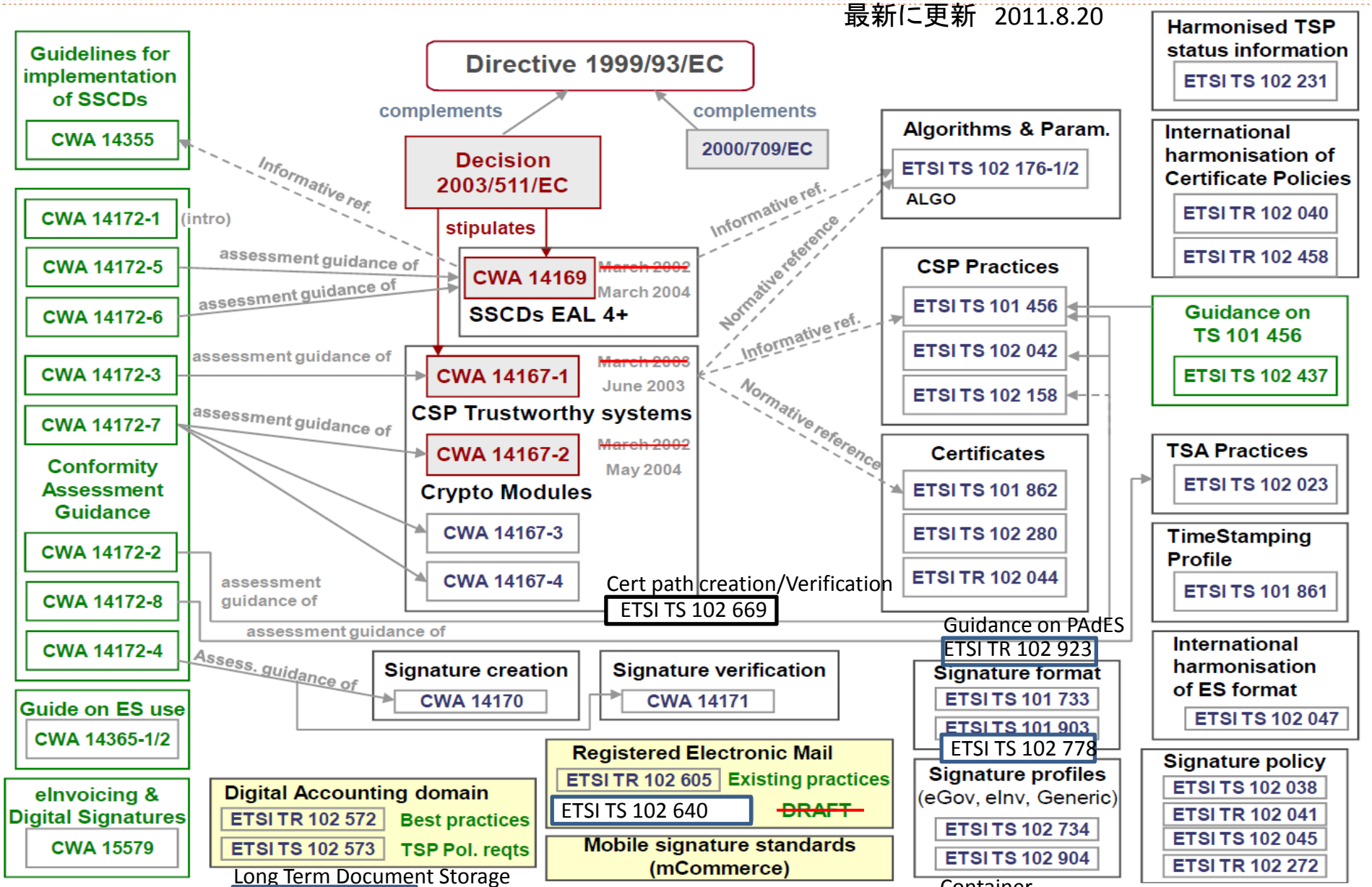
  27の技術委員会(TC)、120人体制の事務局

  ESI：前身は、ETSI TC SEC内のESI WG（1999年～）。2002年5月、ETSI TC SECのクローズに伴いTC SEC内のESI WG（1999年～）とLI (Lawful interception; 合法的傍受)WGをTCに昇格

  – EESSIの調整機能はNetwork and Information Security Steering Group (NISSG) に移管、CENのE-Signワークショップは2003年にクローズ

EU eSignature Standardisation Work overview

SEALEDの資料を
最新に更新　2011.8.20



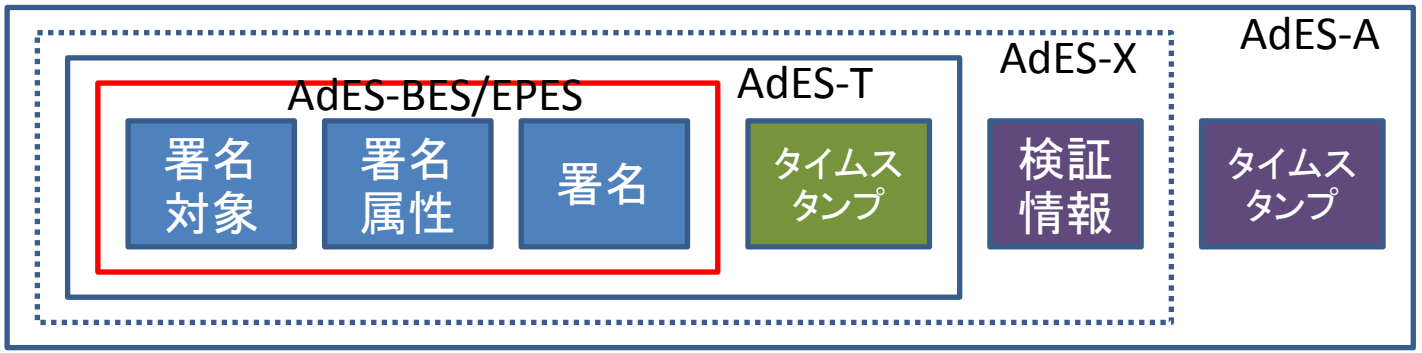
ESI関連STF(Specialist Task Force)

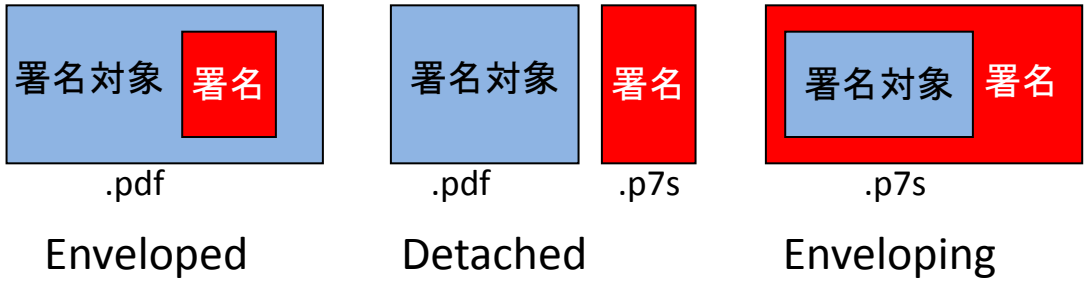
番号	タイトル	成果	開始	終了
155	Electr. Signature	CAdES、適格証明書、適格証明書発行CAポリシ要件、タイムスタンプ、CAポリシ要件の国際調和	1999-12-07	2002-02-28
178	Electronic signature 2001	XAdES、TSPステータス情報提供、CAポリシ要件、TSAポリシ要件、XML署名ポリシ	2001-01-17	2002-03-31
209	Electronic signature	属性証明書要件、拡張ビジネスモデル署名ポリシ	2002-01-22	2003-02-28
220	Electronic Signature	属性証明書発行CSPポリシ要件、証明書プロファイル、TSPステータス情報提供（TS）	2002-07-01	2004-03-26
242	Electronic signature	署名フォーマットの国際調和	2003-02-17	2004-02-29
288	Internat. Harmoniz.	電子署名応用、USブリッジCAとの対応付け	2005-02-28	2006-03-24
290	TSP Status List	TSL	2005-03-01	2005-12-23
298	Electr. Sign. profiles Ph.1	CAdES/XAdESプロファイル	2005-12-05	2006-12-23
305	Digital Accounting (SODA)	署名操作のベストプラクティス、TSPポリシ要件	2006-04-03	2007-03-31
317	Algo-Paper param. revision	SHA256	2006-11-20	2007-08-01
318	Registered e-mails	REM	2006-11-20	2009-09-30
364	PDF AdES	PAdES	2008-10-06	2010-07-31
401	Long term storage	長期保存	2010-03-31	2011-06-11
402	REM protocols	REM相互運用	2010-03-31	2011-06-30
412	Guide Ext'd Valid. Cert.	EV証明書ガイド	2011-01-20	2012-03-15
425	ES framework	電子署名標準の枠組み	2011-02-28	2012-04-30
426	Quick fix profiles	ベースラインプロファイル	2011-02-28	2012-02-28
427	Quick fix standards	既存標準見直し	2011-02-28	2013-04-30
428	Quick fix testing	PAdES、ASiCプラグテスト	2011-02-28	2012-04-30

AdES（Advanced Electronic Signature）

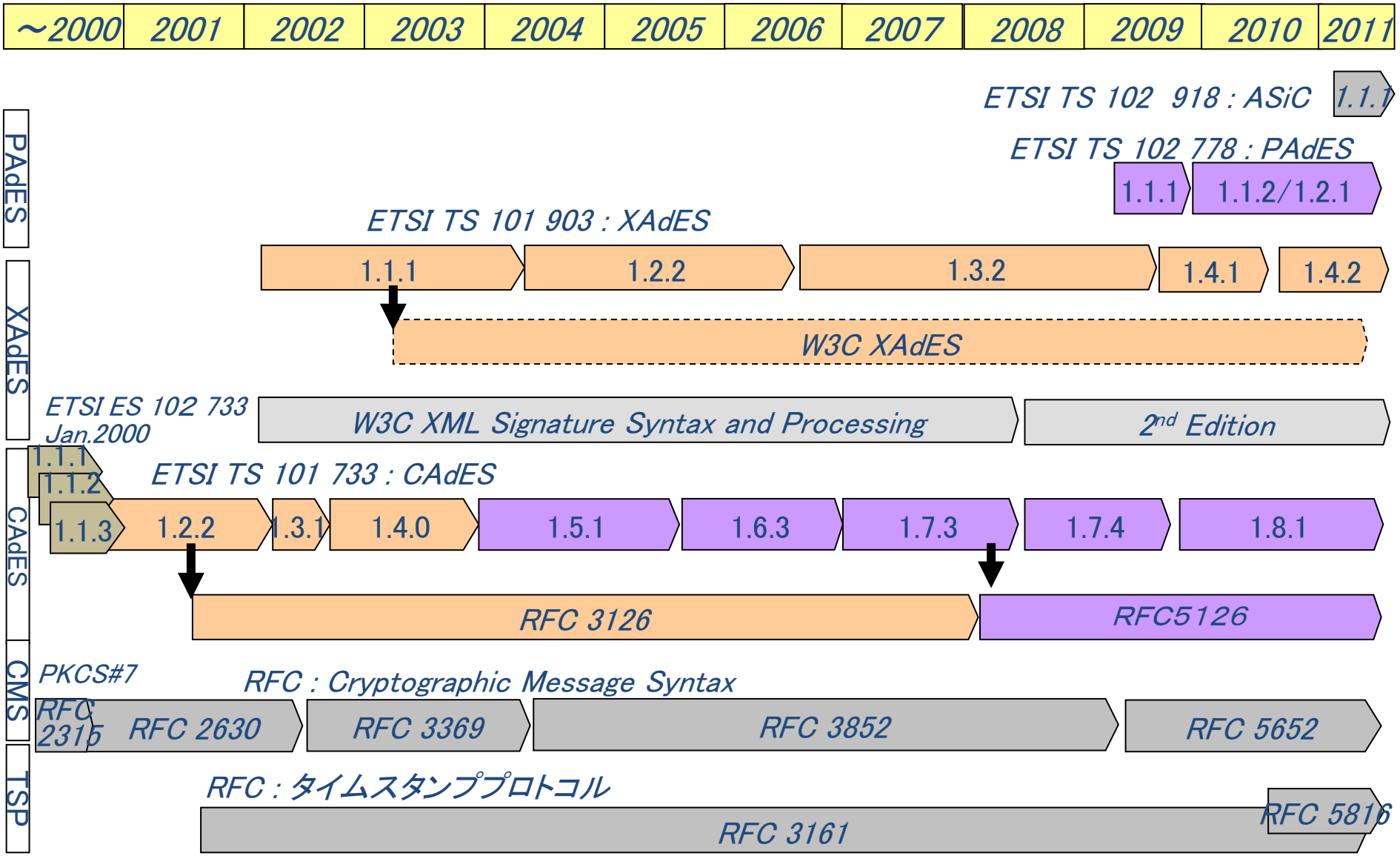
- CAdES･･･CMS版
- XAdES･･･XML版
- PAdES･･･PDF版
- ASiC･･･コンテナ版

AdESの基本フォーマット



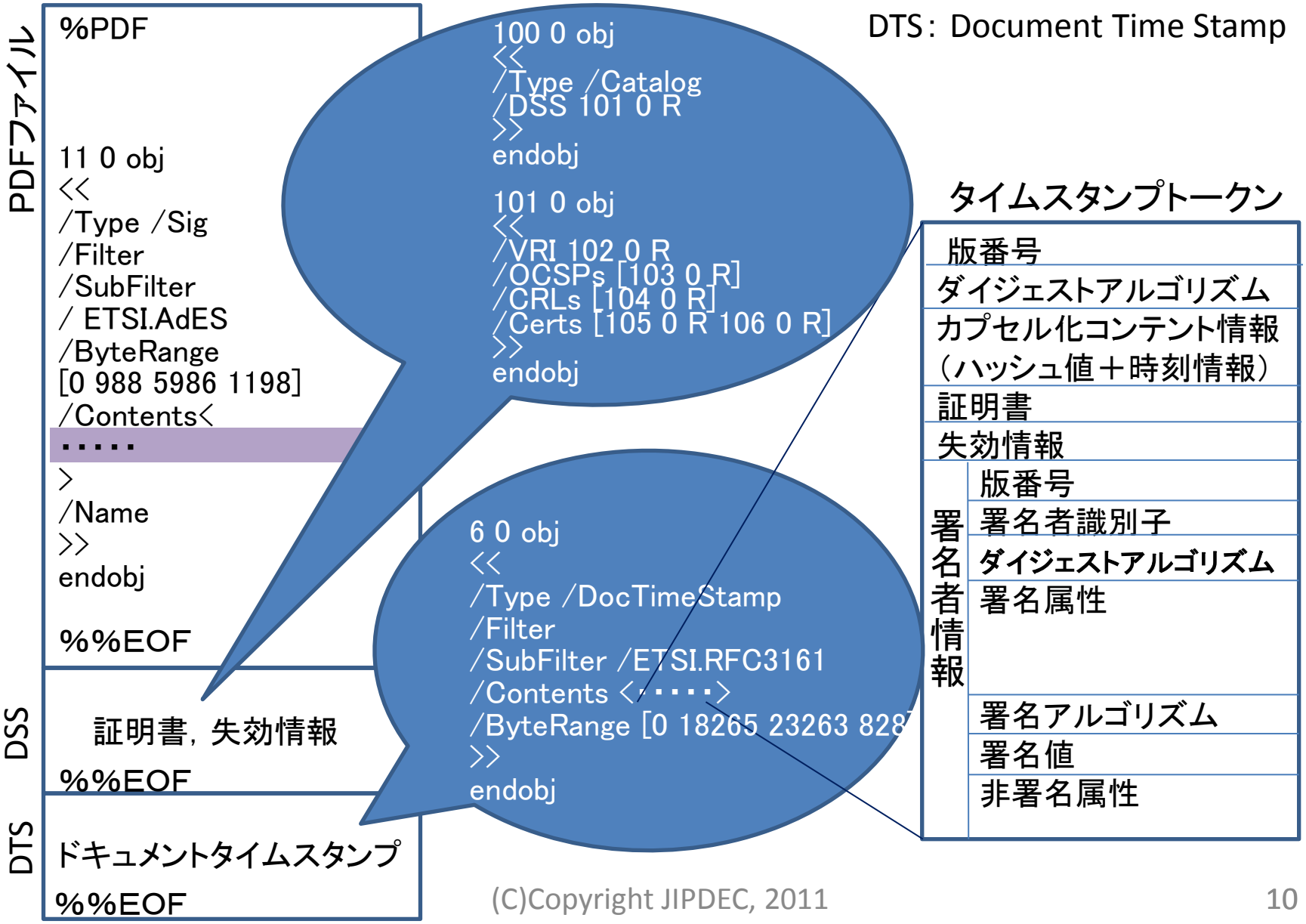


AdES関連標準の歴史



PAdES

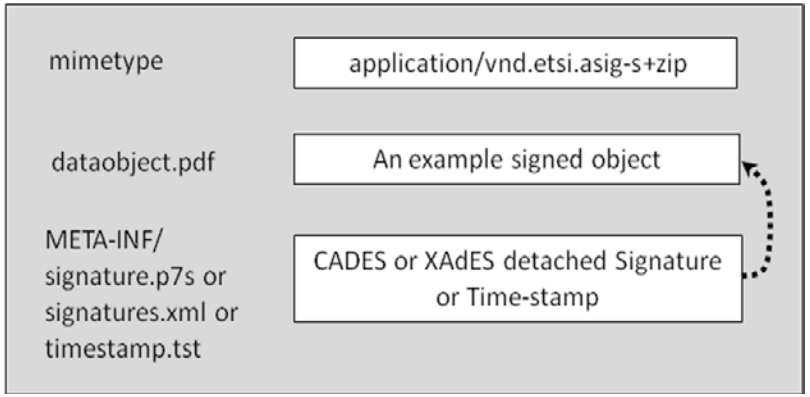
DSS：Document Security Store
DTS：Document Time Stamp

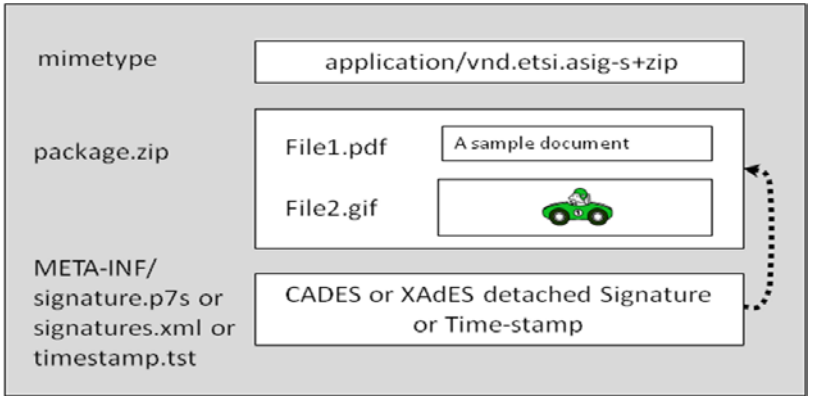


ASiC（Associated Signature Containers）

- コンテナ： OCF、UCF、ODF
- 署名and/orタイムスタンプ

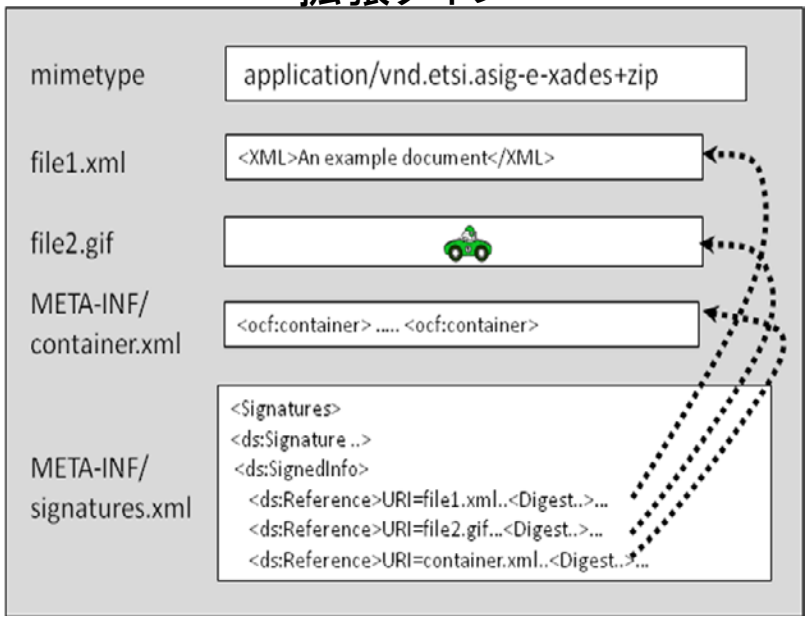
シンプルタイプ





注記　CAdES適用に制約あり

拡張タイプ



TSPステータス情報リスト(TSL)

信頼サービス提供者(TSP)のステータス情報を提供するための署名付きリスト

- 相互運用のための今後の信頼モデル？(メッシュ、ブリッジ、TSL)
- 基準を満たした認証局をリストアップし公開
- 本年1月から運用開始

信頼サービス提供者(TSP):

- 1または複数の信頼サービスを運用している組織
  指令1999/93/ECによる

信頼サービス(TS, Trusted Service):

- 信頼と電子商取引の信頼性を高めるサービス(通常は、必ずしも暗号技術を使用したり、機密資料を含まない)

信頼サービストークン(TrST):

- 信頼サービスの利用の結果として生成されるか発行された物理的またはバイナリ(論理的)オブジェクト。証明書、タイムスタンプトークンなど

スキーム運用者

- アセスメントスキームの運用および/または管理に責任をもつ組織(政府、産業界、民間)

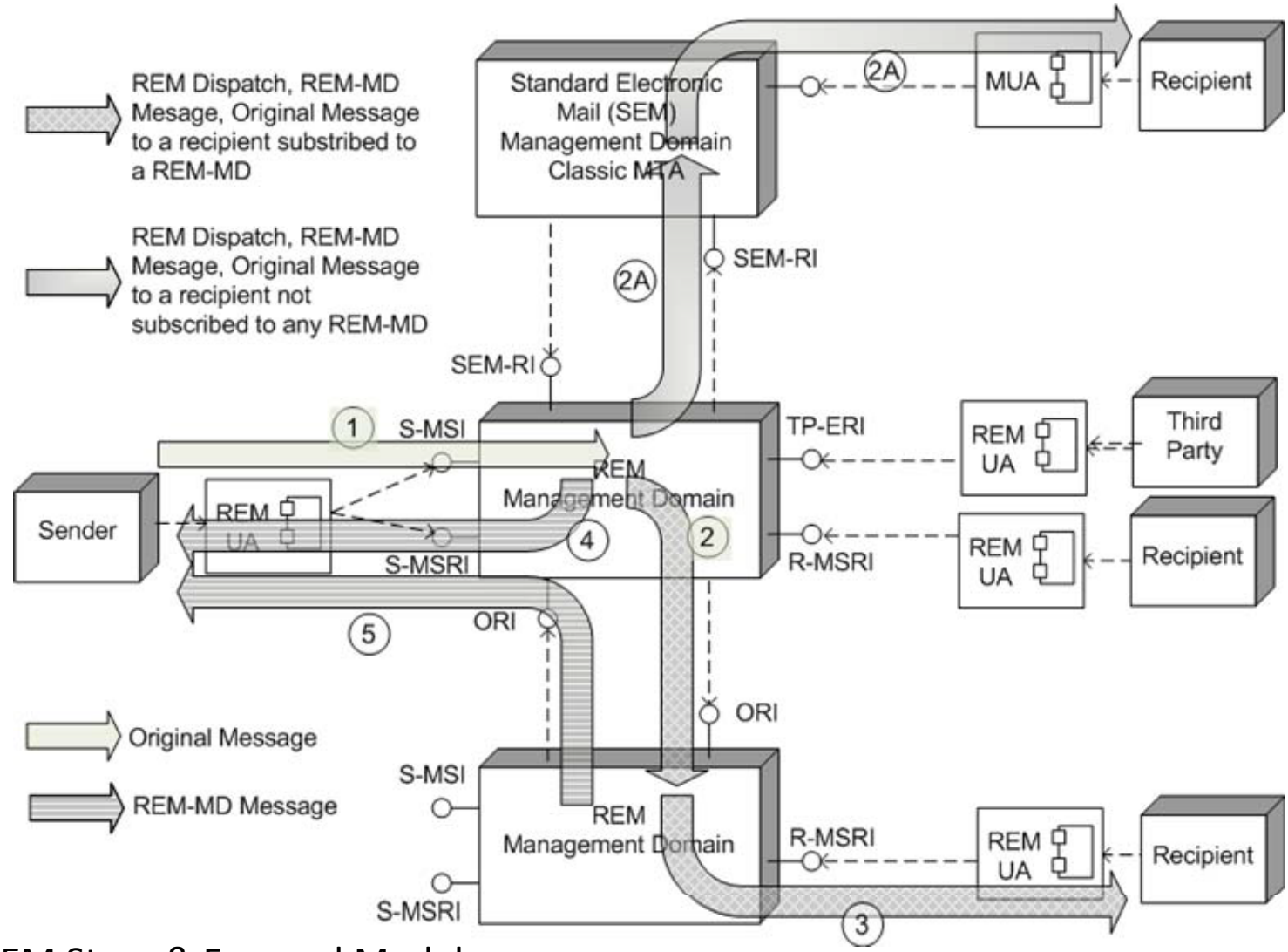
サービスタイプ

認証局（CA）
適格証明書(Qualified Certificate)発行局
タイムスタンプ局（TSA）
リポジトリ（OCSP） Certificate status provider
リポジトリ（CRL）
登録局（RA）
An Identity verification service.
A Certificate generation service which responds to requests for certificate generation from an authenticated source of identity information
属性認証局（AA）
アーカイブ Archival service.
A Registered Electronic Mail service
A Key escrow service.
Issuer of PIN- or password-based identity credentials.
Service responsible for issuing, publishing or maintenance of signature policies
An assessment scheme which is a system of supervision as defined in, and which complies with all applicable requirements of Directive 1999/93/EC
An assessment scheme which is a voluntary approval [accreditation] scheme as defined in, and which complies with all applicable requirements of Directive 1999/93/EC
TSL発行者.
A trust service of an unspecified type.

TSLフォーマット

TSL ::= ContentInfo
ToBeSignedTSL ::=SEQUENCE {
tSLTag TSLTag,
version Version,
sequenceNumber SequenceNumber,
tSLType TSLType,
schemeOperatorName SchemeOperatorName,
schemeOperatorAddress SchemeOperatorAddress,
schemeName SchemeName,
schemeInformationURI SchemeInformationURI,
statusDeterminationApproach StatusDeterminationApproach,
schemeTypeCommunityRules [0] SchemeTypeCommunityRules OPTIONAL,
schemeTerritory [1] SchemeTerritory OPTIONAL,
tSLpolicy [2] TSLpolicy OPTIONAL,
historicalInformationPeriod HistoricalInformationPeriod,
pointersToOtherTSLs [3] PointersToOtherTSLs OPTIONAL,
listIssueDateTime ListIssueDateTime,
nextUpdate NextUpdate,
schemeExtensions [4] Extensions OPTIONAL,
distributionPoint [5] DistributionPoints OPTIONAL,
tSPlist TSPlist OPTIONAL
}

書留電子メール（REM, Registered e-mail）



REM Store & Forward Model

MD間配信エンベロープ構造

MIMEヘッダ			
署名データ	MIMEヘッダ		
	導入	MIMEヘッダ	
		テキスト	MIMEヘッダ
			テキスト
		HTML	MIMEヘッダ
			HTML
	オリジナルメッセージ	MIMEヘッダ	
		オリジナルメッセージ	
	拡張	MIMEヘッダ	
		拡張	
	エビデンス	MIMEヘッダ	
		エビデンス	
署名	MIMEヘッダ		
	署名		

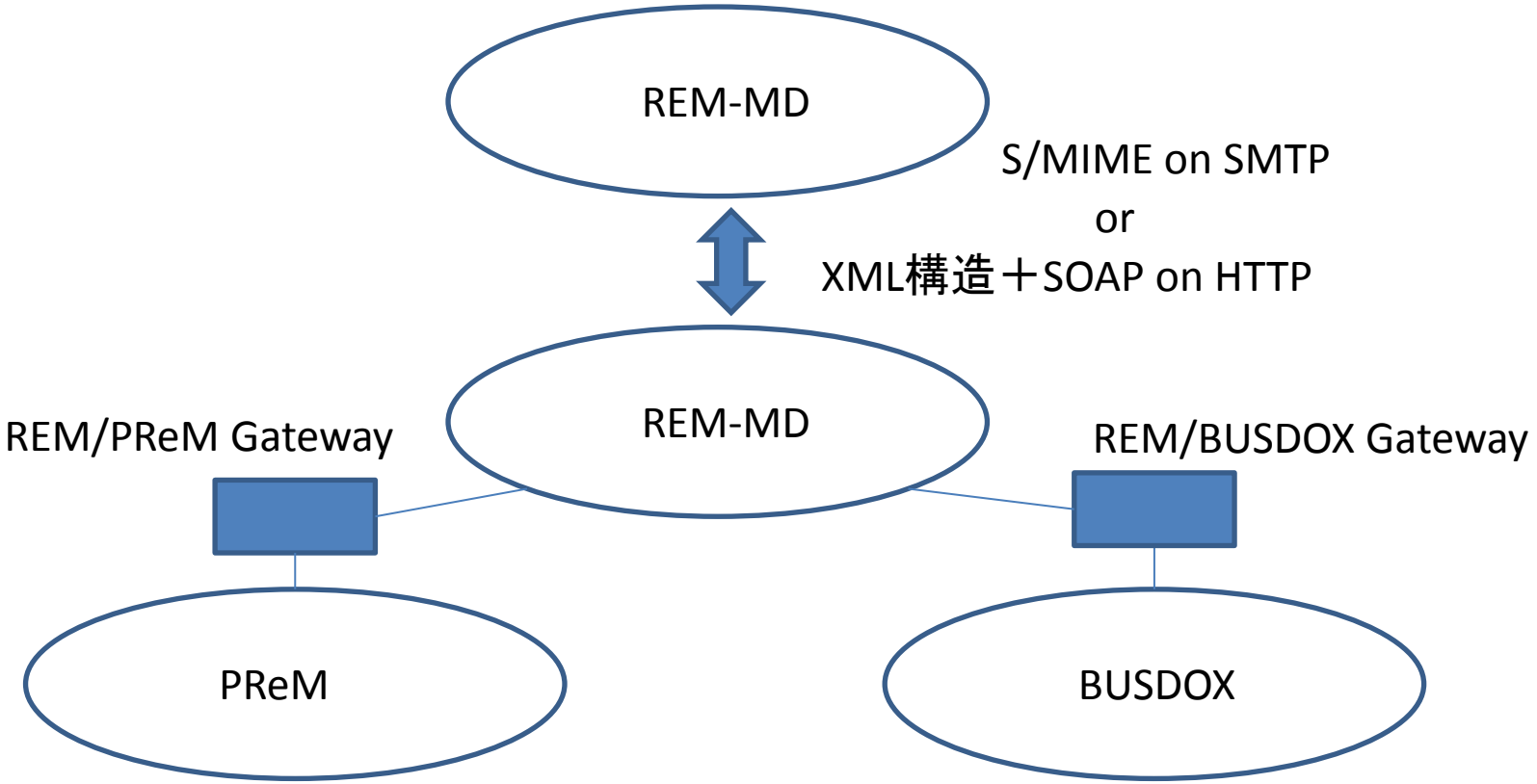
ASN.1 or XML or PDF

コア要素	エビデンスのID、タイプ、事象、理由、バージョン、時刻、ログ情報
REM-MD要素	エビデンス発行者のポリシID、詳細、署名
アイデンティティ関連要素	送信者詳細、受信者詳細、受信者代理詳細、エビデンスにより参照される受信者、送信者認証詳細、受信者認証詳細
メッセージング要素	メッセージ/ディスパッチ詳細、reply-to、通知メッセージタグメッセージ提出時刻、内部転送
拡張	

事象とエビデンス

事象		エビデンス
A1	送信側REM-MD受理	オリジナルメッセージ提出受理/拒否
A2	送信側REM-MD拒否	
B1	受信側REM-MD受理	REM-MDへの転送受理/拒否
B2	受信側REM-MD拒否	
B3	REM-MDへの配信タイムアウト	REM-MDへの転送失敗
C1	メッセージ配信	受信者への送達/不達
C2	メッセージ配信タイムアウト	
D1	通知配信	
D2	通知配信タイムアウト	
E1	レポジトリダウンロード	受信者からのダウンロード/非ダウンロード
E2	レポジトリダウンロードタイムアウト	
E4	代理によるレポジトリダウンロード	
F1	メールボックス読出し	受信者による読出し/非読出し
F2	メールボックス読出しタイムアウト	
F3	代理によるメールボックス読出し	
E3	受信者ダウンロード拒否	受信者による受理/拒否
H1	通常eメールへの転送成功	非REMシステムへの転送
H2	通常eメールへの転送失敗	
G1	印字への転送成功	
G2	印字への転送失敗	
I1	通常eメールシステムからのeメールメッセージ受信	非REMシステムによる受信

他ドメインとの相互接続



UPU S52-1 UPU Postal Registered electronic Mail functional specification (PReM)
Business Document Exchange Network service metadata and transport specification (BUSDOX)

2. 直近の動向

EC指令460

STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

- ECの電子署名規格の軽量化と再編成
- 有効期限切れのCENのCWAの更新または廃棄
- 技術標準(TS)の統合
- 理解と利用を促進するTSの簡素化
- プレゼンテーションフレームワーク（ポータル、動的更新）
- TS生成からENやISOへの進化が定義されたライフサイクル
- 4年スパンの行動計画
- TS普及とプレゼンテーションインフラ維持のための恒久的な予算措置

European Standard, telecommunications series (EN)
ETSI Standard (ES)
ETSI Technical Specification (TS)
ETSI Technical Report (TR)

EC指令460対応STF

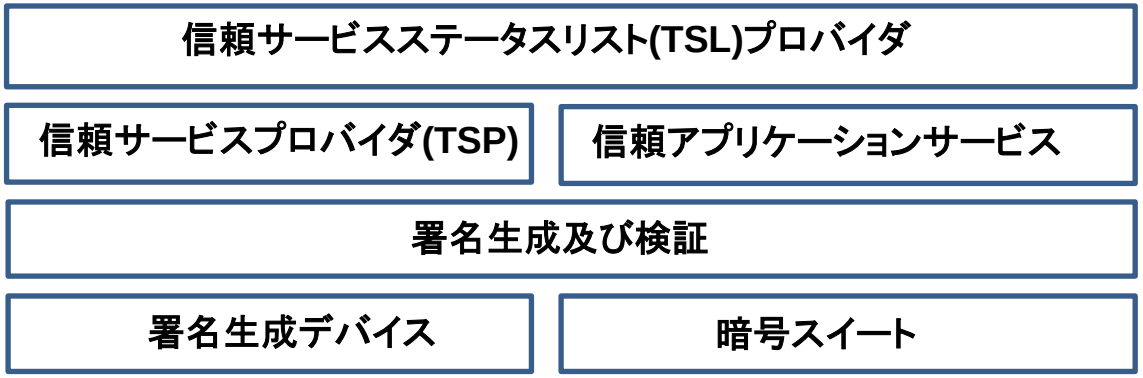
- STF425　フレームワーク Electronic Signature Standardization in Rationalised Framework
- STF426　プロファイル Quick fixes to electronic signatures profiles
- STF427　スタンダード Quick fixes to electronic signatures standards
  1. 認証局（CSP; Certificate Service Provider）の適合性評価 (conformity assessment)要件及びガイダンス策定
  2. 相互運用性のある適格証明書のプロファイル策定
  3. 署名検証手順策定
  4. 署名アルゴリズム保守
- STF428　プラグテスト Quick fixes to testing of electronic signatures standards

EC指令460対応作業（新規/見直し）

SR	Rationalized framework
TS	XAdES Baseline Profile
TS	PAdES Baseline Profile
TS	CAdES Baseline Profile
TS	ASiC Baseline Profile
TS102 918	Associated Advanced Electronic Signatures Profile
EN301 862	ESI Qualified Certificate profile
TS102 280	ESI Certificate Profile for Natural Persons
TS	Conformity assessment guidance
TS	Security Requirements for signature creation applications
EN301 456	Policy requirements for certification authorities issuing QC
EN302 042	Policy requirements for CAs issuing public key certificates
TR101 564	guidance on TS 102 042
TR	Guidance for auditors of CSP issuing EV certificates
SR	Recommendations on governance and audit regime for assessing CSPs issuing EV certificates in EU
TS 102 853	Signature verification
TR102 038	XML format for signature policies
TS102 042	Policy requirements for CAs issuing public key certificates
TR 103 071	Test suite for future REM interoperability Plugtest Events
TS	Conformance testing for XAdES baseline profile
TS	PAdES Signatures Interoperability testing
TS	Associated Signatures Interoperability testing

フレームワーク

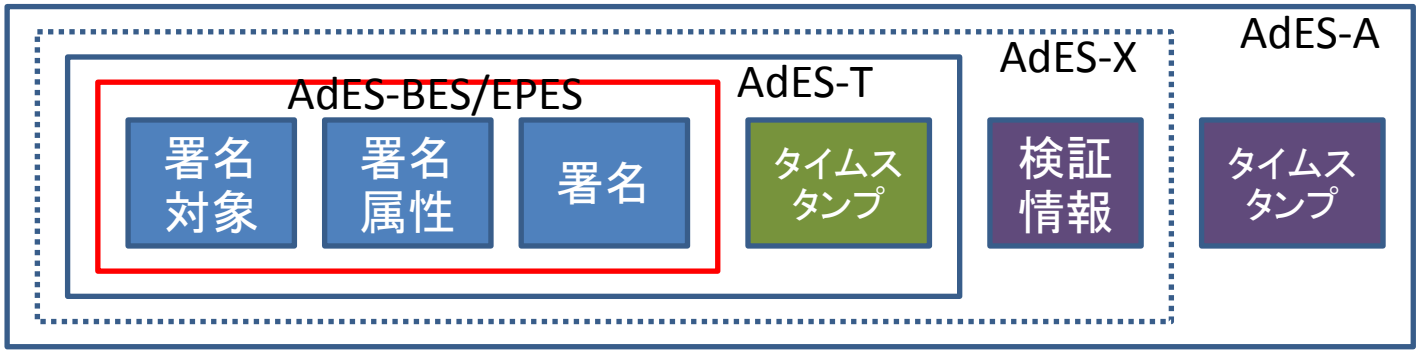
- 方針
  - ビジネスオリエンテッド/ビジネスドリブン
  - オプションの削減
  - アセスメントガイドの提供
  - 試験仕様と試験設備の提供
  - 法的要件との対応
- 6つの機能領域
- 5種類のドキュメント
  - ガイダンス
  - ポリシー要件
  - 技術仕様
  - 適合性評価
  - 相互運用性試験



注記：信頼アプリケーションサービスには、REM （Registered E-Mail)、デリバリ、長期保存などがある

ベースラインプロファイル

- AdES-BES、AdES-EPES部分のプロファイル



- 特記事項
  - MandatoryとOptionalのみ（should, mayの廃止）
  - Signing TimeがMandatoryに！
- プロファイリング対象AdES
  - XAdES・・・XML版
  - PAdES・・・PDF版
  - CAdES・・・CMS版
  - ASiC・・・コンテナ版
- CAdES-T/-A、XAdES-T/-A部分のプロファイルは現在DIS段階(15433-1,-2)
  40.99

認証局適合性評価

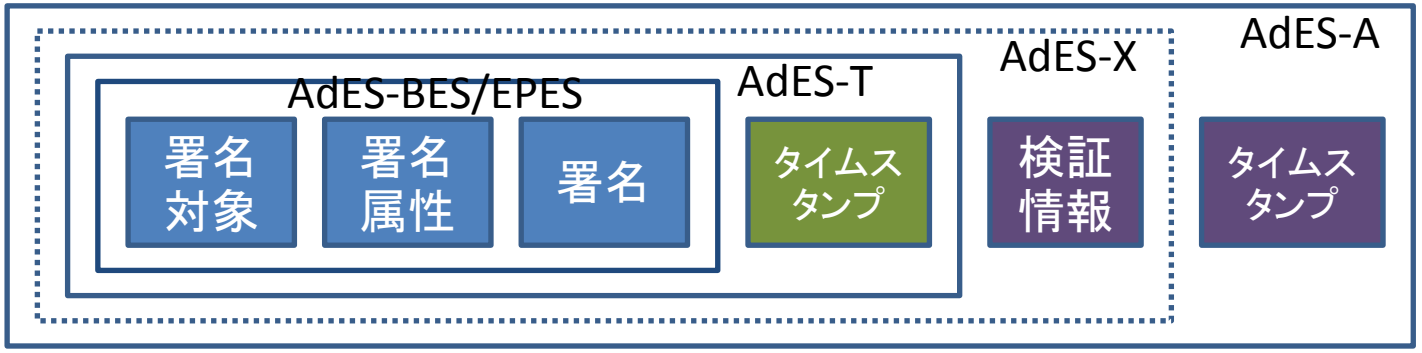
- 背景
  - 現状は各国バラバラ（hands off　～　regular full audit）

- 適格証明書を発行する認証局を信頼サービスリスト（TSL）に登録するための各国におけるアセスメントスキームを策定
  - ISO 17021（＝JIS Q 17021、適合性評価－マネジメントシステムの審査及び認証（certification）を行う機関に対する要求事項）が候補
  - スキーム運用者（スーパバイザ；政府、産業界、民間）がアセスメントスキームの運用および/または管理に責任をもつ
  - 原則、監査を前提とした自己適合宣言を行う
  - 11月に最終ドラフト作成の予定

署名検証

- 単に、有効(valid)か無効(invalid)かの2値ではなく、検証情報の何が欠けているかの情報を伴う“不定”(indeterminate)を設ける方向
- 署名を、短期、中期、長期に分類
  - 短期　AdES-BES/EPES
  - 中期　AdES-T
  - 長期　AdES-A

  ※　短期の場合、検証の基準時刻をどうすべきか？



署名ポリシ・・・検討の方向性

〔署名ポリシーに対する視点〕
- トラストアンカーなど個々の署名に関する従来の署名ポリシー
- 複数署名等におけるワークフロー的な視点からの署名ポリシー
- 署名を要する業務と文書の視点からの署名ポリシー

→今後、来年の2月に向けて方向性を詰めて行く

〔署名ポリシーにおけるTSLの位置付け〕
- トラストアンカーとTSLの関係

案1 トラストアンカーまで検証を済ませた上での制約条件としてTSL適用する
案2 TSLを検証のエンドポイントにする

〔XML版署名ポリシー〕
- ASN.1版の署名ポリシー（フォーマット）をXML記法で焼き直し

課題
- ASiCで扱うコンテナ構造への対応方針
- アルゴリズムIDや要素の識別の統一化（ASN.1ではOID、XMLではURLsを使っており二重管理となっている）
- XAdESのバージョンが明示的に表れることへの改善

2011年のプラグテスト

- テスト申込期限　11月1日
- テスト期間　11月24日～12月9日、対象はPAdESとASiC（アソシエート署名）
- テスト環境（Web)　9末に提供
- PAdES　Part2、3、4、5の順にテストを実施
- 8/4、JIPDEC/eRAP（電子記録応用基盤フォーラム）内に支援チーム結成

注　XAdESベースラインプロファイルは適合性チェックツール提供予定(10月)

ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles;

~~Part 1: PAdES Overview - a framework document for PAdES"~~

Part 2: PAdES Basic - Profile based on ISO 32000-1"

Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles"

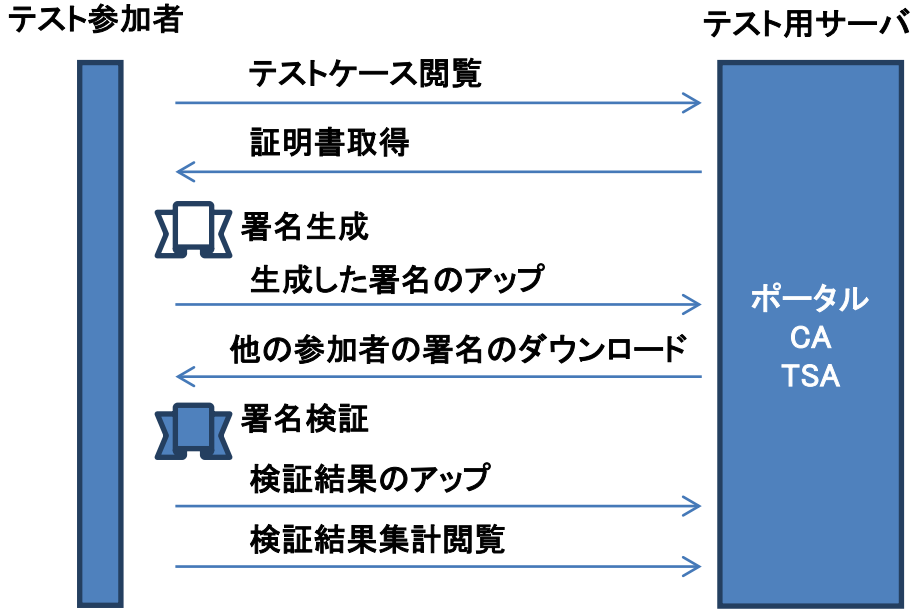
Part 4: PAdES Long Term - PAdES LTV Profile

Part 5: PAdES for XML Content Profiles for XAdES signatures

~~Part 6: Visual Representations of Electronic Signature~~

プラグテスト概要

- テスト方法： リモートテスト
- 通信連絡手段：
  - 電話会議（チャットを併用）
  - メールリスト（通常はメールリストを使用）
  - ウェブポータル（テストデータや結果のアップ/ダウンロード）
- テストの流れ：



ご清聴有り難うございました

一般財団法人日本情報経済社会推進協会（JIPDEC）
電子情報利活用推進部
TEL　03 3436 7500
e-mail　dupc-erm@tower.jipdec.or.jp