



PKI Day 2014

電子署名をめぐる国内外の最新動向

宮崎 一哉

電子署名WGリーダー
(三菱電機株式会社)
2014 年3月13日

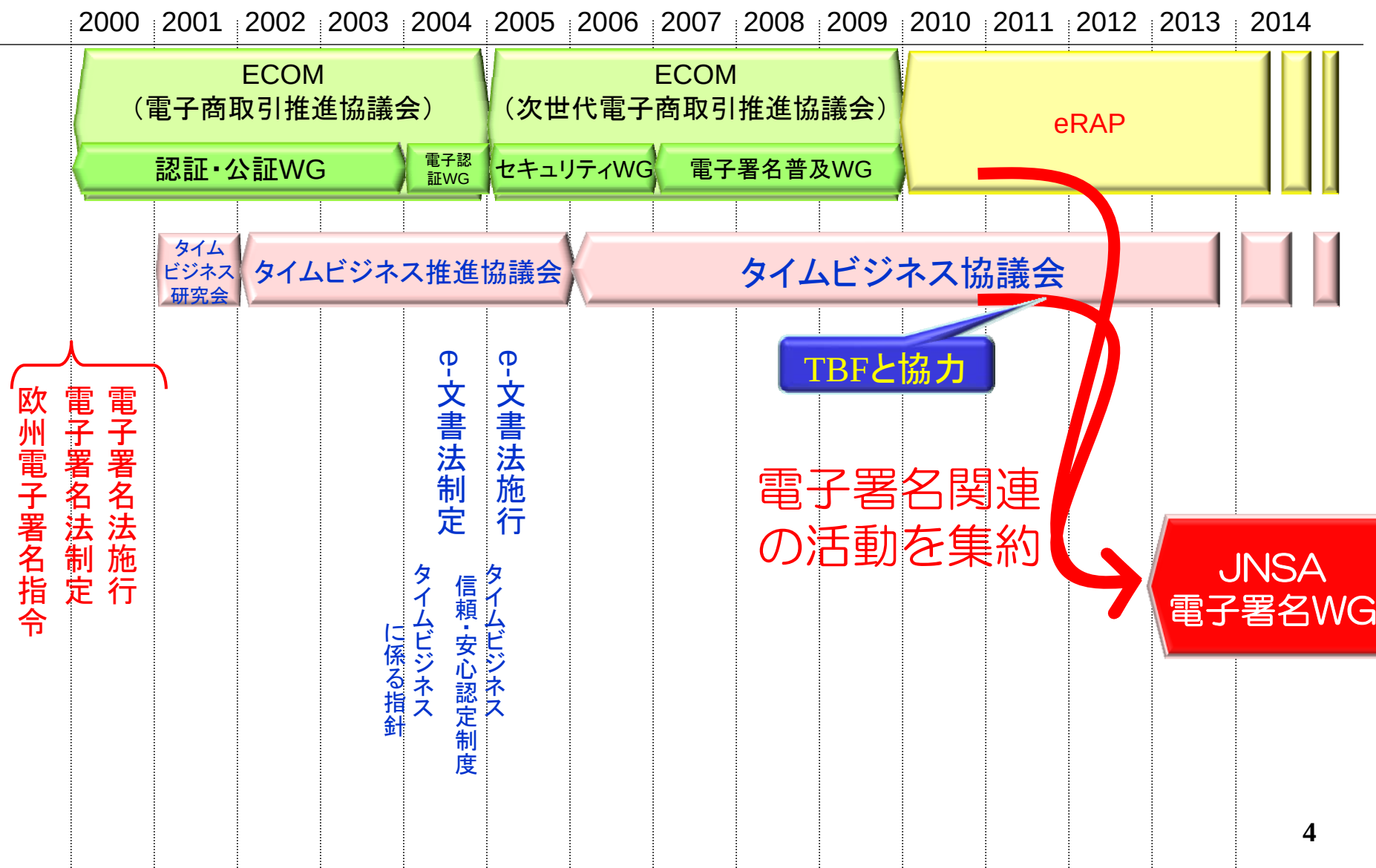
午後の部の講演



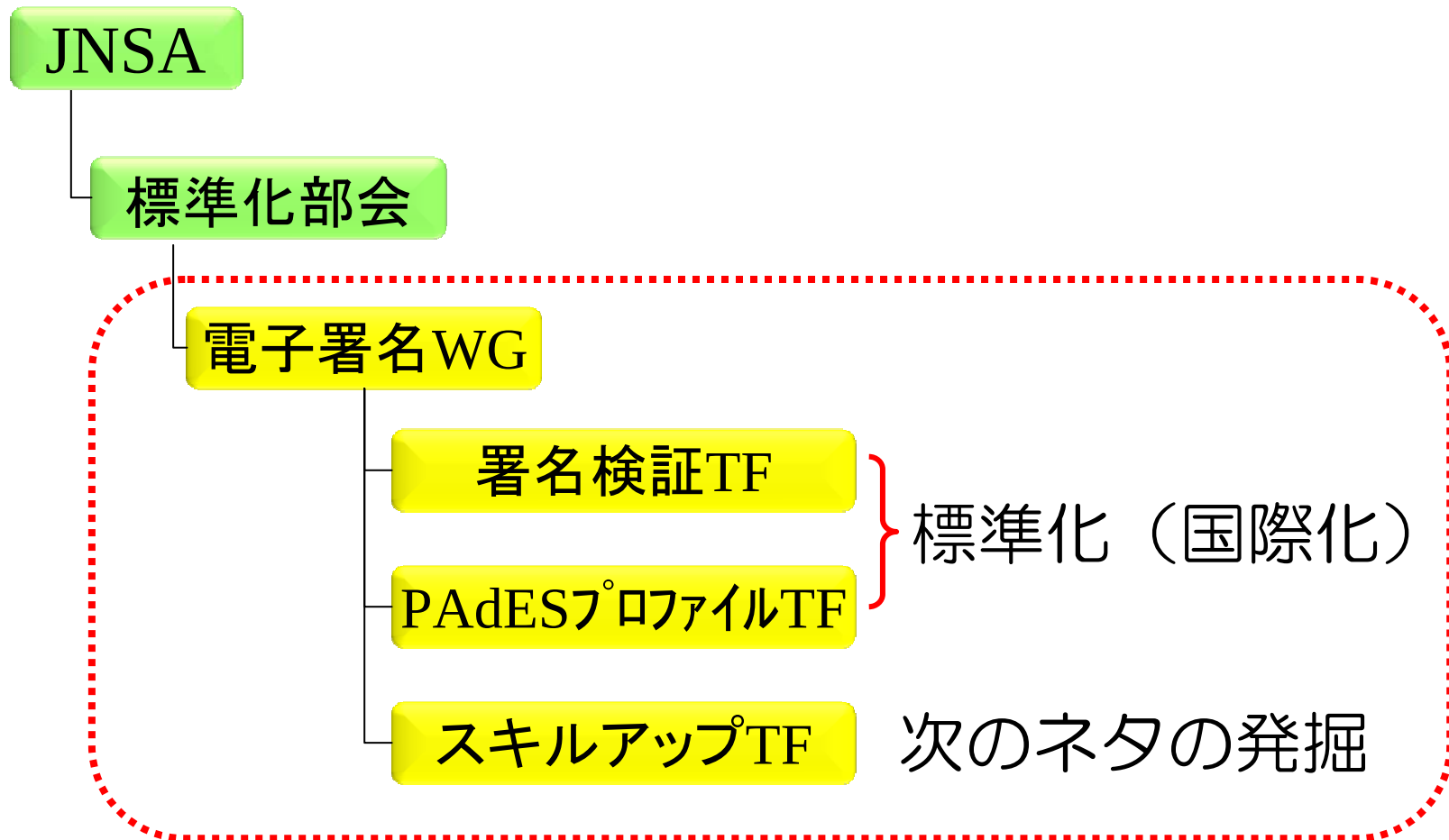
- ・ 「電子署名をめぐる国内外の最新動向」
 - 電子署名WGの紹介 宮崎
 - 電子署名WGの標準化活動
 - ETSI/TC ESIを中心としたEU等の動向
 - 技術解説 石本さん
- ・ 「新しい電子署名 ～クラウド/モバイル署名と非PKI署名～」 宮地さん
 - クラウド/モバイル署名、非PKI署名
 - 電子署名WGの新たな活動 亀田さん

電子署名WGについて

電子署名WGについて：設立経緯



電子署名WGについて：活動内容 **JNSA**



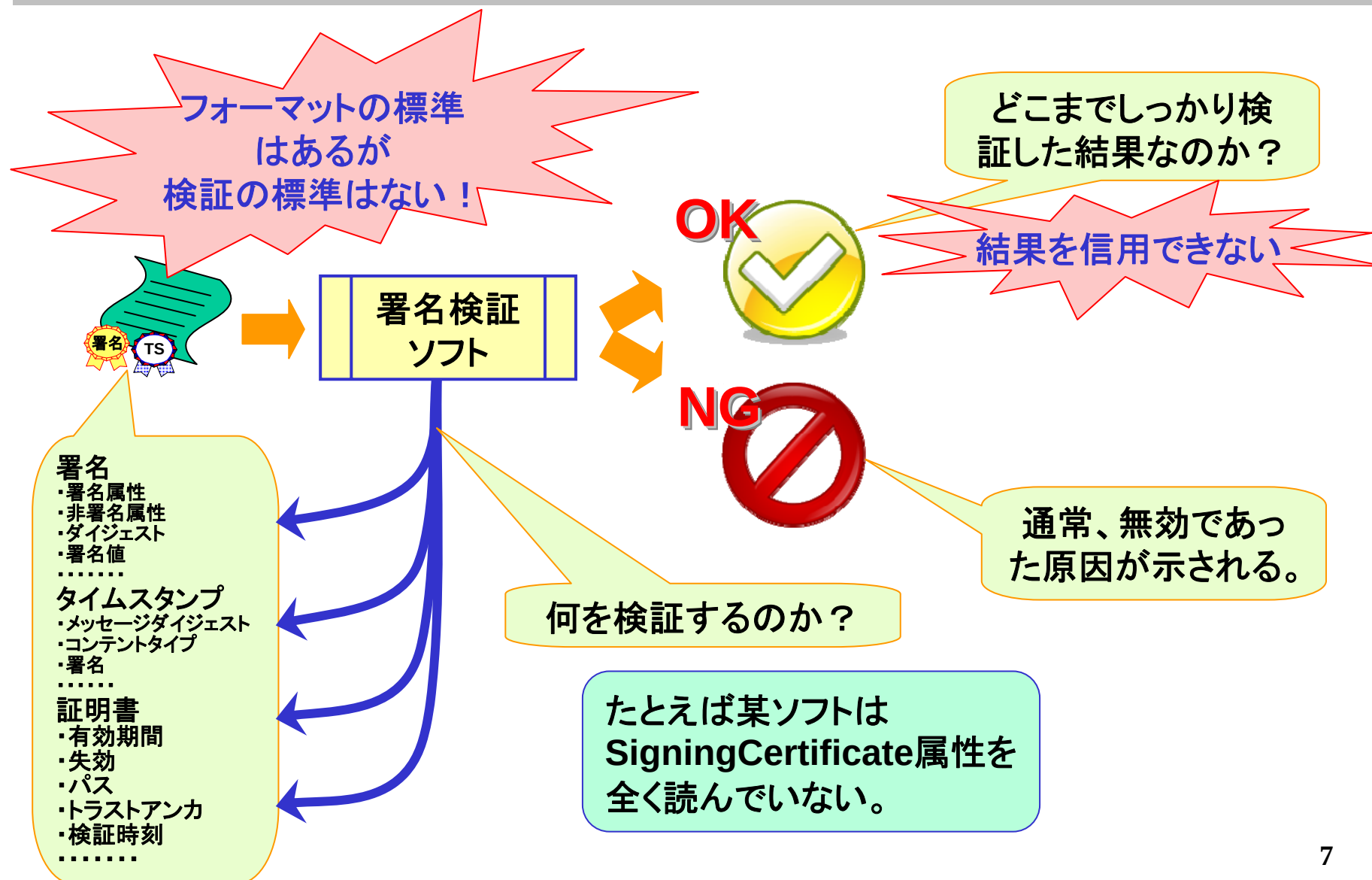
① 署名検証処理要件の標準化

- ・ 電子署名の検証処理に関する要求事項を定義し、JIS原案、ISO原案とする。
- ・ ETSI/TC ESIと調整を図りつつ進める。

② PAdESプロファイルの標準化

- ・ PAdESの長期保存のためのプロファイルを定義し、JIS原案、ISO原案とする。
- ・ ETSI/TC ESIと調整を図りつつ進める。

①署名検証要件の標準化 署名検証の問題点



署名検証標準規格の意義

- 署名検証における検証項目や要件を定義
- 検証結果の出力内容を定義
- 検証ソフトウェアの検証範囲を明示できる枠組み（適合宣言書）を提供

⇒実装者にとって、実装方法がわかる。

⇒調達者・利用者にとって、検証範囲がわかる。

⇒安全・安心な署名検証ソフト

署名検証標準規格の作成状況



TS 1xx xxx V0.0.4 (2013-05)			
TECHNICAL SPECIFICATION			
		電子署名検証ガイドライン	
		V1.0.0	
Requirements of Signature validation procedures			
This draft spec 853, and spec Current ETSI implementation			
5.7.1 Simple ES (ES).....		5.3.2 署名タイムスタンプ付き署名(ES with signature timestamp).....	
5.7.2 ES with signature timestamp (ES-T).....		5.3.3 検証情報の参照付き署名(ES with validation data reference).....	
5.7.3 ES with archive validation data (ES-A).....		5.3.4 検証情報付き署名(ES with validation data).....	
Annex A (normative): Supplier's Declaration of Conformity and its Attachment.....		5.3.5 アーカイブ付き署名(ES with archive validation data).....	
A.1 General.....		5.4 検証基準時刻.....	
A.2 Form of the Supplier's Declaration of Conformity.....		5.4.1 Simple ES検証における検証基準時刻.....	
A.3 Form of the Attachment to the Supplier's Declaration of Conformity.....		5.4.2 ES with signature timestamp検証における検証基準時刻.....	
A.4 Procedures.....		5.4.3 ES with validation data reference検証における検証基準時刻.....	
A.4.1 Common Validation.....		A.6.3 TSA証明書のX.509 証明書バス検証.....	
A.4.2 CAdES Validation.....		付属書B (参考) 参考文献.....	
A.4.3 XAdES Validation.....			
A.5 Data.....			
History.....			

初版ドラフト
“Requirements of Signature validation procedures”
をETSI/ESI会議にて紹介

我々の標準案の特徴

- 実装方式に依存しない汎用的な要求仕様
- 作成された実装のチェックが容易なテーブル表記をベースとした記述
 - チェックリスト⇒付録に「適合宣言書」

テーブル表記の例

検証対象

要求レベル

Object	Criteria	Semantics	M/O	Status Indication	Report (example)
Data structure	Validity of the data structure	The signature data structure is contained all the mandatory elements of Table 15.	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Missing elements
	CMS data type	"ContentType" is object identifier of "id-signedData".	M	VALID	- Validation result
				INVALID	- Reason of INVALID
Signed data type	Signed data type	"eContentType" is object identifier of "TSTInfo".	M	VALID	- Validation result
				INVALID	- Reason of INVALID
TSA certificate	Validity of TSA certificate	It is verified according to the requirements of TSA certificate validation in Clause 5.7.2.	M	Refer to Clause 5.7.2.	
Signature of TSA	Validity of "digestAlgorithms" field	"digestAlgorithms" field in "Content" is verified according to the requirement of the Digest algorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
	Validity of "digestAlgorithm" field	"digestAlgorithm" field in "signerInfo" is verified according to the requirement of the Digest algorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
	Consistency of "MessageDigest" attribute	The following two values in "signerInfo" are matched. 1) The hash value of "eContent" value computed with the algorithm specified in "digestAlgorithm" field 2) The value of "MessageDigest" in "signedAttrs" field	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Each hash value
	Consistency of the hash value for TSA certificate in "SigningCertificate" attribute	The following two values in are matched. 1) The hash value of TSA certificate computed with the algorithm used in "SigningCertificate" attribute 2) The value of "certHash" in "SigningCertificate" attribute	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Each hash value
	Validity of "signatureAlgorithm" field	"signatureAlgorithm" field in "signerInfo" is verified according to the requirement of the Signature algorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
Validity of the signature value by public key in a TSA certificate	Validity of the signature value by public key in a TSA certificate	According to the algorithms of "signatureAlgorithm" and "digestAlgorithm" in "signerInfo", the consistency of the signature value in "signerInfo" and the hash value for the content verified with public key in TSA certificate	M	VALID	- Validation result
				INVALID	- Reason of INVALID

検証基準

出力内容

ETSIの標準案



- ETSI EN 319 102, “Electronic Signatures and Infrastructures (ESI); **Procedures for Signature Creation and Validation**”
- ドラフトのレビュー中。

仕様ドラフト間の相違



ETSI	JNSA
実装方式依存	汎用仕様
プロセスフロー	テーブル
出力メッセージ	未定義
POE (何らかの存在証明)	検証基準時刻 (時刻ありき)

- とにかく読みにくい。
- 160個のレビューコメント。

Timestampに関する記述が足りない

コントロールタイムやフレッシュネスの概念が分かりにくい

②PAdESプロファイルの標準化

- PAdES(PDF Advanced Electronic Signature)
 - ベース規格 ETSI TS 102 778 Part1~Part6
 - 現在策定作業中のPDF規格(ISO 32000-2)に取り入れられる予定。
- PAdESの主な特徴と問題点
 - 従来のPKCS#7ベースのPDF署名(PAdES Basic)に加え、CAdESを用いたPAdES Enhancedを定義している。
 - 検証に必要な証明書や失効情報を格納するためにDSSというPDFの要素を定義している。
 - PDFに適用するタイムスタンプ(ドキュメントタイムスタンプ)を定義している。
 - **問題点**: DSSや署名、ドキュメントタイムスタンプ等の様々な要素の組み合わせの自由度が高い一方で、**様々なパターンに応じた利用方法(生成・検証)が示されておらず、相互運用性の問題が生じる。**
- PAdESプロファイルの考え方
 - **長期にも保存可能なPAdESを実現するうえで必要な各要素の利用方法(生成・検証)を定める。**
 - ベース規格へ反映すべき事項はETSIやISOに提言する。

PAdESプロファイルの位置付け



CAdES

(CMS Advanced Electronic Signature)

バイナリデータ形式 (ASN.1)
のフォーマット

関連する代表的な規格

ETSI TS 101 733

RFC 5126 (IETF)

ECOM/eRAPが原案作成

JIS X 5092:2008

ISO 14533-1

XAdES

(XML Advanced Electronic Signature)

XML形式のフォーマット

関連する代表的な規格

ETSI TS 101 903

ECOM/eRAPが原案作成

JIS X 5093:2008

ISO 14533-2

PAdES

(PDF Advanced Electronic Signature)

PDF形式のフォーマット

関連する代表的な規格

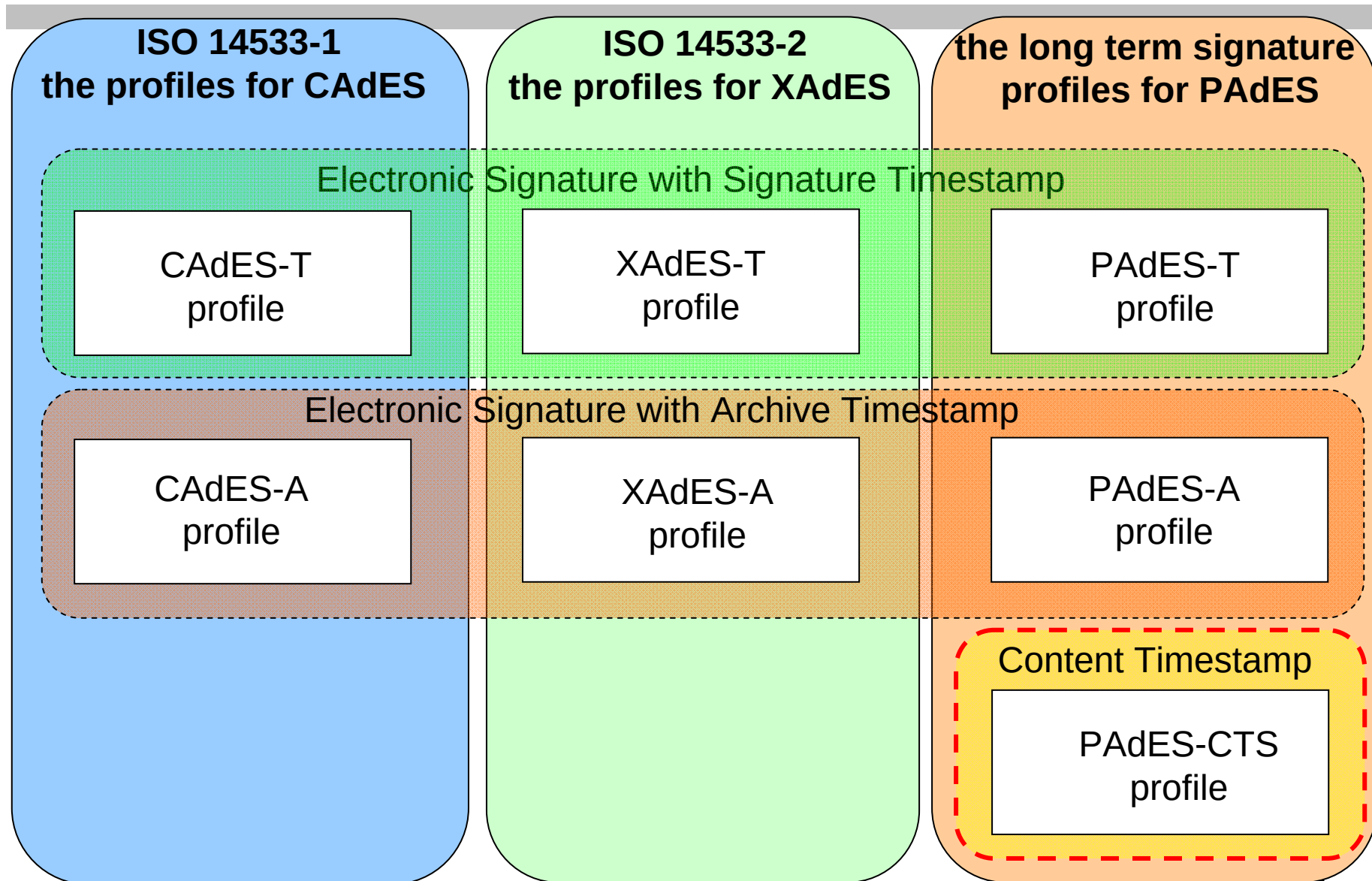
ETSI TS 102 778

ISO 32000-2(draft)

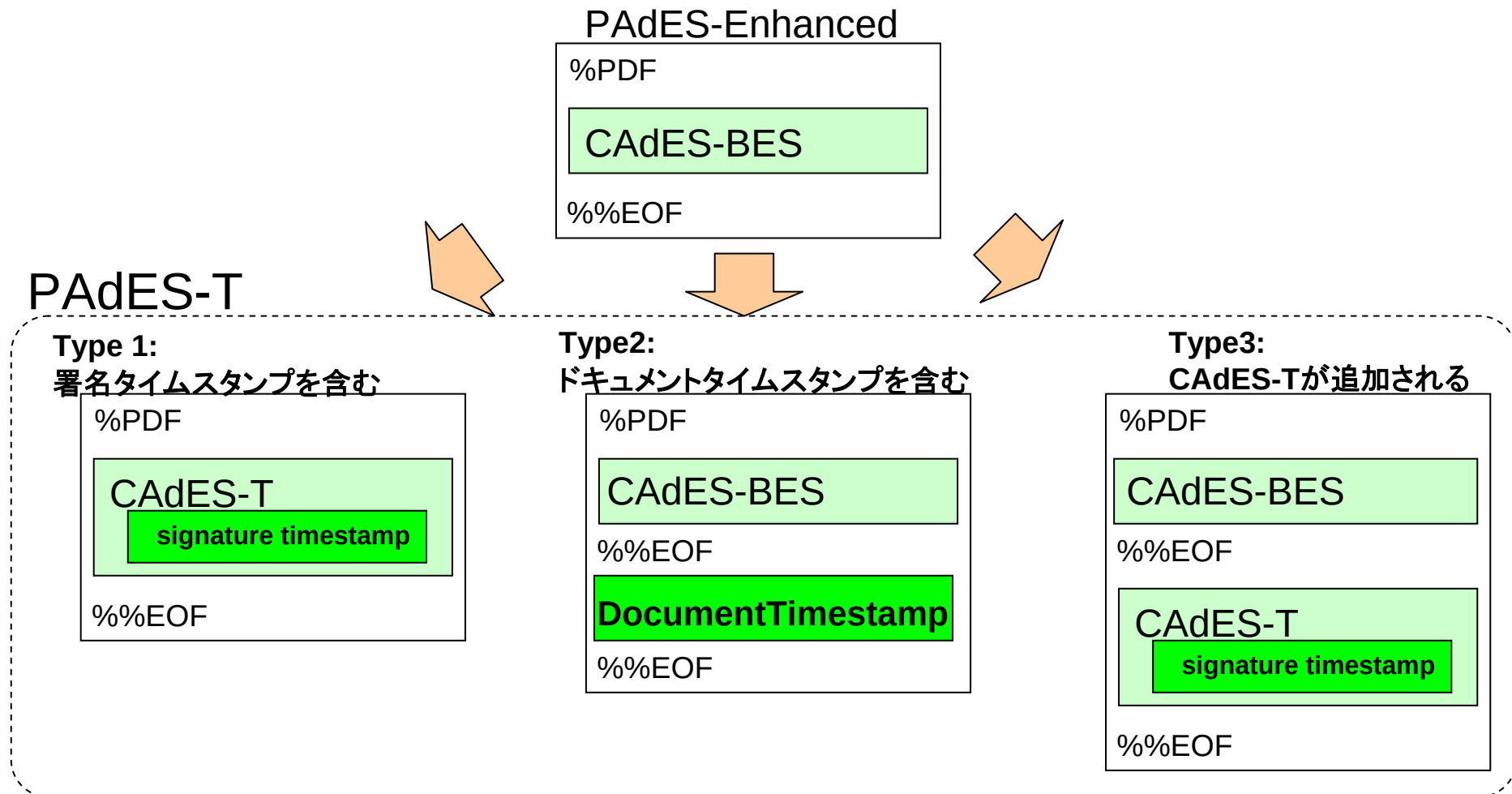
同じ位置付けのもの
がない！

長期保存のためのプロファイル

長期署名保存のためのプロファイルの構造



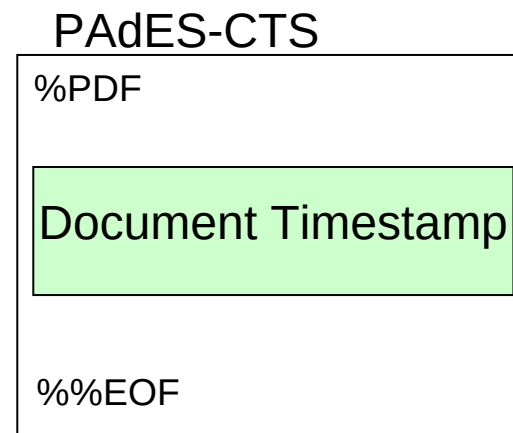
PAdES-Tプロファイル



PAdES-CTSプロファイル

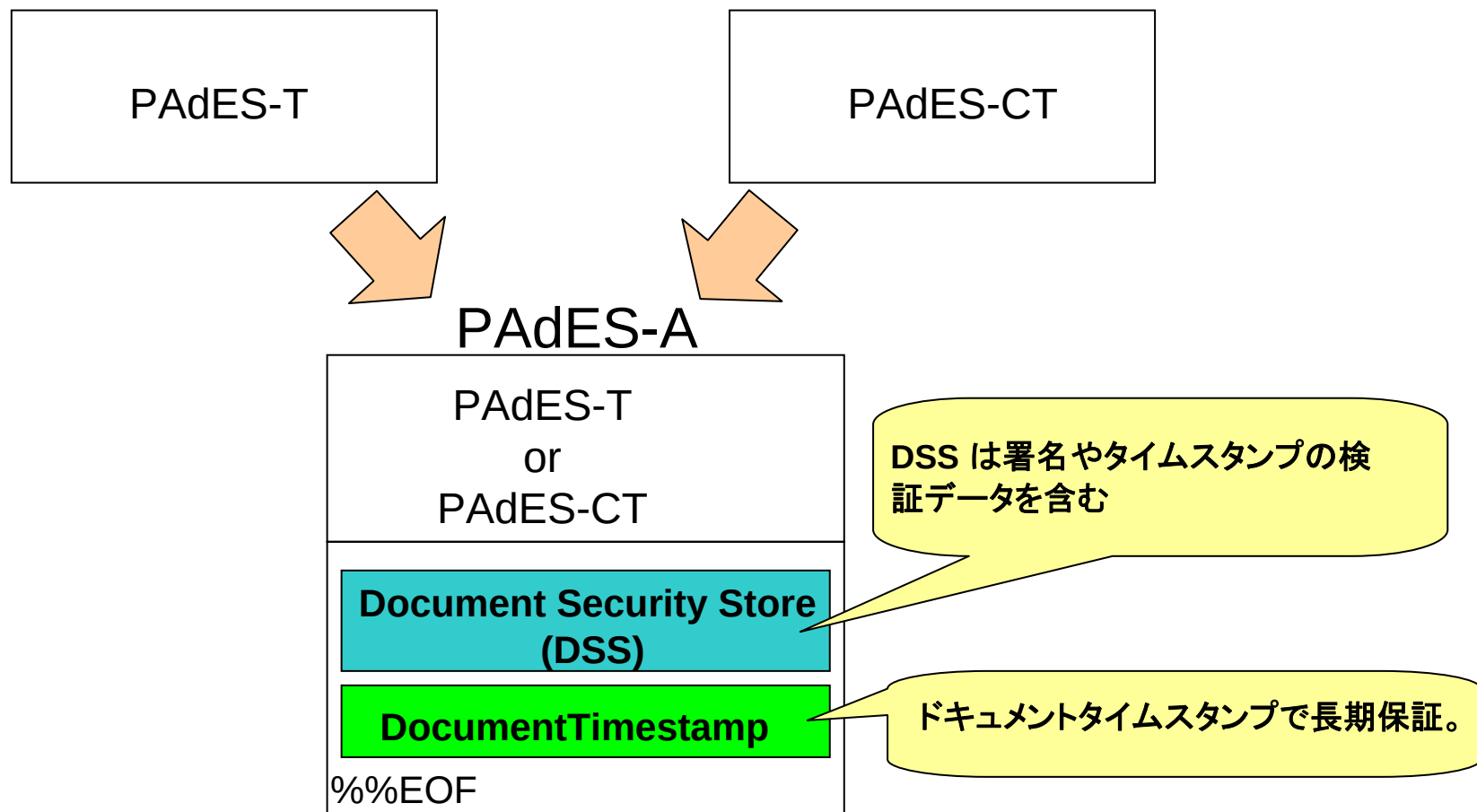


署名を含まず、タイムスタンプのみ含む。



PAdES-Aプロファイル

PAdES-T と PAdES-CTSの両者の有効性を延長するプロファイル。



ETSI/TC ESIの動向

電子署名標準化イニシアティブ

- 1999年、ICTSBがEESSIを設立
EESSI: European Electronic Signature Standardization Initiative
 - 目的はEC電子署名指令の実装を支援する標準化の調整
 - CENが要件、ETSIが仕様を分担
- 2002年、ETSI/TC SEC/ESI WGがTC ESIに昇格
 - ETSI/TC SECをクローズし、TC SEC内のESI WGとLI WG(Lawful interception; 合法的傍受)をTCに昇格
- 2003年、CENがE-Signワークショップをクローズ
- 2004年、EESSIをクローズ
 - Network and Information Security Steering Group (NISSG) に移管
 - 電子署名技術の標準化はETSI/TC ESIが継続

→ 要件・仕様・実態の乖離拡大化

(欧州自由貿易連合)

ICTSB: ICT Standard Board メンバはCEN、CENELEC、ETSI、EC/EFTA(オブザーバ)

CEN: 欧州標準化委員会

CENELEC: 欧州電気標準化委員会

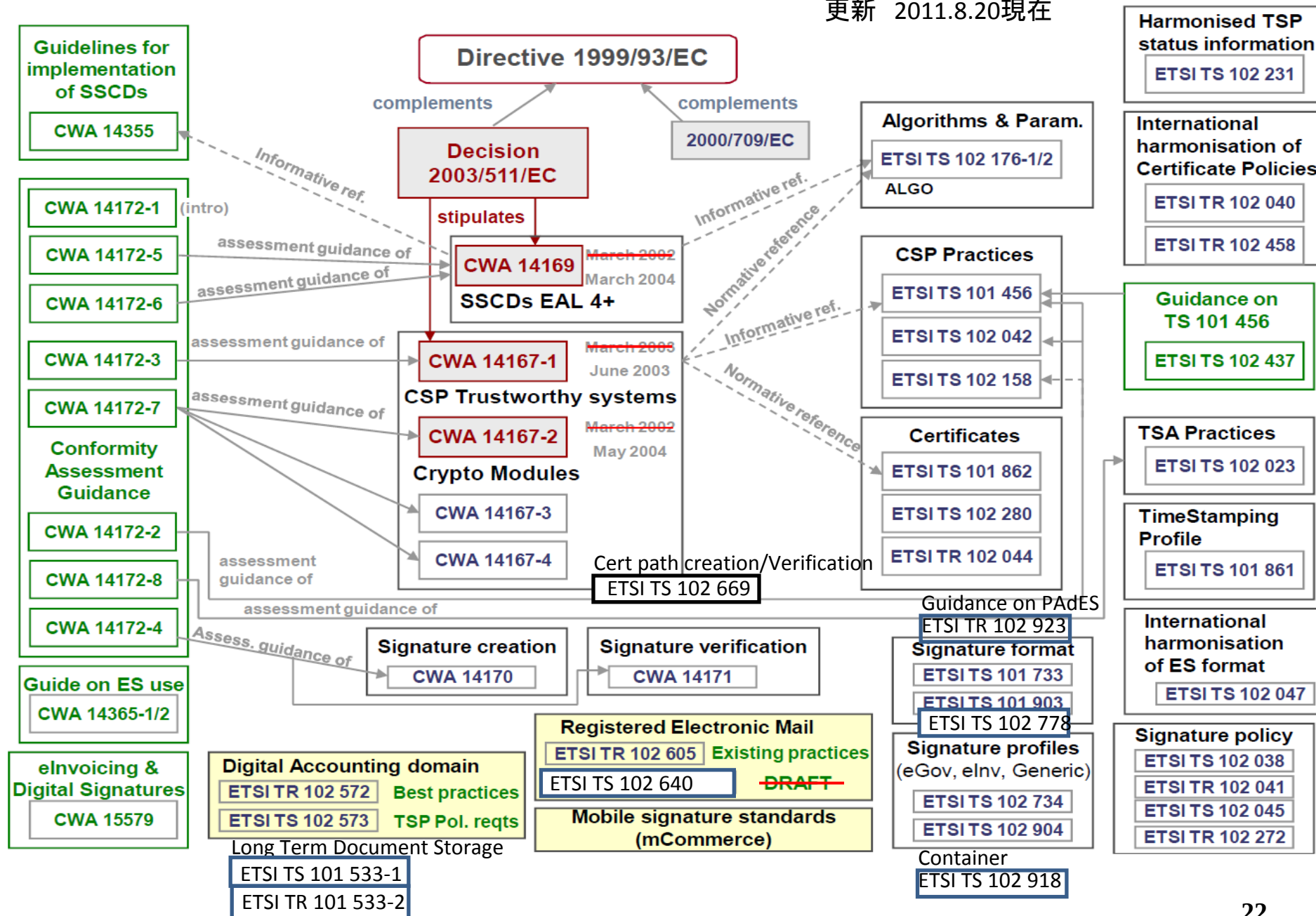
ETSI: 欧州電気通信標準化機構 正会員はCEPT(欧州郵便電気通信主管庁会議)メンバ

TC ESI: Electronic Signatures and Infrastructure 電子署名基盤技術委員会

EU eSignature Standardisation Work overview

SEALEDの資料を
更新 2011.8.20現在

(© SEALED, 2007)



M/460 STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS
CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES
APPLIED TO ELECTRONIC SIGNATURES

主旨

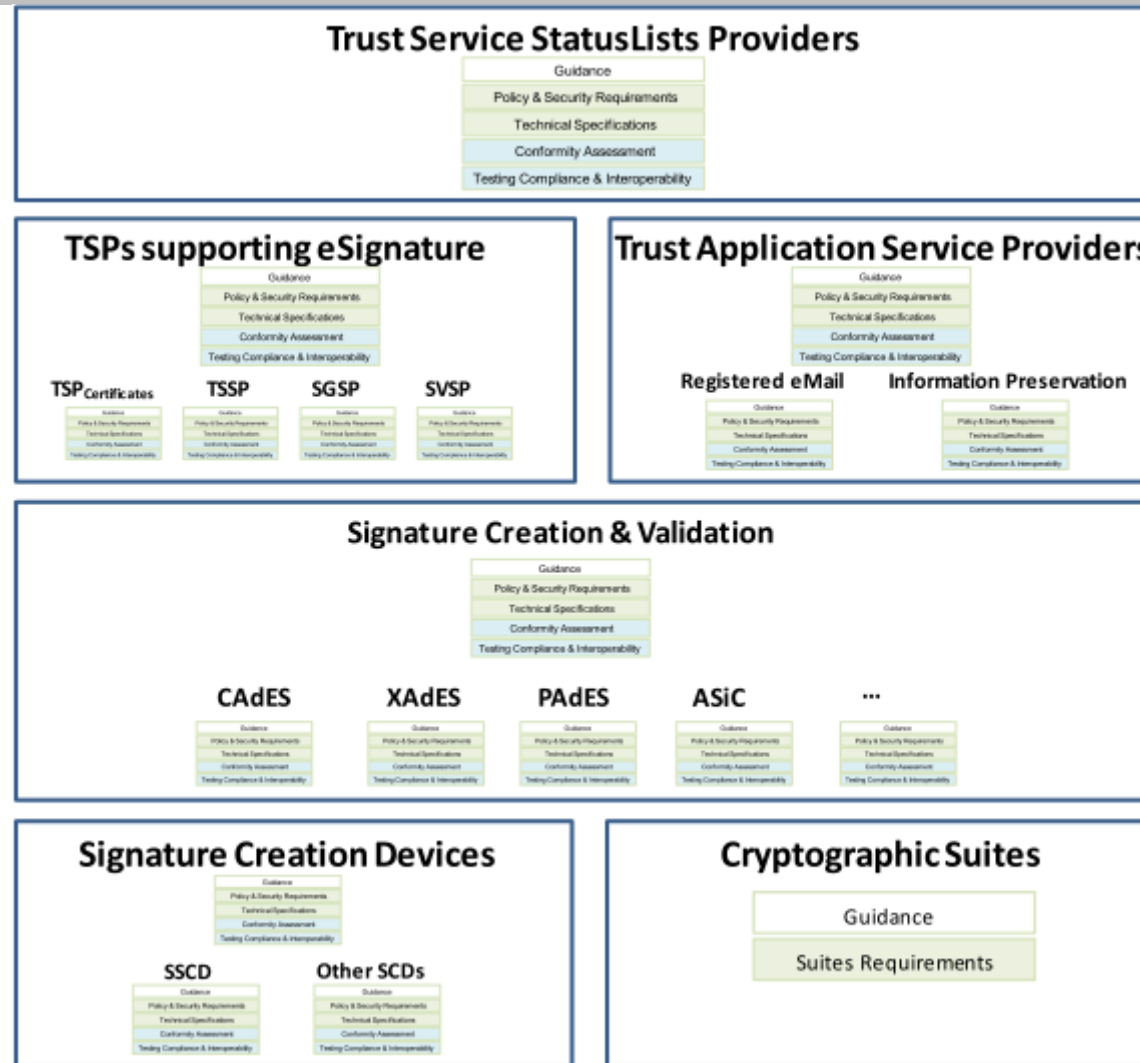
- ECの電子署名規格の軽量化と再編成
- 有効期限切れのCENのCWAの更新または廃棄
- 技術標準(TS)の統合
- 理解と利用を促進するTSの簡素化
- プレゼンテーションフレームワーク(ポータル、動的更新)
- TS生成からENやISOへの進化が定義されたライフサイクル
- 4年スパンの行動計画
- TS普及とプレゼンテーションインフラ維持のための恒久的な予算措置

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

EC指令460対応STF（フェーズ 1）

- 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

新フレームワーク



- 6つの機能領域
 - 複数のサブ領域
- 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
- 一貫した番号体系

EC指令460対応STF（フェーズ 2）



2012/9から4年程度

- STF457 **フレームワーク、調整**
 - フェーズ1で定義したすべての領域に跨るフレームワークの実現
- STF458 **署名生成/検証と信頼サービスプロバイダ**
 - 署名生成/検証プロセス及びフォーマット仕様の整備と欧州標準化
 - 電子署名をサポートする信頼サービスプロバイダ仕様の整備と欧州標準化
- STF459 **準拠性/相互運用性テストと信頼アプリケーションサービス**
 - 電子署名を適用した電子配送 (Electronic Delivery) の要求仕様標準化の検討
 - 必要不可欠な標準規格を実装することを促進する技術標準やツールの開発

eIDと信頼サービスに関する新規制



REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on electronic identification and trust services for electronic
transactions in the internal market

2012年6月4日に欧州議会で採択

1章 総則

2章 eID

3章 トラストサービス

1節 総則

2節 TSP(Trust Service Provider)及びTS監督(supervision)・・・適格TSPの監督、
トラステッドリスト、推奨適格TSP

3節 電子署名・・・電子署名→自然人、適格電子署名→手書署名と同等の法的効果、
適格電子署名生成デバイス→HW及びSW、
適格電子署名の検証要件、
適格電子書名適格検証サービス、適格長期保存サービス、
公共サービス用署名フォーマット→CAAdES、XAdES、PAdES

4節 電子シール・・・法人（電子署名を準用）

5節 電子タイムスタンプ・・・適格タイムスタンプ

6節 電子文書・・・紙・電子非差別

7節 適格電子配信サービス・・・要適格タイムスタンプ

8節 Webサイトの認証(Website Authentication)・・・適格Webサイト認証証明書(authentication certificate)

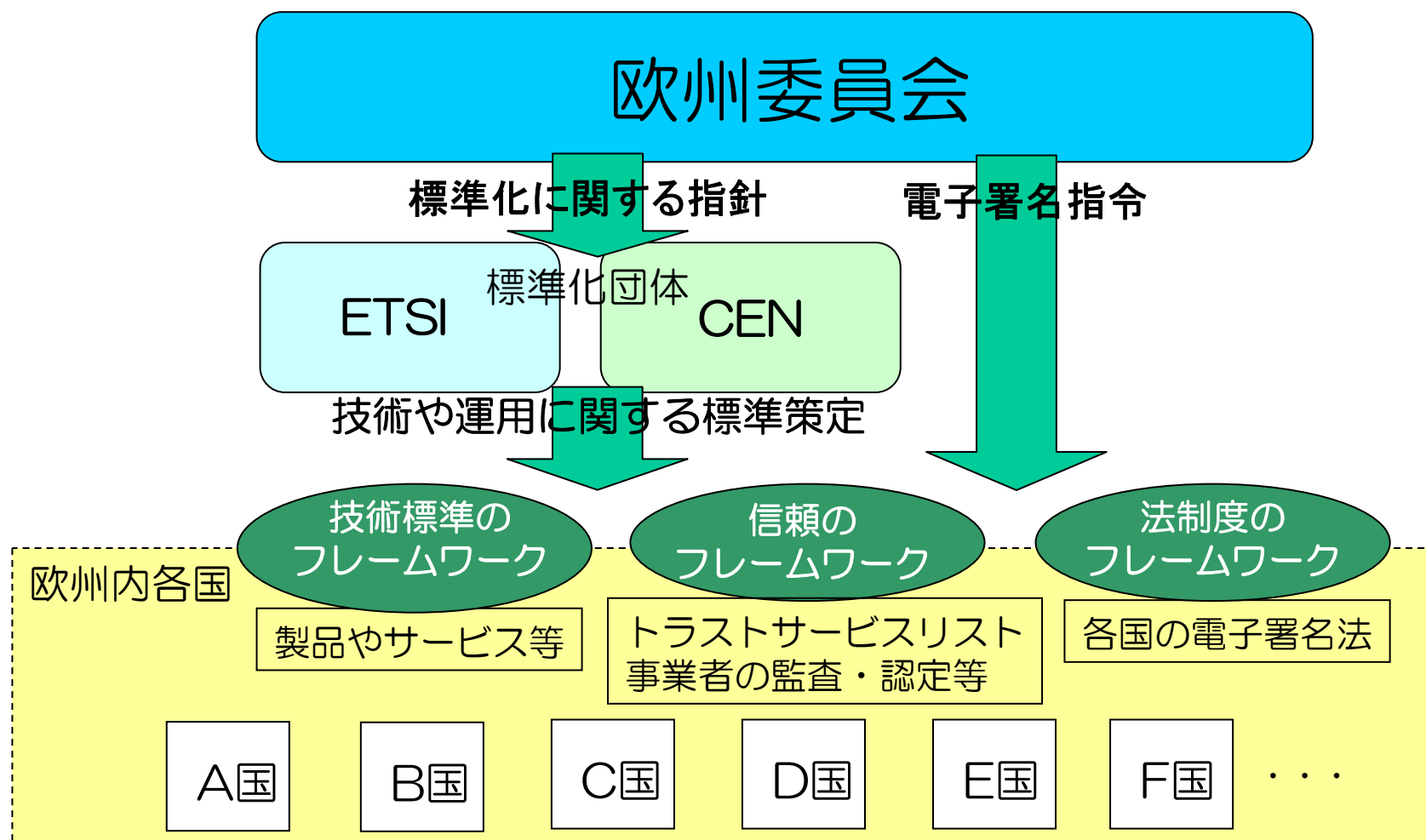
4章 委任

5章 施行

6章 最終規定・・・4年毎の報告、既存の適格証明書→max5年有効

付属書 適格証明書、適格署名生成デバイス

欧州の電子署名の体系



欧州委員会のトップダウンによる体系化されたアプローチ。
制度と技術が結びついた整合性のあるフレームワークを目指している。

トラステッドリスト e-Seal

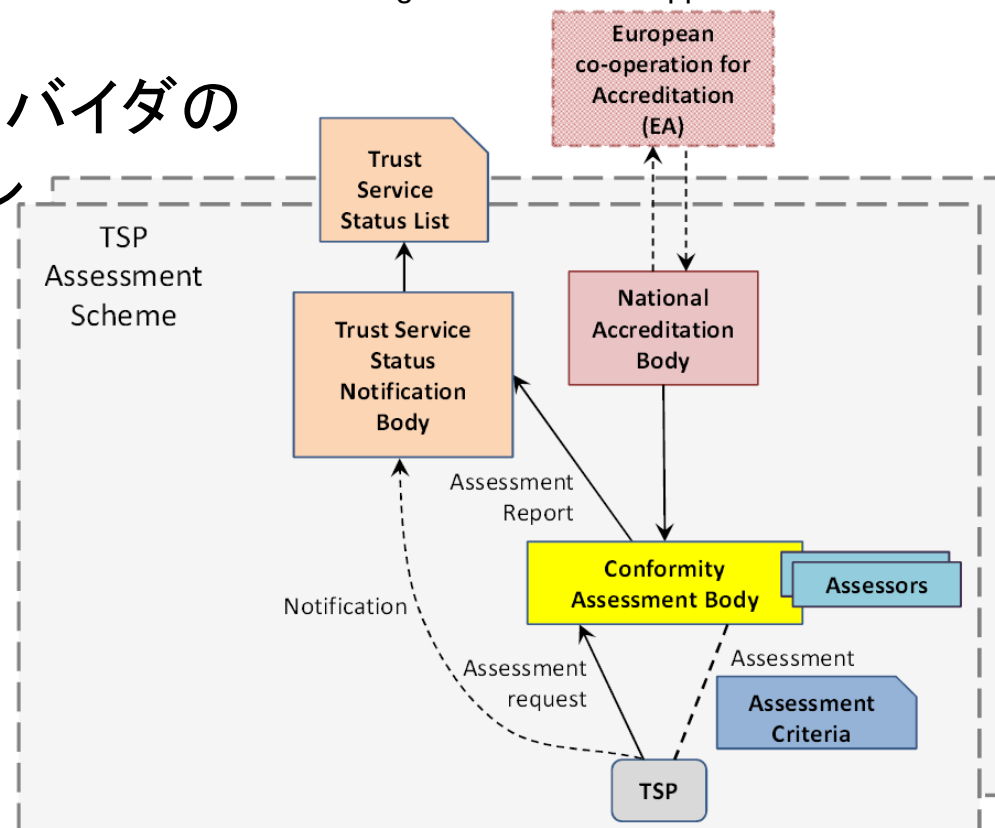
トラステッドリスト

- 国毎にトラステッドリスト (TSL: Trust-service Status List) を発行
⇒ CA、TSA 等の信頼性を各国間でレベル合わせ
- MS、Adobe とも協調

“Alignment of Adobe-Approved Trust List (AATL) and EU Trust List (EUTL)”

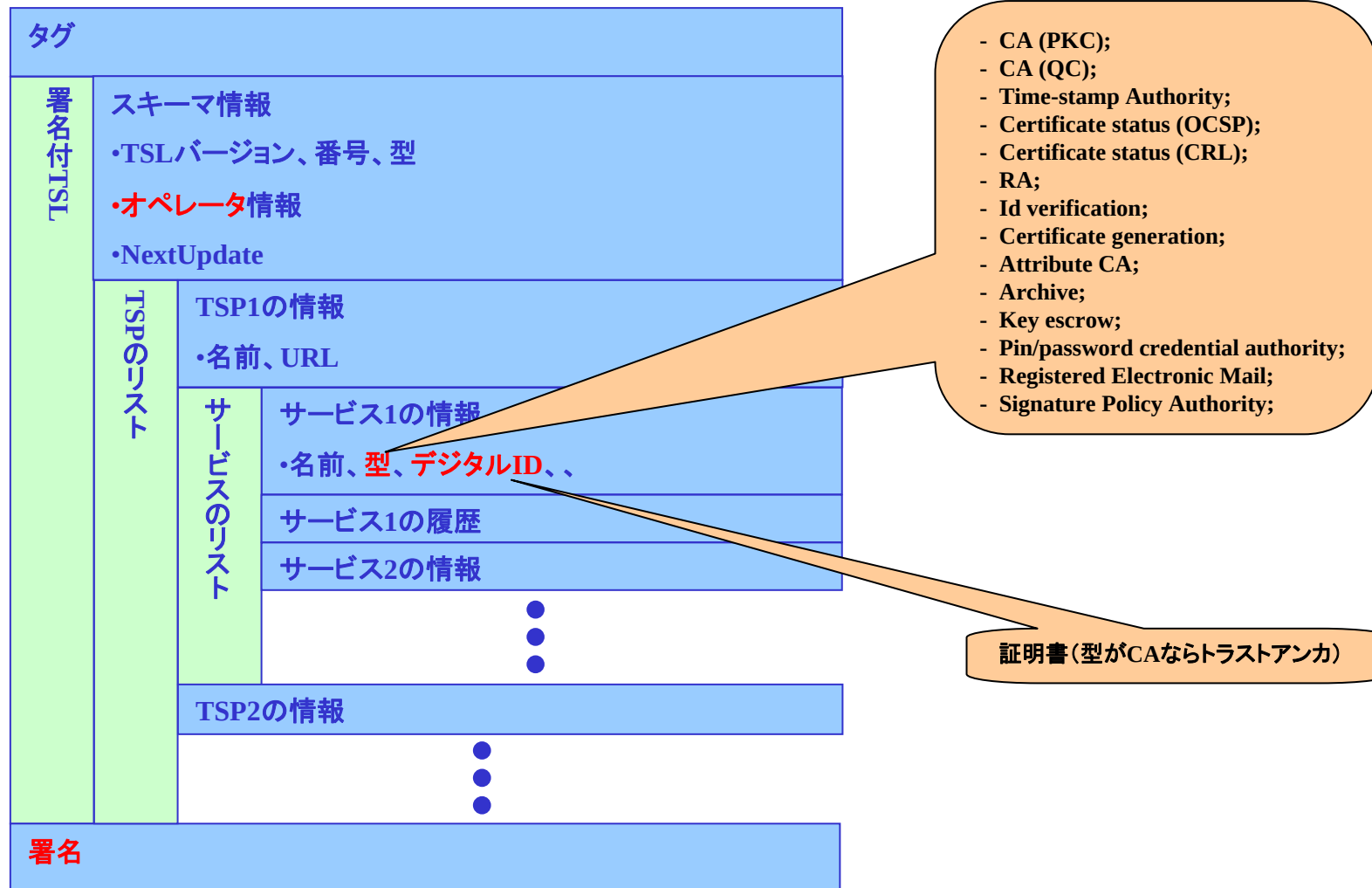
<http://blogs.adobe.com/standards/2013/06/25/alignment-of-adobe-approved-trust-list-aatl-and-eu-trust-list-eutl/>

信頼サービスプロバイダの アセスメントモデル



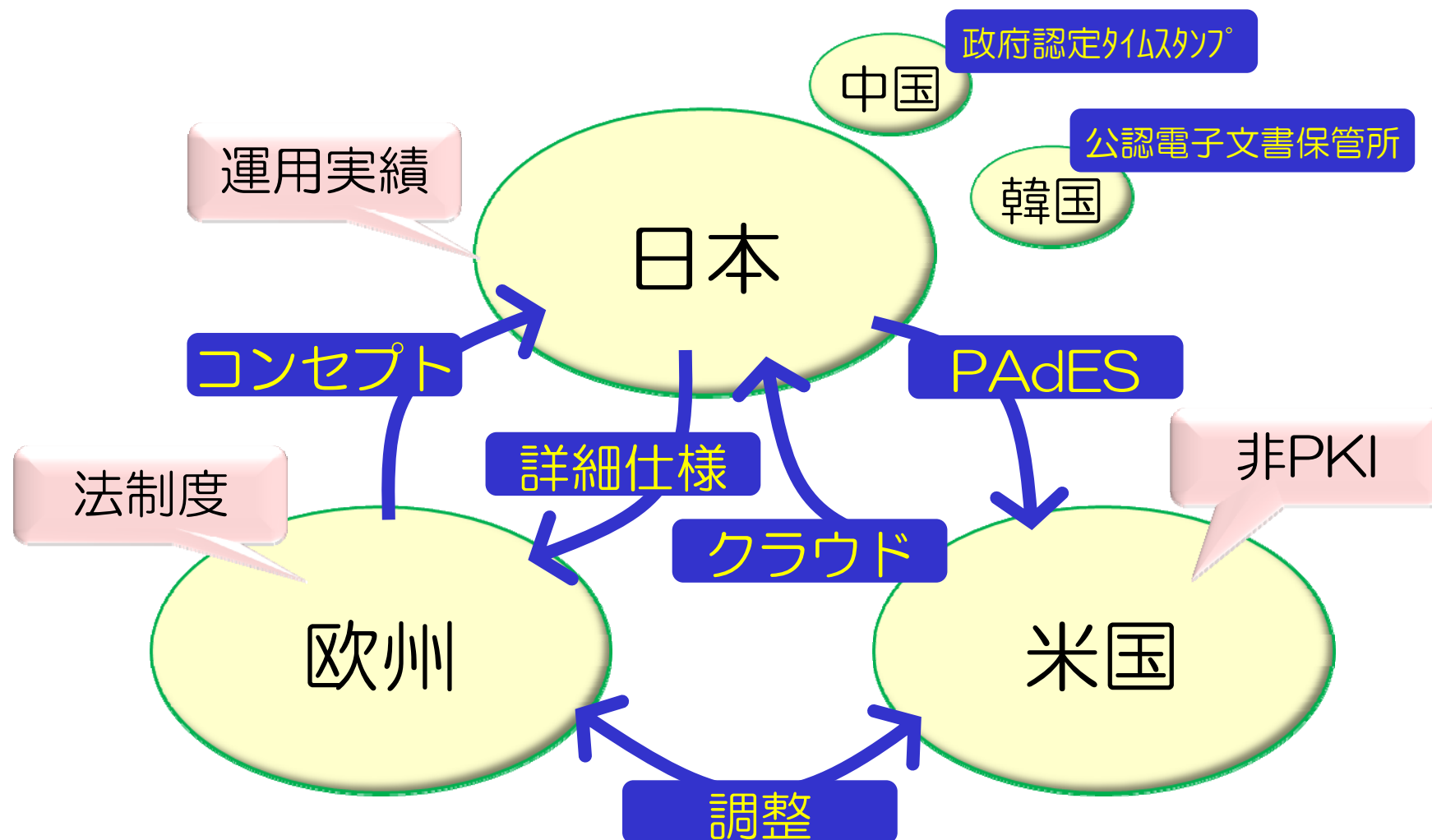
出典: ETSI TS 119 403

TSP Status Listのモデル



- eSignature ⇒ 自然人
 - eSeal ⇒ 法人
 - ドキュメント認証のための手段
 - 発信元と完全性を保証する
 - 基本的にeSignatureと同等
- ⇒ 技術的には同等で法的な問題のみ？

電子署名をめぐる国内外の情勢





ご清聴ありがとうございました。