

# Introduction of JT2A activities

2019.05.23

Japan Network Security Association (JNSA)

Japan Trust Technology Association (JT2A)

Hirohisa OGAWA

## ● Authenticity Guarantee Task Force

- Support for creating guidelines
- Leader : Tadakazu Yamanaka
  - Mitsubishi Electric Corporation.,
  - JNSA Electronic signature WG member

## ● Remote Signature Task Force

- Create Remote Signature Guidelines
- Leader : Shinichi Murao
  - Seiko Solutions Inc.,
  - JNSA Electronic signature WG member

政府CIOポータル

・本文へ 文字サイズの変更: 標準  拡大

Language: 日本語  検索

IT総合戦略室について お知らせ 政策 法令 刊行物 その他

政府CIOポータルホーム > お知らせ > 「デジタル・ガバメント技術検討会議」を設置しました。

電子行政

## 「デジタル・ガバメント技術検討会議」を設置しました。

2018.5.18

デジタル社会に対応した電子行政を実現するため、デジタル・ガバメント推進方針（平成29年5月30日 IT本部・官民データ活用推進戦略会議決定）が決定しました。この方針を推進するに当たって、政府職員だけでは解決が困難な技術的、専門的な課題等について検討するため、政府CIO補佐官から構成される「デジタル・ガバメント技術検討会議」を各府省情報化統括責任者（CIO）連絡会議の下に設置しました。

また、個別内容について集中的に検討するため、「デジタル・ガバメント技術検討会議タスクフォース（以下、「TF」という。）」として「ガイドTF」、「データTF」、「技術TF」及び「人材TF」を設置しました。

今後は各TFにおいて、データ標準や技術標準等、デジタル・ガバメントの推進に係る技術的かつ横断的な内容について具体的な検討を行い、その結論をCIO連絡会議に提案していくこと等を通じて、行政サービスの向上や行政の効率的な運営等の成果につなげていくこととしています。

・技術TF（2018年4月時点）

主査	満埴尚史政府CIO補佐官
副主査	西村毅政府CIO補佐官
メンバー	細川努政府CIO補佐官
	楠正憲政府CIO補佐官
	高橋邦明会計検査院CIO補佐官
	山中忠和日本トラステクノロジー協議会 真正性検証タスクフォースリーダー
主な検討内容	政府情報システムに係る標準的な技術の 取扱いに関する検討

お知らせ  
会見  
報道発表  
行事案内  
関連イベント  
調達・公募情報  
パブリックコメント等  
関連リンク集  
内閣官房のSNS公式アカウント一覧

Participated in the technology study of digital government  
<https://cio.go.jp/node/2361>

政府CIOポータル

Language: 日本語

IT総合戦略室について お知らせ 政策 法令 刊行物 その他

政府CIOポータルホーム > 刊行物 > 政府共通ルール等 > 標準ガイドライン群

電子行政

## 標準ガイドライン群

政府では、ITを徹底活用し、行政内の利便性、効率性、透明性の向上を実現するだけでなく、行政サービスを見直し、デジタル社会に対応したデジタル・ガバメントを目指しています。このデジタル・ガバメントへ変革していくために、政府CIOを中心に各府省CIOがリーダーシップを発揮し、「共通ルール」の下、各府省及び政府全体のITガバナンスを強化する必要があります。

このため、行政のサービス・業務改革に伴う政府情報システムの整備及び管理について、その手順や各組織の役割等を定める体系的な政府共通ルールとして、「デジタル・ガバメント推進標準ガイドライン」(2019年2月25日各府省情報化統括責任者(CIO)連絡会議決定。以下「標準ガイドライン」という。)を決定しました。また、標準ガイドラインに関連する指針類等に係る文書体系を「標準ガイドライン群」と称します。

なお、標準ガイドライン群に記載された会社名、製品名等は、各社の商標又は登録商標である場合があります。

- 標準ガイドライン群リスト

### 行政手続におけるオンラインによる本人確認の手法に関するガイドライン

PDF DOCX

略称 本人確認ガイドライン  
最終改定 2019年2月25日  
対象 各府省  
概要 各種行政手続をデジタル化する際に必要となる、オンラインによる本人確認の手法を示した標準ガイドラインの附属文書

## 行政手続におけるオンラインによる本人確認の手法 に関するガイドライン

2019年(平成31年)2月25日

各府省情報化統括責任者(CIO)連絡会議決定

【標準ガイドライン群ID】

1004

【キーワード】

本人確認、身元確認、本人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

【概要】

各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

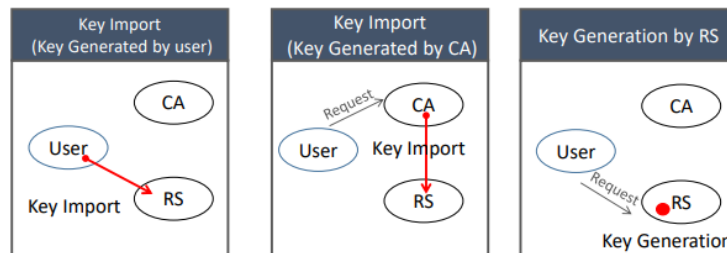
Standard Guidelines Group Government CIO Portal  
<https://cio.go.jp/guides>  
Guidelines for methods of online identification and authentication in administrative procedures.

## Status of Remote Signature Adoption and Implementation in Japan

Japan Network Security Association  
Remote Signature Task Force Leader  
Mizuho Information & Research Institute, Inc.  
Management & IT Consulting Div Manager  
Hirohisa OGAWA

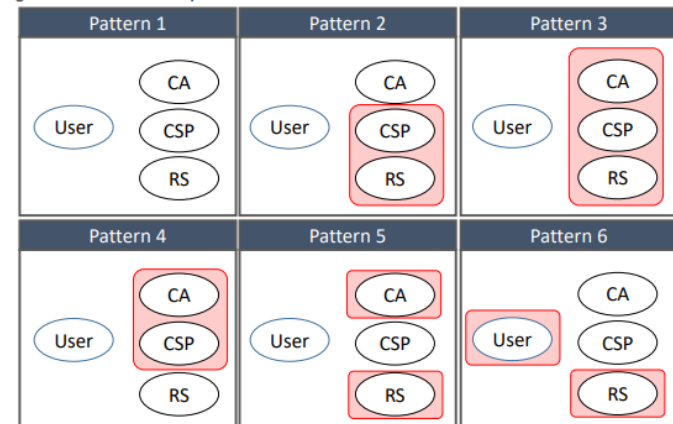
### 7. Installation of Signing key of user

- It is about importing and generating signing keys. The user registers the user in the remote signature and sets the signature key to be used.



### 1. Players and roles of Remote Signature

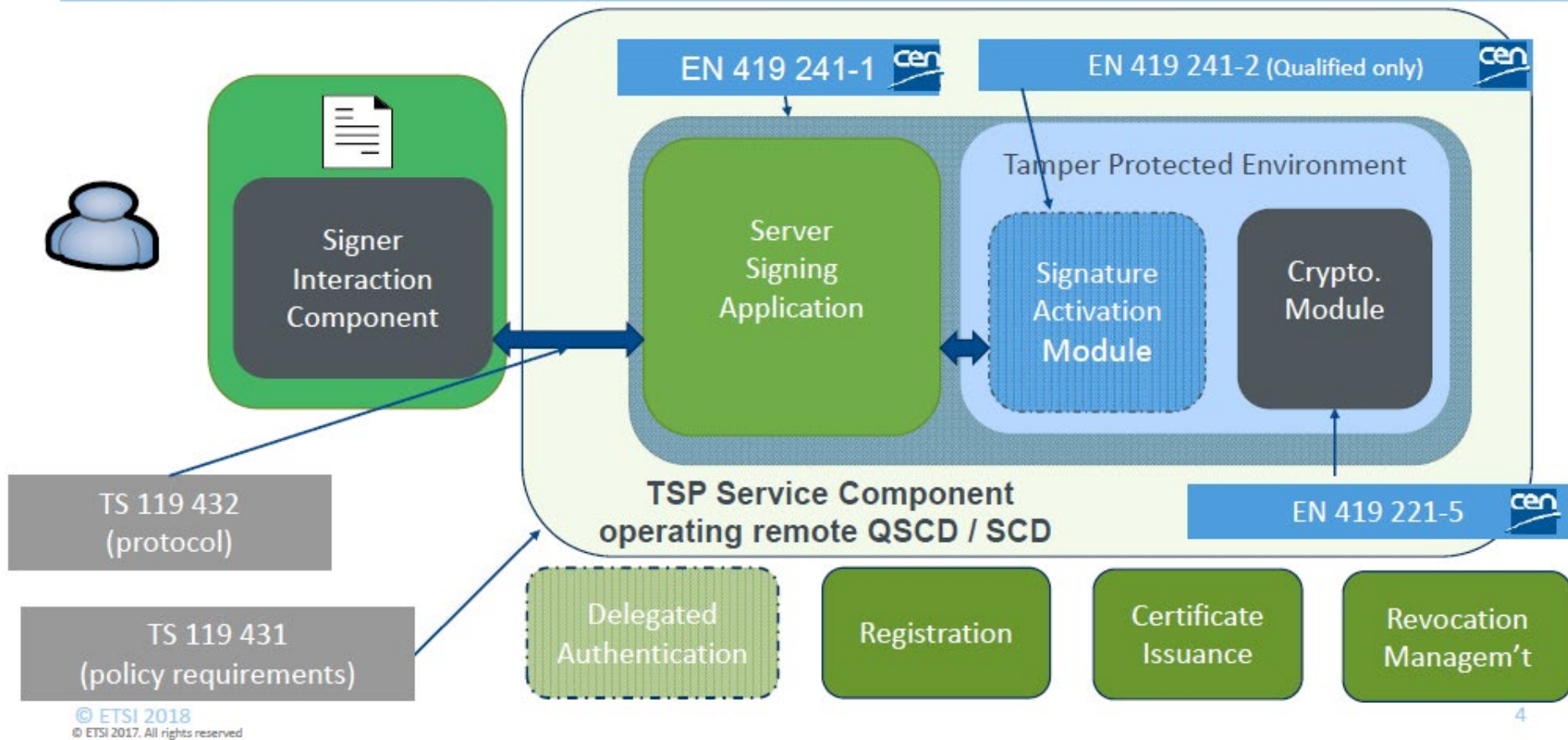
- Assumed remote signature pattern (Including concrete examples)
- A single company carries out the part surrounded by red.
- By implementing it in a single company, efficiency of user registration can be expected. But governance is necessary.



Japan-Europe Internet Trust Symposium 2017  
<https://itc.jipdec.or.jp/event/20170704.html>  
<https://itc.jipdec.or.jp/English/event/20170704.html>

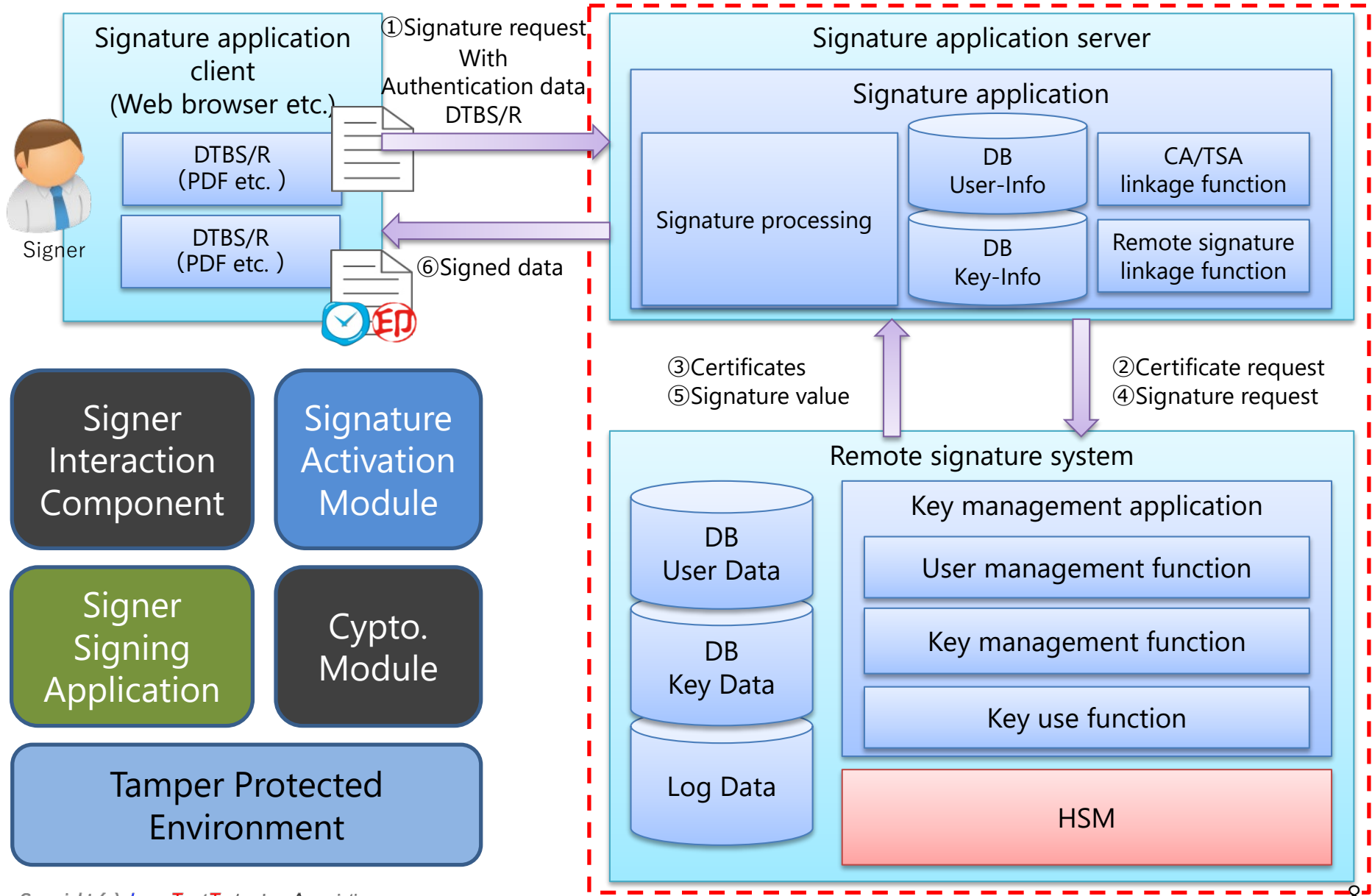
# EU Remote Signature configuration

## Scope of remote signing standards



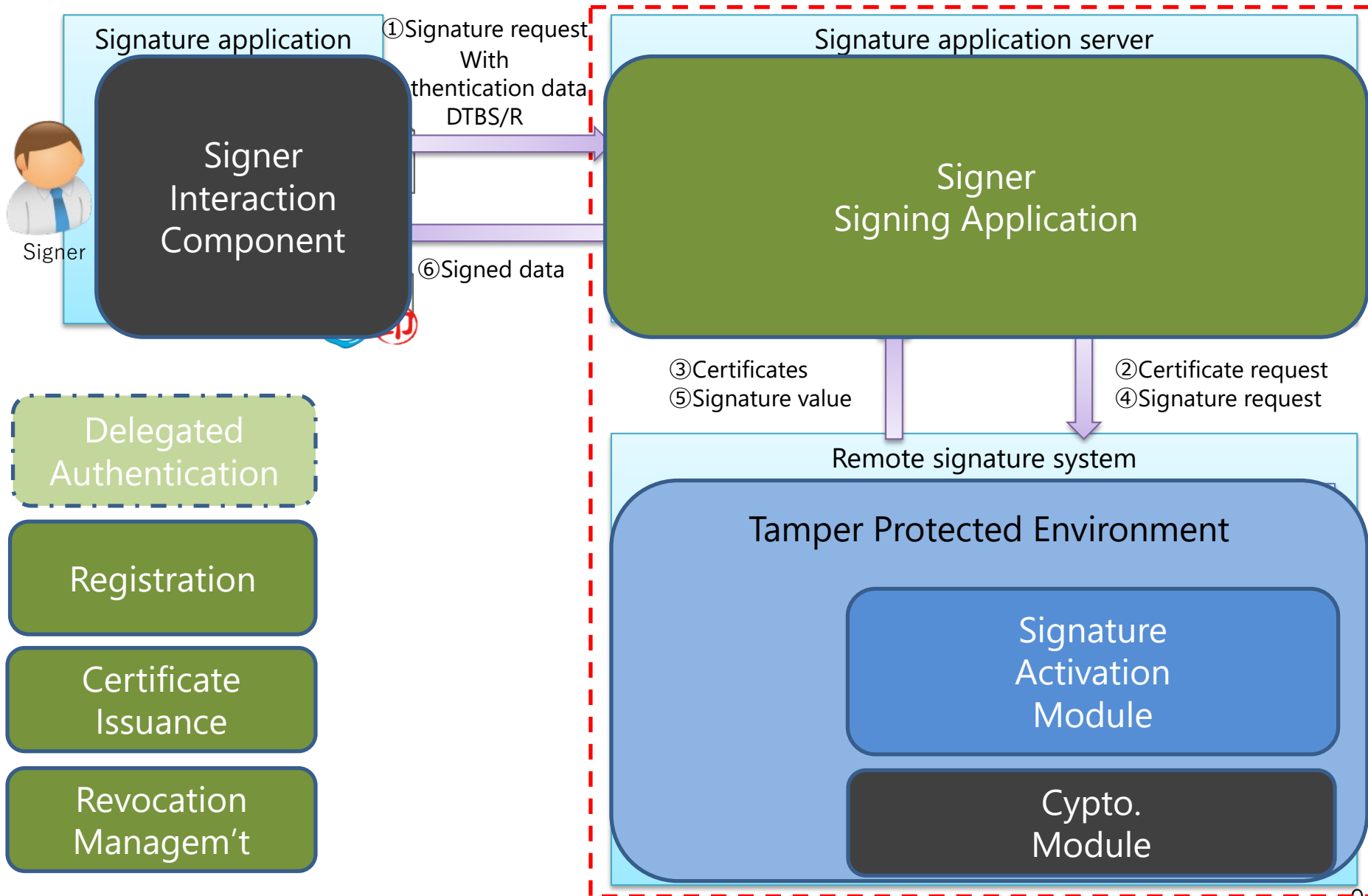
仕様名	タイトル
EN 419 241-1	Security Requirements for Trustworthy Systems Supporting Server Signing
EN 419 241-2	Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
EN 419 221-5	Protection profiles for Trust Service Providers (TSP) Cryptographic modules - Part 5: Cryptographic Module for Trust Services
TS 119 431-1	Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
TS 119 431-2	Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
TS 119 432	Protocols for remote digital signature creation

# Japanese Remote Signature configuration





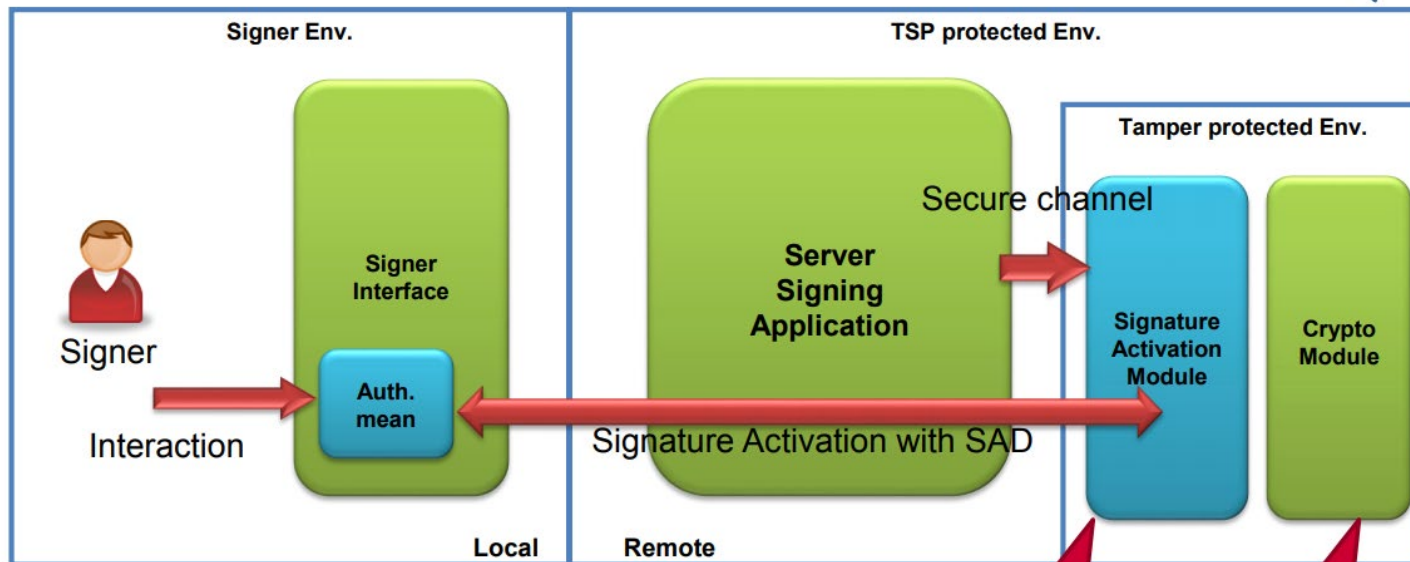
# Comparison of Japan and EU



## REMOTE SIGNING OVERVIEW

Sole control Assurance Level 2

419 241-1  
Level 2



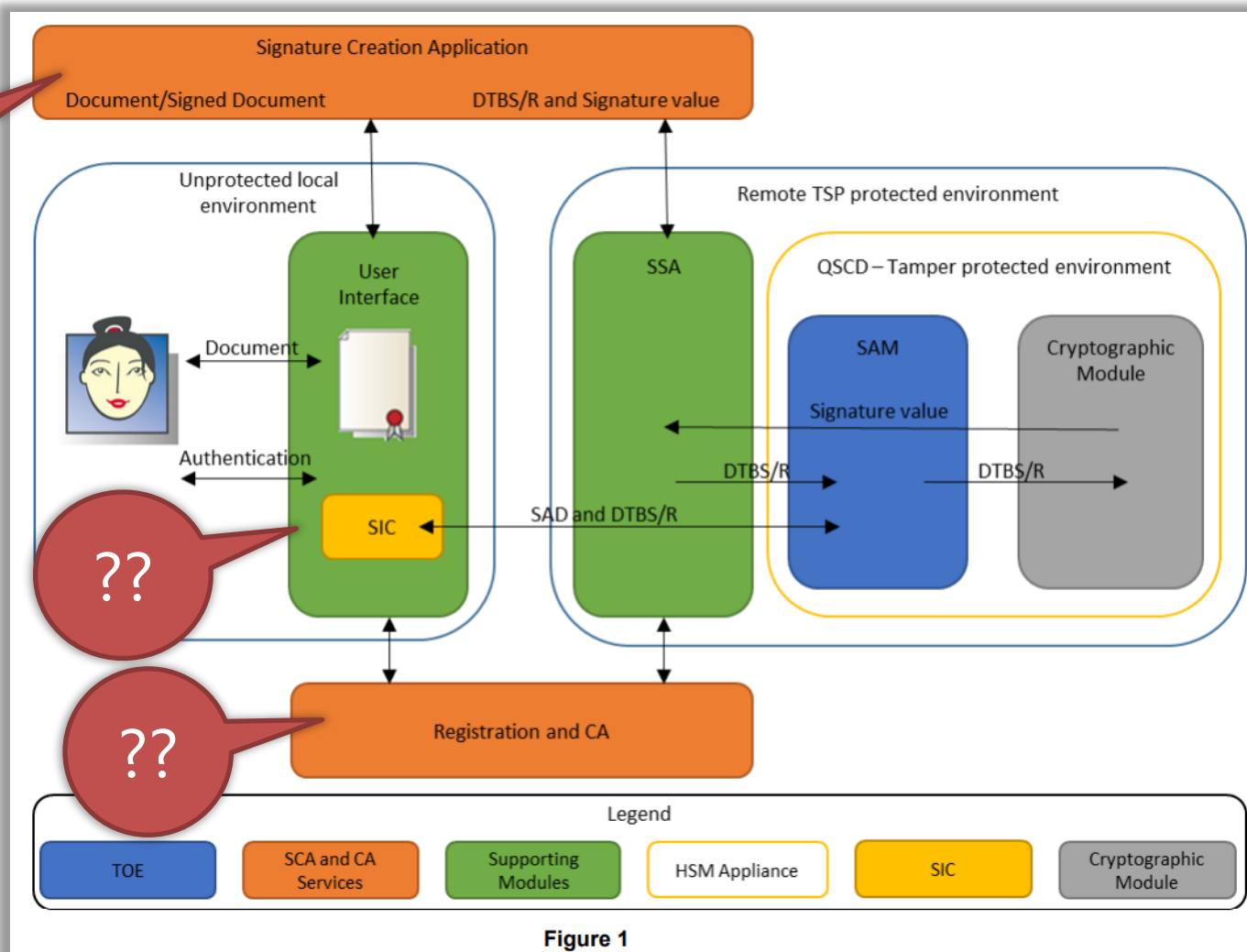
- SCAL1 components
- SCAL2 components

PP-QSCD  
419 241-2

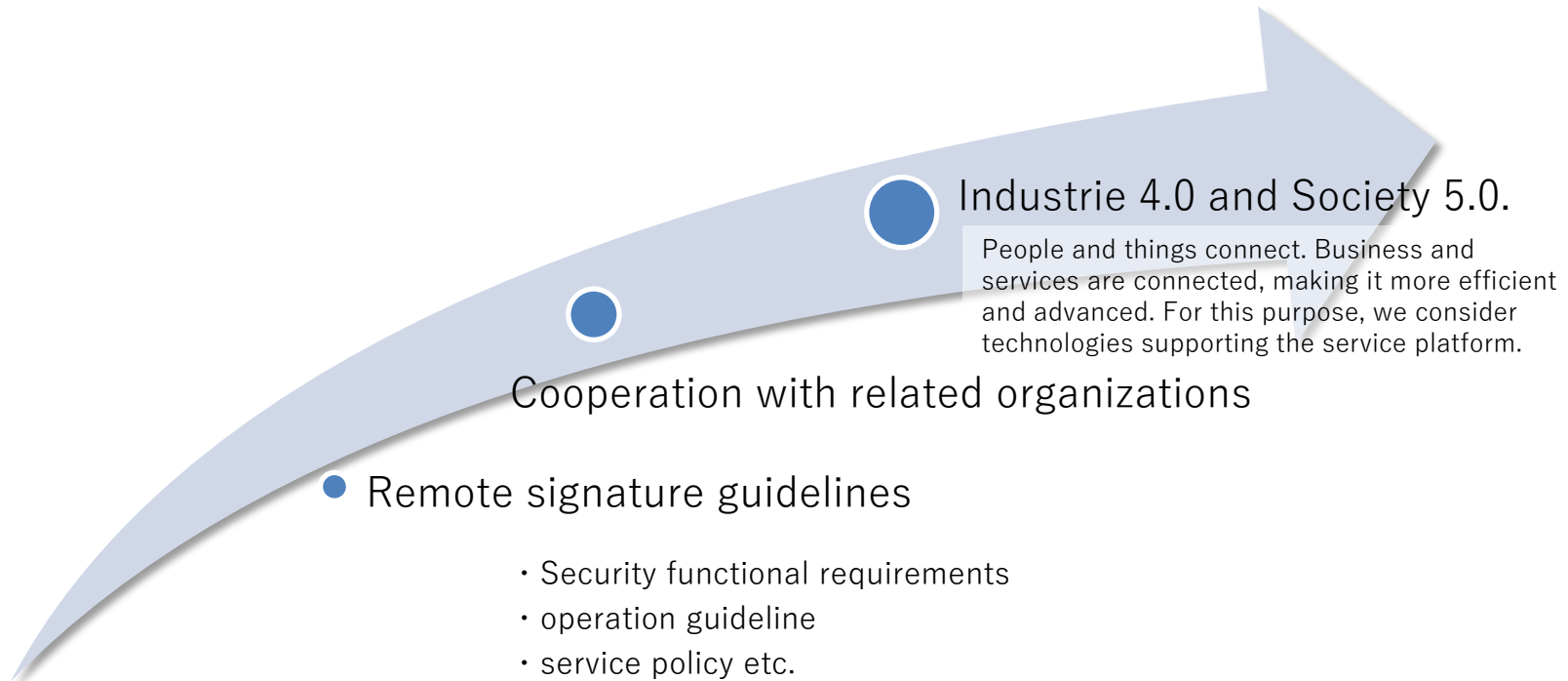
PP-Crypto  
419 221-5

- Describe remote signature technical standards (security requirement specifications), operation and management, general security, etc.
- Minimum security requirements
  - Overview and commentary of remote signature
  - General security including organizational measures, environment, operation
- Recommended criteria
  - Criteria to add to the Minimum security requirements
  - Multi-Factor Authentication
  - Verified cryptographic module
- Recommended criteria + additional rules
  - Add additional clauses to recommended criteria
  - Assume QES level in Europe (SAM, SCDev etc)

# Future issues and examinations



Date:2018-05-11, 419 241-2, CEN/TC 224, Secretariat: AFNOR, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing  
[https://www.ssi.gouv.fr/uploads/2018/09/anssi-cc-pp-2018\\_02fr\\_pp.pdf](https://www.ssi.gouv.fr/uploads/2018/09/anssi-cc-pp-2018_02fr_pp.pdf)



Japan Trust Technology Association

