資料９－３

リモート署名の検討

2019年8月8日

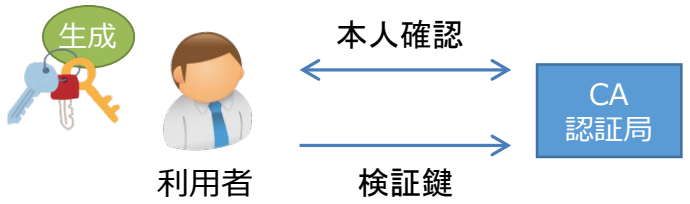
日本トラストテクノロジー協議会（JT2A）
小川 博久

1．現状のローカル署名とリモート署名の違い

現状（ローカル署名）

(1) CAが鍵ペアを生成

(2) 利用者が鍵ペアを生成

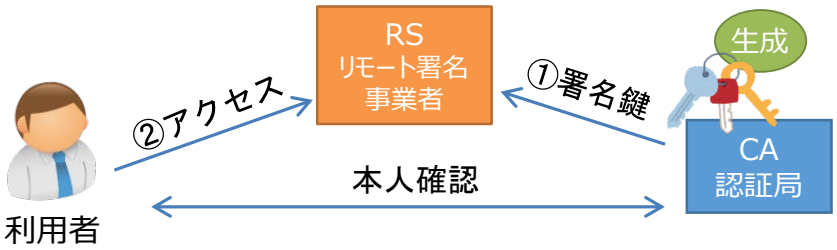


認定認証事業者の認定基準に規定

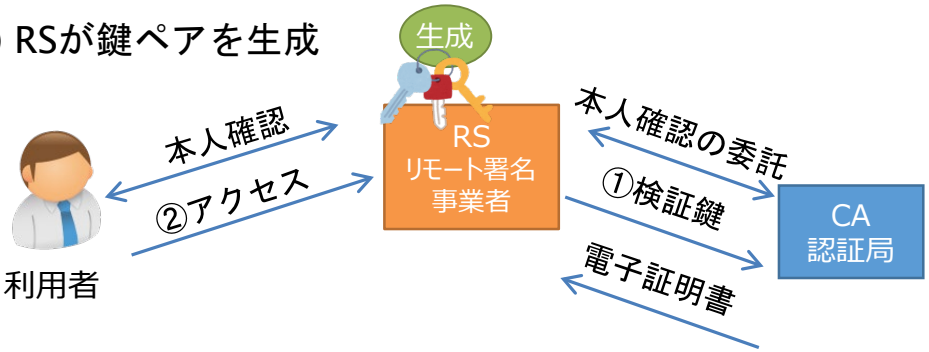
①利用者に対する署名鍵の安全な交付　　①利用者からの検証鍵の安全な取得

リモート署名

(1´) CAが鍵ペアを生成



(2´) RSが鍵ペアを生成



安全なリモート署名の基準に盛り込むべき要素

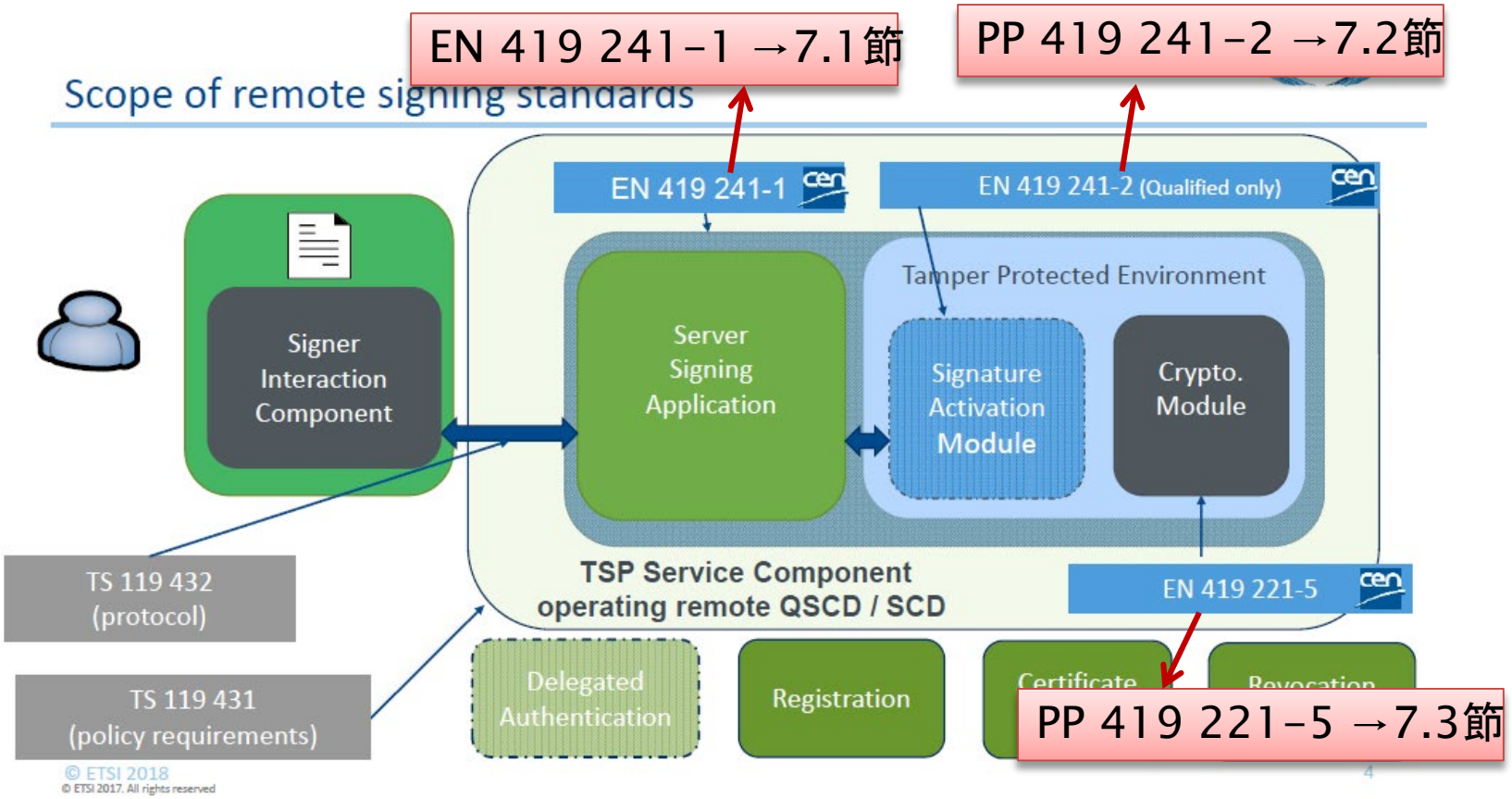
①署名鍵をRSに安全かつ確実に届ける　　①検証鍵をCAに安全に届ける

②署名鍵に利用者だけがアクセスして使える　　②署名鍵に利用者だけがアクセスして使える

JT2Aにて具体的基準のガイドライン化を検討中

２．リモート署名ガイドラインの章構成

2.EUのリモート署名の構成



Q1-8. セキュリティターゲット(ST)とプロテクションプロファイル(PP)について教えてください。
ST(Security Target)は、IT製品のセキュリティ機能について、その目的や対抗手段、想定される運用環境などを記載したセキュリティ基本設計方針書のようなものです。製品調達の際、このSTを読むことで対象製品が自らの環境や目的に合致しているかを判断できますし、同類製品をSTにより比較することもできます。
PP(Protection Profile)は、特定の分野の製品について必要とされる典型的なセキュリティ要件、環境などを記述した要求仕様書であり、STをより抽象的(実装非依存）にしたものとなっています。製品調達者が、PPという標準化された要件形式を用いることで、調達者や開発者などが共通の解釈をもつことができます。
一般的には調達者はセキュリティ要件としてPPを提示し、応札者はPPに準じたIT製品のSTを作成し、それに基づく評価を受けることとなります。

情報処理推進機構：情報セキュリティ：セキュリティ評価・認証に関するFAQ
https://www.ipa.go.jp/security/jisec/cc_tutorial/faq_index.html#IQ1-8

３．JT2Aのガイドラインの概要

リモート署名事業者は、利用者の署名鍵を預かることから“最低限”必要なセキュリティ対策、JT2Aが“推奨”するセキュリティ対策、欧州規格とのハーモナイズを“附帯”として記載している。

項目	署名鍵の生成・設置方法
要件化の目的	署名鍵データ自身の安全性、保管時の安全性を高める
最低限	• 署名鍵の生成可能 （HSM※1に限らない） • 署名鍵のインポート可能
推奨	• 署名鍵の生成可能 （HSMのみ可能であり、署名鍵の保管はHSMに限定） • 認定認証事業者など信頼できるCAからの署名鍵のインポートのみ可能
附帯	• 署名鍵の生成可能 （欧州の署名生成デバイスの評価・認証取得品※2のみ可能） • 署名鍵のインポート不可

※1: Hardware Security Moduleの略称。耐タンパ性を有する頑強なモジュール。
※2:署名生成デバイス（SCDev）の欧州規格。

3．JT2Aのガイドラインの概要

項目	署名鍵の活性化（認可）
要件化の目的	署名鍵のアクセスまでの確実性を高める
最低限	単要素認証 ※単要素認証の例； • パスワードのみ • 認証デバイスのみ • 生体認証のみ
推奨	複数要素認証必須 ※多要素認証の例； • パスワード＋二経路認証アプリ • パスワード＋ワンタイムパスワード生成アプリ • パスワード＋生体認証
附帯	複数要素認証に加え、署名鍵活性化モジュールの評価・認証取得※3が必要

※3:署名活性化を行うモジュール（SAM）の欧州規格（耐タンパな環境での設置が必須）。

- EUにおいては、「附帯」に記載の内容までを適格事業者の要件としているが、日本では、安全でかつ利便性が高いサービスが求められているため、認証を得るための条件は「推奨」の内容までとすることが適当と考える
- 逆にEU規格にないもので日本の基準に定める必要があるものとして署名鍵のインポートやCSR （ Certificate Signing Request、証明書署名要求）といった要素がある（詳細は次頁）

4 JT2Aガイドラインと EU規格との相違点①

■署名鍵のインポート

- EUの適格事業者は認証局がリモート署名事業者を兼ねている場合もあり、署名鍵のインポートに関する規定及びセキュリティ機能要件がない。
- 一方、日本では認証局とリモート署名事業者が別の主体の場合もあり、署名鍵のインポートをどのように行えば安全・確実といえるか、JT2Aガイドラインに規定する必要がある。
  - 例えば、インポートする際は、改ざん検知可能な通信を用いる等

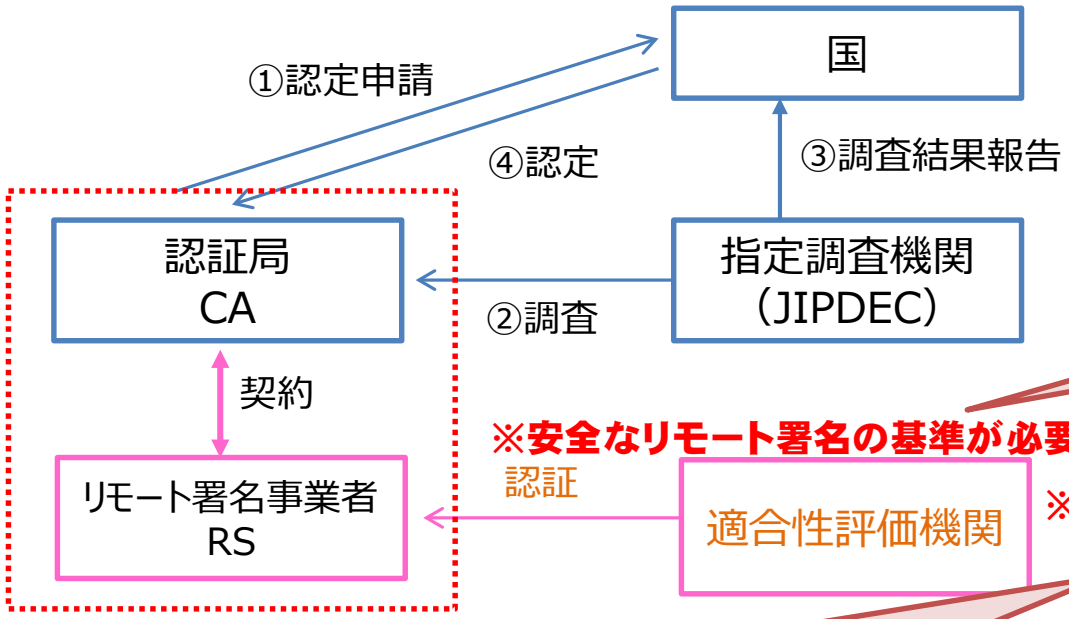
4 JT2Aガイドラインと EU規格との相違点②

■CSRの詳細化

- CSRとはCertificate Signing Request （証明書署名要求） のことであり、EUの規格では上記と同様の理由で詳細な規定及びセキュリティ機能要件がない。
- 一方、日本においてはCSRをどのように行えば安全・確実といえるか、JT2Aガイドラインに規定する必要がある。
  - 例えば、CSRを行う際は、改ざん検知可能な通信を用いる等

５．リモート署名に関する検討事項

○現在、認証局（CA）がローカル署名サービスを提供する場合については、
電子署名法に基づく国による認定制度がある。
○認証局（CA）がリモート署名事業者（RS）と契約しリモート署名サービスを提供する
場合について、電子署名法上の扱いを整理する必要。



● JT2Aガイドラインを2019年9月までに策定・公表予定
● ガイドラインを基に今後JIS化が必要

※適合性を評価する仕組み（評価機関）が必要

【参考】
現状では、リモート署名を用いた電子契約サービスについて、独自の審査基準に基づき適合性を評価する民間制度として、「JCANトラステッドサービス登録」がある。（次頁に概要）

● 将来的には、評価認証制度の国際標準への対応が望ましい
（例）
・ISO/IEC17025（試験所及び校正機関の能力に関する一般要求事項）導入
・ISO/IEC17065 （適合性評価-製品、プロセス及びサービスの認証を行う機関に対する要求事項）導入
・EN 319 403 （トラストサービスプロバイダの適合性評価機関に対する要求事項(欧州規格)） 等

参考：ＪＣＡＮ　トラステッド・サービス登録について

2017年度、欧州トラストサービスプロバイダのシステム運用・管理に係る審査基準やリモート署名の技術基準等を参考にしてJIPDECで作成した審査基準案について、同年電子契約ワーキンググループを設置し（構成員は、認証局ベンダー、電子契約ベンダー、弁護士、税理士、シンクタンク等）、有識者の意見等を集約して、2018年３月に審査基準（JCAN トラステッド・サービス登録（電子契約）–リモート署名版–）を作成の上、概要を公表している。

JIPDECが策定した基準に基づく、形式審査、文書審査、現地審査を経て、適合性を評価した結果を登録証として発行する。