JT2A 日本トラストテクノロジー協議会
Japan Trust Technology Association

第7回サイバーセキュリティ国際シンポジウム
～JT2A リモート署名TFの活動～

2018.11.27

日本ネットワークセキュリティ協会（JNSA）
日本トラストテクノロジー協議会（JT2A）
セイコーソリューションズ株式会社
村尾 進一

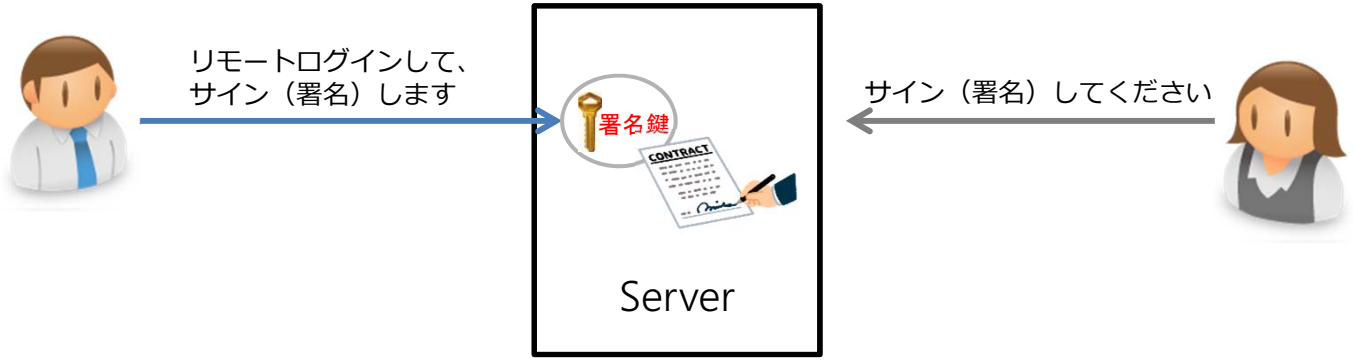
（代打　㈲ラング・エッジ　宮地 直人）

Copyright (c) Japan Trust Technology Association

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

Copyright (c) Japan Trust Technology Association

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

Copyright (c) Japan Trust Technology Association

リモート署名TFの概要①

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（他にエディタやレビュアー多数）

- 村尾進一 リーダー（セイコーソリューションズ株式会社）
- 佐藤雅史 サブリーダー（セコム株式会社 IS研究所）
- 濱口総志 サブリーダー（株式会社コスモス・コーポレイション）
- 宮崎一哉 サブリーダー（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

Copyright (c) Japan Trust Technology Association

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

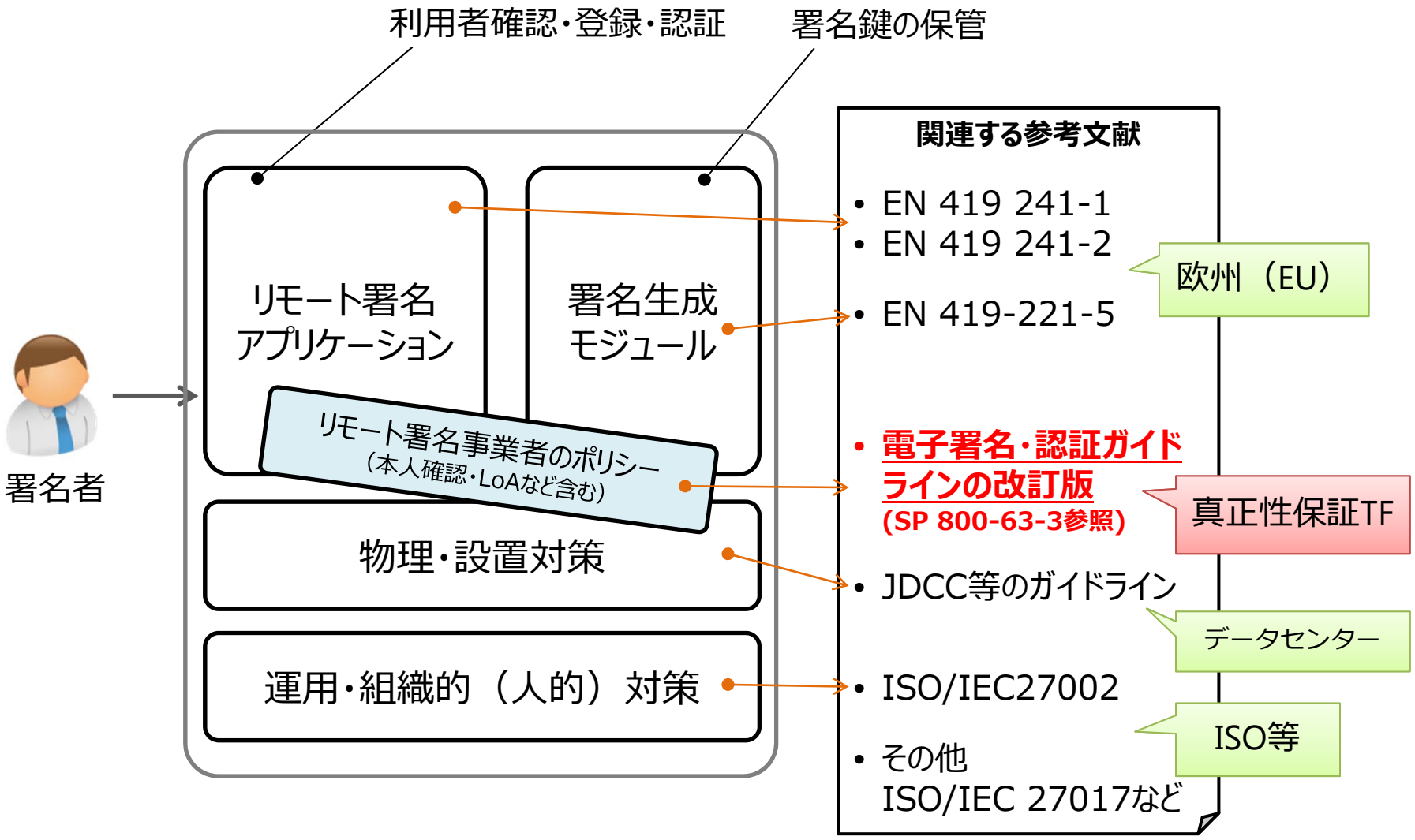
- 事業名
  - ✓ 平成３０年度経済産業省デジタルプラットフォーム構築事業
    （継続的・効果的な法人共通認証基盤の在り方に関する調査研究）

- 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。

Copyright (c) Japan Trust Technology Association

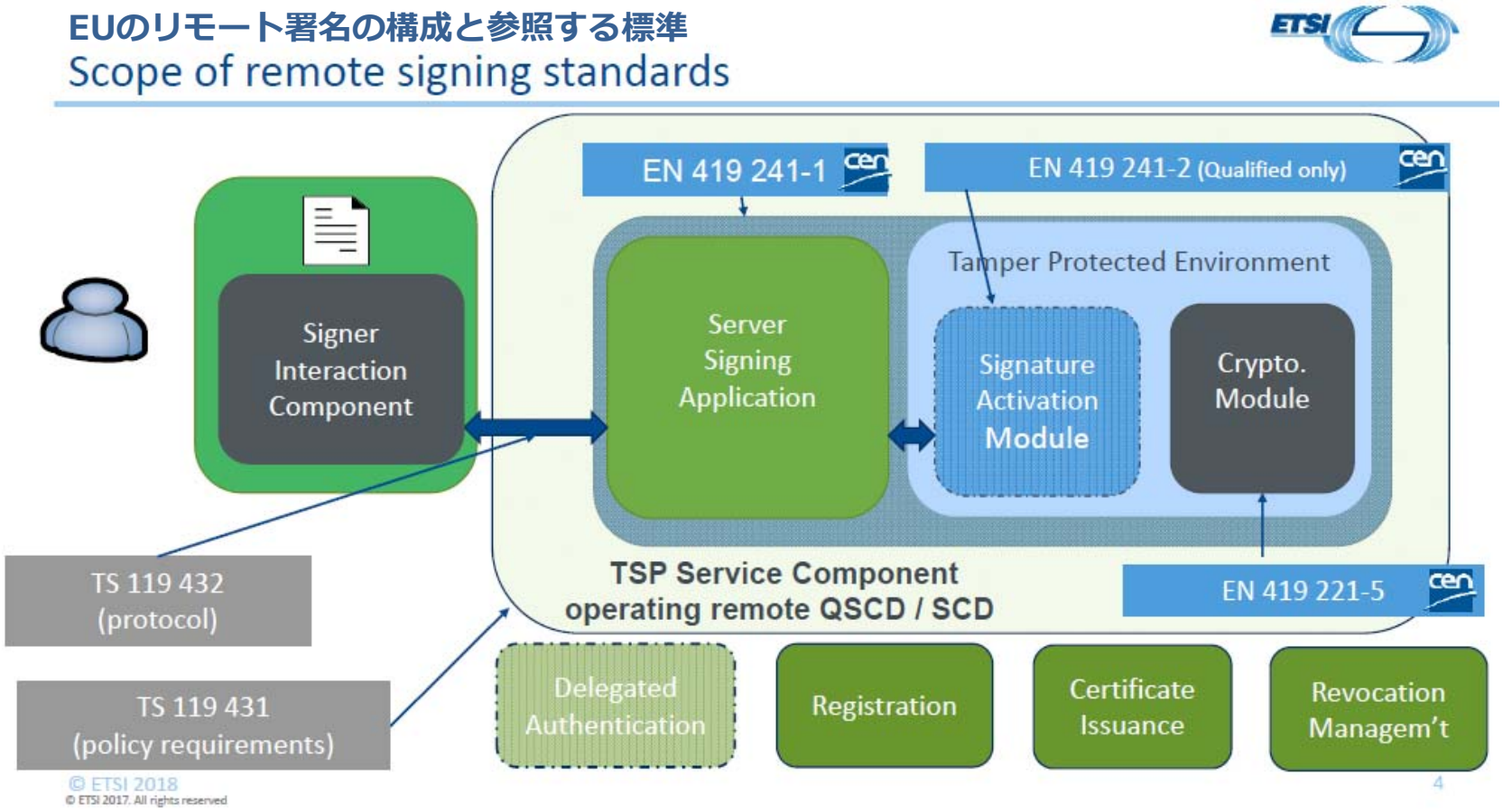
リモート署名TFの議論内容



Copyright (c) Japan Trust Technology Association

EU（欧州）のリモート署名の状況

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 / ETSI & CEN & CSC



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

Copyright (c) Japan Trust Technology Association

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）

Copyright (c) Japan Trust Technology Association

CSC: クラウド署名コンソーシアム

JT2A

Cloud Signature Consortium とは

2016年初め、ソリューション、テクノロジー、トラストサービスプロバイダを含む業界や学術界の専門家から成る国際的な協力グループによって設立された団体で、以下を目的として活動。ETSI/CENとも連携。

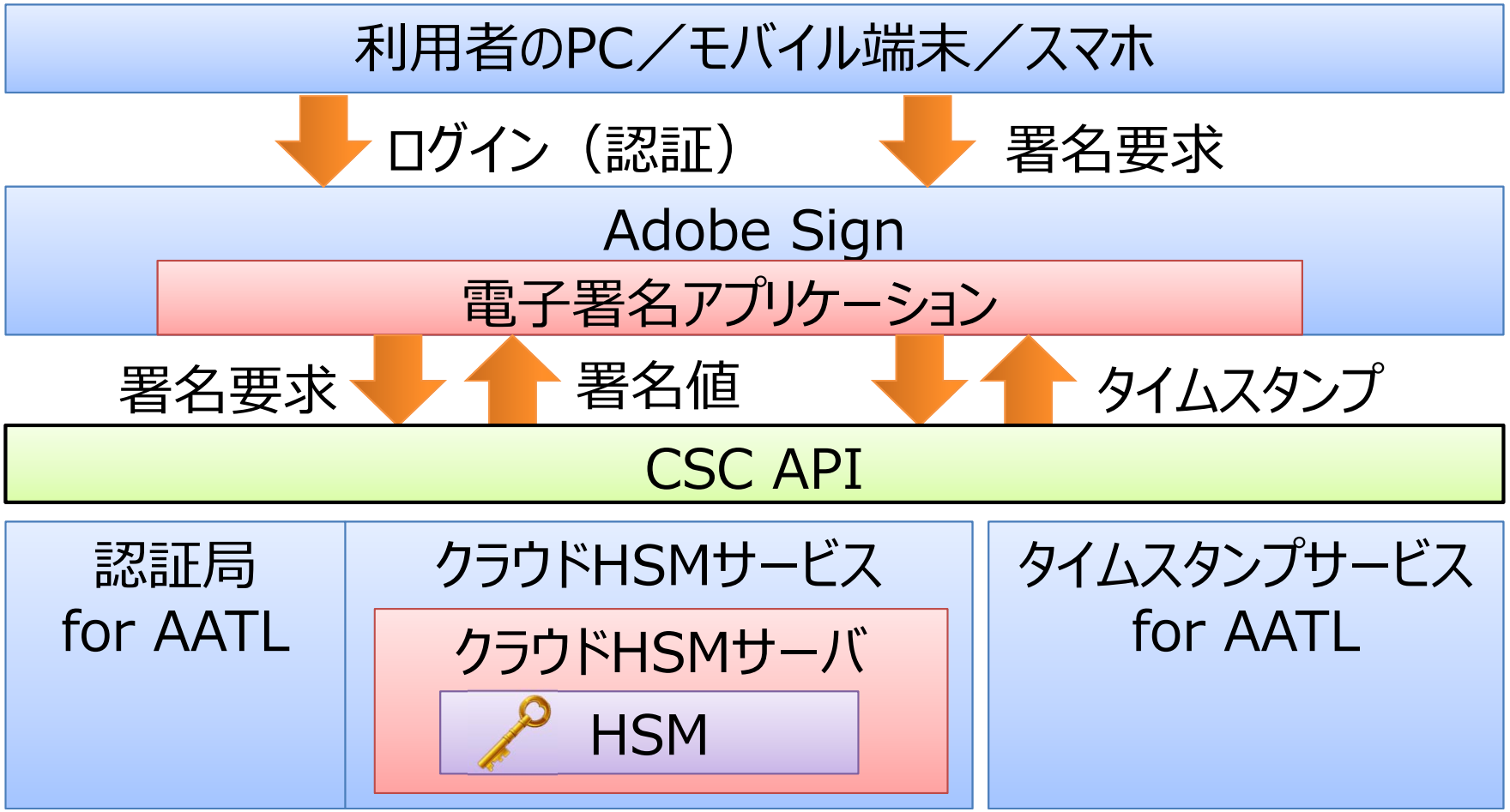
・共通のアーキテクチャ設計と構成要素構築によって、ソリューション、テクノロジー、トラストサービスプロバイダ間の相互運用性を実現
・サービス間の連携を相互運用可能にするべくプロトコルとAPIの技術仕様開発
・オープンスタンダードとしてAPI仕様を公開
・クラウド署名のコンセプトを促進

出典：https://itc.jipdec.or.jp/event/20170704.html （Cloud signature consortiumの概要）

Copyright (c) Japan Trust Technology Association

クラウド署名の例（Adobe Sign）

Adobe Sign と CSC API の連携イメージ



AATL：Adobe Approved Trust List

Copyright (c) Japan Trust Technology Association

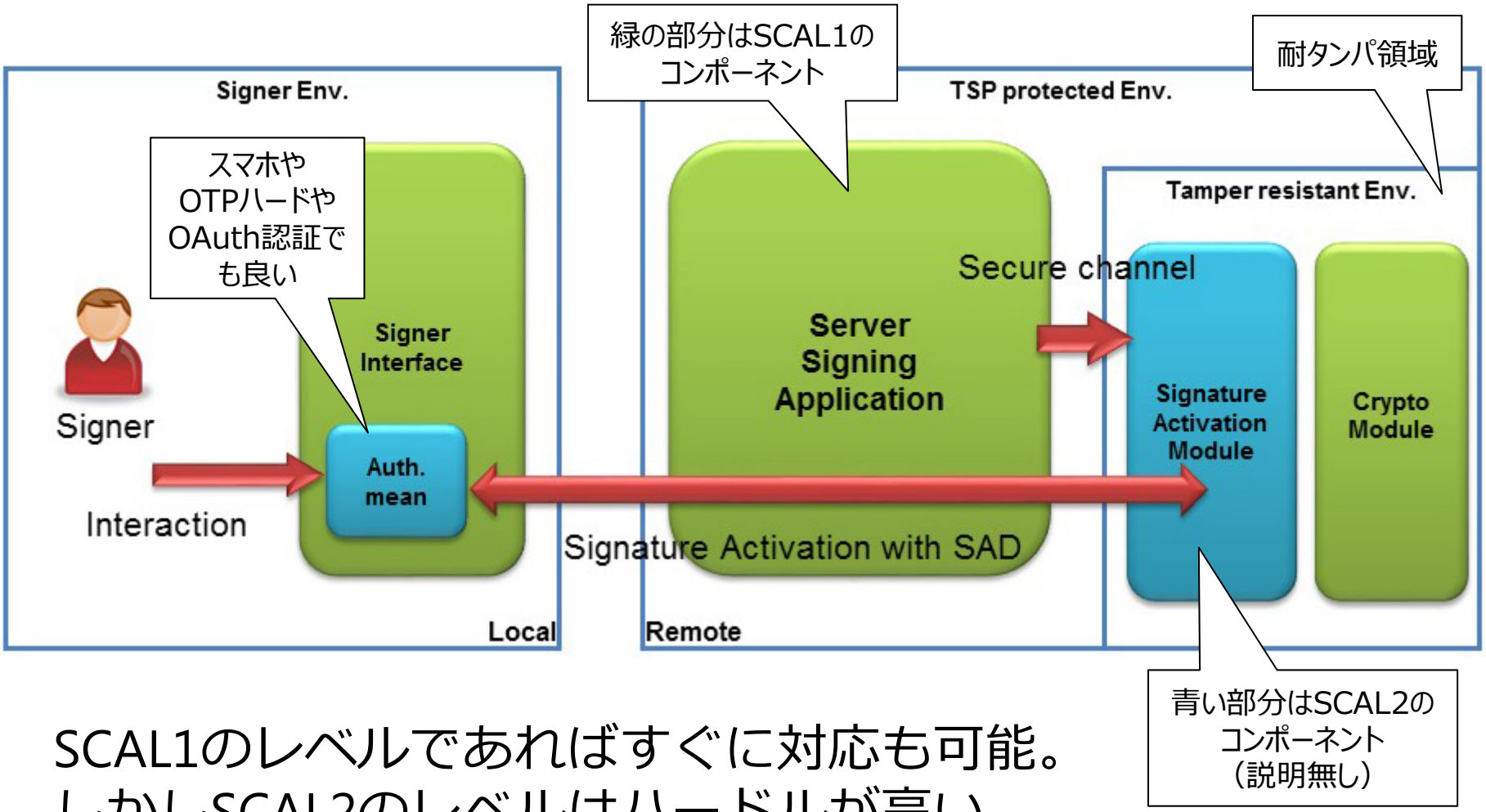
CEN: Sole control assurance level

※ **CEN 419 241-1の定義**（CEN仕様書は有償）

- **Sole control assurance level 1 (SCAL1):**
  Non Qualified Level（１国内の電子取引に有効なレベル）
  - ✓ 基本的な（署名アプリ側の間接的な）認証があれば、SADとSAMは使わなくても良い（SADとはSAM発行のトークンであり、使っても良い）
    ※ SAD: Signature Activation **Data** / SAM: Signature Activation **Module**
  - ✓ ハードウェアを使わずソフトウェアで実現しても良い
- **Sole control assurance level 2 (SCAL2):**
  Qualified Level（国を跨った電子取引でも有効なレベル）
  - ✓ SAM発行のSADと、SAM管理の2要素認証メカニズムが必要
  - ✓ 耐タンパ領域にSAMと鍵管理（HSM）を持つハードウェアで実現
    ※ CEN/FIPS等の標準化されたセキュリティ基準への準拠が必要
  - ✓ eIDAS規制のスタンドアロンQSCDと同じレベルを要求。
    ※ QSCD（**Qualified** electronic Signature Creation Device）

Copyright (c) Japan Trust Technology Association

Sole control assurance level 構成例



SCAL1のレベルであればすぐに対応も可能。
しかしSCAL2のレベルはハードルが高い。

Copyright (c) Japan Trust Technology Association

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。

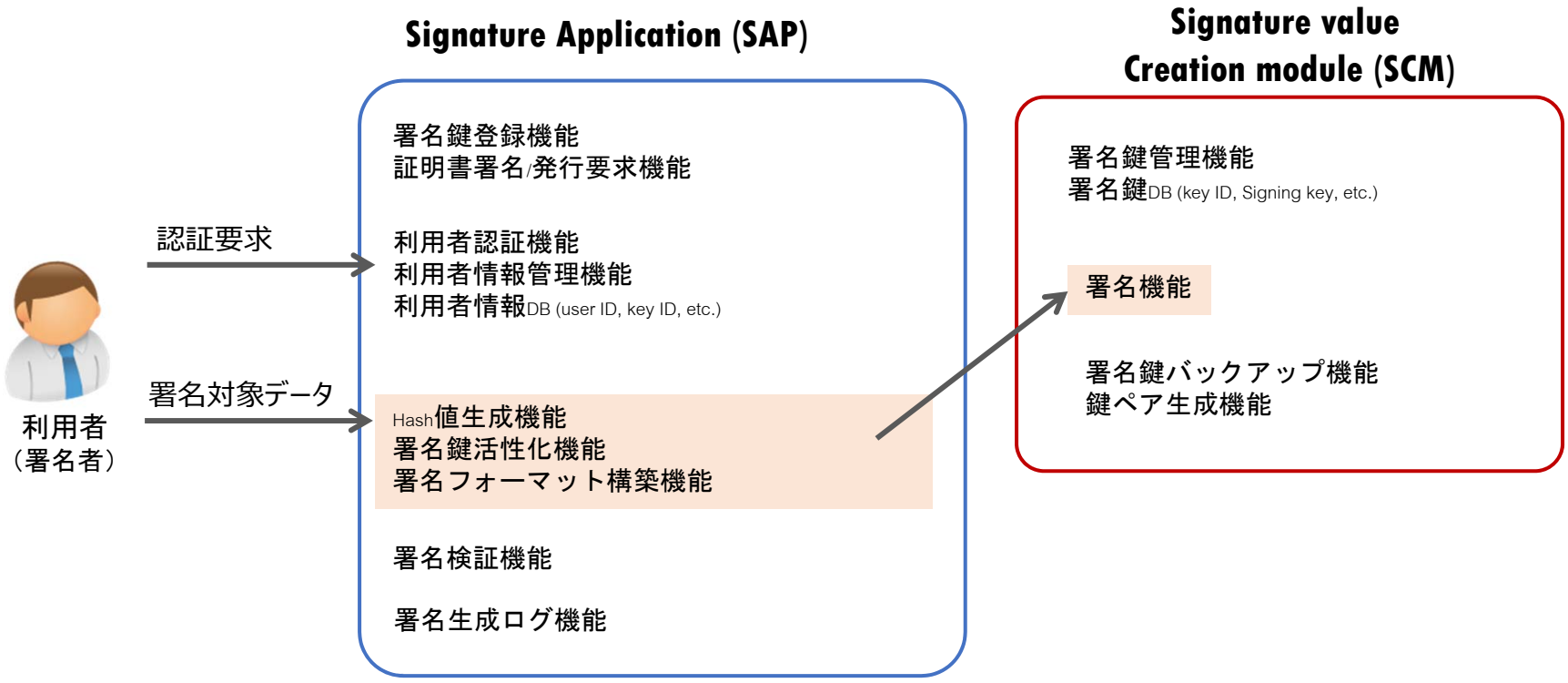
例えば…　（これですべでではありませんが）

- 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）

Copyright (c) Japan Trust Technology Association

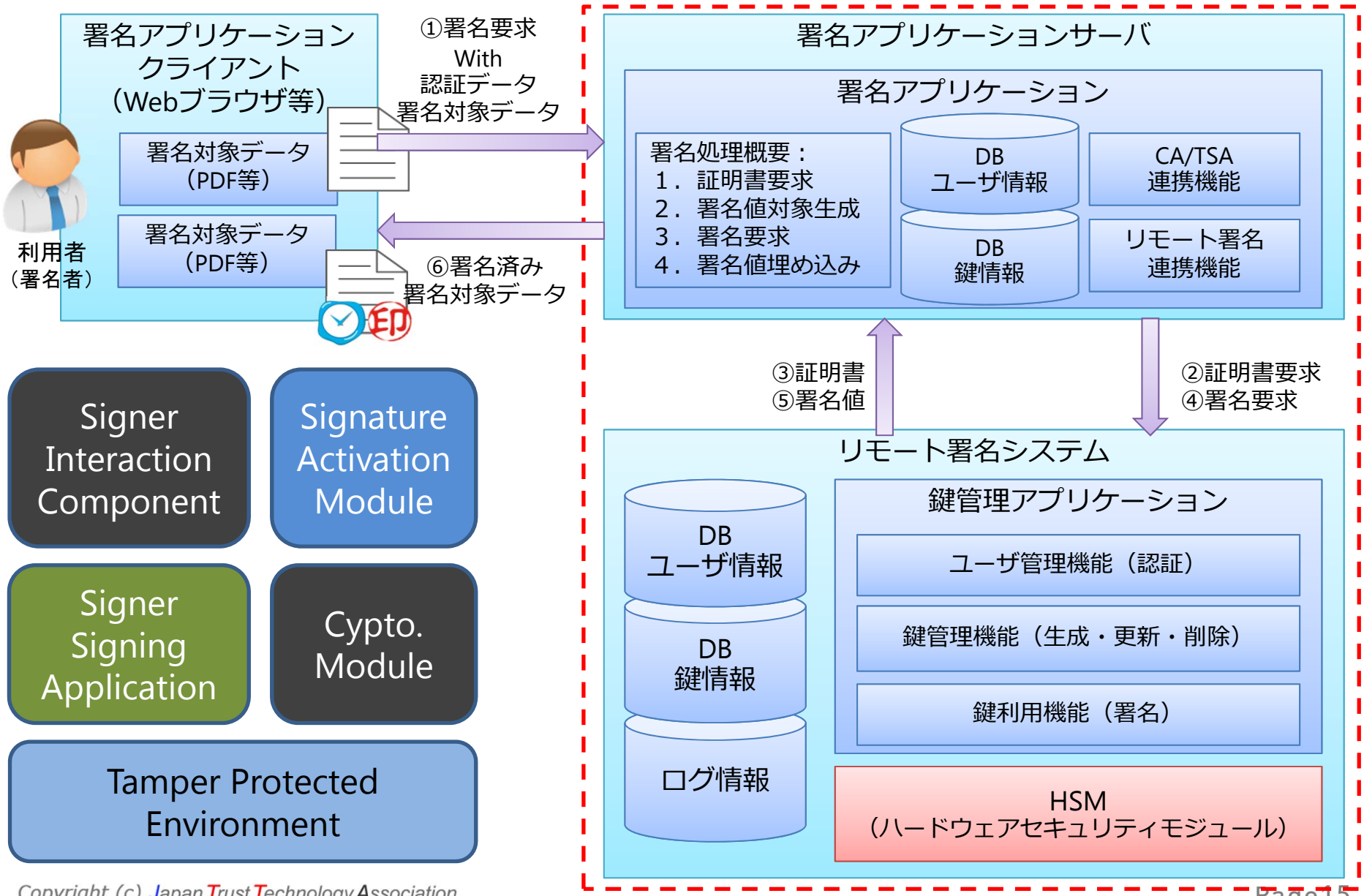
日本の検討：基本構成（署名フェーズの動作）

先行している欧州（EU）の技術要件との整合性が重要



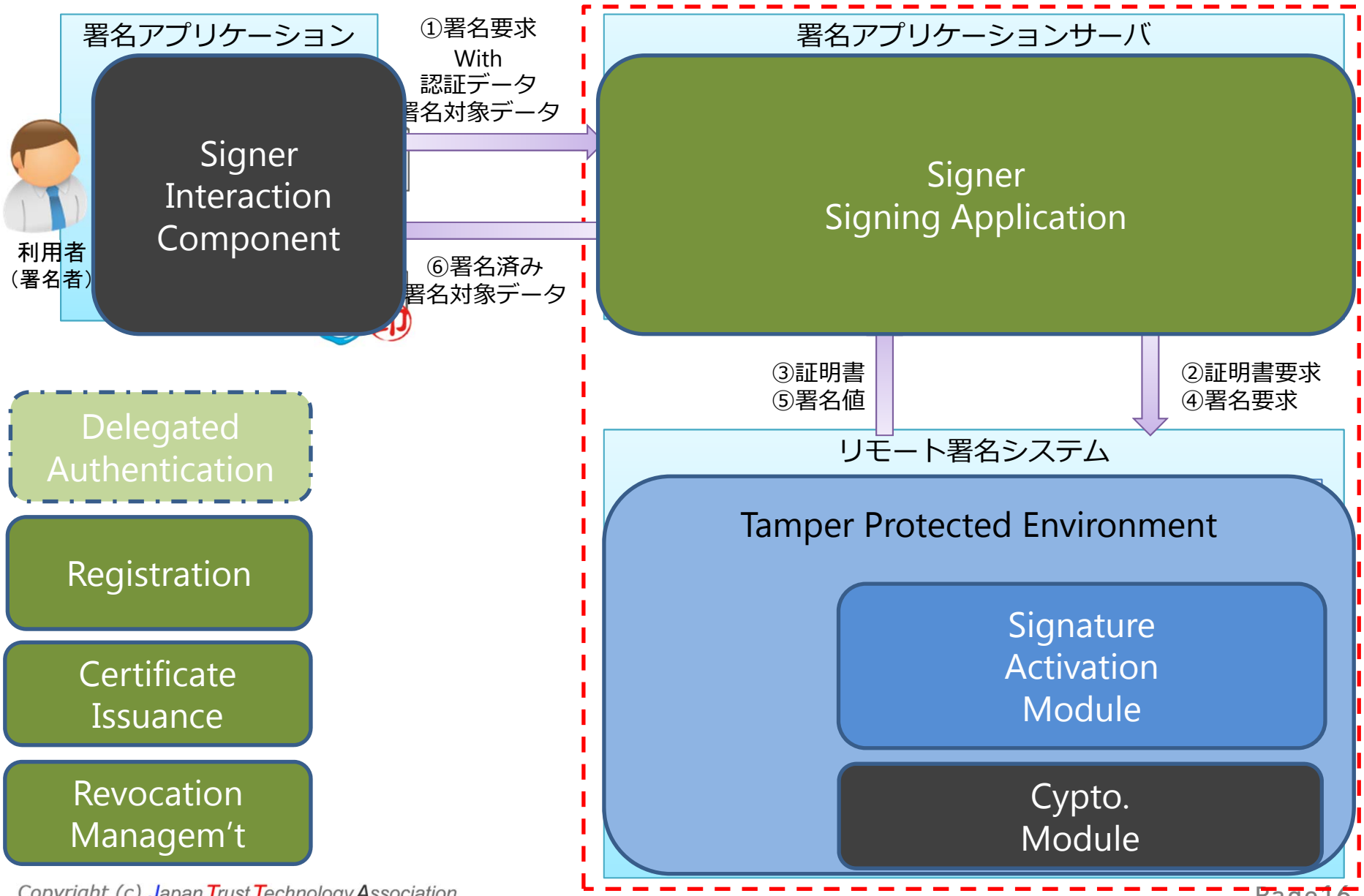
Copyright (c) Japan Trust Technology Association

日本版のシステム構成（案）



Copyright (c) Japan Trust Technology Association

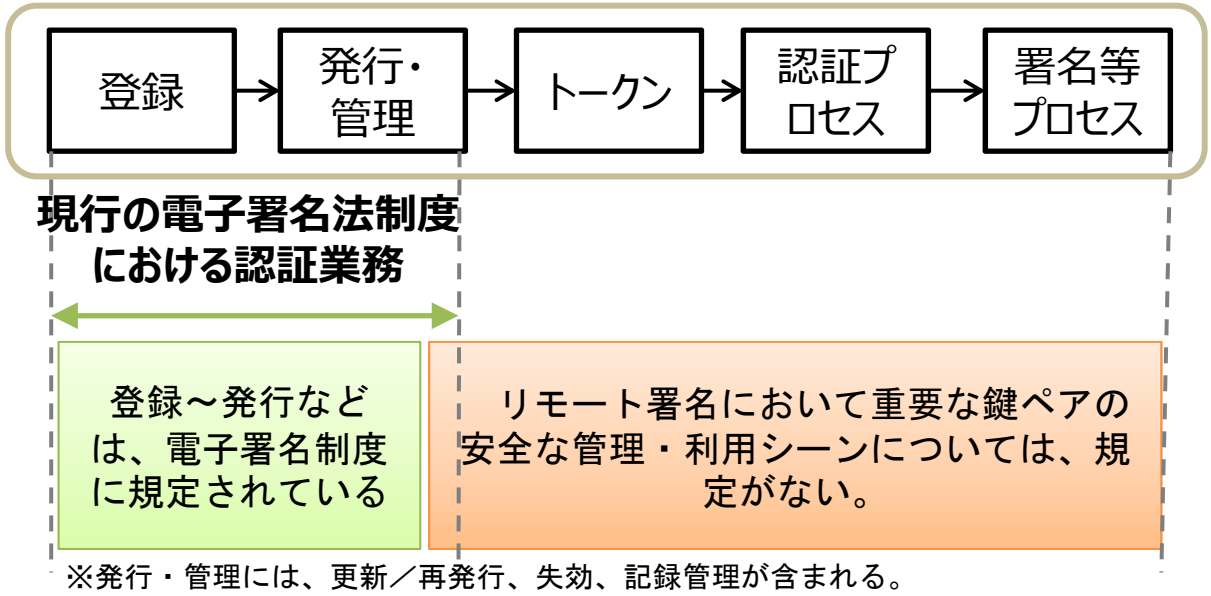
日本版のシステム構成（案）



Copyright (c) Japan Trust Technology Association

日本国内の検討で厄介なこと

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

Copyright (c) Japan Trust Technology Association

ありがとうございました

JT2A

Thank you !

Copyright (c) Japan Trust Technology Association