令和5年度
電子委任状の普及及びリモート電子署名基準等に関する調査研究業務

最終報告書
（概要版）
リモート電子署名基準の検討

2024年3月22日

一般社団法人デジタルトラスト協議会
リモート電子署名基準調査TF

報告書目次

1. 背景と目的

近年、リモート署名が電子契約サービスの基盤技術として利用され、新型コロナウイルスの感染拡大に伴うリモートワークの普及に後押しされ急速に拡大している。
※リモート署名：一般に、事業者のサーバーに利用者の署名鍵を設置・保管し、利用者がサーバー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ー上で電子署名を行うこと（経産省平成27年度、電子署名・認証業務利用促進事業調査報告書での定義から抜粋）

上記調査報告書では次のようにも言及されている。
「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った。
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。」

電子署名については、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。以下「電子署名法」）に基づく認定を受けている認証業務が9業務あるが、いずれもローカル署名向けであり、リモート署名については前述のようにニーズが高まりつつある一方で、電子署名法上の認定基準が存在しないことから、基準の策定に向けた検討を行う必要がある。

上記を踏まえ、本調査研究業務ではリモート署名サービス（調達仕様書のリモート電子署名サービスと同義）の評価基準の検討を実施した。

2. リモート署名サービスの評価基準の検討

2.1 リモート署名サービス評価基準の事例調査

国内外のリモート署名サービスに関する基準を調査し、リモート署名サービスの評価基準を検討するに当たって以下の通り整理した。

国内のリモート署名サービスに関連するガイドライン等は、ETSIの関連規格を選択的に参照して構成されており、すべての要件を包含しているわけではない。

ETSIの関連規格では、リモート署名事業者の署名生成装置で鍵ペアを生成する前提となっており、認証局で鍵ペアを生成する場合の基準がなく、日本の事情にそぐわない部分がある。また、ETSIの関連規格では規定されていないものの、日本として追加すべき項目があれば付け加える必要がある。

ETSI、CENのプロテクションプロファイル関連規格は、現時点では日本としての類似規格を別途作成する必然性が無いと思われるため＊、一旦、それを参照するに留める。

＊国際的な標準の中で検討されており各国ともに共通で利用されているため。

2. リモート署名サービスの評価基準の検討

2.2 国内のサービス事業者へアンケート調査

期間	2023年9月19日～9月29日
アンケート依頼事業者	国内サービス事業者全26社
	リモート署名サービス事業者（RSSP） 8社
	電子契約サービス 10社
	認証局 7社
	HSMベンダ 2社
有効回答数	14社

アンケート結果に基づき、リモート署名サービスの評価基準を検討する際に必要と考えられる事項を以下のとおり整理。

リモート署名サービスの基準に基づき国の認定を受けたいというニーズが高い。
リモート署名サービスの基準は、１つの保証レベルだけではなく、簡易レベル、電子署名法の認定認証業務と同等として扱うことのできるレベル、国際相互運用が可能なレベルが求められている。
リモート署名事業者の多くは、電子契約などアプリケーションサービスをリモート署名サービスと併せて提供している。

【参考】アンケート内容①

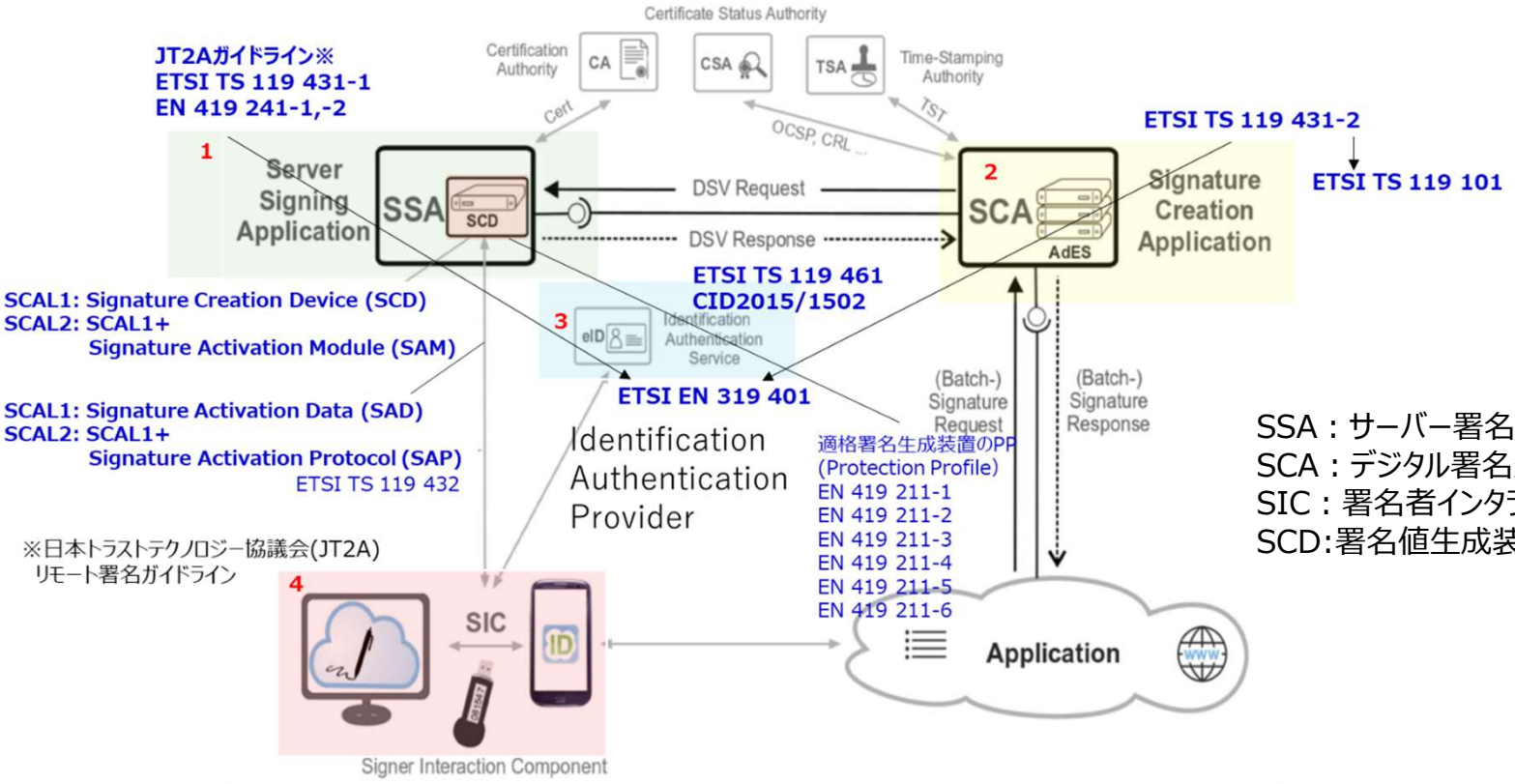
1. 提供機能
    1-1 ユーザ（サービス利用者）の秘密鍵を保管し、電子署名を行っているサービス（リモート署名機能を含むサービス）を提供しているか
    1-2自社のサービス名称
    1-3 他社サービスを利用している場合にはそのサービス名称
    1-4 リモート署名機能に付随して提供している機能
    1-5 提供している署名フォーマットの形式
    1-6 リモート署名アプリケーションを提供している場合：提供しているサービス内容
    1-7 電子証書発行サービスを提供している場合：発行している証明書
2. 準拠性
    2-1 日本トラストテクノロジー協議会（JT2A）が公開している「リモート署名ガイドライン」を参照しているか
    2-2 リモート署名ガイドラインにおける「レベル分類」のいずれを提供しているか
    2-3 リモート署名ガイドラインにおける「重要項目におけるセキュリティレベル」の鍵生成（署名鍵の生成）、鍵インポート、鍵保持、鍵認可（署名鍵の活性化）の 4つについていずれのレベルを提供しているか
    2-4 提供しているサービスがリモート署名ガイドラインのいずれの認証モデルに該当するか
3. CSC準拠
    3-1 Cloud Signature Consortium（CSC）が規定している仕様に準拠したAPIを提供しているか
4. 秘密鍵の管理
    4-1 秘密鍵は、Hardware Security Module(HSM)に格納し管理しているか、HSMに格納し管理している場合の該当するセキュリティレベル
    4-2 HSMに格納している場合、使用しているHSMが受けている認定の種別
    4-3 利用者の秘密鍵に対してどのようなセキュリティ対策を施して管理されているか
5. SAM（署名活性化モジュール）
    5-1 署名する際に署名鍵の活性化を行う認証機能において貴社サービスで実装されている方式
    5-2 署名生成装置について、欧州では認証制度があるが、わが国でも同等な認証制度が必要か
    5-3 鍵の活性化時の本人認証レベルについて、NIST SP800 63-3に定義されているAuthenticator Assurance Level（AAL）のうち、最も近いもの
    5-4 提供している認証方式

【参考】アンケート内容②

6. 認定
    6-1　取得済みのセキュリティなど基準および外部監査の種別
7. 身元確認
    7-1　【リモート署名アプリケーション（電子契約サービス等）を提供している場合】サービス利用者の身元確認方法
    7-2　【リモート署名アプリケーション（電子契約サービス等）を提供していない場合】リモート署名サービスにおけるサービス利用者の身元確認方法
    7-3　身元確認レベルについて、NIST SP800 63-3に定義されている Identity Assurance Level（IAL）のうちどれか
8. 証明書発行の認証局
    8-1　連携可能な認証局について、認証局の管理主体
    8-2　連携可能な認証局について、認証局が登録されている認証局ストア等について
    8-3　証明書発行先
9. 現状のサービス提供について
    9-1　課題と考えられること
    9-2　事業継続上のリスク
    9-3　セキュリティ上の懸念点
10. リモート署名サービスの認定制度について
    10-1　リモート署名サービスの認定制度について
    10-2　上記の回答の理由
    10-3　リモート署名サービスの認定制度ができたら認定を受けたいか
    10-4　受けたい認定のレベル
11. 要望・実績
    11-1　現在検討しているリモート署名基準に対して考慮してもらいたい点
    11-2　利用者（エンドユーザ）について

3. リモート署名サービスの評価基準の作成①

2.1 の評価基準の事例調査の結果を踏まえ、リモート署名サービスの評価基準案を作成。ETSI TS 119 432で示されたリモート署名サービスのアーキテクチャーと、国内外のリモート署名サービスに関する基準は下図のとおり対応付けられる。



SSA：サーバー署名アプリケーション
SCA：デジタル署名生成アプリケーション
SIC：署名者インタラクションコンポーネント
SCD:署名値生成装置等（SCDev）

3. リモート署名サービスの評価基準の作成②

構成要素とリモート署名サービス基準案の作成対象

1. サーバー署名アプリケーション（SSA: Server Signing Application）	対象
署名者の署名鍵を内蔵し署名演算を実施する署名値生成装置等（SCDev）を運用し、署名者の直接の指示やSCAにより経由された指示により、署名者の認証情報、署名に用いる署名鍵を特定する情報及び署名対象データのハッシュ値などを含む署名活性化データに基づきデジタル署名値を生成するアプリケーション。デジタル署名値の生成に使用する署名鍵の生成、保持、ライフサイクル管理、使用などの機能を有する。署名者視点から見た場合、署名値生成装置等はリモート環境に設置されるため、ここで利用されるSCDevをリモート署名値生成装置（リモートSCDev）と呼ぶ場合がある。SSAの機能を提供するサービスをリモート署名サービス、サービスを提供する業者をリモート署名サービス事業者（RSSP）と呼ぶ。	
2. デジタル署名生成アプリケーション（SCA: Signature Creation Application）	対象
CAdES/XAdES/PAdES等、標準フォーマットに準拠したデジタル署名を構築するアプリケーション。署名者からの署名リクエストを受け、SSAに署名者、署名鍵、署名対象文書等を特定するための情報（署名活性化データ）を引き渡し、SSAによって生成されたデジタル署名値を受信、利用してデジタル署名を生成する機能を有する。SCAの機能を提供するサービスをデジタル署名生成サービス、そのサービスを提供する事業者をデジタル署名生成サービス事業者（SCASP）と呼ぶ。	
3. 本人認証サービス（IAS: Identification Authentication Service）	—
利用者の身元確認を実施し、必要に応じて電子識別手段（認証用秘密鍵やこれを格納するICカードなど）を発行し、オンラインで本人認証や認可を行うサービス。SSA内に設置する場合と、外部事業者のサービスを利用する場合がある。	
4. 署名者インタラクションコンポーネント（SIC: Signer Interaction Component）	—
署名者がSCAやSSA等を利用してデジタル署名の生成を指示するためのユーザーインターフェースを提供するコンポーネント。	

3. リモート署名サービスの評価基準の作成③

リモート署名サービスの評価基準の作成方針

リモート署名サービスの各コンポーネントの中で、リモート署名事業者（RSSP）及び、デジタル署名生成サービス事業者（SCASP）に対して適用する。		
3レベルの保証レベルを想定した評価基準を示す。		
	Level 1	簡易なレベル
	Level 2	電子署名法の認定認証業務と同等として扱うことのできるレベル
	Level 3	国際相互運用が可能なレベル
要求項目毎に、適用すべきレベルの欄に○印をつけて示す。		
リモート署名サービス評価基準の文書構成は次頁の通り。		

3.1 リモート署名サービスの評価基準の文書構成

(1) リモート署名サービスの評価基準概説

リモート署名サービスの評価基準の全体像を説明。用語定義、記号・略語、参照規格を集約。

(2) リモート署名生成装置等を運用するTSPの一般ポリシー要求事項/解説（ETSI TS 119 431-1）

リモートSCDevを操作するサーバー署名アプリケーションサービスコンポーネント（SSASC）を管理・運用するTSPに対して適用されるポリシーとセキュリティ要件。要件の一部は(3)を引用。ポリシーレベルは、署名者の鍵ペアをSCDevの中で生成する際の３つのポリシー（簡易的な”LSCP”、標準的な”NSCP”および欧州の適格レベルを満たす”EUSCP“）に加え、署名者の鍵ペアを認証局が生成してSCDevにインポートするポリシー”LSCP+”を規定。

(3) サーバー署名アプリケーションサービスの一般セキュリティ要求事項/解説（EN 419 241-1）

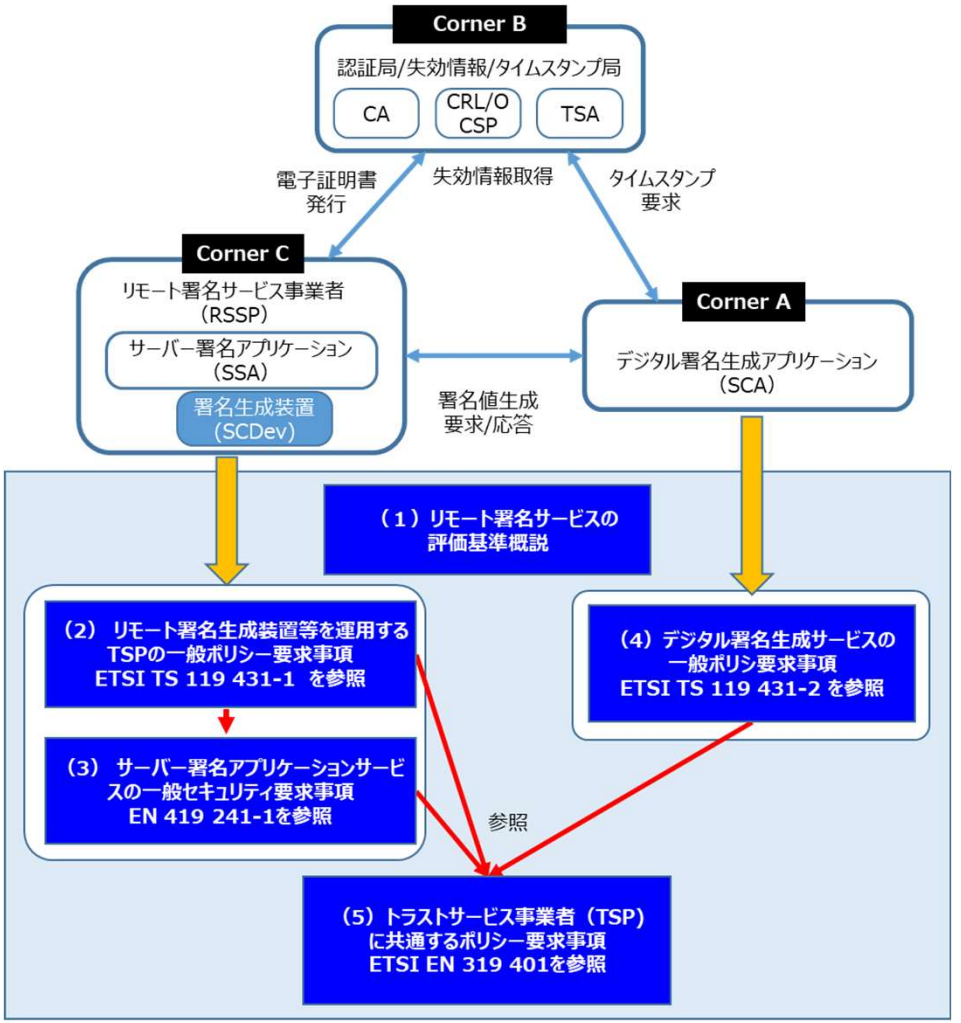
サーバー署名アプリケーションサービスを提供する信頼できるSSASCに対するセキュリティ要件を規定。SSASCは、承認された署名者の制御下でSCDevを使用するため、認可された署名者による独占的な制御（単独制御）の保証が必要。単独制御レベルをSCAL（Sole Control Level）と定義し、信頼度によりSCAL1（低）とSCAL2（高）の2つの基準を規定。

(4) デジタル署名生成サービスの一般ポリシー要求事項/解説（ETSI TS 119 431-2）

デジタル署名の生成をサポートするサービスコンポーネント（SCASC）及び、SCASCを管理・運用するサービスプロバイダー(SCASP)のポリシー及びセキュリティ要件を規定。

(5) トラストサービスプロバイダーに共通するポリシー要求事項/解説（ETSI EN 319 401）

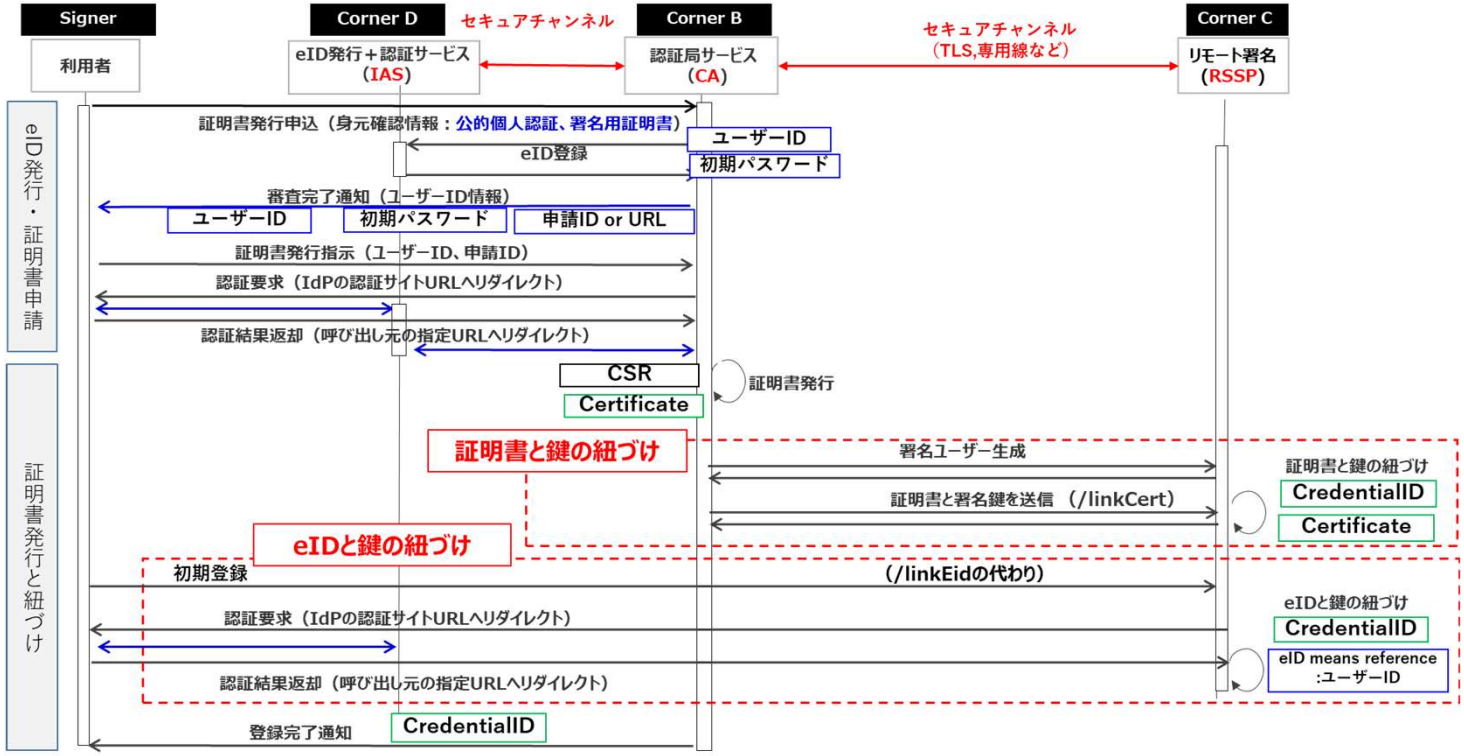
TSPの種類を問わず、TSP の管理及び運用の実施に関する一般的なポリシー要件を規定。特定の種類のTSPについては、別の文書によって評価基準、要求事項等が追加される。



4. 電子署名法の認定認証業務におけるリモート署名サービスの利用検討

電子署名法の認定認証事業者がリモート署名サービスを利用する場合に現在の認定基準に加えて必要となる事項を整理し、電子署名法の施行規則等の改定案の検討を行い、電子署名法モダナイゼーションTFに素案を提示、合同で改定案の作成を行った。改定案については電子署名法モダナイゼーションTFの報告書に記載した。

検討にあたり、前提として考慮が必要と考えられる、各ステークホルダーの役割、リモート署名サービスの運営形態（ビジネスモデル）、および利用申請からサービス開始までの登録フローを整理。例として、CA、IAS、RSSPが別会社の場合の登録フローを示す。



5. 参照規格

■国内

① 日本トラストテクノロジー協議会（JT2A） リモート署名ガイドライン

② JT2A リモートｅシールガイドライン（案）

③ JT2A 民間電子サービスにおける真正性保証の解説書

④ 一般財団法人日本情報経済社会推進協会（JIPDEC） リモート署名サービスの審査基準（案）-20230217

⑤ JIPDEC トラストサービスプロバイダの共通基準（案）

⑥ 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

⑦ （一社）OpenID ファウンデーション・ジャパン 民間事業者向けデジタル本人確認ガイドライン

⑧ 電子署名法施行規則、指針等の関連条項

■国外

⑨ ETSI EN 319 401 General Policy Requirements for Trust Service Providers

⑩ EN 419 211 Protection Profile for QSCD（適格署名生成装置）

⑪ EN 419 241-1 サーバー署名の一般セキュリティ要求
Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

⑫ EN 419 241-2 サーバー署名で用いる適格署名生成装置のProtection profile
Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

⑬ EN 419 221-5 トラストサービス事業者が用いる暗号モジュールのProtection Profiles
Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

⑭ ETSI TS 119 431-1 リモートQSCD/SCDev のポリシ要求事項
Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

⑮ ETSI TS 119 431-2 AdES digital signature creationを提供するTSPのポリシ要求事項
Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (remote signing)

⑯ ETSI TS 119 432 Protocols for remote digital signature creation

⑰ ISO/IEC 27002 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls