セコムIS研究所
Intelligent Systems Laboratory

PKI Day 2016
電子署名標準化動向から今後の方向性を探る

2016年4月22日

セコム株式会社　IS研究所
佐藤　雅史

セコムIS研究所
Intelligent Systems Laboratory

はじめに

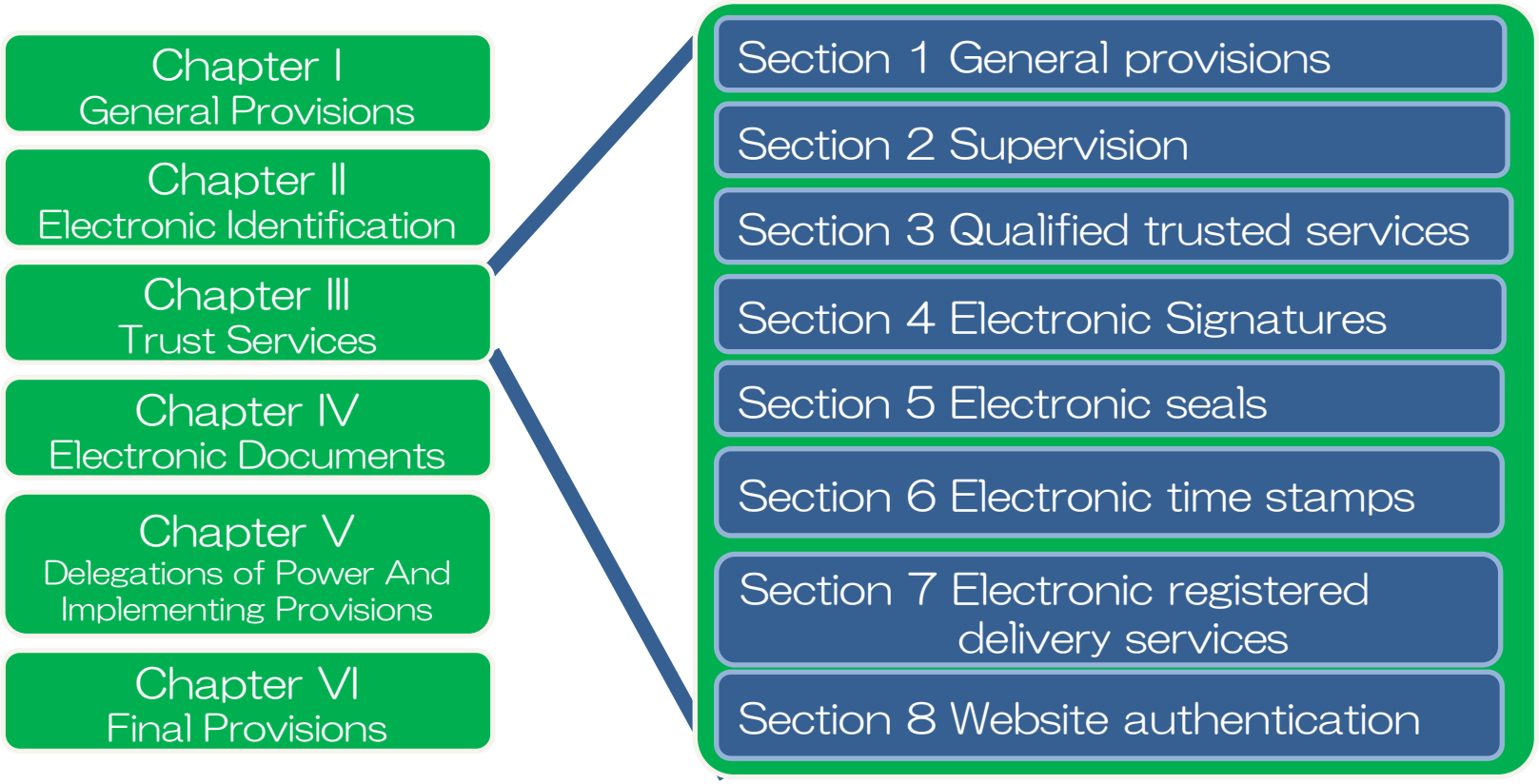
- 電子署名に関する欧州の標準化動向を中心に、関連がありそうな日本の動向を（半ば強引に）探っていきます。
- 日本の動向については、公開情報より引用して紹介しております。講演内容は、関連する団体・企業・組織を代表するものではありません。

eIDASとは？

- eIDAS: Electronic identification and trust services
- EUで定めた電子認証や電子署名を含めたトラストサービスに関する規則。
- 電子認証やトラストサービスを普及させることで、国境を越えた電子取引を安全かつシームレスに実現させることが目的。

EU-Regulation eIDASの構成

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014
on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

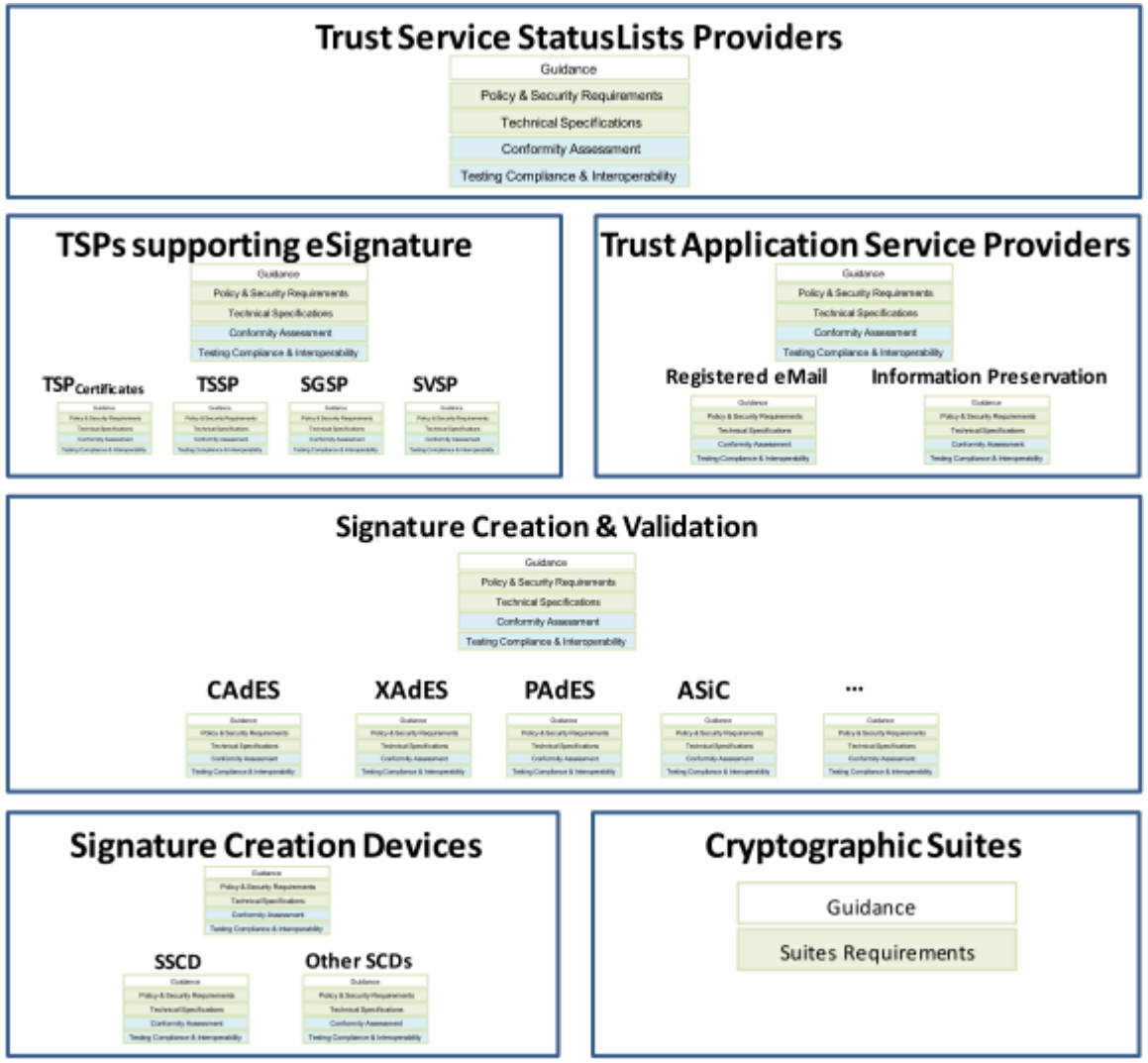


EC指令460(mandate460:2009/12

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

- 欧州の電子署名規格の軽量化と再編成
  - 期限切れの規格の更新や廃棄
  - 規格の統合、再構成
  - 理解と利用を促進するための規格の簡素化
- ETSI技術仕様(TS)の生成から欧州規格(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

欧州電子署名標準フレームワーク



ETSI SR 001 604より

電子署名フォーマット規格

CAdES
(CMS Advanced Electronic Signature)

- バイナリデータ形式のフォーマット。
- 任意のデータ形式に署名可能。
- 最も歴史が古い。
- 現在も改定が進んでいる。

XAdES
(XML Advanced Electronic Signature)

- XML形式のフォーマット。
- 任意のデータ形式に署名可能。
- 特にXMLデータとの親和性が高い。

PAdES
(PDF Advanced Electronic Signature)

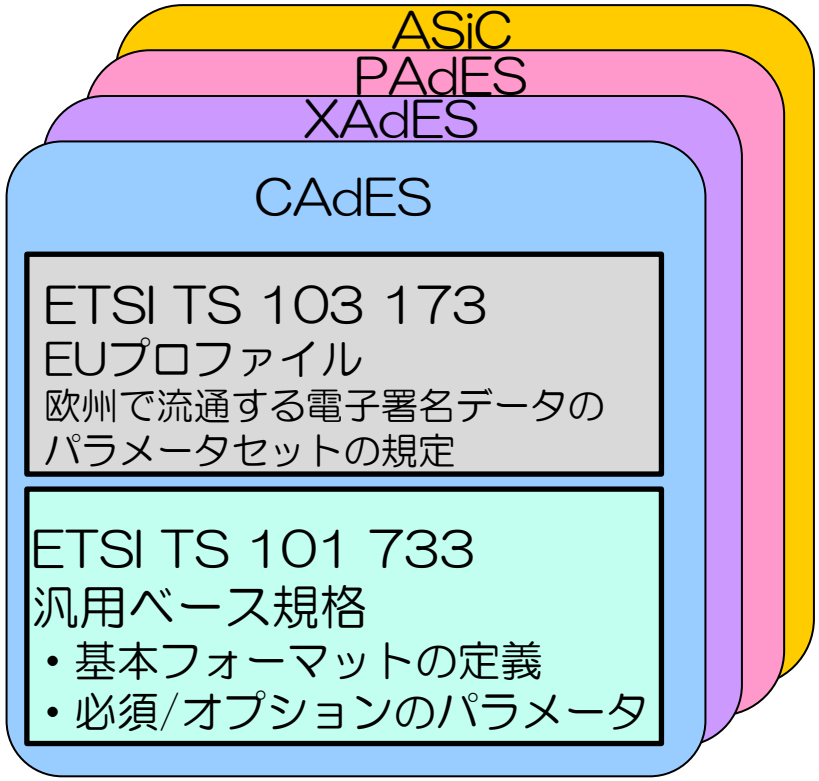
- PDFに特化したフォーマット。
- 同仕様がPDF規格に取り込まれる。
（ISO/DIS 32000-2）

ASiC
(Associated Signature Container)

- 関連する複数の電子データを一つにパッケージングするフォーマット。
- CAdES/XAdESを適用した形式がある。

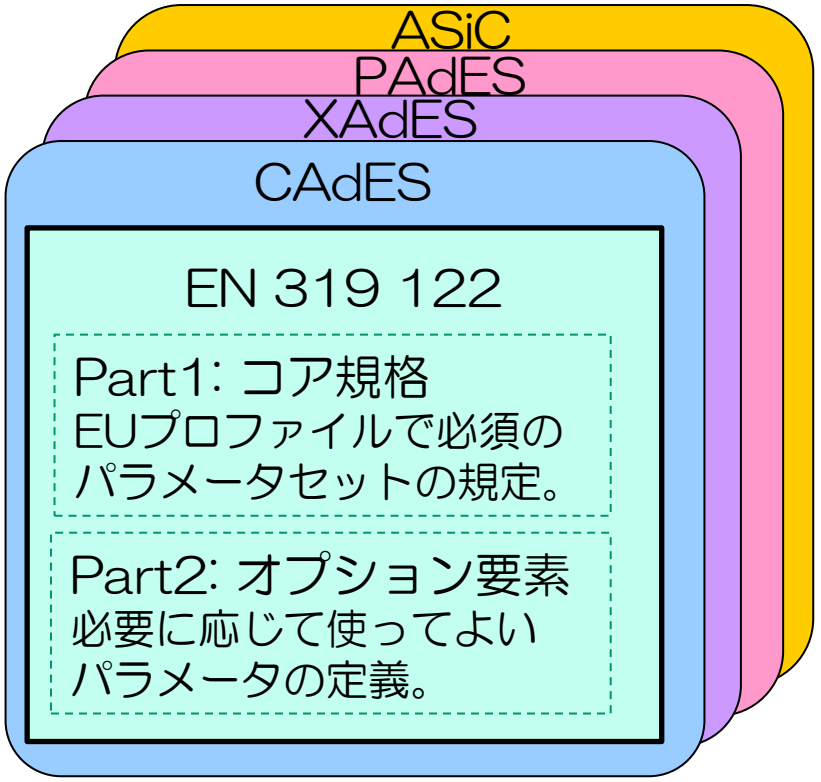
電子署名フォーマット規格の再構築

従来のTS版



ベース規格とプロファイルが独立しているため、
ベース規格のみ参照することができた。

EN版（4月発行予定）



EUプロファイルをもとにコア規格を作成。
これまでEUプロファイルと無縁だった所
（特に日本）も影響を受ける。

EN化での変更点

- 構成や方針など
  - 規格の構成が全く異なる。欧州プロファイルベース。
  - TS時代の旧仕様はPart2に押し込まれた。
  - 従来のTS規格はHistorical1として公開するがメンテしない。
- 機能面
  - 欧州プロファイルベースなので日本では不要なSigningTime属性などが必須になってしまった。
  - SAMLアサーションなど署名者に関する属性情報を格納できるようになった。RFC【CAdES/XAdES/PAdES】
  - 署名の可視化に関する規格は無くなった。【PAdES】

電子署名フォーマットの標準化状況

	CAdES	XAdES	PAdES
EN規格	EN 319 122	EN 319 132	EN 319 142
JIS 規格 (長期署名プロファイル)	JIS X 5092	JIS X 5093	―
ISO規格 (長期署名プロファイル)	ISO 14533-1	ISO 14533-2	ISO14533-3 (現在CD)
ISO規格 (ヘルスケア)	ISO 17090-4	ISO 17090-4	―
ISO規格 (文書フォーマット)		ISO/IEC 29500 (OOXML) ISO/IEC 26300 (ODF)	ISO/DIS 32000-2 (PDF2.0)
その他	JAHIS標準	JAHIS標準	

整合化が必要

※矢印は参照の向き

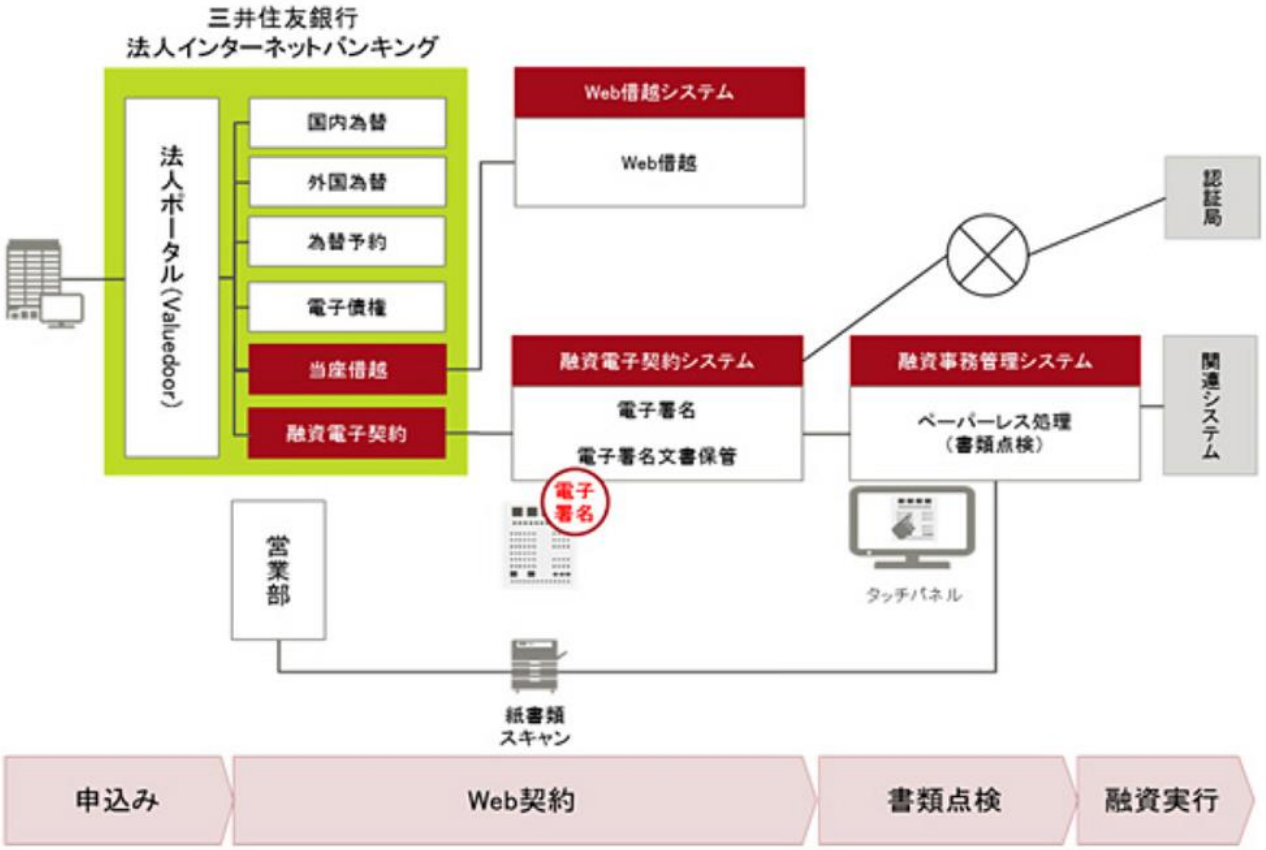
CAdES/XAdESに関してはJIS/ISO規格の見直しが必要。

日本の動向
～電子署名フォーマット標準化～

- 標準化関連
  - ISO 14533シリーズ（長期署名プロファイル）
    - Part1（CAdES）, Part 2（XAdES）に続き、ISO 14533-3（PAdES）を推進。現在はCDの段階に。
      【PJリーダー兼エディタは佐藤が担当（宣伝）】
  - ISO 17090-4（ヘルスケア電子署名規格）
    - 日本のJAHISが推進。
  - ISO/IEC 29500（OOXML）, ISO/IEC 26300（ODF）
    - XML文書フォーマットへの電子署名（XAdES）適用に関する議論を先導。
  - ISO/DIS 32000-2（PDF2.0）
    - PAdES規格との整合化に関して日本と欧州が協力。

日本の動向
～電子署名フォーマット活用（電子契約）～

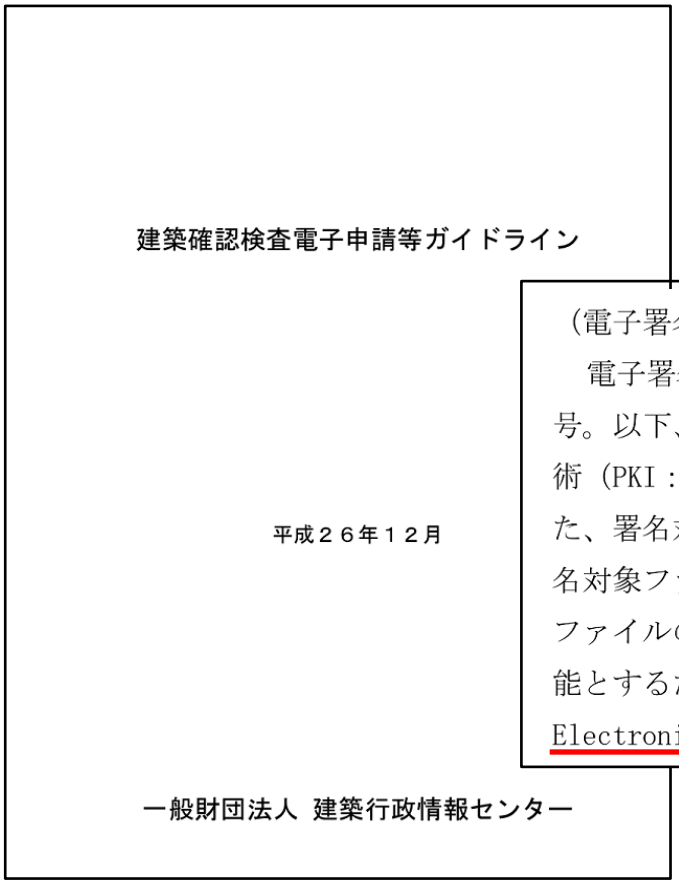
株式会社三井住友銀行の融資契約電子化（平成28年2月）



＜システムイメージ図＞

http://pr.fujitsu.com/jp/news/2016/03/4.html

日本の動向
～電子署名フォーマット活用（建築業界）～


建築確認検査電子申請等ガイドライン

平成２６年１２月

一般財団法人 建築行政情報センター

（電子署名と署名者）

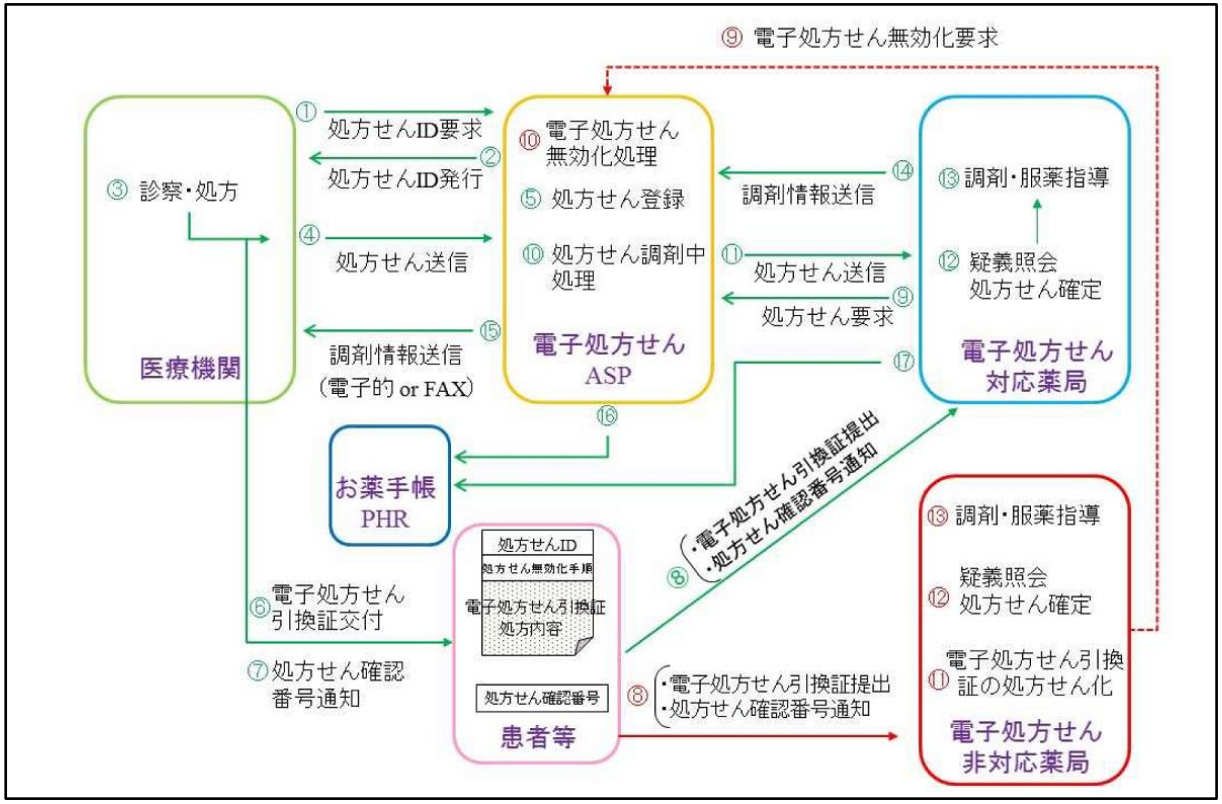
電子署名の方式は、「電子署名及び認証業務に関する法律」（平成12年5月31日法律第102号。以下、電子署名法という。）第2条第1項の電子署名とし、電子署名の作成には標準技術（PKI：Public Key Infrastructure技術による標準形式）を用いる必要がある。また、署名対象データの中に署名値を格納することができる内包形式（Enveloped型）が署名対象ファイルと署名データが１つのファイルとなるので扱いやすい。申請データがPDFファイルの場合は署名済みファイルの長期保存を考慮すると、長期間電子署名の検証を可能とするためにPDFファイルの長期署名標準規格であるPAdES-LTV（PDF Advanced Electronic Signatures Long Term Validation）形式が適している。

※赤線は講演者が追記

http://www.icba.or.jp/index/20141217_denshi_shinsei_guideline.pdf

日本の動向
～電子署名フォーマット活用（医療）～

電子処方せんの運用ガイドライン（平成28年3月31日、厚労省）

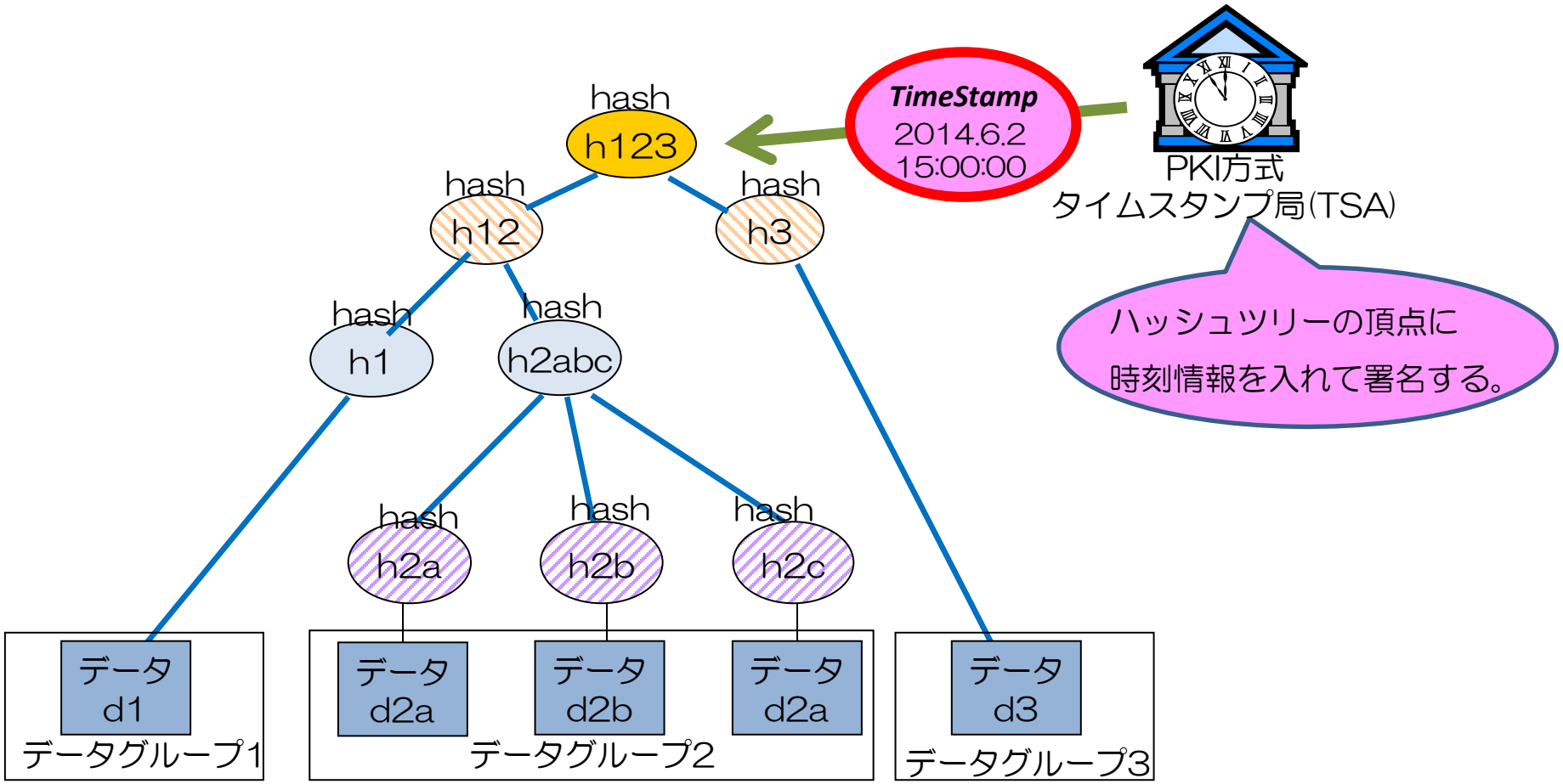


http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119545_2.pdf

医師の電子署名、薬局側の電子署名にXAdESを用いることになっている。

ETSIの新規格化作業
(ERS in CAdES/XAdES)

ERS: Evidence Record Syntax (RFC 4998, RFC 6283)



ERSの末端データとしてCAdES/XAdESの電子署名を投入し、
複数の電子署名の延長処理（長期署名化）をまとめて行う仕様を明確化する。

日本の動向
～ERS関連～

セコムIS研究所
Intelligent Systems Laboratory

「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則」（電子帳簿保存法）H.27年度改正
国税庁Q&Aより
https://www.nta.go.jp/shiraberu/zeiho-kaishaku/joho-zeikaishaku/dennshichobo/jirei/ans2/03.htm#a47

問47　規則第3条第5項第2号ロ（タイムスタンプ）に規定するタイムスタンプについては、「一の入力単位ごと」に付すこととされていますが、このタイムスタンプが一の入力単位ごとに検証できるものである場合には、書類種別や部署ごとの電磁的記録の記録事項にまとめて付してもよいのでしょうか。

回答

まとめてタイムスタンプを付しても差し支えありません。

解説

規則第3条第5項第2号ロ（タイムスタンプ）の規定によれば、「一の入力単位ごとの電磁的記録の記録事項に、一般財団法人日本データ通信協会が認定する業務に係るタイムスタンプ…を付すこと」とされています。

このタイムスタンプを付す方法については、①一の入力単位である単ファイルごとにタイムスタンプを付す方法及び②複数ファイルにまとめてタイムスタンプを付す方法が考えられます。

上記②の方法の改ざんの検証については、通常、複数ファイルのうち1つの単ファイルが改ざんされた場合には、その複数ファイルのうち改ざんされた単ファイルのみを検証することができないため、その複数ファイルの全体について、変更されていないことの確認ができなくなります。

しかしながら、上記②の方法の改ざんの検証については、単ファイルのハッシュ値を束ねて階層化した上でまとめてタイムスタンプを付す技術を使用する方法によりタイムスタンプを付した場合には、改ざんされた単ファイルのみを検証することができ、また、このような方法であれば、一の入力単位である単ファイルごとにその単ファイルのハッシュ値を通じてタイムスタンプを付している状態となり、実質的には「一の入力単位ごと」にタイムスタンプを付しているものと解することができます。

したがって、このような方法であれば、まとめてタイムスタンプを付しても差し支えありません。

※赤線は講演者が追記

モバイルやクラウド等を想定した署名環境

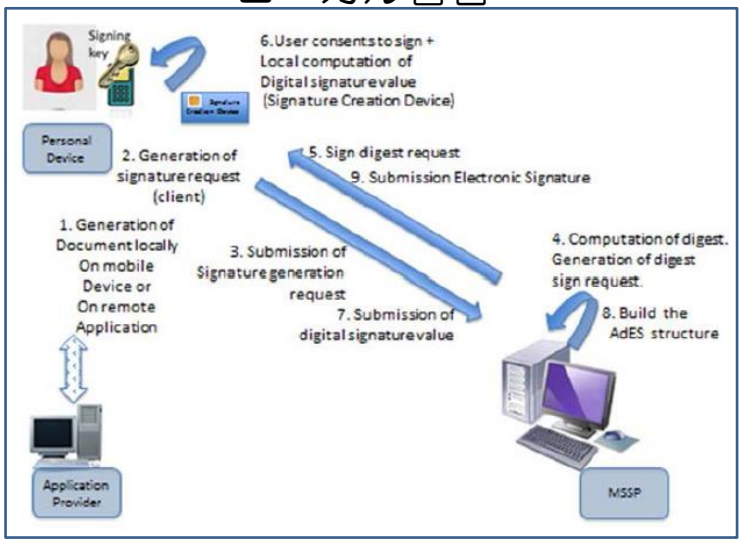
- ETSI SR 019 020 V1.1.1
  The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environment [2016年2月]
- EN 419 241
  Security requirements for trustworthy systems supporting server signing (signature generation services) [策定中]
- EN 419 251
  Protection profiles for authentication device [策定中]
- EN 419 261
  Security requirements for trustworthy systems managing certificates for electronic signatures [策定中]

ETSI SR 019 020 V1.1.1 [2016年2月]

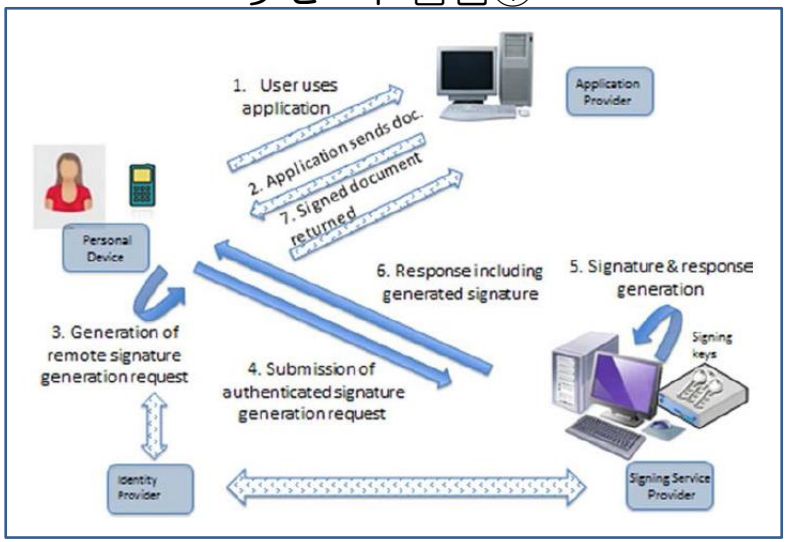
The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environment

セコムIS研究所 Intelligent Systems Laboratory

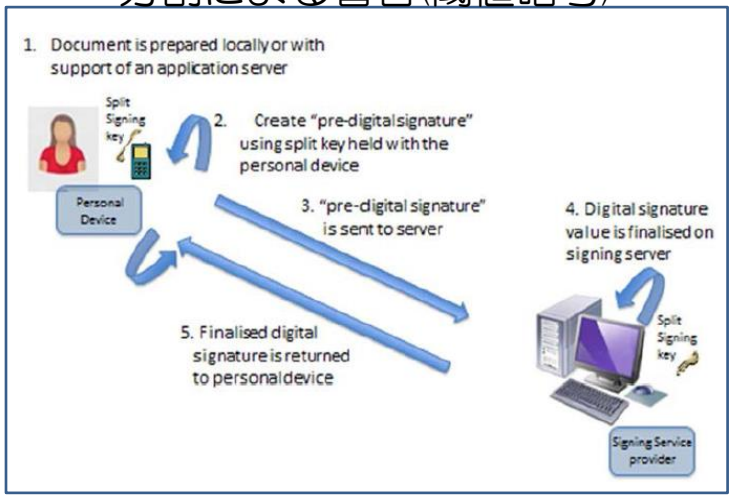
ローカル署名



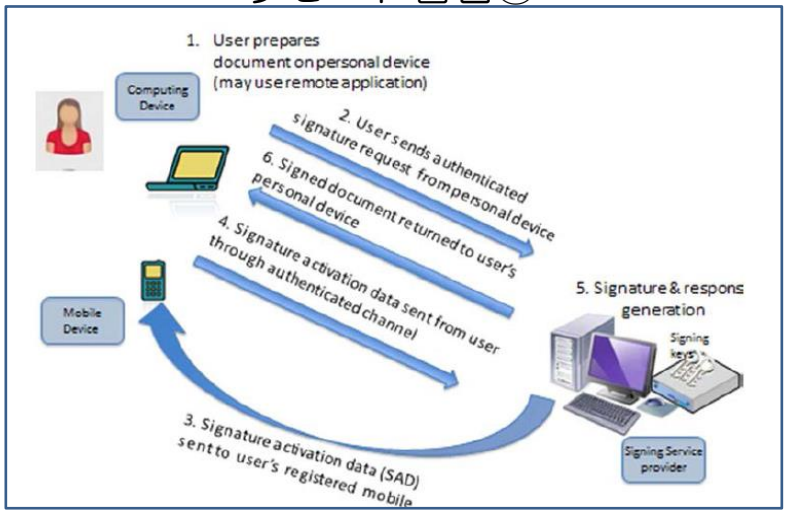
リモート署名①



分割による署名(閾値暗号)



リモート署名②



※各図はETSI SR 019 020 V1.1.1より引用

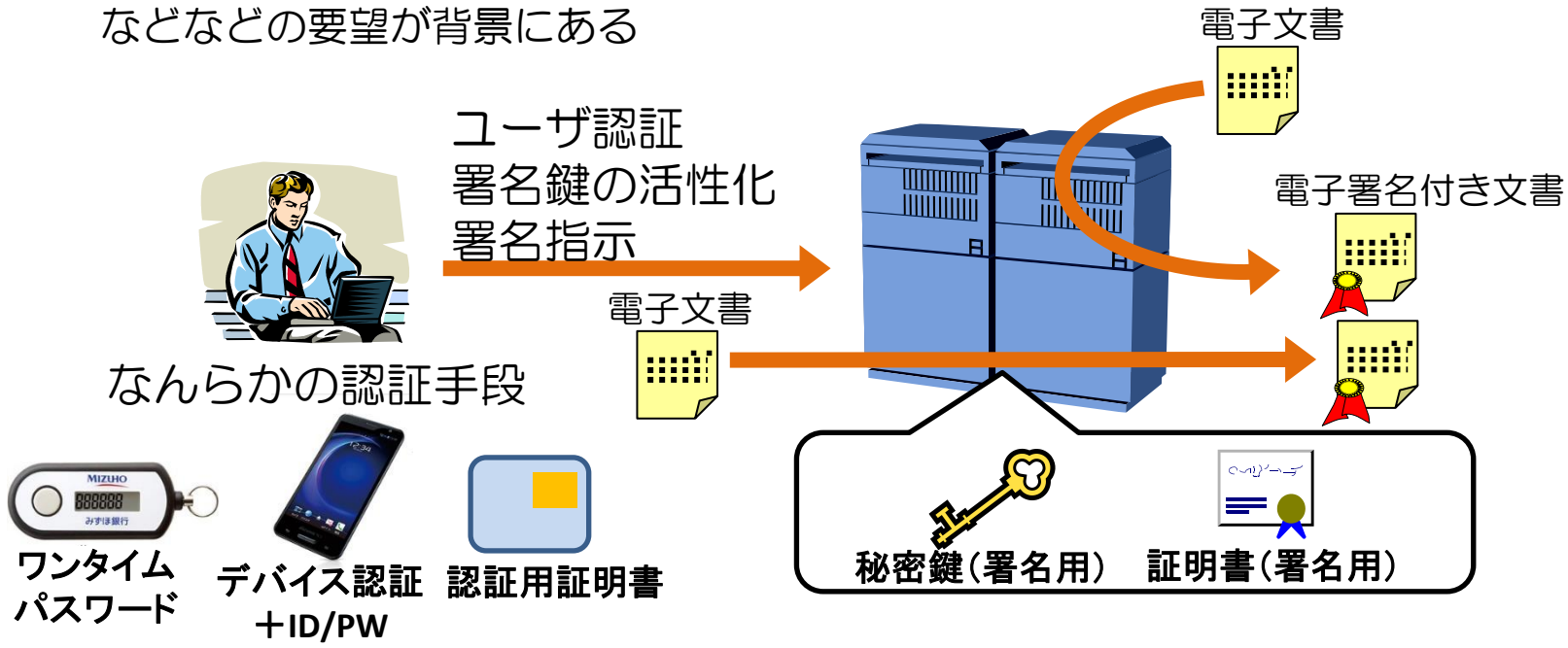
リモート署名(サーバ署名)って？

セコム IS 研究所
Intelligent Systems Laboratory

一言で言えば、個人の署名鍵をサーバ上で管理して使わせる形態。

- デバイスが変わっても同じ署名鍵が使いたい…
- クラウド等での文書管理と連携しやすくしたい…
- 個々のデバイスで署名鍵を管理したくない…

などなどの要望が背景にある



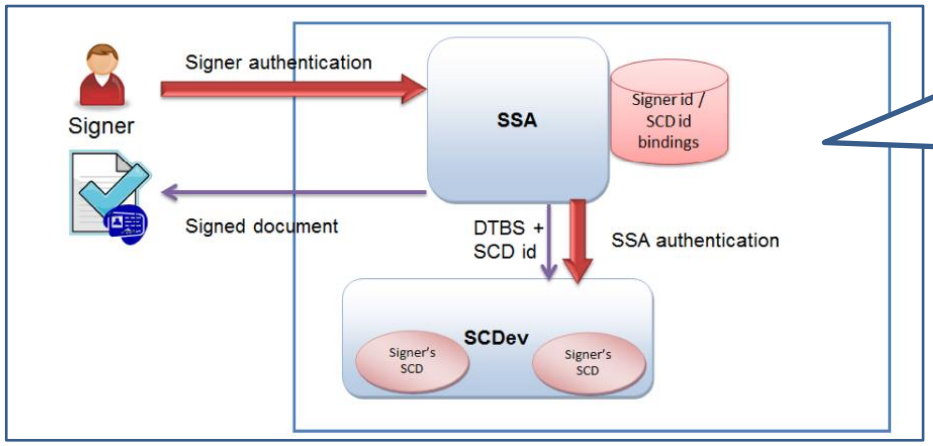
サーバ上にある署名鍵がそのユーザ本人のコントロール下にあって、そのユーザの意図通りに署名鍵を使える必要がある（他の人が使えてはいけない）。

リモート署名が要望される背景や課題は、欧州も日本も同じ。

CEN/TS 419 241
Security Requirements for Trustworthy Systems Supporting Server Signing

セコム IS研究所 Intelligent Systems Laboratory

リモート署名を提供するサーバに関するセキュリティ要件（2014年4月発行）。
現在策定中のEN 419 241のベースと思われる。

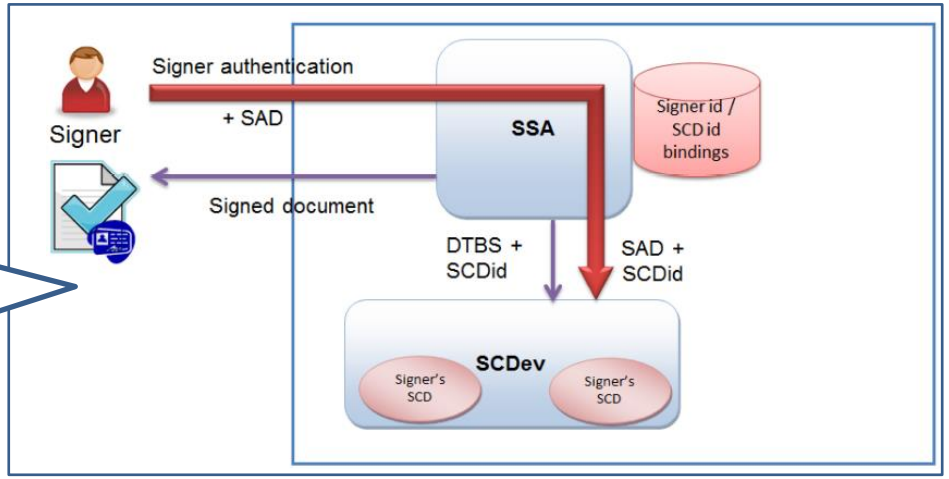


level 1 sole control

- サーバ署名アプリ(SSA)が署名者の認証をする。
- 署名鍵を管理するSCDev (HSM等)は署名者の認証を必要としない。

level 2 sole control

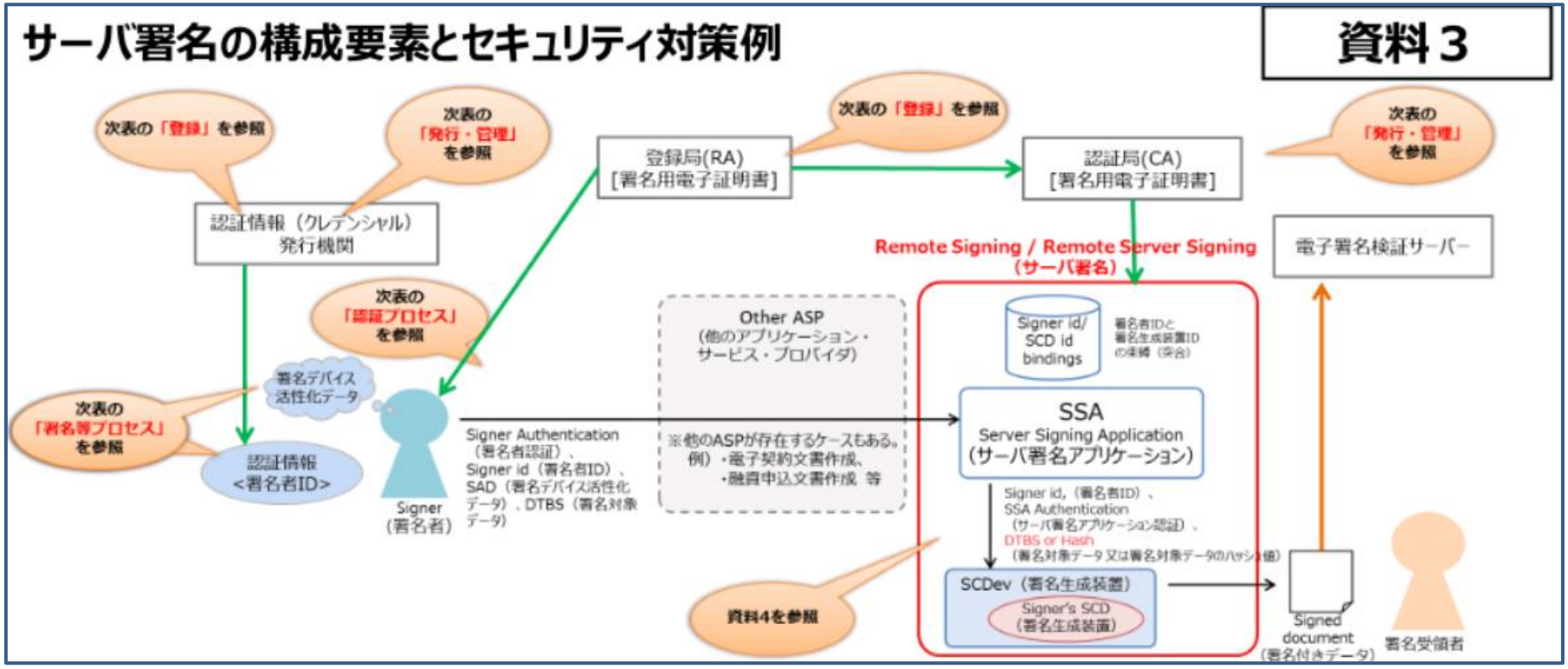
- 署名鍵を管理するSCDevでも署名者の認証をする。
- 多要素認証必須。
- EUのQualifiedレベルはlevel 2を満たす必要がある。



※各図はCEN/TS 419 241より引用

日本の動向
～リモート署名の検討～

- 電子署名法研究会(平成27年度)による検討
  http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou



http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h27_003_03_00.pdfより引用

2016年3月発行済のEN規格

- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
  - 319 411-1 v1.1.1: General requirements
  - 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates
- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- EN 319 412 Certificate Profiles
  - 319 412-1 v1.1.1: Overview and common data structures
  - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons
  - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons
  - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations

EU証明書プロファイル(法人)の概要

- 証明書のSubjectにorganizationIdentifier属性を入れ、法人IDを指定する。
- organizationIdentifierは法人番号の種別を表す略記をプリフィックスとして法人IDを表記する。
  - 種別を表す略記は、3文字の略記や、2文字の略記及び国名略記（ISO 3166)。
- これらのorganizationIdentifierの構文はid-etsi-qcs-SemanticsId-Legal1として定義されており、このOIDをQCStatement拡張のqcStatement-2に格納することで識別可能になっている。
  - QCStatementはRFC 3739, Internet X.509 Public Key Infrastructure: Qualified Certificates Profileを参照のこと。

日本の動向
～証明書関連～

- 公的個人認証サービスの民間開放
  - 認証用証明書、署名用証明書
  - プラットフォーム事業者
- 総務省 個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会―属性認証検討ＳＷＧ
- 電子証明書に格納された属性情報の信頼性と利用に関するガイドラインv1.10（平成28年3月25日、電子認証局会議）
  - 資格や所属等の証明書記載
  - 組織番号（法人番号含む）など

法人に関する証明書(EUと日本の比較)

	EU	日本
電子署名法	eIDASでは法人による署名(e-Seal)を規定。	自然人に対してのみ規定。
法人に関する証明書の例	法人証明書プロファイルの規定。 （実際の例は？）	・商業登記に基づく証明書 ・民間の認証事業者による法人情報が記載された証明書
法人に関する証明書の発行対象	法人	自然人。法人の代表者や、法人に属する者。
備考	法人証明書の利用や運用の方法は自然人の証明書とは異なると考えられ、詳細については調査が必要。	属性ガイドラインで法人情報が格納された証明書に関する指針を検討している。

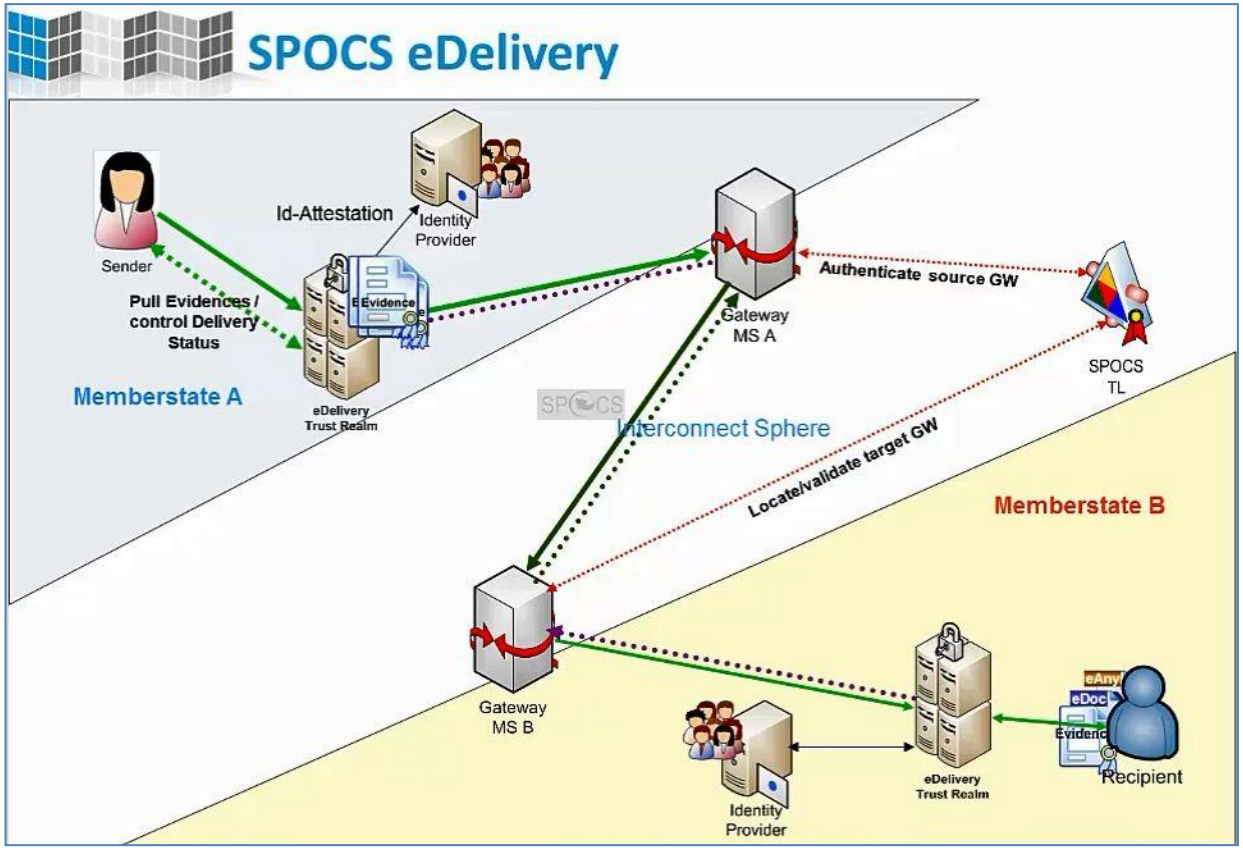
日本でもe-Seal証明書が議論が必要では？
否認防止の用途ではなく、文書の出所の証明や改ざん検知の目的で使える可能性がある（例：電子領収書、企業発行のドキュメント、etc.）

e-delivery/registered e-mail(REM)

電子データ配送サービス/電子メールの配達記録

従来の規格：ETSI TS 102 640 Registered Electronic Mail (REM) [2010年10月]

規格のEN化に向けて新たに活動が開始



www.eu-spocs.eu より

- 電子データの配送記録の作成（電子署名付き）
- インタフェース機能要件
- サーバのセキュリティポリシー要件

など

日本の動向
～e-delivery関連～

日本郵政グループ

PRESS RELEASE

2016 年 1 月 14 日
日本郵便株式会社

デジタルメッセージサービス「MyPost」の提供開始

日本郵便株式会社（東京都千代田区、代表取締役社長　高橋 亨／以下「日本郵便」）は、ICT を高度に活用した便利で効率的な社会の実現に向けた取組の一環として、本日から、デジタルメッセージサービス「MyPost（マイポスト）」の試行的な提供を開始します。

記

1　背景

重要書類をはじめとした大切なメッセージの中には、現在広く利用されている E メールや Web サイトでの配信になじまないものがあるため、社会の ICT 化が進むにつれて、これらの送付にも対応できる新たなデジタルメッセージサービスが求められており、諸外国においては、各国の郵政事業体等がサービスの提供を開始しています。

2　「MyPost」とは

「MyPost」は、大切なメッセージをインターネット上でやり取りするために日本郵便が提供する「インターネット上の郵便受け」です。日本郵便が会員の本人確認や氏名・住所の確認を必要に応じて行うことで、差出人は、会員本人と安心してメッセージをやり取りすることができます。会員は、自分が選択した差出人からのメッセージのみを受け取り、クラウド上で長期保管することができます。これまで郵便サービスが担ってきた大切なメッセージをやり取りできるインフラの役割をデジタル分野において実現することを目指します。

3　試行サービスの概要

試行サービスでは、企業・官公庁などから会員に対し、重要書類をはじめとした様々な電子データ（以下「レター」といいます。）を配信する機能を提供します。この結果を踏まえ、会員から企業・官公庁に対する各種手続機能をはじめ様々な機能を拡充する予定です。

（1）サービスの流れ

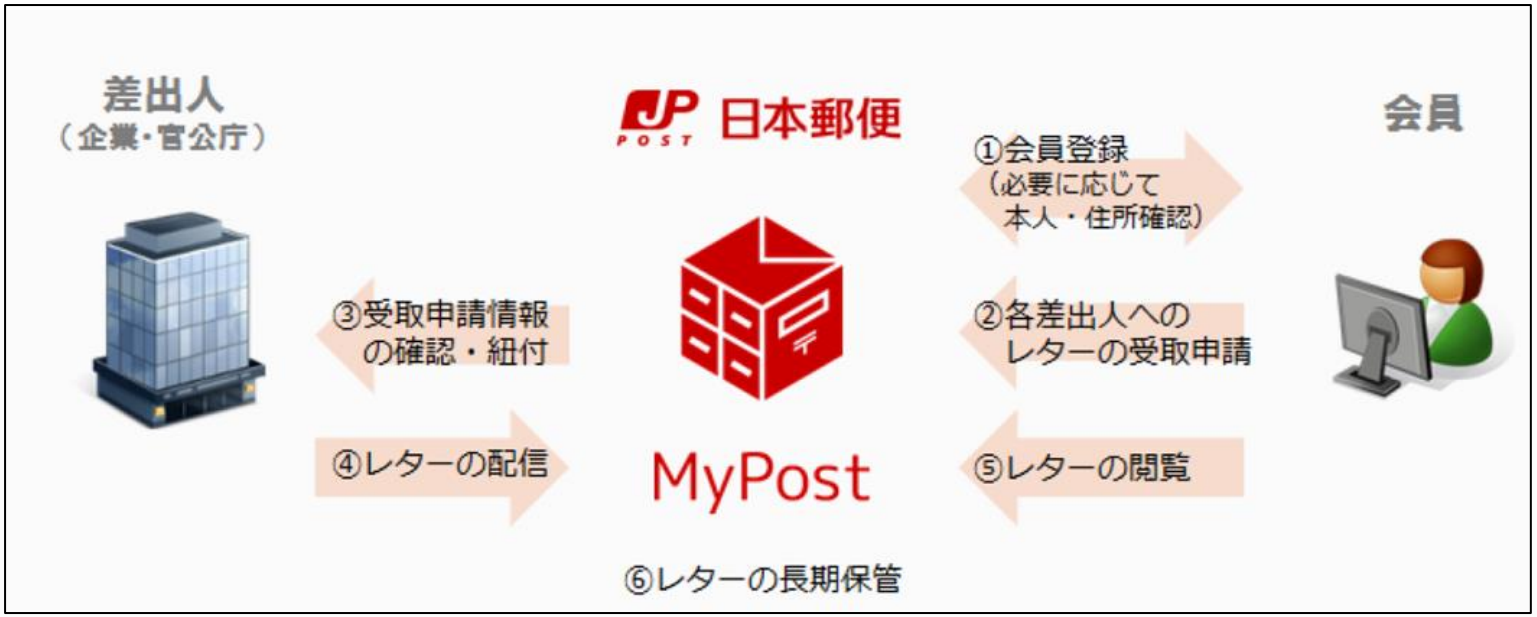
必要に応じて日本郵便による本人確認等を受けた会員が、あらかじめメッセージの配信を希望する差出人を選択することで、差出人からレターの配信を受けることができるようになります。会員は、差出人から配信されたレターを、当社が責任を持って管理する機密性の高いクラウド上で閲覧・保管することができます。これまで電子的な配信に適さなかった重要な電子データも、会員本人に確実にお届けします。

http://www.post.japanpost.jp/notification/pressrelease/2016/00_honsha/0114_01_01.pdf

日本の動向
～e-delivery関連～

セコムIS研究所
Intelligent Systems Laboratory

日本郵政株式会社のMyPostサービス



http://www.post.japanpost.jp/notification/pressrelease/2016/00_honsha/0114_01_01.pdf

現状ではあくまで日本郵政株式会社のサービスか。

このようなサービスについて、（EUのe-deliveryのように）電子データの配送記録やインタフェースの仕様、サーバのセキュリティポリシー要件等を標準化することによって、様々な事業者のファイル保管/メッセージ交換サービスも相互運用できるようになるのでは？

トラストサービス

- 電子取引等の信頼（trust and confidence）を向上させる電子上のサービス
  - 暗号技術を使うとは限らない（が、現在は暗号技術を使ったものがメインのスコープか？）
- 具体的な例
  - 電子署名の生成/検証サービス
  - タイムスタンプ局、タイムスタンプの検証サービス
  - 認証局（電子署名用、タイムスタンプ局用、Webサイト証明用、etc.）
  - e-deliveryサービス
  - 電子署名の保存サービス
  - などなど

(再掲)2016年3月発行済のEN規格

- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
  - 319 411-1 v1.1.1: General requirements
  - 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates
- EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- EN 319 412 Certificate Profiles
  - 319 412-1 v1.1.1: Overview and common data structures
  - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons
  - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons
  - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations

日本の動向
～トラストサービス関連～

- 従来の認証局、タイムスタンプ局に加え、以下の例もトラストサービスに分類されると思われる。
  - 各社の電子署名サービス（リモート署名）
  - 日本郵便のMyPost
  - 公的個人認証のプラットフォーム事業者
  - 独立行政法人 工業所有権情報・研修館（INPIT）のタイムスタンプ保管サービス

  etc.

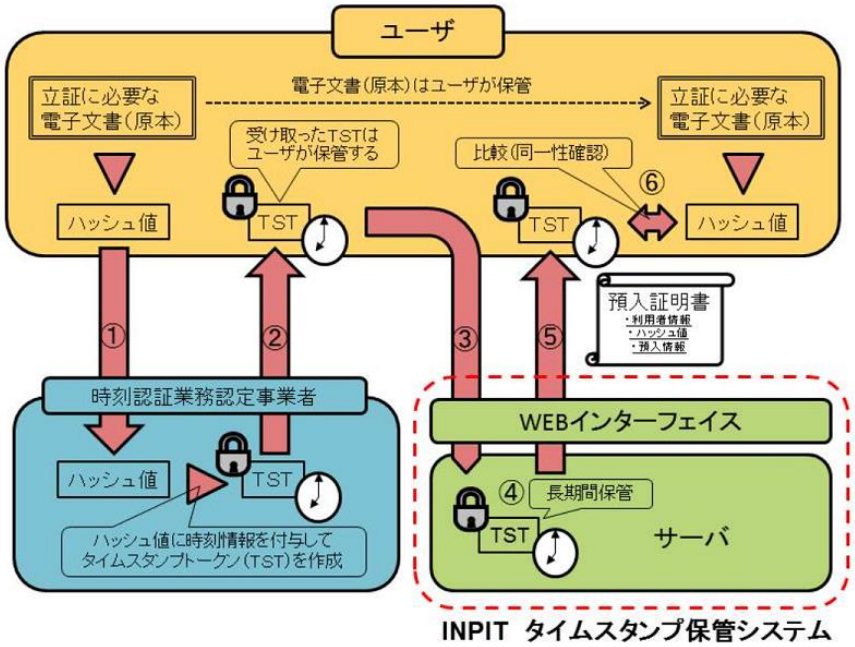
独立行政法人 工業所有権情報・研修館（INPIT）
タイムスタンプ保管サービス

セコム IS研究所
Intelligent Systems Laboratory

2. サービスの概要

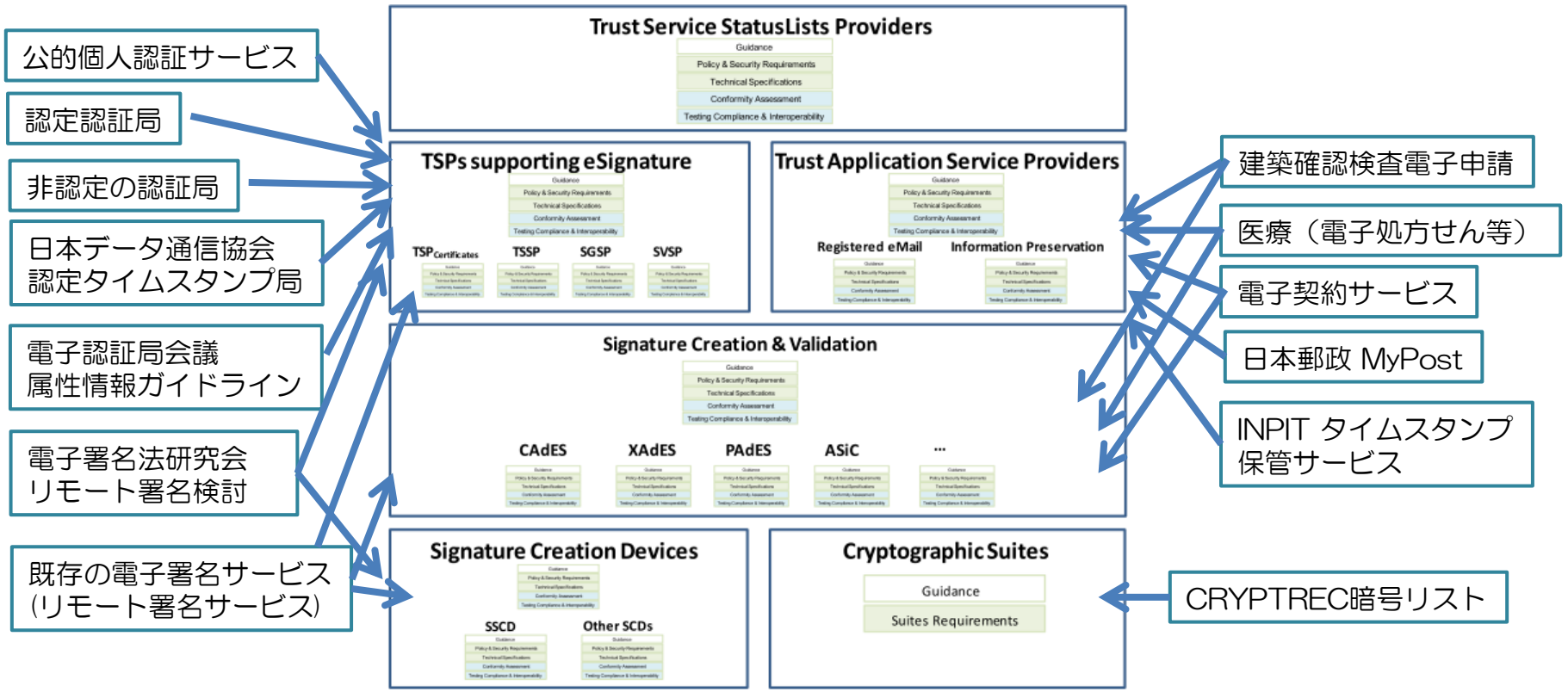
ＩＮＰＩＴは、時刻認証業務認定事業者が発行したタイムスタンプトークンを、ユーザから預かって長期間安全にバックアップとして保管します。そして、ユーザがそのタイムスタンプトークンを必要とした場合には、預入証明書とともにタイムスタンプトークンを提供します。このタイムスタンプ保管サービスを活用して原本証明を行うまでの流れは、以下の図1に示すとおりです。

（図1：タイムスタンプトークン（ＴＳＴ）発行から同一性確認までの流れ）



http://www.inpit.go.jp/katsuyo/tradesecret/ts.html

全体を眺めてみて…



ETSI SR 001 604の図に
講演者が追記

日本のサービスや各種ガイドライン等の動向を見ると
欧州のフレームワークに当てはまるものもありそう？

おわりに

- 欧州だけではなく日本もトラストサービスが既にあり、また、今後も新しいトラストサービスが登場するだろう。
- 日本においても、トラストサービス毎に閉じたスコープで個別に議論するのではなく、整合性のとれた共通の土台を構築できるように議論すべきでは？
  - トラストサービスを連携するためには必須。
- 日本においても、俯瞰的に中長期的な視点で検討していく必要があるのでは？
- 欧州はこれまで時間と予算をかけて実証実験と標準化を行ってきた。それらの成果をeIDASのもとに結実させようとしている。これらの知見をうまく参考にしつつ、日本に適した基盤を検討したほうがよいのでは？