

# 欧州におけるリモート署名環境に 関する調査

2021年3月26日  
富士通株式会社

- EUにおけるリモート署名の要件
- EUにおけるリモート署名の技術基準
- EUでのリモート署名規格におけるeシールの位置付け
- EUにおけるリモートeシールでの一括署名について
- EUにおけるリモートeシールの署名者の認証について
- EUにおけるリモート署名方式での認証要素の管理について
- EUにおけるeシールの失効に関する要件について

- 欧州ではeIDAS規則において適格電子署名をリモート署名方式で提供することが認められており、**その際にはリモート署名事業者が特定の管理・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かつ署名者単独の管理\***の下で使用されることを保証する為に、信頼できるシステムや製品を使用すべきであるとされている。
- このサービスを提供する事業者が**適格トラストサービスプロバイダ**でなければならないともされている。

\*単独の管理とは、そのリモート署名が本人の意思によって行われたことを保証する為に、サーバに保管されている署名者の秘密鍵が署名者本人の意思のみによって電子署名に利用されることを保証する仕組みであり、これによってローカル署名と同等の保証レベルを実現する。

## eIDAS規則 序文から引用

(52) 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、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、署名者の**単独の管理**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件を適用すべきである。

## ■ ETSI及びCENによるリモート署名の標準化

- ETSI TS 119 431-1 トラストサービスプロバイダのポリシー及びセキュリティ要件;パート1：リモートQSCD/SCDevを運用するTSPサービスコンポーネント  
上述の**特定の管理・運用セキュリティ手順**を規定している。
- CEN EN 419 241-1 サーバ署名をサポートする信頼できるシステム - パート1：一般システムセキュリティ要件  
上述の**信頼できる署名生成環境と署名者単独の管理**について規定している。

## ■ ETSI TS 119 431-1

- リモート署名生成装置を運用するサービスコンポーネントを実装するトラストサービスプロバイダに一般的に適用可能なポリシーとセキュリティ要件を三段階のレベルで規定している。
  - LSCP (Lightweight SSASC (Server Signing Application Service Component) Policy)
    - NSCPよりも低いリスクの取引に使用する為のポリシー
  - NSCP (Normalized SSASC Policy)
    - あらゆる種類の取引に対応する為のベストプラクティス
  - EUSCP (EU SSASC Policy)
    - NSCPに適格電子署名レベルを達成する為の追加の法的要件を加えたポリシー

## ■ CEN EN 419 241-1

- 署名者単独管理を実現するシステムの保証レベルとしてSCAL (Sole Control Assurance Level) を定義しており、SCAL1とSCAL2の2段階の要件を定めている。
  - SCAL1
    - 低いレベルの信頼性による署名者単独管理を実現する保証レベル
  - SCAL2
    - QES(適格電子署名、eシール)の要求する署名者単独管理を実現する保証レベル

# ETSI TS 119 431-1とCEN EN 419 24-1の対応関係及び リモート署名ガイドラインとの対応

## ETSI TS 119 431-1

### ポリシー及びセキュリティ要件

1. 運用規程及びポリシーに関する一般規定
2. TSPの運用
  - 2.1 公開及びリポジトリ
  - 2.2 署名鍵の初期化
  - 2.3 署名鍵のライフサイクル管理
  - .....
  - .....
  - .....
- 2.6 適合性評価
- 2.7 その他のビジネス及び法的事項
- 2.8 その他の規定

## CEN EN 419 241-1

### 一般システムセキュリティ要件

1. 署名者の認証
  - 1.1 電子識別手段
  - 1.2 認証メカニズム
  - 1.3 認証対象
2. 署名活性化データ
3. 署名活性化プロトコル
- .....
- .....
6. セキュリティ要件



例

【ETSI TS 119 431-1】

6.2.1 秘密(署名)鍵の生成

CEN EN 419 241-1 [3]のSRG\_KM.1.1項を適用する。

ETSI TS 119 431-1	CEN EN 419-241-1	リモート署名ガイドライン
LSCP	SCAL1	レベル 1
NSCP		レベル 2
EUSCP	SCAL2	レベル 3

\*レベル2(推奨要件)は、我が国の認定認証業務に基づいてリモート署名サービスを提供する際に満たすべき基準として定めており、その大部分はNSCP、EUSCPと同等である。EUSCPとの違いは署名鍵の活性化について第三者評価を取得したモジュール(SAM、Signature Activation Module)の利用を義務化していない点にある。

- ETSI TS 119 431-1はリモート署名サービスのポリシー及びセキュリティ要件であるが、ここでの署名サービスは技術としてデジタル署名サービスを示しており、**電子署名とeシールの両方がサポート**されている。ETSI TS 119 431-1の4.1項には以下の記載がある。

## ETSI TS 119 431-1 4.1項

本文書には、参照によりCEN EN 419 241-1 [3]要件が組み込まれている。CEN EN 419 241-1 [3]は、単独管理の保証レベルを定義している。「単独管理」という用語は、規則(EU)No 910/2014 [1]で定義されている**電子署名にのみ要件が適用されることを意味するものではない。要件は、必要な変更を加えてeシールに適用できる。**言い換えれば、読者は、CEN EN 419 241-1 [3]の箇条5.3で説明されているように、「単独管理」という用語を「管理」に置き換えることができる。

- CEN EN 419 241-1においても電子署名とeシールについて必ずしも同じ信頼レベルが署名鍵の管理において期待されていないとしながらも、本規格はリモート環境化におけるデジタル署名システムについての技術的な要件をまとめたものであり、**本規格における署名者は自然人と法人の両方を対象としている**ことが示されている。

## CEN EN 419 241-1 5.3項

**デジタル署名は、電子署名又はeシールに使用することができる。**

署名鍵のコントロールの信頼のレベルは、デジタル署名がシールを表現する場合は、署名を表現するために使用されるときと必ずしも同じであることを期待されない。

本規格に従って生成されるデジタル署名は、自然人又は法人の管理の下で生成することができる。

**署名者という用語は、本規格においては自然人又は法人を対象として使用されている。**

- 適格電子署名/eシールにおいて個々の電子データ/文書ではなく、多数のデータ/文書に対する一括署名方式を認めるかについては加盟国で対応が分かれています。
- ETSIやCENの技術規格上では：
  - SCAL1は署名者の認証後、SSA(サーバ署名アプリ)が一定期間/一定の署名回数において署名者の秘密鍵を利用して署名することができる。
  - SCAL2では複数の署名対象文書/データに一括で署名指示することのみが認められている(SCAL1のやり方は認められていない)
- なお、ローカル電子署名/eシールにおいては署名対象及び秘密鍵共に署名者の管理下にあり、その際の一括署名に関する特段の規定はない。

## ■ SCAL1

- 鍵認可は単要素認証(必要な認証の保証レベルは低)
- 利用認証で鍵認可を行ってもよい
- SAM(署名活性化モジュール)の実装は不要

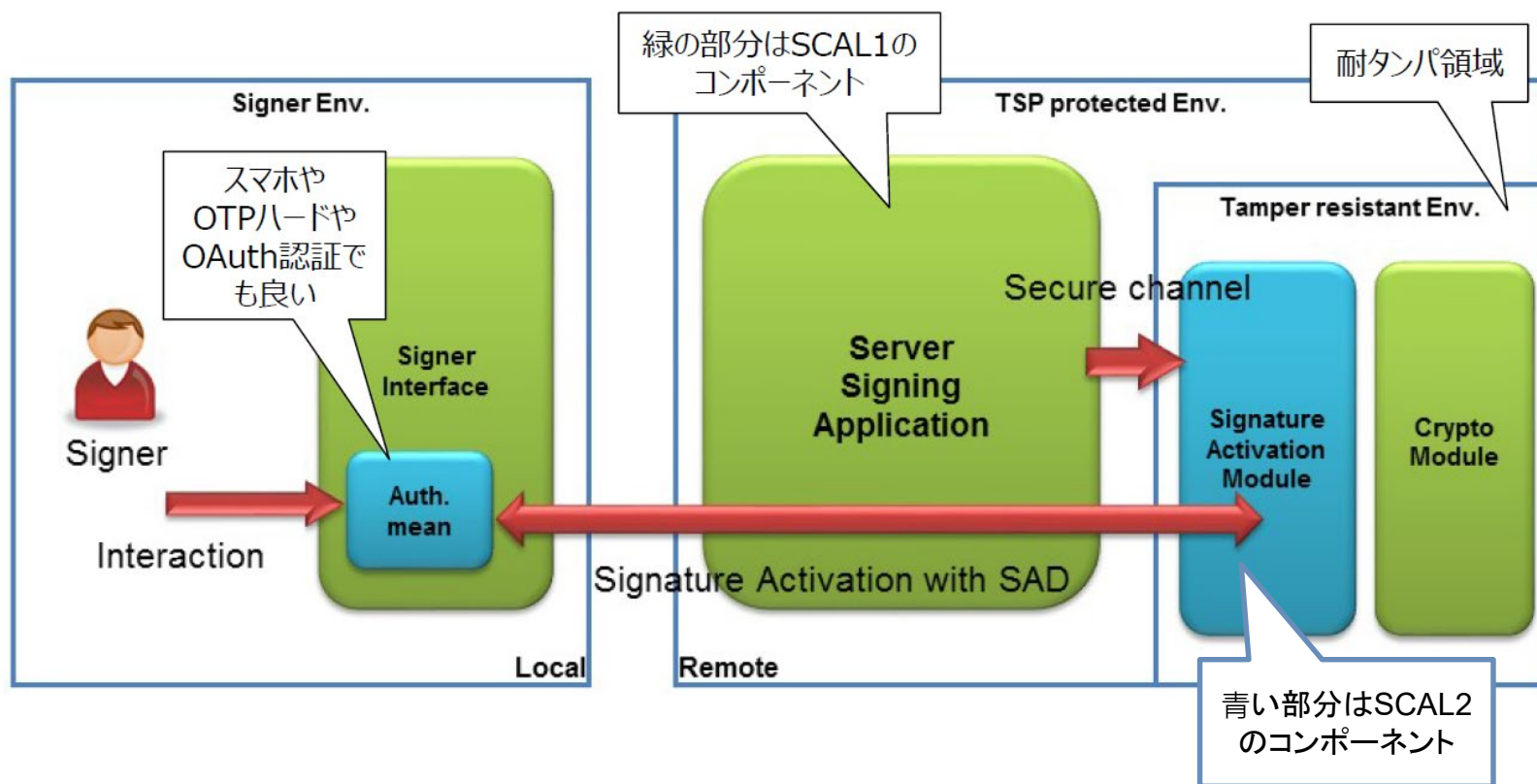
## ■ SCAL2

- 鍵認可は複数要素認証(必要な認証の保証レベルは中)
- 利用認証と鍵認可を個別に実施
- SAMを用いた署名者の認証が必須
  - SAMはコモンクライテリアEAL4+の認証製品

\* eIDAS規則ではeIDに関する保証レベル(低、中、高の3段階)を定めており、その要件は実施規則EU2015/1502で詳細化されている。



- SCAL1はサーバー署名アプリケーションがユーザ認証に基づいて署名鍵を活性化することを認めている一方で、SCAL2では署名鍵の活性化を技術的に署名者だけが実施できることを保証する為にSAM(署名活性化モジュール)を耐タンパ領域に実装することを求めている。
- SAMに対してはISO/IEC 15408(コモンクライテリア)評価が要求されている。



出典: CEN EN 419 241-1

## ■ 認証要素(PINコード等)の管理

- 認証要素の管理は法人の責任内での管理が求められているため、法人(eシールの利用者)が信用する第三者(或いはサービス)が管理することも、当該法人のリスクとなるが可能と思われる。
- 一方、リモート署名サービス事業者が、法人の認証要素を管理することは認められてないと思われる。(秘密(署名)鍵を管理しているため)


## ■ 認証局側の要件

### ■ 失効リクエストの検証(真偽、要求者及びソース等)

- 認証局は、以下をCPSの一部として規定しなければならない。
  - 誰が失効を要求できるか  
基本的には法人と認証局間で事前の合意が必要
  - 要求方法  
パスワードやOTPの利用による認証等による要求者の本人確認

### ■ 失効リクエストからステータス情報の反映までは24時間以内

### ■ 失効リクエストが有効であると確認してから実際のステータス情報の反映までは60分以内



**FUJITSU**

shaping tomorrow with you