

JT2Aの活動内容

2019年5月23日

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）

小川 博久

Introduction of JT2A activities

2019.05.23

Japan Network Security Association (JNSA)

Japan Trust Technology Association (JT2A)

Hirohisa OGAWA

●真正性保証TF

- ・ ガイドラインの作成支援
- ・ TFリーダー：山中 忠和
 - ・ 三菱電機株式会社
 - ・ JNSA 電子署名WGメンバ

●リモート署名TF

- ・ リモート署名ガイドラインの作成
- ・ TFリーダー：村尾 進一
 - ・ セイコーソリューションズ株式会社
 - ・ JNSA 電子署名WGメンバ

●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

真正性保証TFの活動

JT2A

政府CIOポータル

Language: 日本語 検索

お知らせ お見聞 報道発表 行政案内 開催イベント 調達・公募情報 パブリックコメント等

内閣官房のSNS公式アカウント一覧

「デジタル・ガバメント技術検討会議」を設置しました。

2018.5.16

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」を各府省横断化責任者（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、その結果をCIO連絡会議に提案していくことを通じて、行政サービスの向上や行政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	渕塙尚史政府CIO補佐官
副主査	西村聰政府CIO補佐官
メンバー	細川努政府CIO補佐官 横正志政府CIO補佐官 奥塙邦明会計検査院CIO補佐官 山中忠和日本トラスト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り扱いに関する検討

デジタル・ガバメント技術検討会議を設置しました。政府CIOポータル
<https://cio.go.jp/node/2361>

Authenticity Guarantee TF activities

JT2A

The screenshot shows the Government CIO Portal homepage. The main content area features a news item titled '「デジタル・ガバメント技術検討会議」を設置しました。' (Established the 'Digital Government Technology Study Conference'). Below the title is the date '2018.5.16'. The text discusses the establishment of the conference to promote digital government through the 'Digital Government Strategy Document' (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). It also mentions the formation of a task force under the CIO's chief of staff to study specific issues like data standards and technology. The conference will be held under the responsibility of the CIO's chief of staff.

Below the news item is a table titled '・技術TF (2018年4月時点)' (Technology Task Force (as of April 2018)). The table lists the following members:

主査	岸塙尚史政府CIO補佐官
副主査	西村聰政府CIO補佐官
メンバー	細川努政府CIO補佐官 横正志政府CIO補佐官 奥塙邦明会計検査院CIO補佐官 山中忠和日本トラスト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

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

真正性保証TFの活動

JT2A

政府CIOポータル

The screenshot shows the Government CIO Portal homepage. In the top right corner, there are links for '日本語' (Japanese), '文字サイズの変更' (Change font size), and '拡大' (Zoom in). Below these are 'Language: 日本語' and a search bar. The main navigation menu includes 'お問い合わせ', '政策', '法令', '刊行物', 'その他', and '標準ガイドライン群'. A sidebar on the left lists '電子行政', '標準ガイドライン群', and '参考資料等'. The main content area is titled '標準ガイドライン群' and contains text about the government's IT strategy and the 'Standard Guidelines Group'. It also mentions the 'Standard Guidelines for Online Identity Verification' (PDF, DOCX) and its details: '標準ガイドライン', '2019年2月25日', '各府省', and '概要: 各種行政手続をデジタル化する際に必要な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別冊文書'.

標準ガイドライン群 政府CIOポータル

<https://cio.go.jp/guides>

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

This is a screenshot of the 'Guidelines for Online Identity Verification in Administrative Procedures' document. At the top right, it says '2019年(平成31年)2月25日' and '各府省情報化統括責任者(CIO)連絡会議決定'. The document is identified as '標準ガイドライン群 ID: 1001'. It includes sections for 'キーワード' (Keywords) and '概要' (Summary), both of which describe the purpose of the guidelines: to standardize online identity verification methods for various administrative procedures.

Authenticity Guarantee TF activities

JT2A

政府CIOポータル

Language: 日本語 検索

標準ガイドライン群

標準ガイドライン群

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

暗号化された会社名、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。

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】
1094
【キーワード】
本人確認、身元確認、当人認証、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の附属文書

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

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

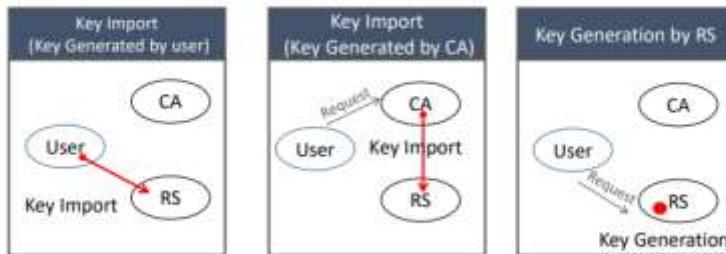
【標準ガイドライン群】
1094
【キーワード】
本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証
【概要】
各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドラインの附属文書

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
Hiroyisa OGAWA

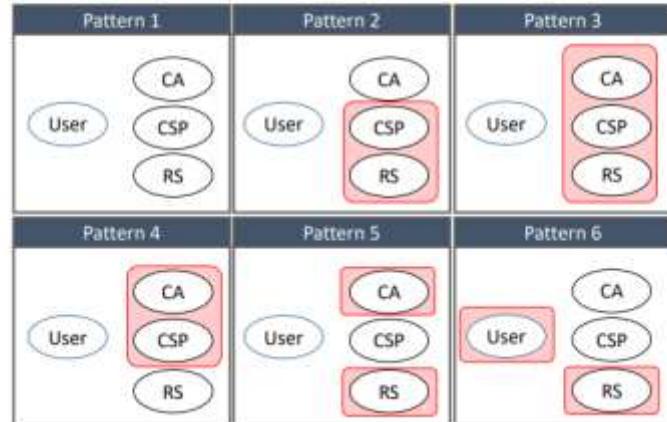
7. Installation of Signing key of user

- 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.



日欧インターネットトラストシンポジウム 2017年
<https://itc.jipdec.or.jp/event/20170704.html>
<https://itc.jipdec.or.jp/English/event/20170704.html>

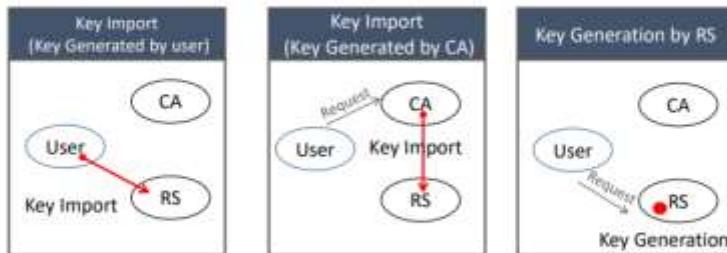
Status of Remote Signature Adoption and Implementation in Japan

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

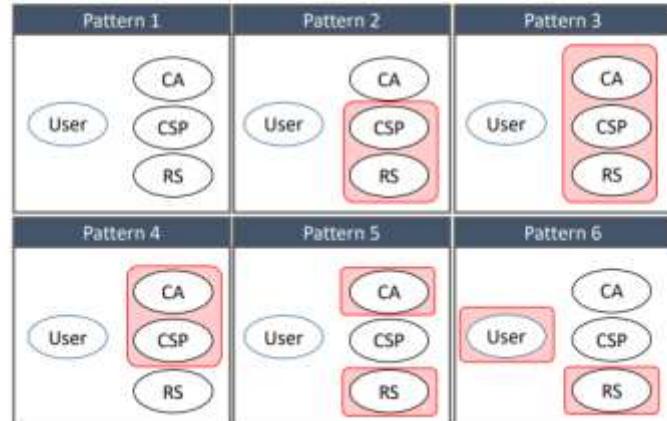


- It is about importing and generating signing keys. The user registers the user in the remote signature and sets the signature key to be used.



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.



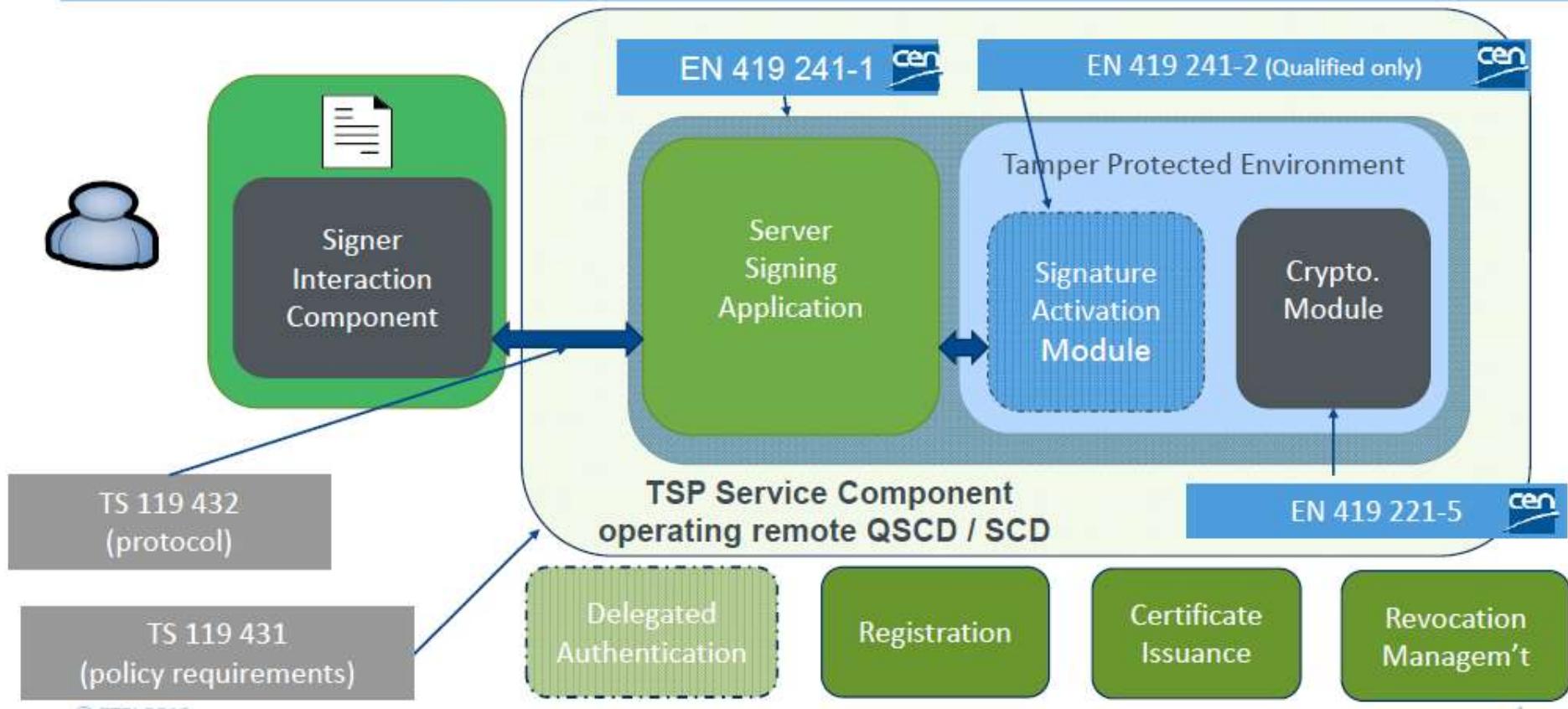
Japan-Europe Internet Trust Symposium 2017
<https://itc.jipdec.or.jp/event/20170704.html>
<https://itc.jipdec.or.jp/English/event/20170704.html>

EUのリモート署名の構成

JT2A



Scope of remote signing standards



© ETSI 2018
© ETSI 2017. All rights reserved

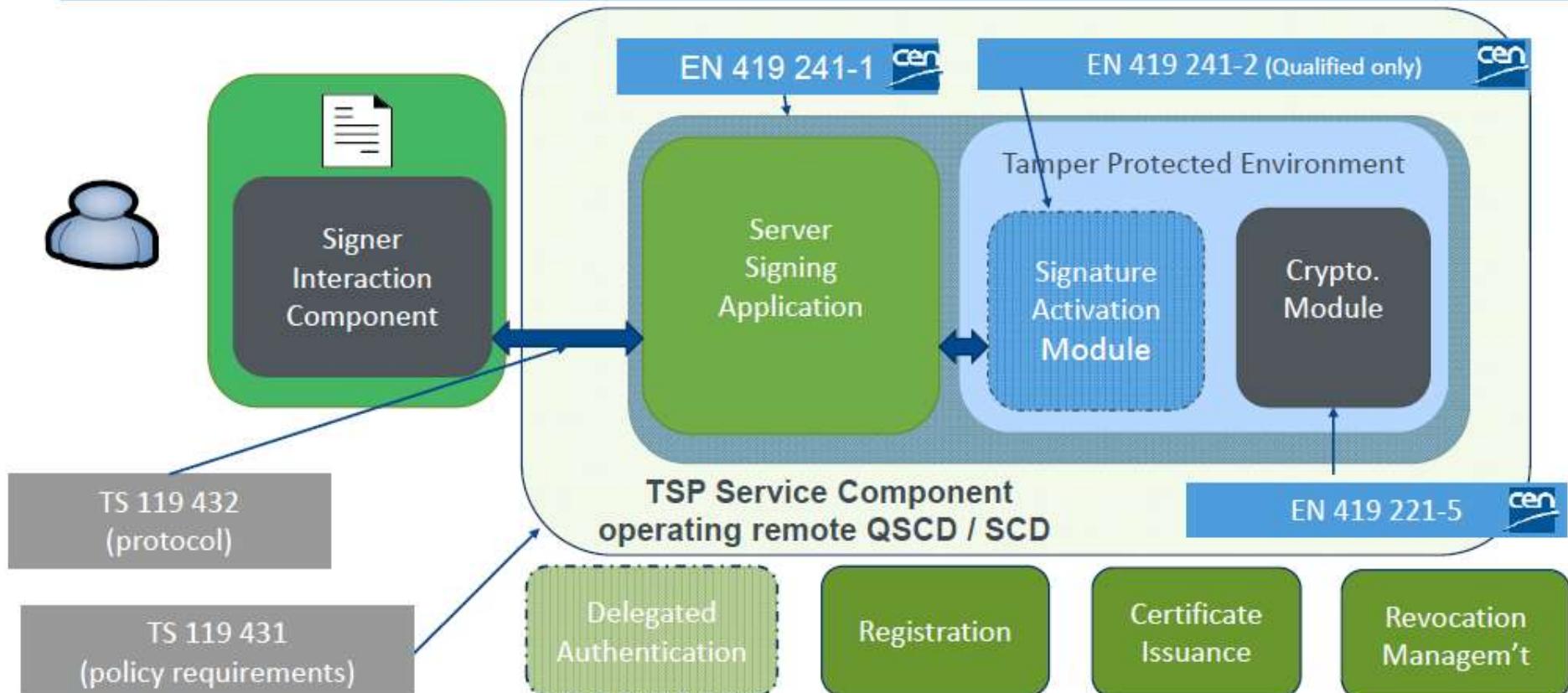
https://docbox.etsi.org/workshop/2018/201806_ETSISECURITYWEEK/REMOTE_SIGNATURE_CREATION/ETSI%20_TC_ESI_POPE.pdf

EU Remote Signature configuration

JT2A



Scope of remote signing standards



© ETSI 2018
ID ETSI 2017. All rights reserved

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する規格

JT2A

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）

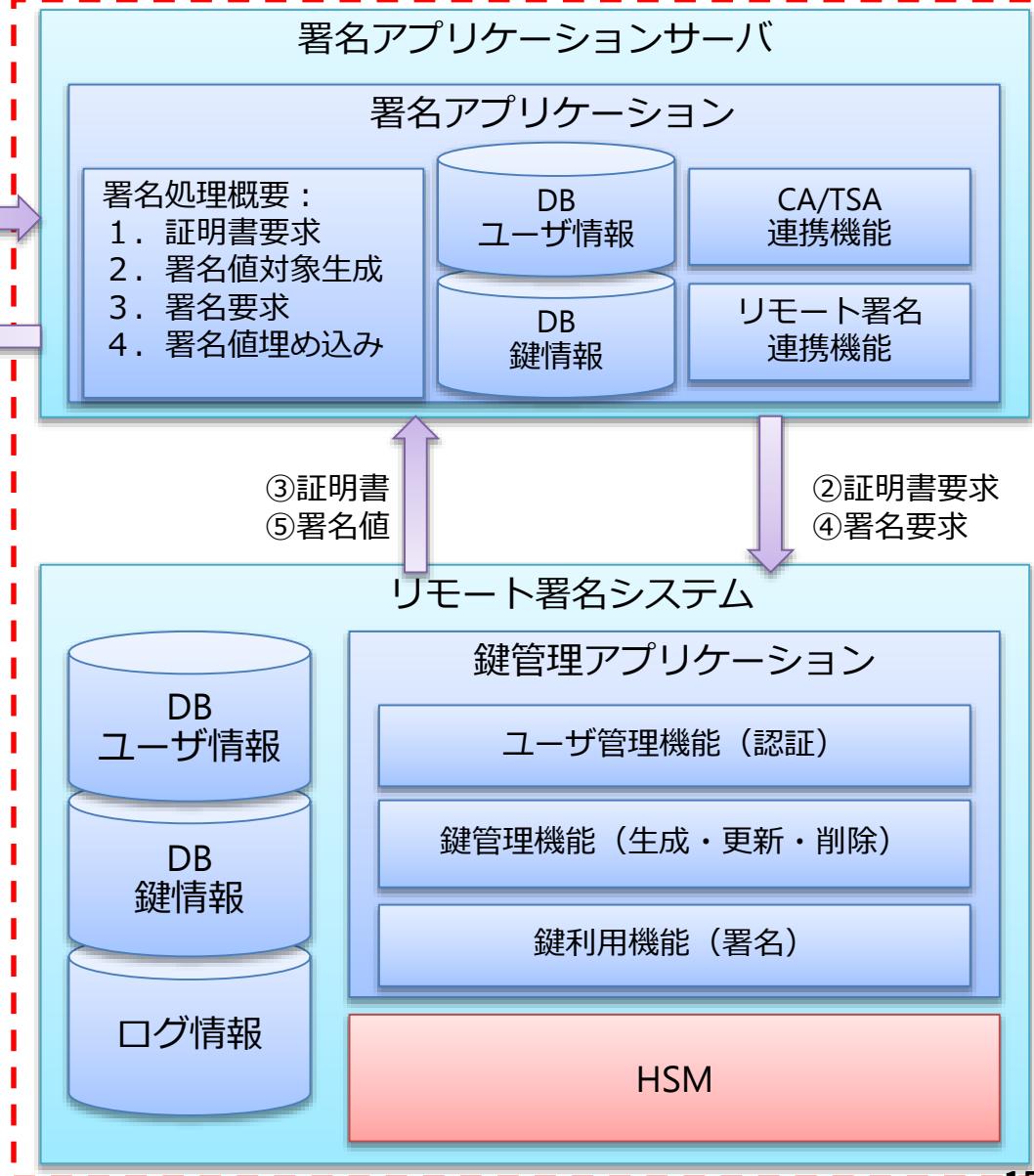
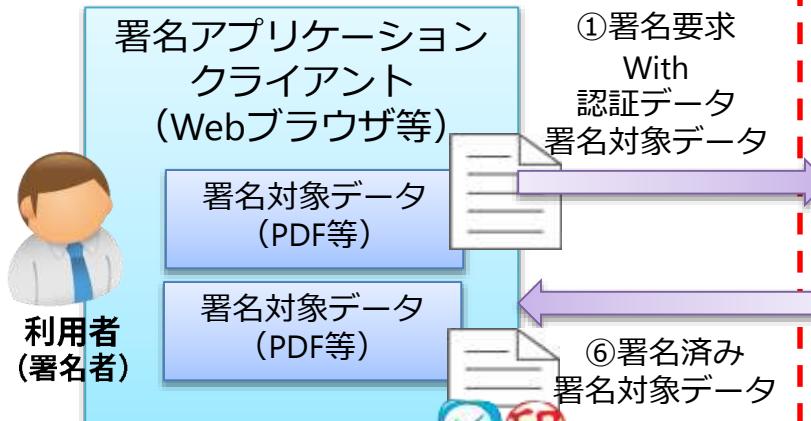
EU Remote Signature Standard

JT2A

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

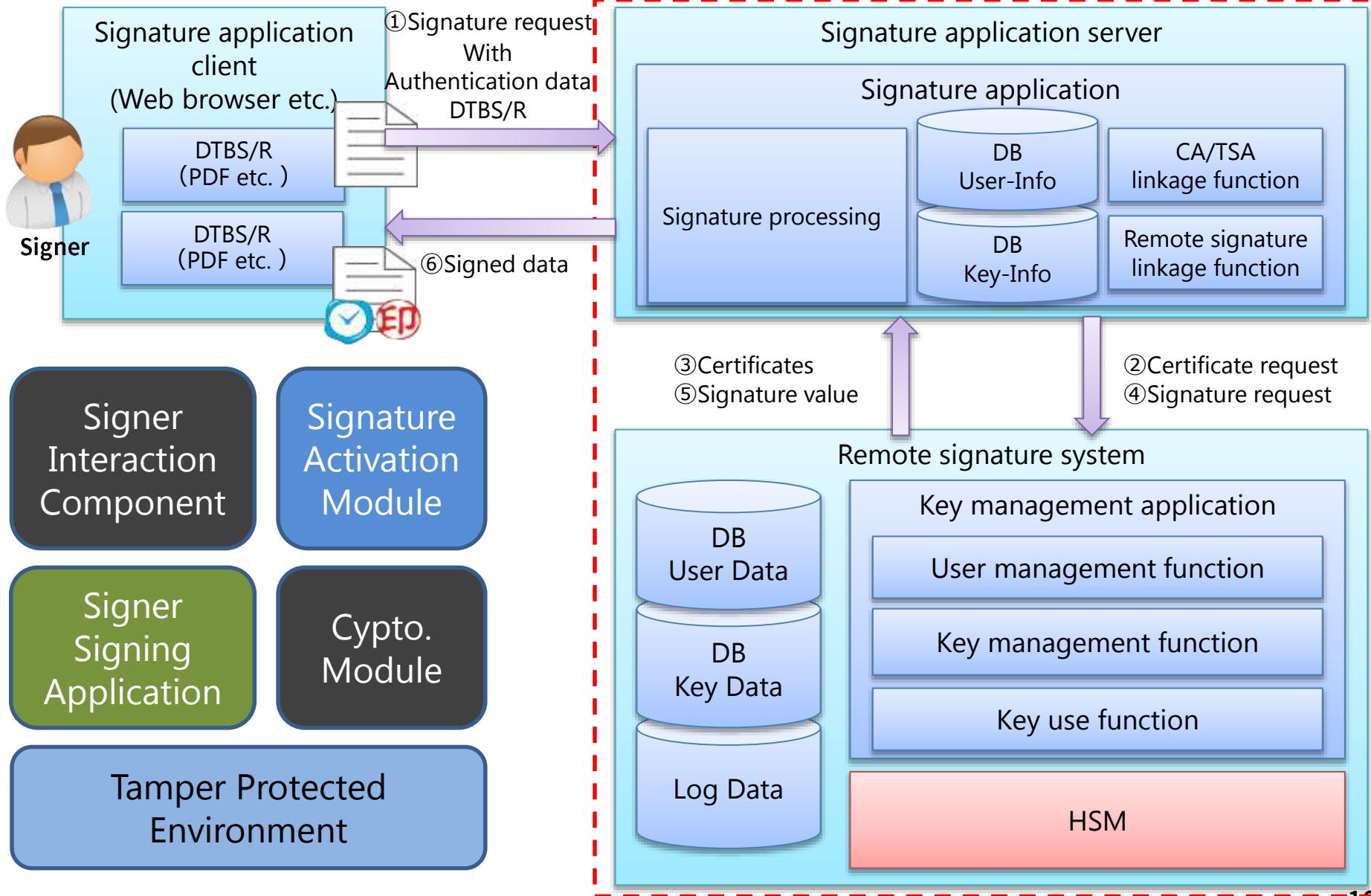
日本のシステム構成

JT2A



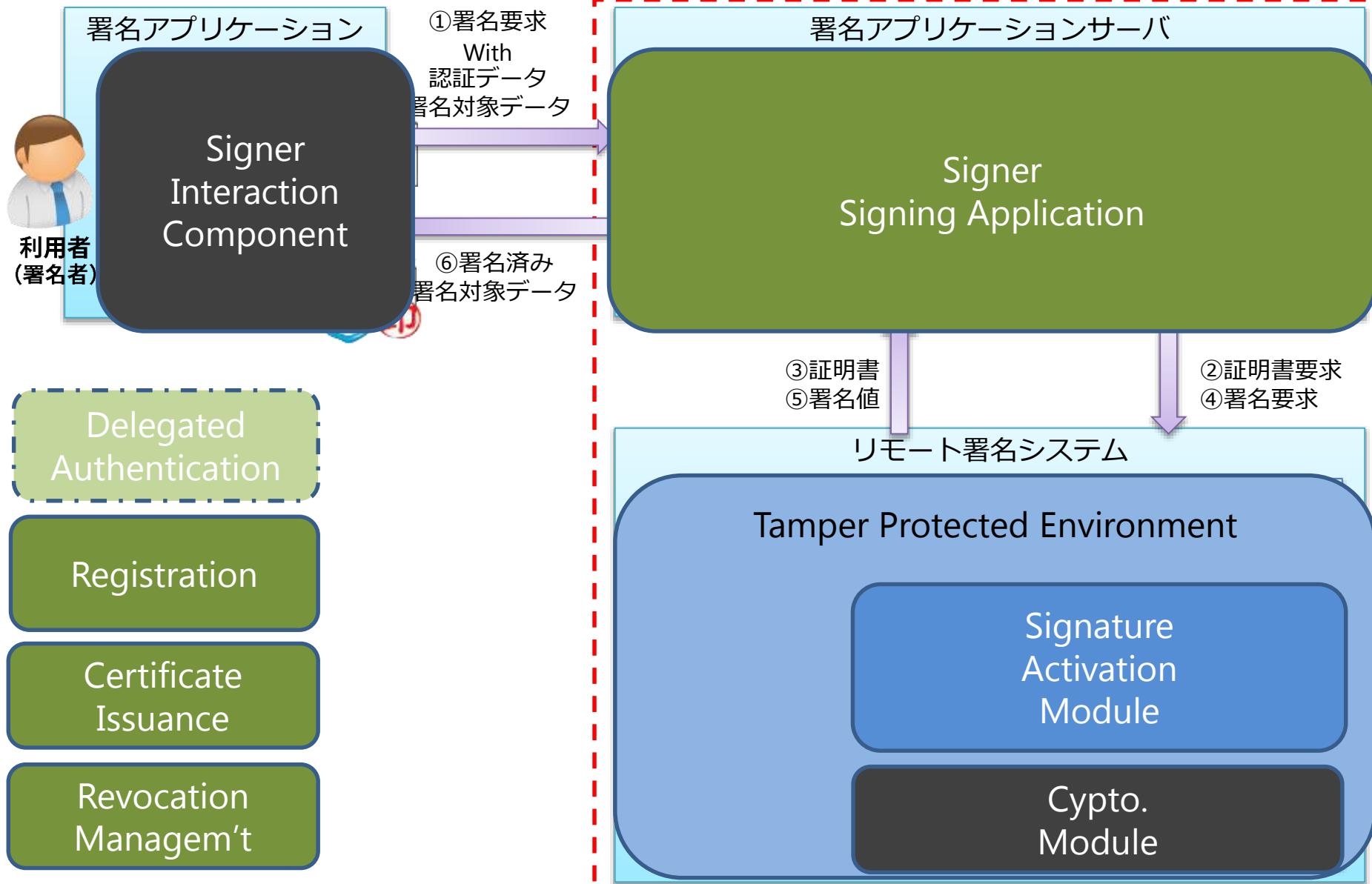
Japanese Remote Signature configuration

JT2A



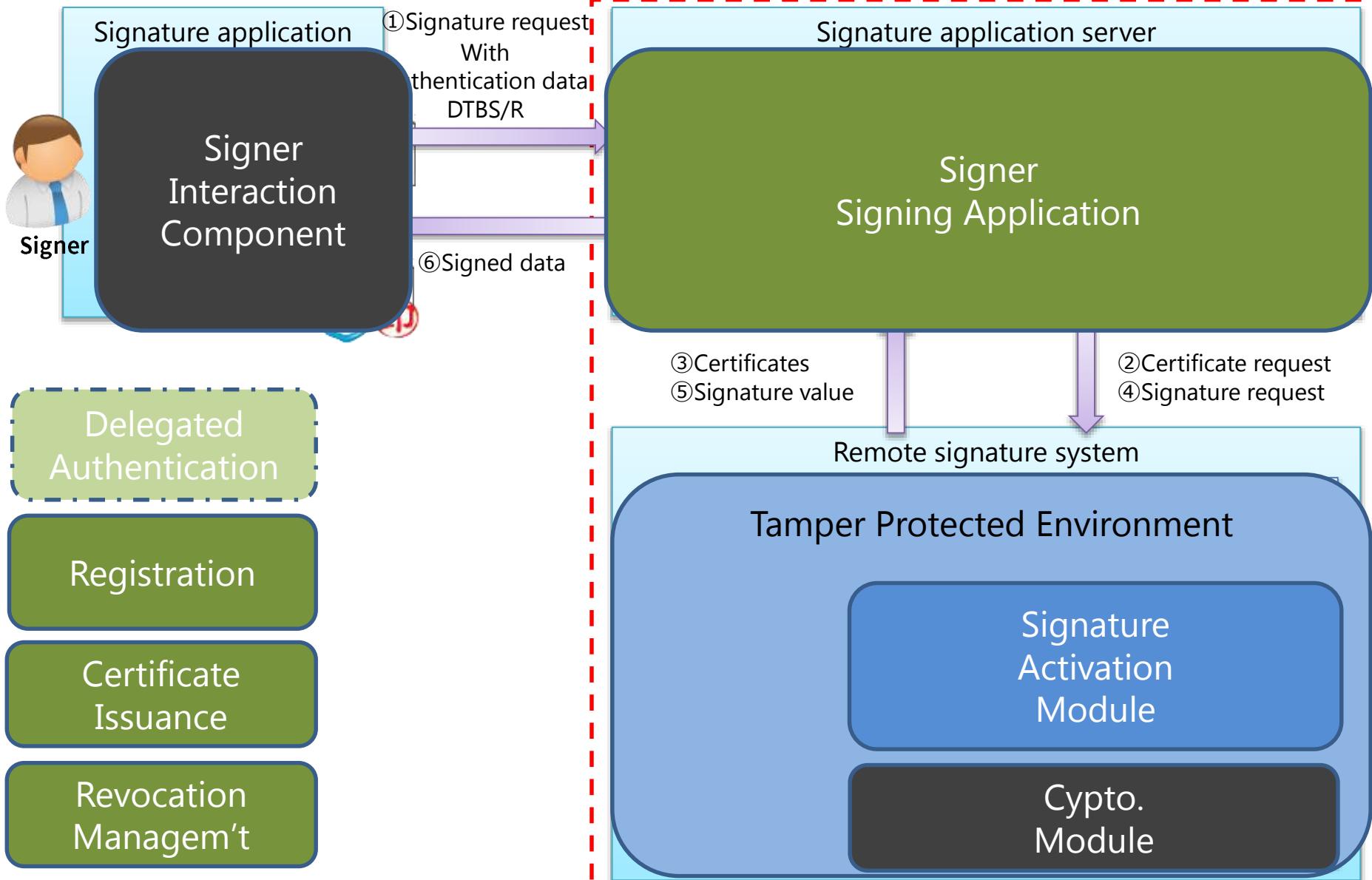
日本とEUの構成比較

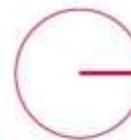
JT2A



Comparison of Japan and EU

JT2A

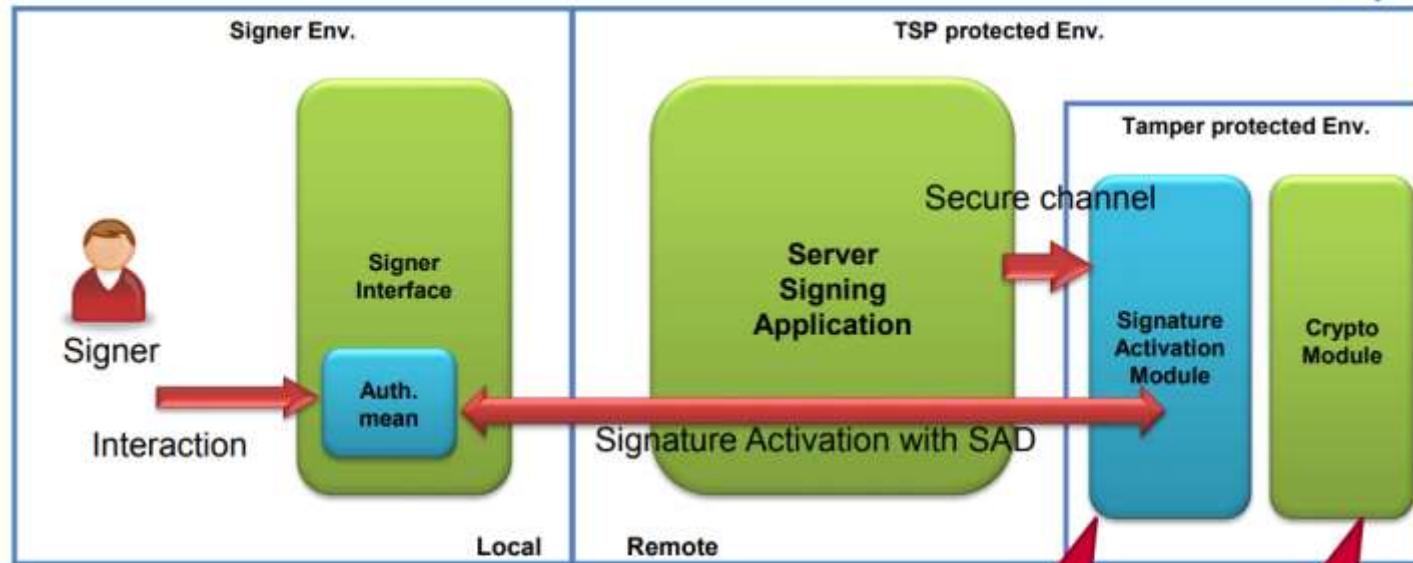




REMOTE SIGNING OVERVIEW

Sole control Assurance Level 2

419 241-1
Level 2

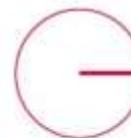


SCAL1 components

SCAL2 components

PP-QSCD
419 241-2

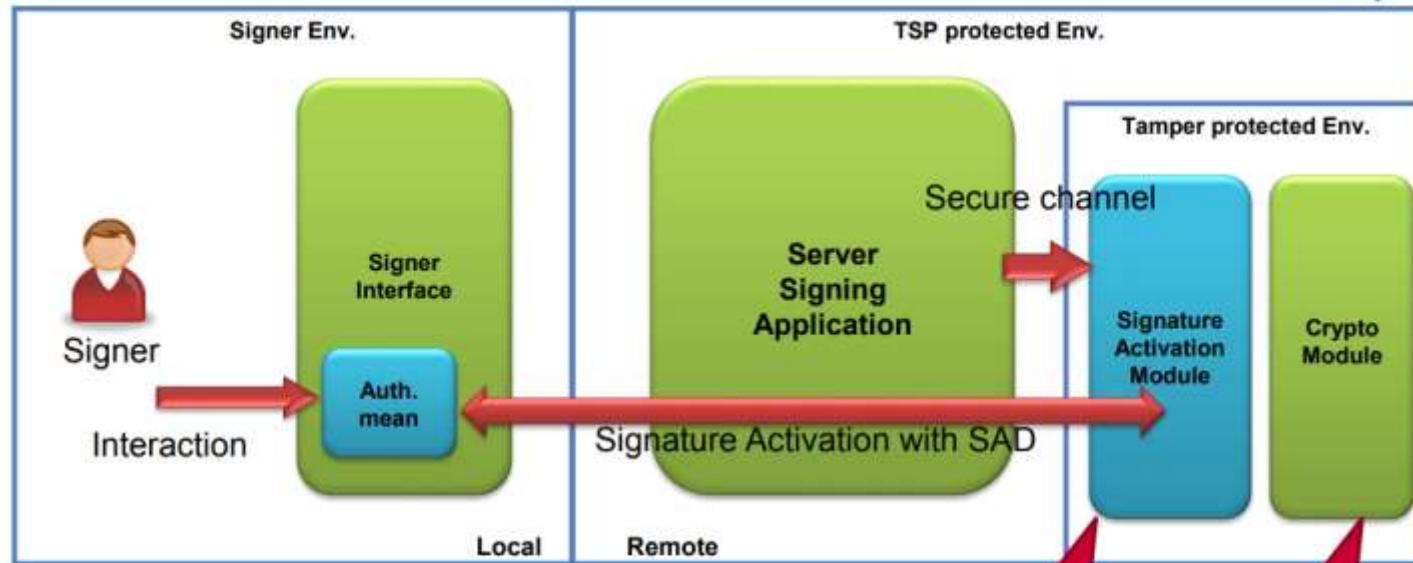
PP-Crypto
419 221-5



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

リモート署名ガイドラインの概要（検討中）JT2A

- ・ リモート署名の技術基準（セキュリティ要求仕様）、運用・管理、一般的なセキュリティなどを記述
- ・ 最低限満たすべき基準
 - ・ リモート署名の概要と解説
 - ・ 組織的対策、環境、運用を含む一般的セキュリティ
- ・ 推奨基準
 - ・ 上記に追加する基準
 - ・ 多要素認証
 - ・ 認証取得した暗号モジュール
- ・ 推奨基準+附則
 - ・ 推奨基準に附則を追加
 - ・ 欧州のQESレベル（SAM、SCDevなど）を想定

- **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)

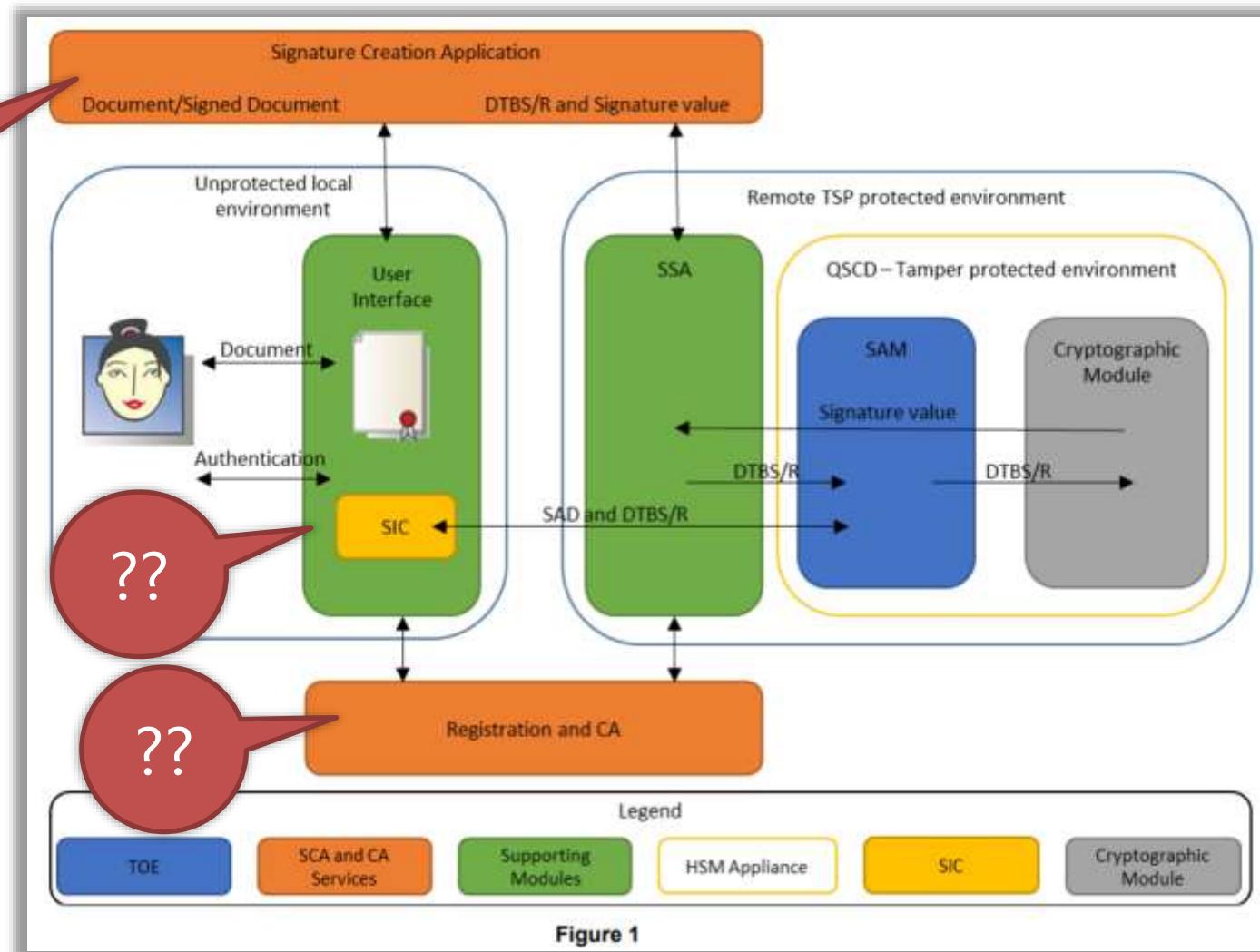
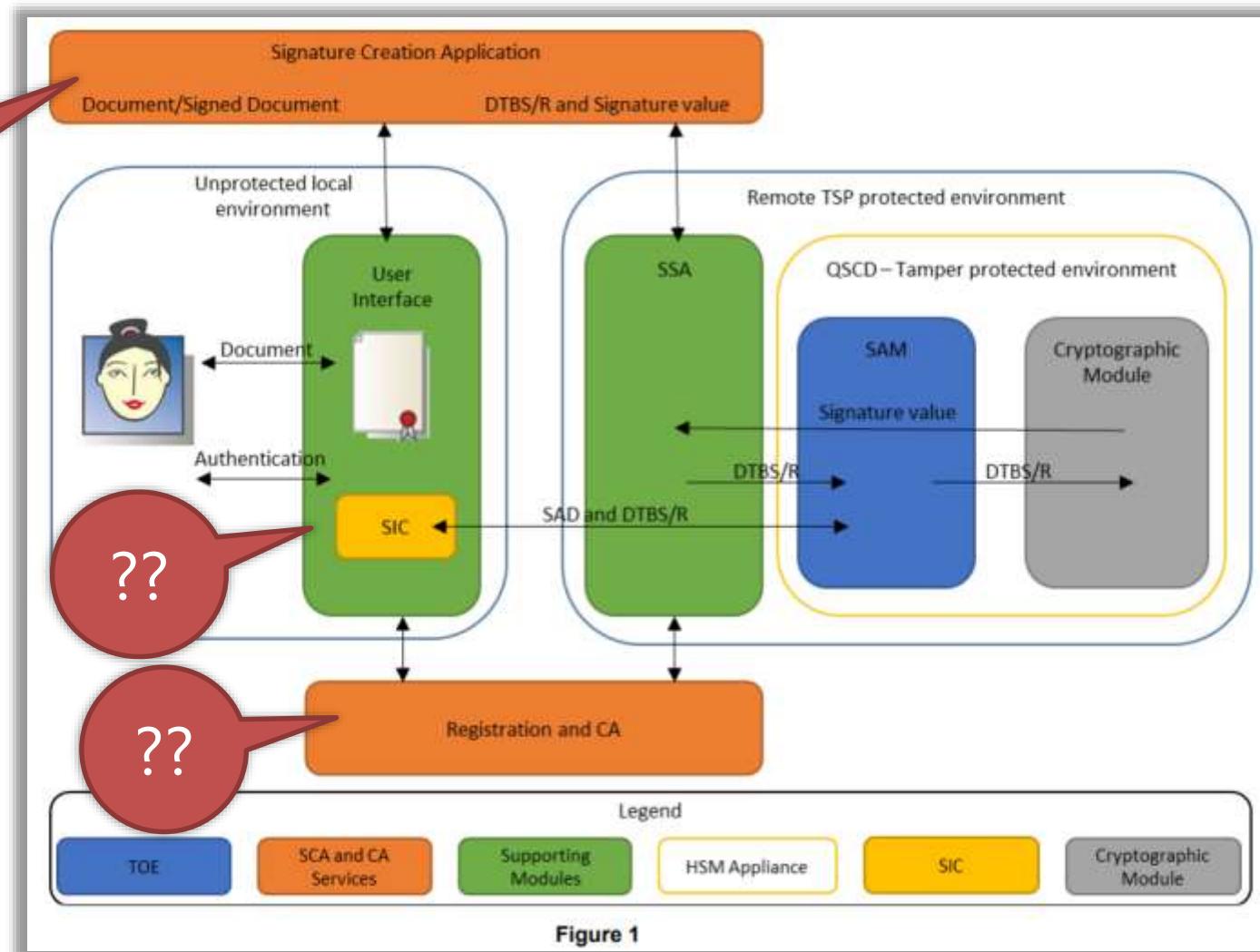


Figure 1

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/ansi-cc-pp-2018_02fr_pp.pdf

Future issues and examinations

JT2A



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/ansi-cc-pp-2018_02fr_pp.pdf

Industrie 4.0 and Society 5.0

超スマート社会の実現に寄与する信頼ベースのサービスや技術の検討と公開を目指す

国内外の関連団体との連携

- ガイドライン策定
 - ・セキュリティ機能要件
 - ・運用ガイドライン
 - ・サービスポリシー規程

Japan Trust Technology Association



Industrie 4.0 and Society 5.0.

People and things connect. Business and services are connected, making it more efficient and advanced. For this purpose, we consider technologies supporting the service platform.

Cooperation with related organizations

- **Remote signature guidelines**
 - Security functional requirements
 - operation guideline
 - service policy etc.

Japan Trust Technology Association

