リモート署名の検討状況

2019.02.15

日本トラストテクノロジー協議会（JT2A）
みずほ情報総研株式会社
小川　博久

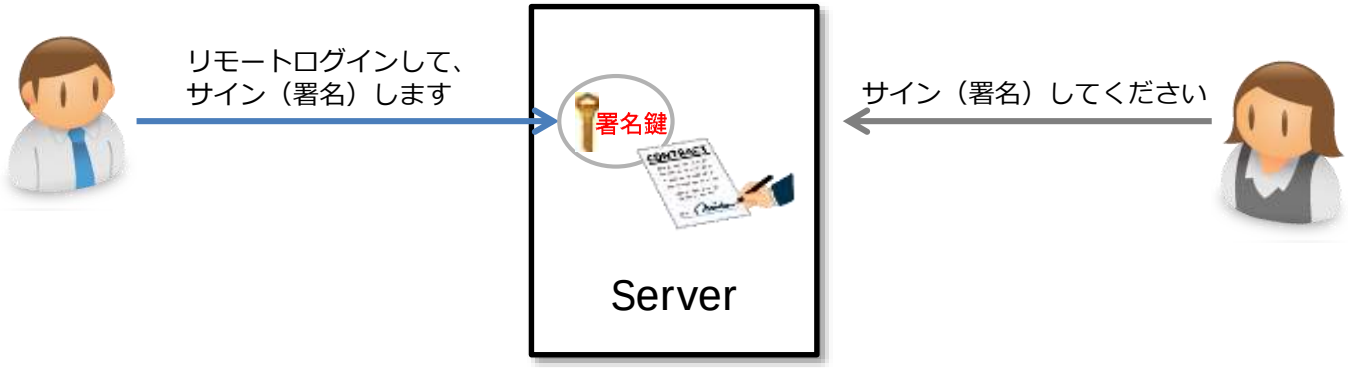
説明内容

1. JT2A国内の検討状況
2. EU（eIDAS）の検討
3. まとめ

リモート署名とはなにか？

リモート署名の定義※

事業者のサーバに利用者（エンドエンティティ）の署名鍵を設置・保管し、利用者がサーバにリモートでログインし、自らの署名鍵で事業者のサーバ上で電子署名を行うこと。



電子署名及び認証業務に関する法律（平成１２年法律第１０２号）第二章　電磁的記録の真正な成立の推定、第三条

電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

※電子署名法研究会（METI/経済産業省）
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou

なぜリモート署名が重要なのか

JT2A

平成27年度 調査報告書のまとめから抜粋

- リモート署名は、すでに欧州や米国において広く利用されているサービスであり、電子証明書及び電子署名の利用を拡大するものである。
- また、我が国においても 2016 年からマイナンバーカードの利活用が進み、2017 年にはマイナポータルにおいて官民が連携し、各種の申請や手続きが電子化されることで国民にとっても電子証明書及び電子署名がより身近に利用できる環境が整う。
- さらに、昨今の電子契約については、利便性が高く、安全なサービスが求められるため、本事業で検討したリモート署名は、この電子契約の促進に資するものであり、より安全な社会経済の更なる発展に向けて大きく貢献する。

平成28年度 第一回電子署名法研究会の議事要旨から抜粋

- クラウド時代の電子署名のあり方が重要であると考えている。仮にリモート署名が実現できないとすると、クラウドサービス上では自然人の意思の推定効を担保する仕組みが出来ないことになってしまう。

電子署名法研究会（METI/経済産業省）
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou
電子署名法研究会（平成28年度第1回） - 議事要旨（METI/経済産業省）
http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h28_01_giji.html

リモート署名TFの概要①

JT2A

1. 活動内容

- リモート署名の重要な論点をまとめ
- ガイドラインとして記載すべき全体構成を議論
- 例えば、このような内容
  - ✓ EUの法制度・要件等との関連性は？
  - ✓ 本当に安全なのか？セキュリティは大丈夫なのか？

2. コアメンバ

- 村尾進一（セイコーソリューションズ株式会社/TFリーダー）
- 佐藤雅史（セコム株式会社 IS研究所）
- 濱口総志（株式会社コスモス・コーポレイション）
- 宮崎 一哉（三菱電機株式会社）

3. 予定成果物

- リモート署名ガイドライン

リモート署名TFの概要②

■ 本年度は、経済産業省からの委託事業を実施

- 事業名
  - ✓ 平成３０年度経済産業省デジタルプラットフォーム構築事業
    （継続的・効果的な法人共通認証基盤の在り方に関する調査研究）

- 事業概要
  - ✓ 我が国として継続的・効果的に法人認証基盤を運用していくため、取り入れるべき技術要素を含め法人認証基盤の将来像について検討し、その実現に向けたロードマップの策定等を行う。

- 調査検討担当
  - ✓ リモート署名の活用に関する調査・検討
    電子署名方式の導入・利活用に関連し、電子署名方式としてリモート署名を活用することにより、電子証明書、電子署名の利用拡大が想定されるとともに、リモート署名は、クラウドベースで構築する法人認証基盤とも親和すると考えられることから、リモート署名の活用に関し、アーキテクチャや法的論点を含め調査・検討を行う。

日本の本格的な検討はH27年～

電子署名及び認証業務に関する法律（平成１２年法律第１０２号）第二章
電磁的記録の真正な成立の推定、第三条

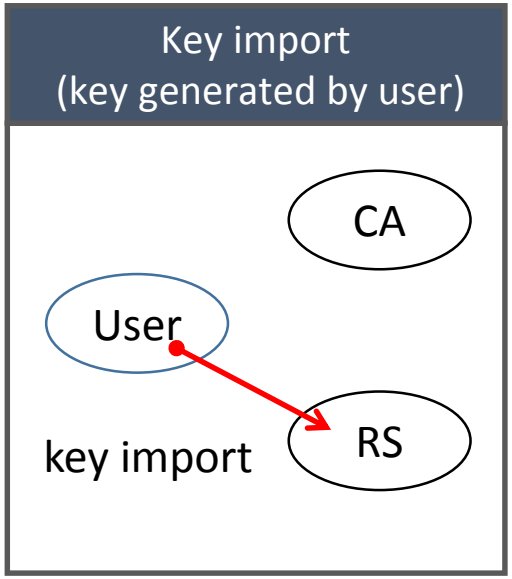
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

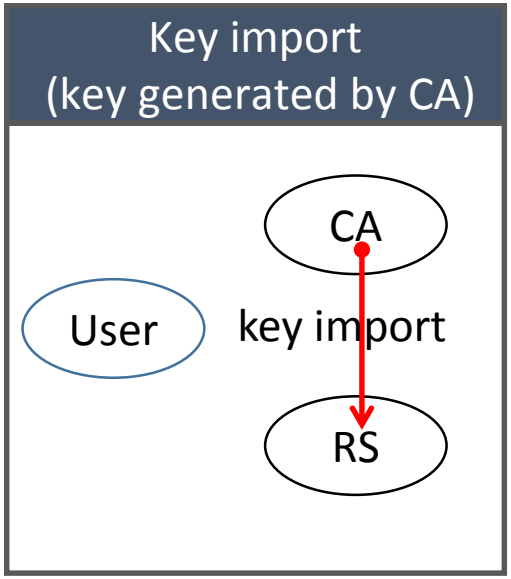
例えば…　（これですべでではありませんが）

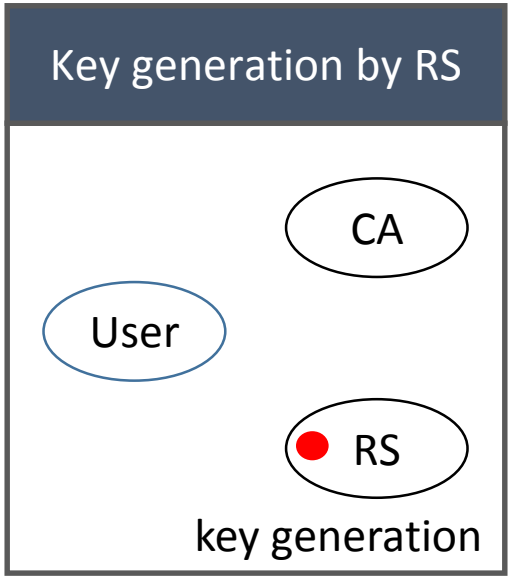
- 利用者（署名者）登録における本人性を確認する
  - 利用者本人でない登録や登録情報の詐称などを防止
- 利用者（署名者）が意図した署名対象データに対して署名
  - 利用者が署名対象データを確認
  - 利用者による署名結果の確認（検証）
- 署名者しか署名できない
  - 署名鍵が利用者本人のコントロール下にあること（管理者でも勝手に使えないこと）

日本の検討1：いろいろなプレイヤが署名鍵を生成する

日本国内で検討した署名鍵生成とインポートのパターン

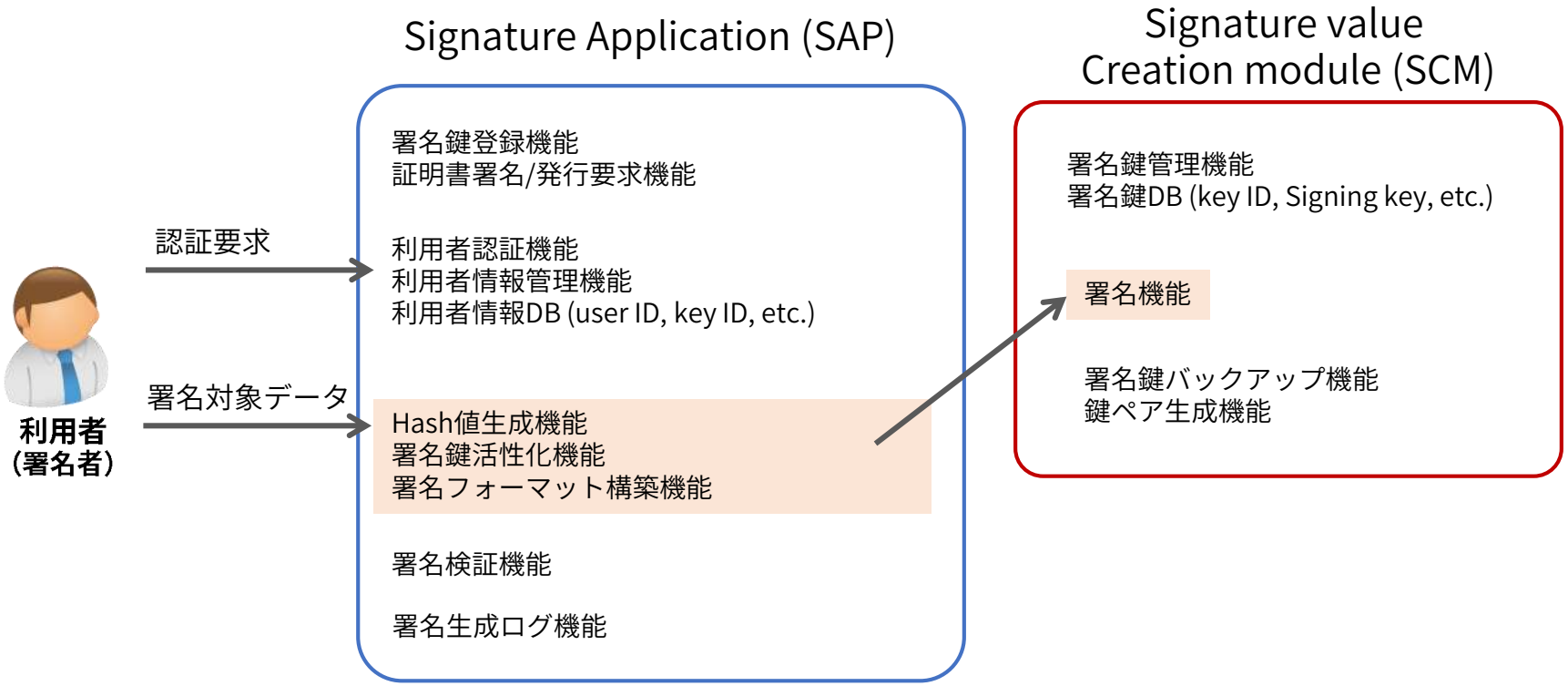






日本の検討2：基本構成（署名フェーズの動作）

先行している欧州の技術要件との整合性が重要



説明内容

1. JT2A国内の検討状況

2. EU（eIDAS）の検討

3. まとめ

電子署名の定義（EU）

Ⅰ.電子署名

➔ 電子形式の署名

Ⅱ.先進電子署名

➔ PKIベースの電子署名（デジタル署名）で基準（ETSI規格）を満たすもの

Ⅲ.適格電子署名

➔ 適格電子証明書とICカードのような安全な装置を用いた先進電子署名

詳細な規定内容

- 「電子署名」とは、電子データに添付されている又は論理的に関係している電子形式のデータであり、署名者が署名する為に使用するものをいう
- 「先進電子署名」とは、第26条で規定される要求事項に適合する電子署名をいう
- 「適格電子署名」とは、適格電子署名生成装置を利用して生成され、電子署名の為の適格証明書に順ずる先進電子署名をいう

＊先進電子署名（26条）

- 署名者に一意的にリンクしている；
- 署名者を識別することができる；
- 署名者が、本人単独の管理のもとに、高いレベルの信頼を持って使用することができる電子署名生成データを使って作成されている；
- その後のデータへの変更を検知できる方法で署名されたデータにリンクされている。

➡ PKIベースの電子署名

濱口総志メンバーの資料抜粋

eIDAS規則における適格電子署名

適格電子署名

＝①適格電子証明書＋②適格署名生成装置＋③先進電子署名

①適格電子証明書　→　本人性を確保

②適格電子署名生成装置　→　秘密鍵と署名生成環境の安全性を確保

③先進電子署名　→　電子署名と署名者の結びつきを確保

＊適格電子署名生成装置＝コモンクライテリア認証を取得したデバイス
（基本的にはスマートカードやHSM)

濱口総志メンバーの資料抜粋

eIDAS規則における電子署名の法的効力

1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

   ➔ 電子形式であること、或いは適格電子署名でないことを理由に電子署名の法的効力は否定されてならない

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

   ➔ 適格電子署名は手書き署名と同等の法的効力

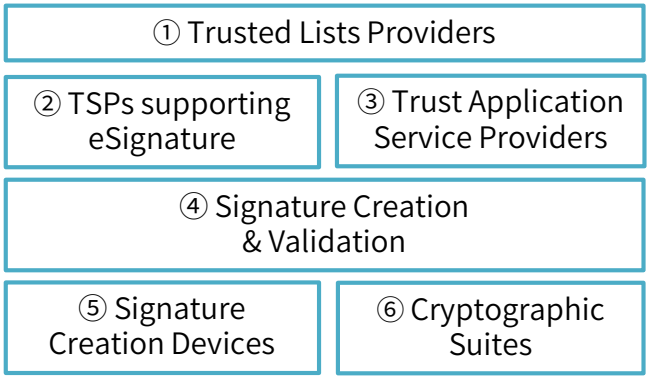
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States

   ➔ **適格電子署名はEU加盟国全体で認められる**

濱口総志メンバーの資料抜粋

欧州（eIDAS）の検討

欧州では、安全なリモート署名についてPPや評価制度も含めて古くから検討されている。eIDAS / eSignature Standards Framework



※①～⑤のフレームワークを定義して、多くの規定を検討。
これは、2015年のデータなので、現時点ではさらに詳細化されている。

① TS 119 612 v1.2.1 Trusted Lists
② EN 319 403 / TS 119 403 TSP Conformity Assessment
EN 319 401 / TS 119 401 General Policy Requirements for TSPs
EN 319 411 / TS 119 411 Policy Requirements for TSPs issuing Certificates
EN 319 412 / TS 119 412 : Certificate Profiles
EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
EN 319 422 Time-stamping protocol and electronic timestamp profiles
③ TS 102 640 Registered e-Mail
E_Delivery
Long term preservation
④TS 119 102-1 / EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures. Part 1: Creation and Validation.
TS 119 122 / EN 319 122: CAdES digital signatures.
TS 119 132 / EN 319 132: XAdES digital signatures.
TS 119 142 / EN 319 142: PAdES digital signatures.
TS 119 162 / EN 319 162: Associated Signatures Containers.
TS 119 172 / EN 319 172-1: Signature policies
⑤ EN 419 211-1 to -5: Protection profiles for secure signature creation device
EN 419 221-1 to -5: Protection profiles for TSP Cryptographic modules
TS 419 241 - Security Requirements for Trustworthy Systems Supporting Server Signing
EN 419 241-2 & 3 Protection profiles for Server Signing
EN 419 231 - Protection profile for trustworthy systems supporting time stamping
EN 419 261 Security requirements for trustworthy systems managing certificates and time-stamps
⑥ ETSI TS 119 312: Cryptographic Suites

Overview CEN/ETSI eSignature Standardization including standards for TSP Compliance
https://www.tuvit.de/cps/rde/xbcr/SID-AE27C844-D865FD46/tuevit_en/ca-day-2015-nick-pope.pdf

欧州（eIDAS）の検討

欧州では、安全なリモート署名についてPPや評価制度も含めて古くから検討されている。eIDAS / eSignature Standards Framework

電子署名生成環境の管理をトラストサービスプロバイダが署名者の代わりに行うリモート電子署名の生成は、複数の経済的利益に鑑みて増加するものである。
ただし、これらの電子署名が、完全にユーザが管理する環境で生成された電子署名と同等の法的承認を受ける為には、

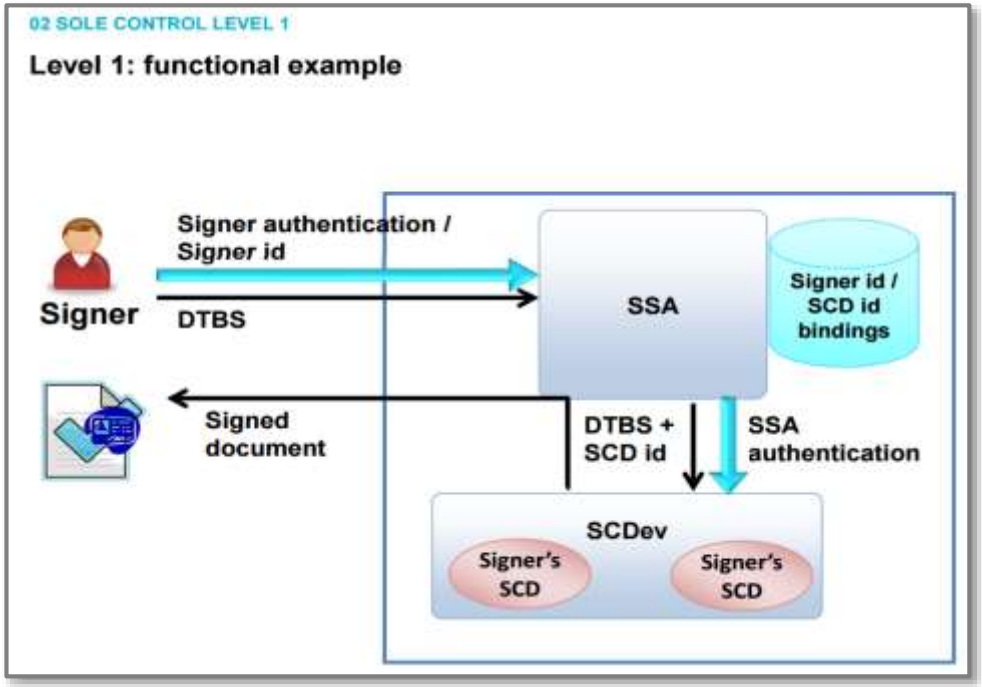
①リモート電子署名サービスプロバイダは特定の管理・運営セキュリティ手順を適用し、電子署名生成環境が信頼できるものであり、
②署名者の単独の管理（*Sole Control*）のもとで使用されることを保証する為に、セキュアな電子通信チャンネルを含む信頼できるシステムや製品を使用すべきである。

適格電子署名がリモート電子署名生成装置を使って作成される場合は、本規則で定める適格トラストサービスプロバイダに対して適用される要求事項を適用すべきである。

※多ここで

Overview CEN/ETSI eSignature Standardization including standards for TSP Compliance
https://www.tuvit.de/cps/rde/xbcr/SID-AE27C844-D865FD46/tuevit_en/ca-day-2015-nick-pope.pdf

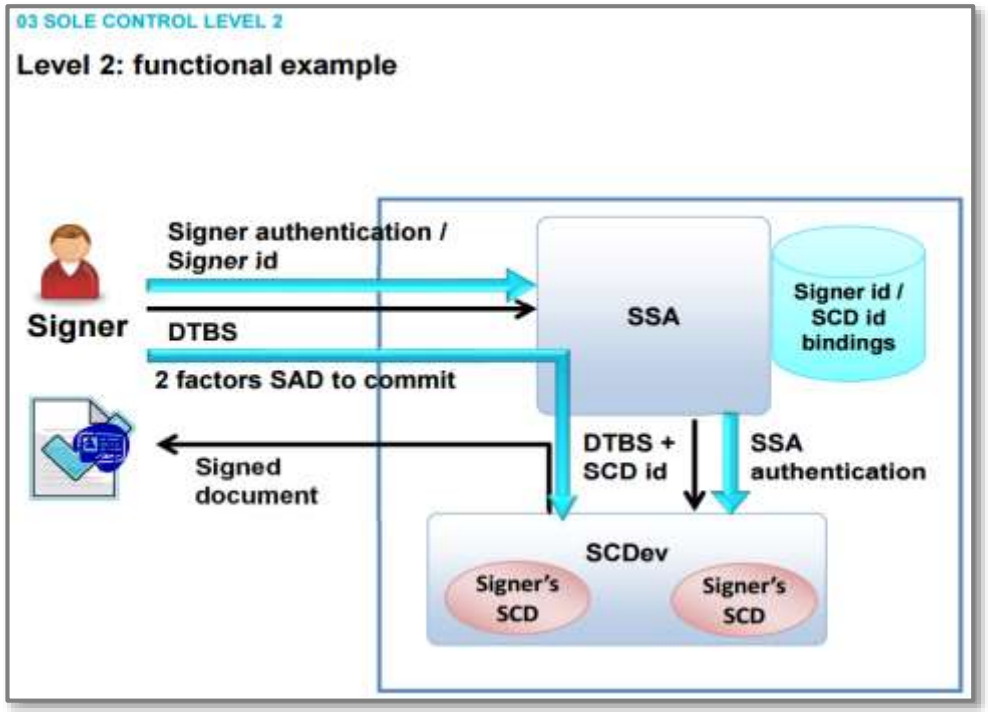
Sole Control Level 1の機能構成例1



- 署名者（Signer）は、署名アプリケーション（SSA）に対して、自らの識別子である署名者ID（Signer id）と署名対象データ（DTBS）を送るとともに、認証要求を行う。
- SSAは、署名者を認証し、署名者が正しく認証された場合、その認証結果とともに、署名者IDに関連付いた署名デバイスID（SCD id）と署名対象データを署名デバイス（SCDev）に送る。
- SCDevでは、署名デバイスIDで指定された署名鍵を用いて署名し、署名付き署名対象データを出力する。
- なお、この機能構成例1では、署名鍵を活性化するSADは言及していない。

SSA：Server Signing Application、署名者：Signer、DTBS：Data to be Signed、SAD：Signer‘s Activation Data、SCDev：Signature Creation Device

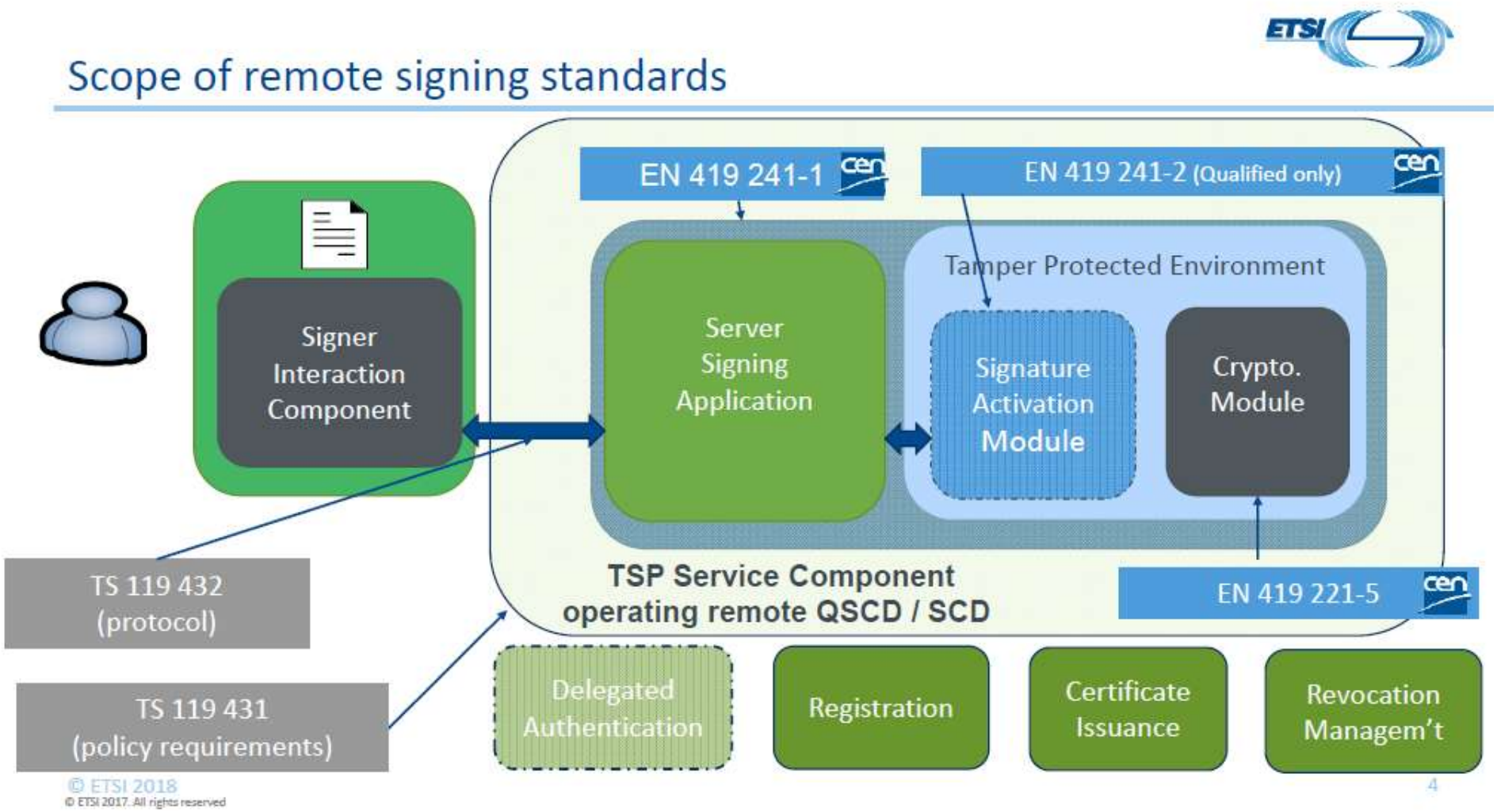
Sole Control Level 2の機能構成例2



- 機能構成例1との違いは、2要素認証を行っている点。
  （二要素認証は、Sole Control Level 2の要求事項）
- 二要素認証として署名鍵を活性化するSADは、セキュアチャネル（セキュリティを実装した通信）によって送信されるため、SADは署名アプリケーション（SSA）には分からない状態で署名デバイス（SCDev）に送る。

SSA：Server Signing Application、署名者：Signer、DTBS：Data to be Signed、SAD：Signer‘s Activation Data、SCDev：Signature Creation Device

EUのリモート署名の構成

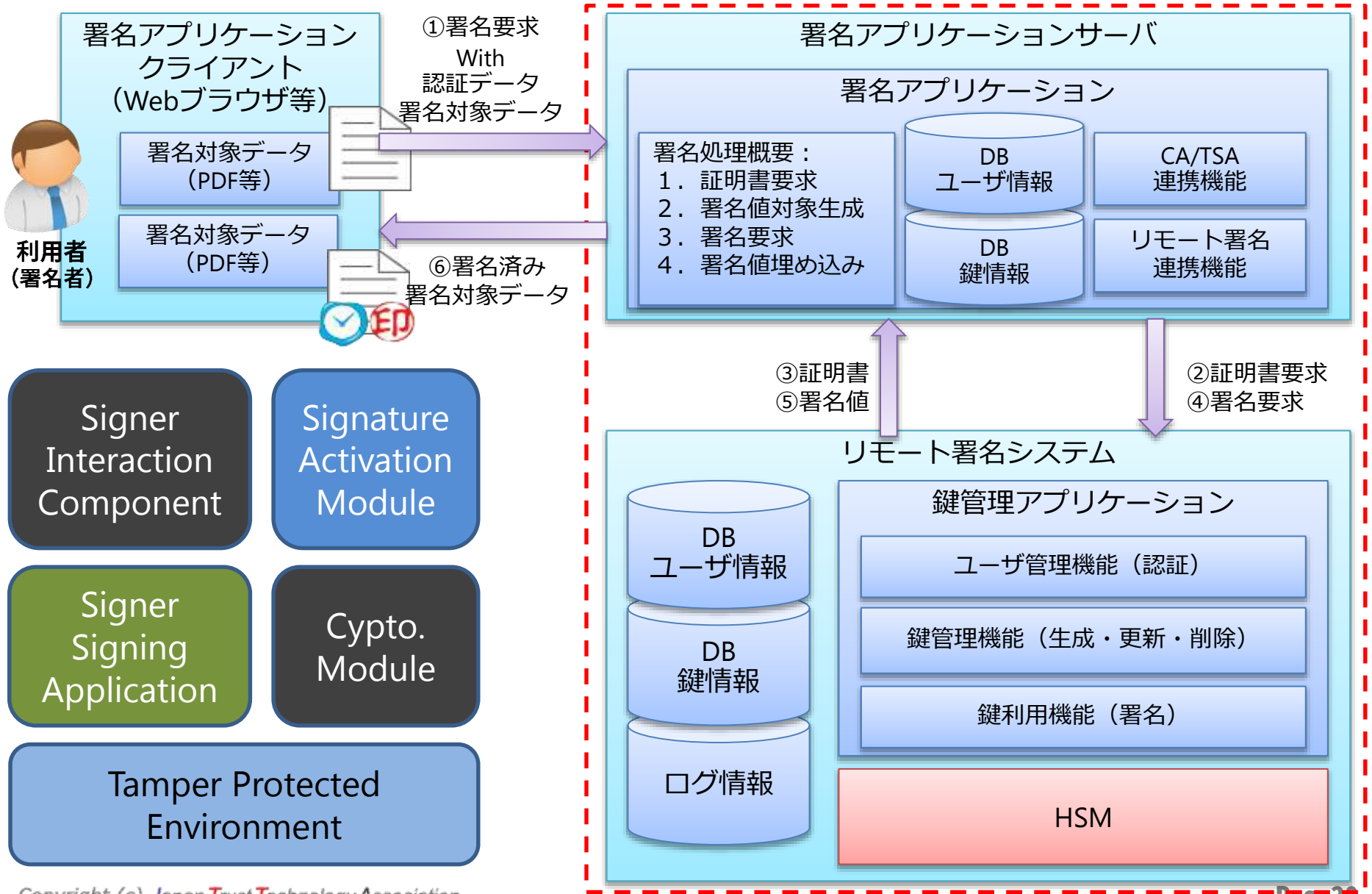


https://docbox.etsi.org/workshop/2018/201806_ETSISECURITYWEEK/REMOTE_SIGNATURE_CREATION/ETSI%20_TC_ESI_POPE.pdf

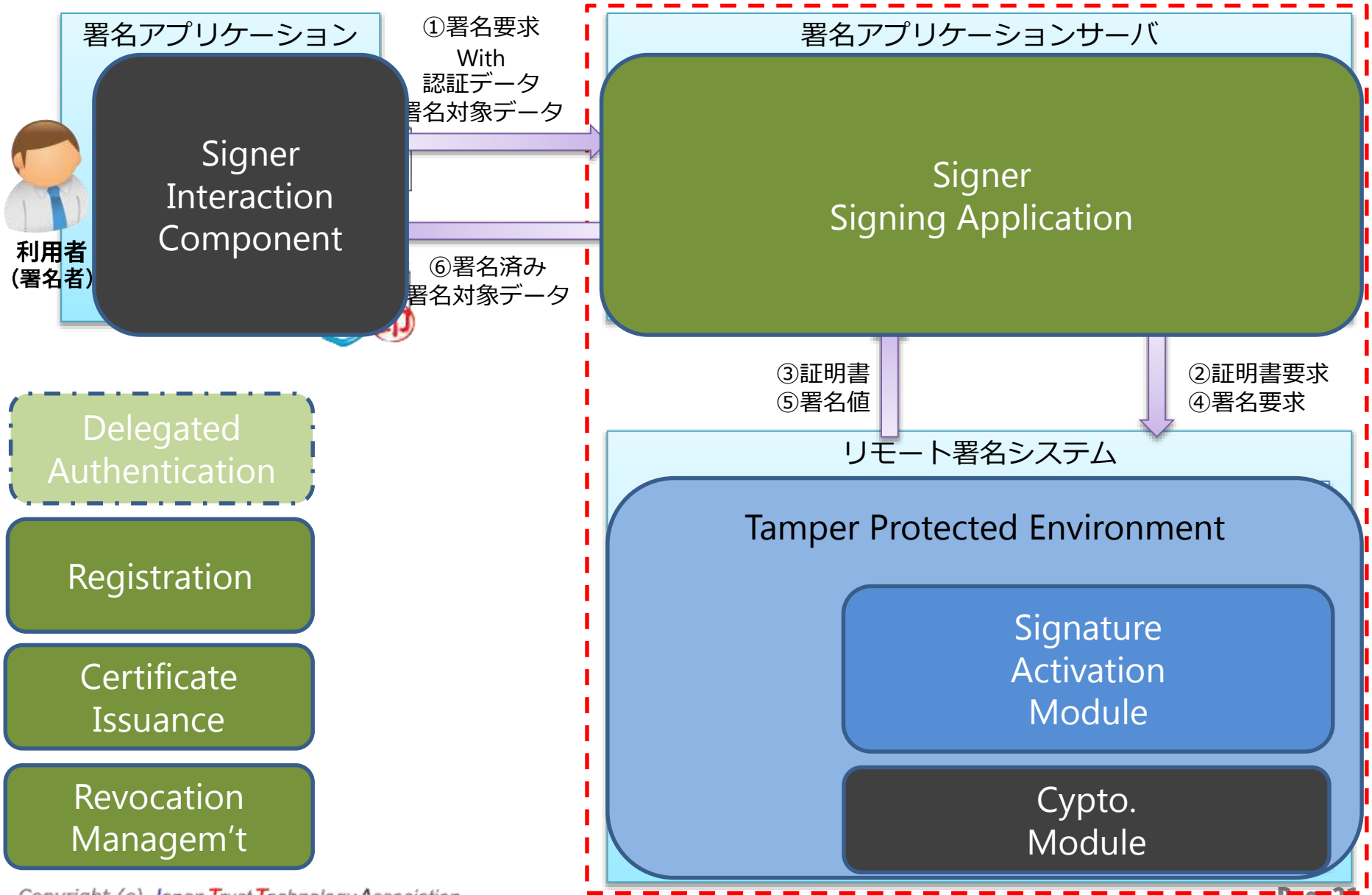
EUのリモート署名に関わる主な規格

仕様名	タイトル	備考
EN 419 241-1	Security Requirements for Trustworthy Systems Supporting Server Signing	サーバ署名に関わるセキュリティ要件
EN 419 241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing	サーバ署名における適格署名生成デバイスのPP
EN 419 221-5	Protection profiles for Trust Service Providers (TSP) Cryptographic modules - Part 5: Cryptographic Module for Trust Services	トラストサービスに対する暗号モジュール（リモート署名を含む）のPP
TS 119 431-1	Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev	リモート署名事業者のあるべきポリシーおよびセキュリティ要件：QSCD/SCD運用
TS 119 431-2	Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation	リモート署名事業者のあるべきポリシーおよびセキュリティ要件：AdES生成
TS 119 432	Protocols for remote digital signature creation	リモート署名のプロトコル（CSCなど）

日本版のシステム構成（案）



日本版のシステム構成（案）

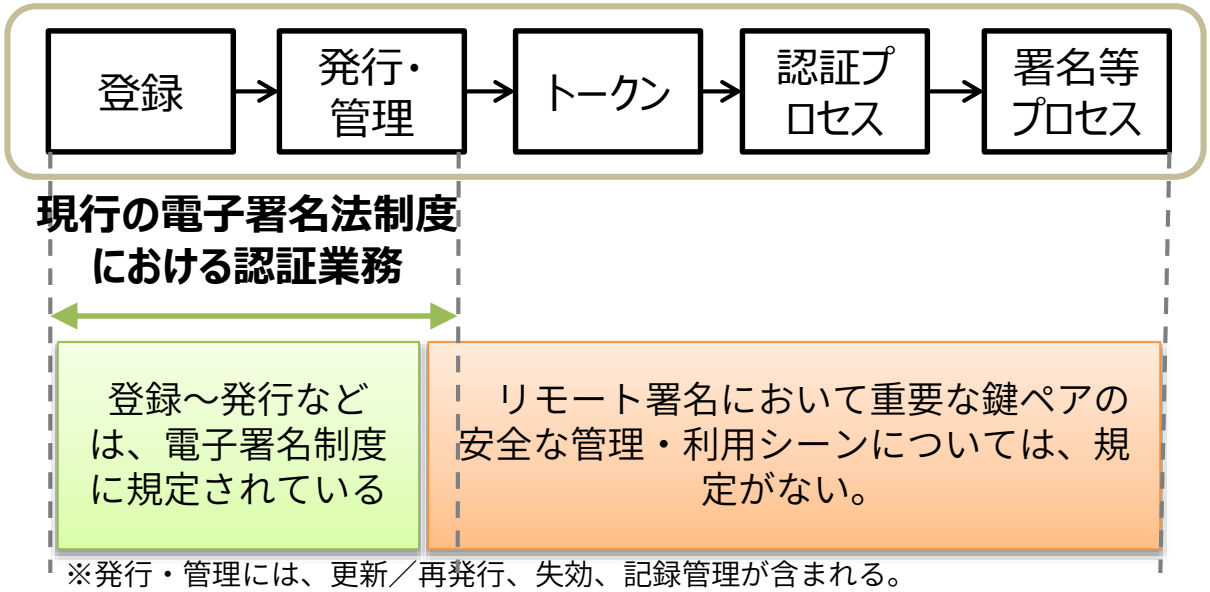


説明内容

1. JT2A国内の検討状況
2. EU（eIDAS）の検討
3. まとめ

まとめ

リモート署名の利用者登録から署名生成までのプロセスで
電子署名法に関係している部分は、ごく僅かである。



※発行・管理には、更新／再発行、失効、記録管理が含まれる。

EUと比較して、
- 法律、施行規則には、デバイス要件はない
- 第三者委託についても書いてない
- 署名レベルの定義が無い
  （Qualified Electronic Signature：適格電子署名）

リモート署名のプロセスは、電子署名・認証ガイドラインを参考に検討。
※電子署名・認証ガイドライン：各府省情報化統括責任者（CIO）連絡会議決定，オンライン手続におけるリスク評価及び電子署名・認証ガイドライン