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（詳細版）
リモート電子署名基準の検討（案）

目次

1. 総則

1.1 本評価基準の位置づけ

本評価基準は、リモート署名サービスの評価基準を定めるものである。本書では、1.4 節の図 1 で示すリモート署名サービスを構成する独立した複数のコンポーネントに対してそれぞれの要求事項を定めているため、評価基準は複数の文書から構成される。また、電子処方箋におけるリモート署名サービスのシステム構成と、図 1 との関係を同節の図 2 にて解説する。

1.2 本書のスコープ

本書は、リモート署名サービスを運営するトラストサービスプロバイダー（TSP）に対して、一般的に適用されるポリシーとセキュリティ要件を示し、これに基づいてリモート署名サービスの要件を規定した。なお、トラストサービスやリモート署名サービスのサービスコンポーネントを提供する事業者をトラストサービスプロバイダー（TSP）と呼ぶ。特にリモート署名サービスを提供する事業者（TSP）は下記に記載するサーバー署名アプリケーション（SSA）及びリモート署名生成装置（リモート SCDev）を運営する事業者を指し、略称として RSSP（Remote Signature Service Provider）という。

本書の規定は 1.4 で示すリモート署名サービスを構成する以下の2つのサービスコンポーネントのいずれにも適用される。

・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）
　署名者に代わってデジタル署名値を生成するサーバー署名アプリケーション（SSA）を管理・運用するサービスコンポーネント。
・デジタル署名生成アプリケーションサービスコンポーネント（SCASC）
　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を管理・運用するサービスコンポーネント。

1.3 本書の目的

本書は、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）、およびデジタル署名生成サービスコンポーネント（SCASC）のいずれか、または両方を提供する TSP が信頼できることを評価する適合性評価の基礎として、独立した組織が使用することを目的とする。

1.4 リモート署名サービスのアーキテクチャー

リモート署名サービスとは、リモート署名事業者のサーバーに署名者の署名鍵を設置・保管し、署名者の指示に基づきリモート署名サーバー上で自ら（署名者）の署名鍵で電子署名を行うサービス[1]であり、下記のアプリケーションから構成される。

① サーバー署名アプリケーション（SSA: Server Signing Application）
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、デジタル署名値を生成するアプリケーション。SSA は、署名者の直接の指示やデジタル署名生成アプリケーション（SCA）により仲介された指示により機能する。また、SSA は、署名者の認証情報や署名に用いる署名鍵を特定する情報、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。 SSA は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、リモート署名値生成装置等と呼ぶが SSA 視点では自らが運用するため“リモート”を省略し署名値生成装置等と記載する。。SSA は、署名対象データのハッシュ値に基づいて生成されたデジタル署名値を署名者または次の②に記載するデジタル署名生成アプリケーションに配信することを目的とする。

[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」より

② デジタル署名生成アプリケーション(SCA: Signature Creation Application)
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取り、SSA に署名者、署名鍵、署名対象文書等を特定する情報(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利用してデジタル署名を生成する機能を有する。

③ 本人認証サービス(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 カードなどのデバイスなど)を発行し、オンラインで本人認証(Authentication)や認可(Authorization)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。

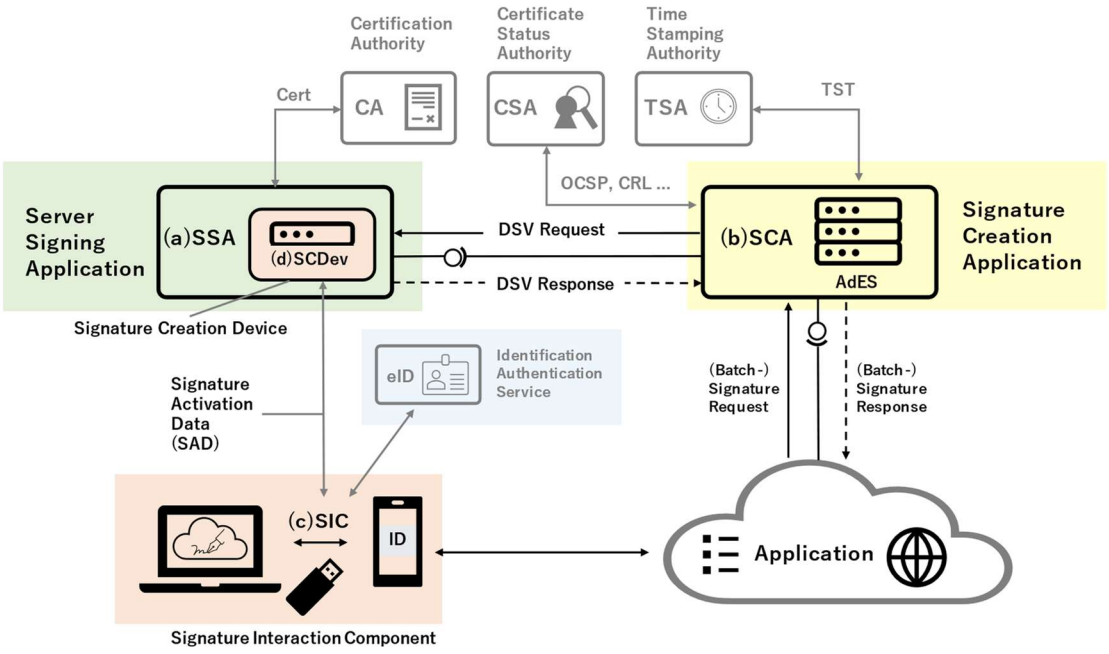


図1 リモート署名サービスのアーキテクチャー
(ETSI TS 119 432 V1.1.1 Figure2 を基に作成)

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

上記の独立したアプリケーション(機能群)を実装するコンポーネントが事業者によりサービスとして提供される場合にはサービスコンポーネント(SC)と呼ぶ。また、それぞれのサービスコンポーネントは事業者により、単独または、複数組み合わせて提供される場合がある。このようなサービスコンポーネントを提供する事業者をサービスプロバイダー(SP)と呼び、ここで対象とするサービスプロバイダーは信頼ある第三者機関として一定のトラストサービスプロバイダーの要件を満たす必要がある。本基準群は SC および TSP の要件を定めるものであり、SC および TSP を対象として本基準群への適合性が評価される。

1.4.1 各コンポーネント提供主体の関係性と役割

リモート署名サービスの各コンポーネントと認証局（CA）および電子識別手段を発行し本人認証サービスを提供する主体となる IAS（Identification Authentication Service）の責任範囲と関係性を以下に整理する。

本人認証サービス（IAS）
電子識別手段(eID 手段)を発行し、当該電子識別手段による本人認証サービスを提供する。ID プロバイダーと言うこともある。申請者本人と鍵の認証に使用する電子識別手段の紐づけに責任を持つ(SHALL)。申請者の身元確認を行うべきである（SHOULD)。

認証局（CA）
本書では、SSA で保持する利用者の署名鍵に対応する公開鍵証明書を発行する認証局を指す。申請者の身元確認と公開鍵証明書の記載内容、および公開鍵と秘密鍵の紐づけに責任を持つ（SHALL)。IAS の身元確認の結果を利用しても良い（MAY)、また、その他の利用者の属性を確認して公開鍵証明書に記載しても良い（MAY)。

サーバー署名アプリケーション（SSA）
前節で述べた、利用者の署名鍵を保持しデジタル署名値を生成するアプリケーション。署名者の署名鍵と IAS が発行する電子識別手段の紐づけに責任を持ち（SHALL)、署名者のみが当該署名鍵を用いて電子署名を行うことを保証する。

■各サービスの提供パターン
上記の各サービスは複数の組織により提供することも考えられ、以下のような提供パターンがあり得る。

① SSA、CA、IAS がそれぞれ別の組織で提供される場合
② CA、SSA が同一組織で提供され、外部の IAS を利用する場合
③ CA、IAS が同一組織で提供され、外部の SSA を利用する場合
④ SSA,IAS が同一組織で提供され、外部の CA を利用する場合
⑤ SSA、CA、IAS を同一組織で提供する場合

プレーヤー	提供サービスの役割分担のパターン				
	①	②	③	④	⑤
サーバー署名アプリケーション（SSA）	A 社	A 社	A 社	A 社	A 社
認証局（CA）	B 社	A 社	B 社	B 社	A 社
本人認証サービス（IAS）	C 社	B 社	B 社	A 社	A 社

■署名者の鍵ペア生成のパターン

署名者の鍵ペア生成や SSA への署名鍵の登録のパターンは以下が考えられる

（1） CA が SSA の署名値生成装置等（SCDev）を利用して鍵ペア生成
（2） 署名者が SSA の SCDev を利用して鍵ペア生成
（3） CA が鍵ペア生成し SSA に送信
（4） 署名者が保持・管理する署名鍵を SSA に送信

本基準では、SSA が保持、運用する署名鍵が SSA の外には存在せず、署名者本人のみが当該署名鍵を利用できることを保証するため、同じ署名鍵が SSA 以外に存在する可能性が生じる（4）の方式は扱わ

ないこととする。

1．4．2 利用登録のフロー(On-boarding)

「図1リモート署名サービスのアーキテクチャー」を基に、それぞれのコンポーネントにデジタル署名生成アプリケーションを Corner A、反時計まわりに Corner B、C、D とし、各コーナー間で行う処理の概要を図2に示す。

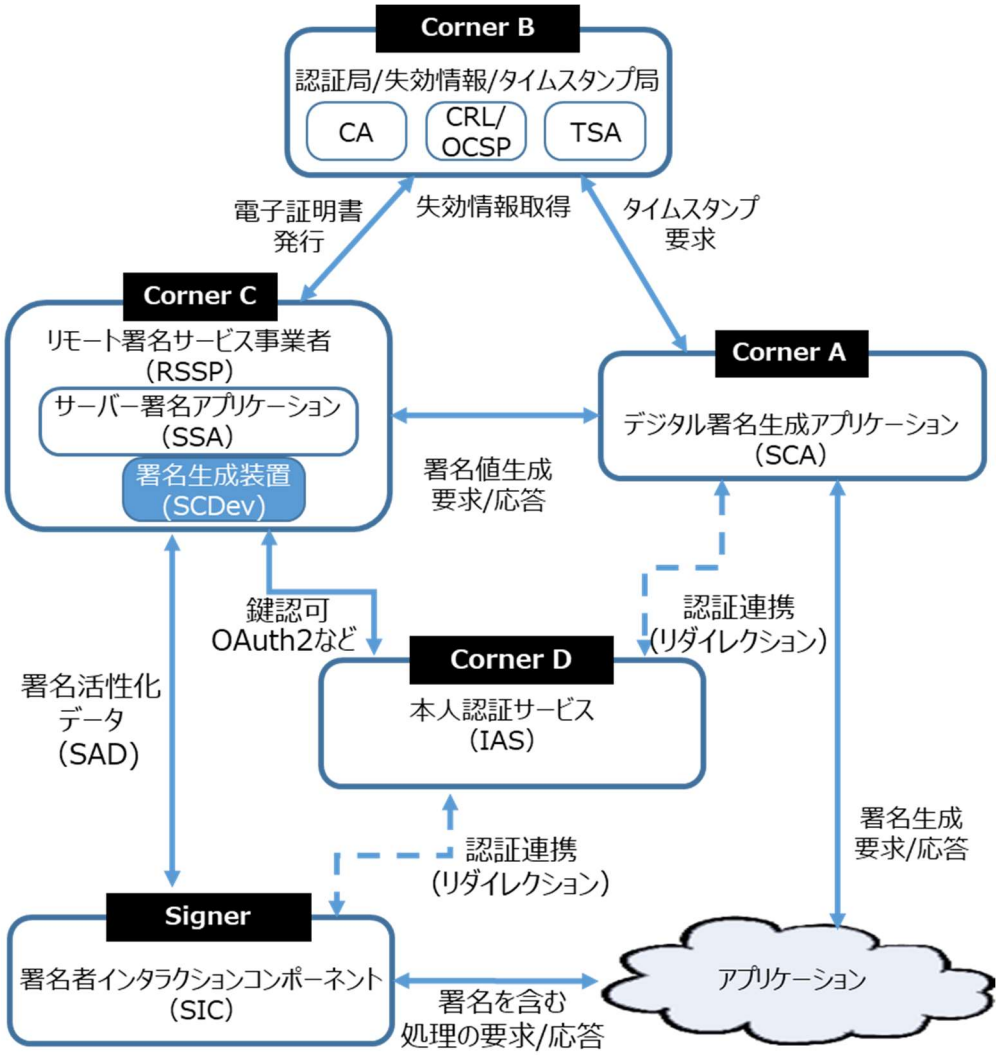


図 2 リモート署名サービスを構成する各コンポーネント間の処理概要

署名者がリモート署名サービスの利用申し込みを行い、登録が終了するまでのエンロールメントプロセスについて代表的なシーケンス図を前節の署名者の鍵ペア生成のパターン別に示す。いずれの場合も SSA と CA は連携に関する事前合意があり、利用者は CA へ電子証明書の利用申請を行う際に CA が連携する SSA の1つを指定することが前提となる

(1) CA が SSA の署名生成装置(SCDev)を用いて利用者の鍵ペア生成を行う場合の例

① 利用者は、リモート署名で使用する電子証明書の発行を認証局に利用申請する。(認証局が定める身元確認書類、電子署名済みの電子文書等を添える)
② 認証局は身元確認後、申請者本人に対し電子識別手段を発行する。外部の IAS(本基準で認められたものに限る)や当該 SSA から当該申請者に発行された電子識別手段を用いても良い。

③ 認証局は②の電子識別手段を用いて利用者の当人認証が成功したことを確認した後に、SSA へ鍵ペア生成依頼を送信する。
④ SSAは申請者の鍵ペアを生成し、当該電子識別手段と当該署名鍵を紐づける。この際、SSA が事前に生成した署名鍵と紐づけても良い。
⑤ SSA は当該公開鍵に当該署名鍵で署名を付した証明書発行要求(CSR:Certificate Signing Request)を認証局に送信する
⑥ 認証局は電子証明書を発行し、安全、確実に SSA へ送信する。
⑦ SSA は受領した電子証明書と対応する署名鍵の紐づけを行い、利用者に完了を通知する。

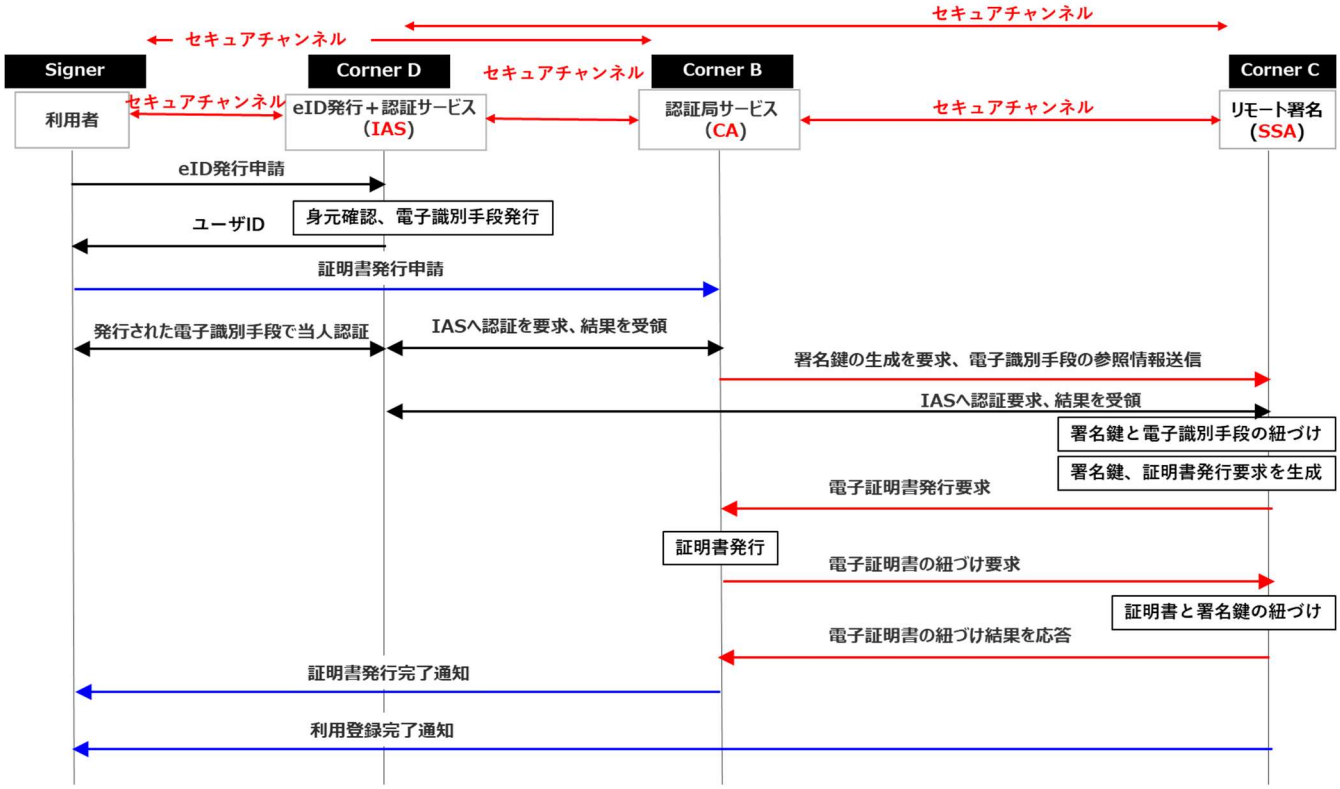


図 3-1　CA が SSA の署名生成装置を用いて利用者の鍵ペア生成を行う利用登録フロー例

(2) 署名者が SSA の署名生成装置(SCDev)をいて利用者の鍵ペア生成を行う場合の例

① 利用者は、リモート署名の利用を SSA に申請する。SSA は申請者本人に対し電子識別手段を発行する。外部の IAS(本基準で認められたものに限る)から当該申請者に発行された電子識別手段を用いても良い。
② SSA は①の電子識別手段を用いて利用者の当人認証が成功したことを確認した後に、申請者の鍵ペアを生成し、当該電子識別手段と当該署名鍵を紐づける。この際、SSA が事前に生成した署名鍵と紐づけても良い。
③ SSA は、当該公開鍵に当該署名鍵で署名を付した証明書発行要求(CSR:Certificate Signing Request)を利用者に返信する
④ 利用者は、リモート署名で使用する電子証明書の発行を認証局に利用申請する。(認証局が定める身元確認書類、電子署名済みの電子文書等を添える)証明書発依頼を送信する。
⑤ 認証局は身元確認後、①の電子識別手段を用いて利用者の当人認証が成功したことを確認した後に電子証明書を発行し、安全、確実に利用者へ送信する。
⑥ 利用者は SSA に電子証明書と署名鍵の紐づけ要求を送信する。
⑦ SSA は①の電子識別手段で利用者認証を行い、成功後、電子証明書と署名鍵の紐づけを行い、利用者に完了を通知する。

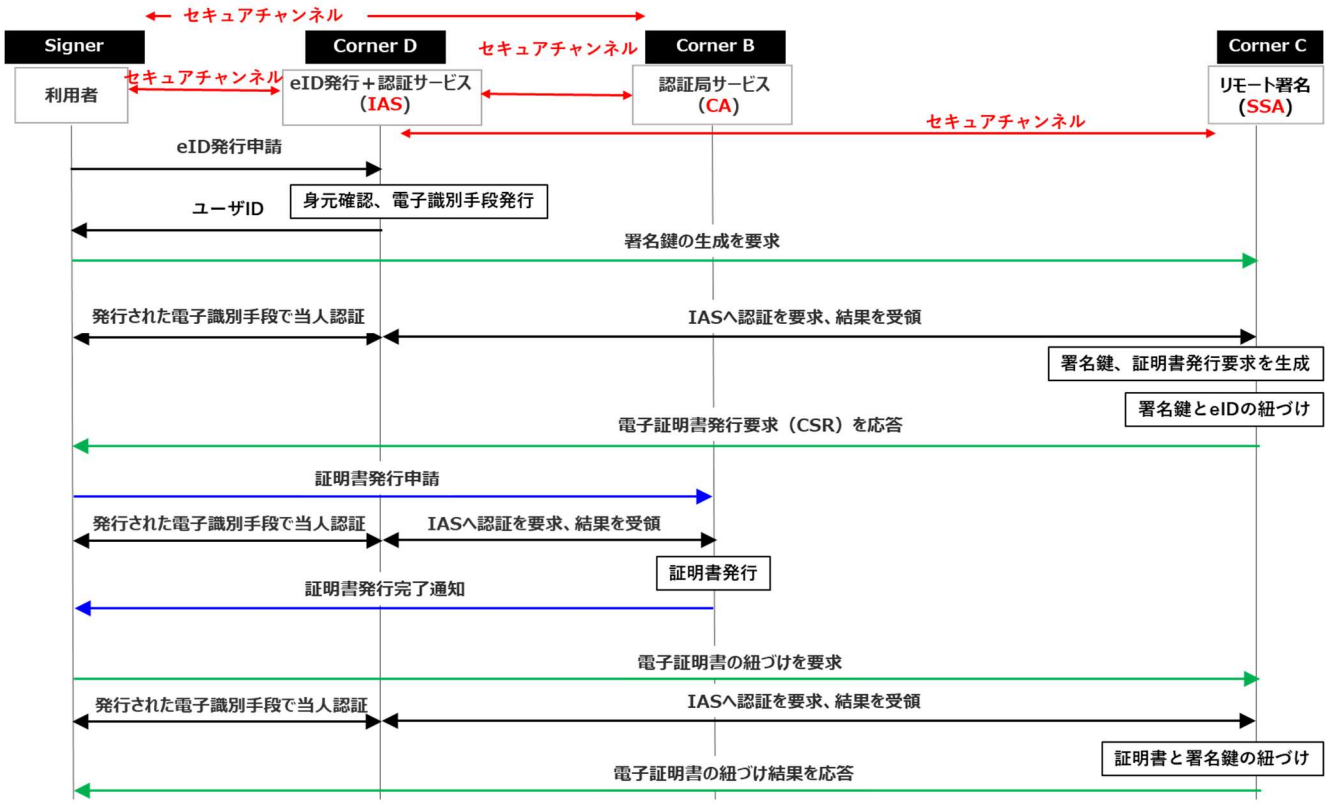


図 3-2　利用者が SSA の署名生成装置を用いて利用者の鍵ペア生成を行う利用登録フロー例

(3) 認証局が利用者の鍵ペアを生成し SSA に送信する場合の例

① 利用者は、リモート署名で使用する電子証明書の発行を認証局に利用申請する。(認証局が定める身元確認書類、電子署名済みの電子文書等を添える)
② 認証局は身元確認後、鍵ペアを生成、電子証明書発行を行い、申請者本人に対し本人認証サービスへの登録情報等の情報を送信する。
③ 認証局は SSA に対して当該利用者の署名鍵、電子証明書、登録情報を安全、確実に送信する。
④ SSA は署名鍵と電子証明書の紐づけを行う
⑤ 利用者は、本人認証サービスにアクセスし登録情報を入力し電子識別手段(スマートフォンなどの認証デバイス)の登録を行う。
⑥ SSA は本人認証サービスから認証結果を受け取り、署名鍵と電子識別手段の紐づけを行う。

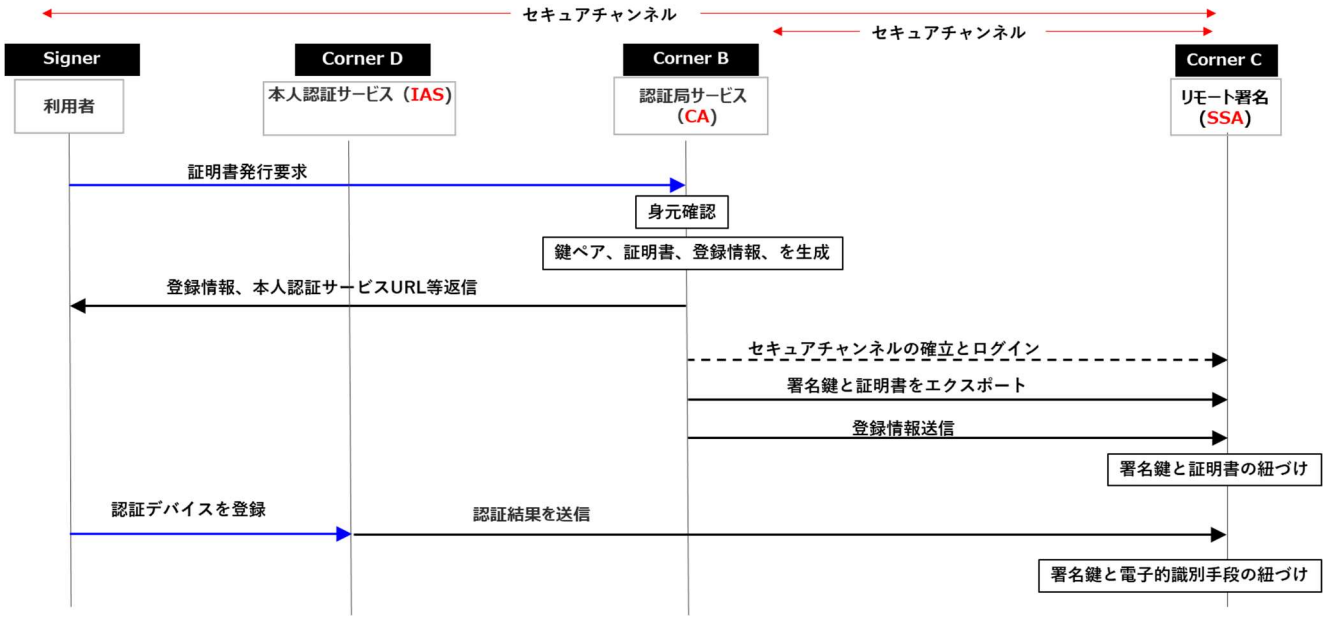


図 3-3　認証局が利用者の鍵ペアを生成し SSA に送信する場合の登録フロー例

1．4．3　サービス利用認証と鍵認可（On-going）

リモート署名で想定する利用シーンの例としては署名対象となる電子的な契約書ファイル等を作成、保管する電子契約サービス等がある。この時、署名対象となる電子的な契約書ファイル等を作成、保管する電子契約サービス等で署名者のサービス利用者認証（利用認証）を行い、その後、リモートでデジタル署名値の生成を行う際に、署名鍵を活性化（鍵認可）を行うこととなる。そのため、リモートで署名の対象となる情報の重要度やリスクに応じて、利用認証と鍵認可の手順や方法が異なる。

下図に示したとおり、利用認証のパターンはパターン A からパターン C の少なくとも 3 つ（図中の青線）、鍵認可のパターンはパターン 1 からパターン 4 の少なくとも 4 つ（図中の橙色線）が考えられる。なお、煩雑となることを避けるため図には本人認証サービス(IAS)を含まないが、IAS が存在した場合も同様に考えることができる。

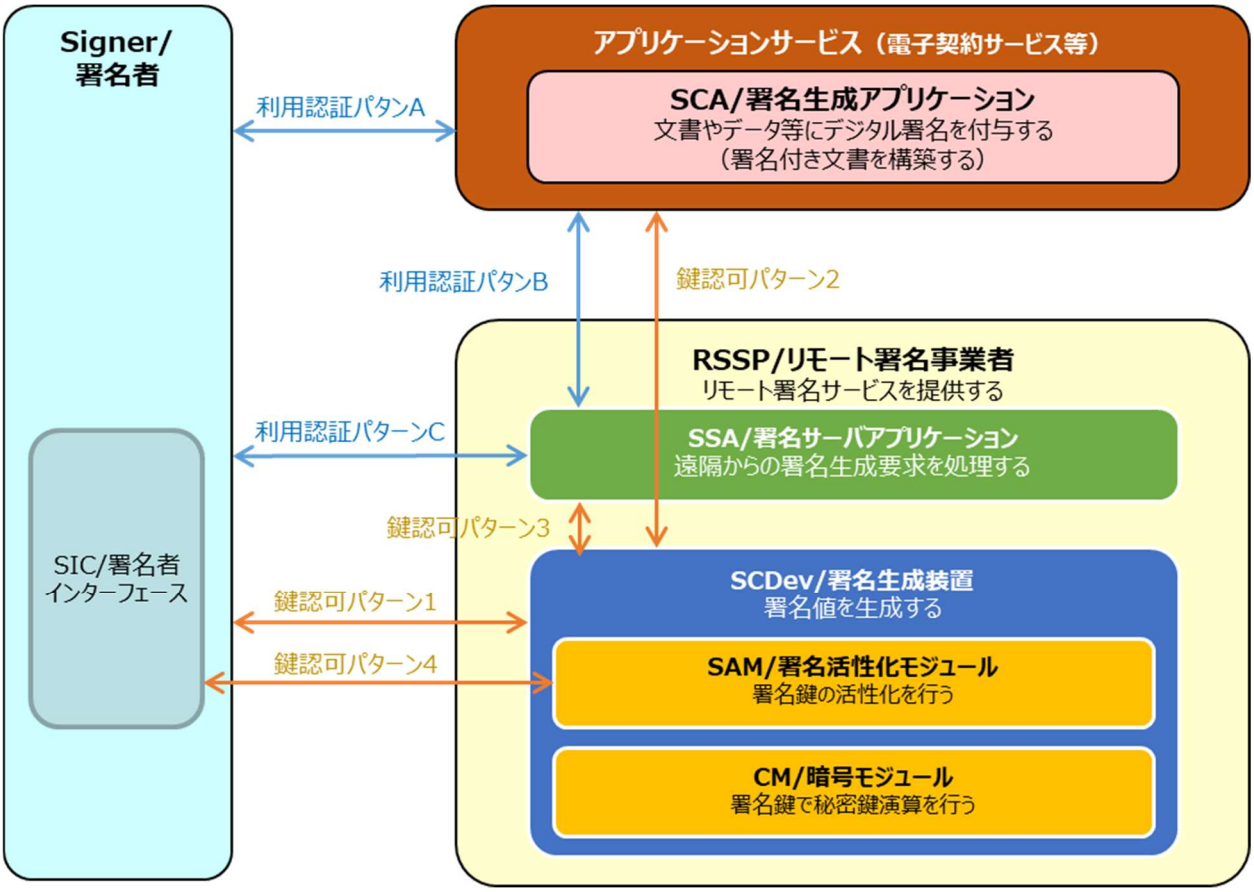


図４　リモート署名サービスの構成例と利用認証・鍵認可のパターン

以下、鍵認可の対策及びレベルの考え方において想定される利用認証のパターンと鍵認可のパターンの関係について説明する。

鍵認可の厳密さ（単独制御に関わるレベル）との対応は以下のとおりである。

鍵認可を利用認証で兼ねてもよいレベル

- RSSP への利用認証を署名者が直接行う場合（利用認証パターン C）のほか、SCA への利用認証パターン A により SSA を介して RSSP への利用認証を自動的に実施する場合（利用認証パターン B）も考えられる。
- SCDev に対する鍵認可は、SCA への利用認証パターン A が兼ねる場合（鍵認可パターン２）あるいは SSA への利用認証（利用認証パターン B あるいは利用認証パターン C）が代行する場合（鍵認可パターン３）が考えられる。

利用認証と別に鍵認可を行わなければいけないレベル

- 鍵認可は必ず利用認証とは別に行わなければならない（鍵認可パターン１または鍵認可パターン４）。この時の利用認証は利用認証パターン A、B、C のいずれでも構わない。

署名活性化モジュールでの鍵認可が必要なレベル（SCAL2）

- 鍵認可は必ず利用認証とは別に、かつ SAM 経由で行わなければならない（鍵認可パターン４）。このとき SIC と SAM が安全に署名活性化データ(SAD)を送受できる必要がある。

なお、利用認証はリモート署名サービスの評価基準には含まず、アプリケーションサービス側の要求によって別途基準を定める必要がある。

1.5　リモート署名サービスの評価基準の文書構成

リモート署名サービスの評価基準は、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、デジタル署名生成アプリケーション（SCA）に対して適用するものとし、下図の（1）「リモート署名サービスの評価基準概説」（本書）及び、次の（2）から（5）の文書群により構成される。

尚、リモート署名サービスの評価基準は、1 つの保証レベルだけではなく、簡易なレベル（Level 1）、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 2）、国際相互運用が可能なレベル(Level 3)の 3 つの保証レベルに応じた評価が可能となるよう、各評価（監査）項目に対して対象となる保証レベルを示した。

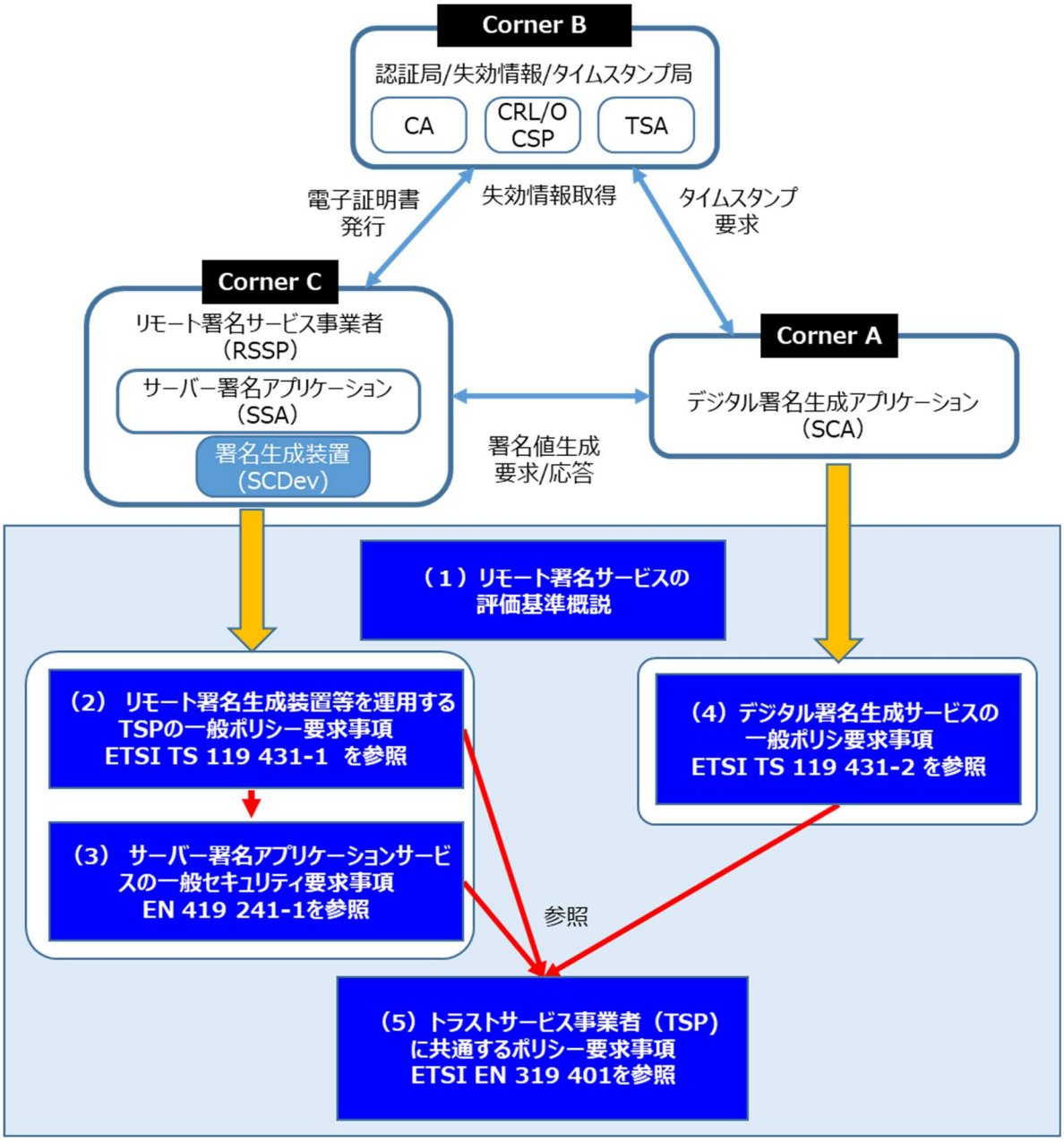


図 5　リモート署名サービスコンポーネントと評価基準の文書構成

リモート署名サービスの監査に用いる具体的な要求事項は、(2)から(5)の各保証レベルに応じた要求事項の欄に〇印が付けられている項目である。

注: 対象文書の重要度に応じて〇印の項目を評価し、署名鍵の漏洩リスクを物理的なSCDevなどを用いて十分に低減するか、または、たとえ漏洩した場合であっても署名者以外が署名できないような必要な管理策を検討すべきである。

（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構成を説明する文書。下記(2)から(5)の用語定義、記号・略語、参照規格はここに記載する。

（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、および
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を参考に作成）
ここでは、リモート署名生成装置(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“トラストサービスプロバイダー(TSP)”に対して、適用されるポリシーとセキュリティ要件を規定した。このSSASCに対するセキュリティ要件の一部は次の(3)を引用している。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、すなわち簡易的な″LSCP(Lightweight SSASC Policy)″、標準的な″NSCP(Normalized SSASC Policy)″および欧州の適格レベルを満たす″EUSCP(EU SSASC Policy)“の3レベルに加え、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+″を規定した。

（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、および
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を参考に作成）
ここでは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した。
SSAは、承認された署名者の制御下でSCDevを使用するため、認可(Authorization)された署名者による独占的な制御(単独制御)が保証されなければならない。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つの基準が示されている。

（4） デジタル署名生成サービスの一般ポリシー要求事項、および
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を参考に作成）
ここでは、デジタル署名生成アプリケーションを管理・運用するサービスコンポーネント。(SCASC)及び、同サービスコンポーネントを管理・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した。

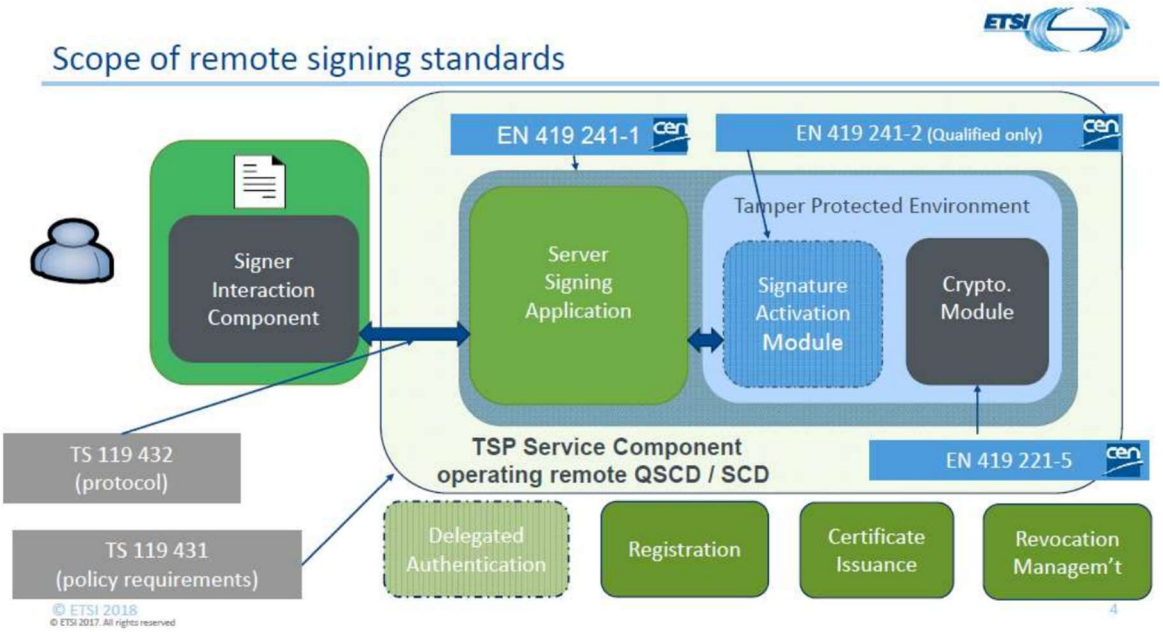
（5） トラストサービスプロバイダーに共通するポリシー要求事項、および
トラストサービスプロバイダーに共通するポリシー要求事項解説
（ETSI EN 319 401を参考に作成）
ここでは、トラストサービスプロバイダー(TSP)の種類を問わず、TSPの管理及び運用の実施に関する一般的なポリシー要件を定義する。特定の種類のTSPについては、別の文書によって評価基準、要求事項等が追加される場合がある。

1.5.1 リモート署名に関係するプロテクションプロファイル

リモートSCDevの中でも欧州において、適格レベルの要件を満たしたものをリモートQSCDと言い、ここでは、リモートQSCDの要件と関連規格を紹介する。リモートQSCDはSAMとHSMの二つのコンポーネントで構成される。欧州では、このSAMとHSMに対してプロテクションプロファイル[2]と呼ばれる基準を策定しており、

[2] 特定のセキュリティ要件や目標を満たすために、セキュリティ機能や措置の要件を定義した文書。プロテクション

ISO/IEC 15408[3]をベースにした製品認証の枠組みを整備している。 欧州は、SAM と HSM に対して欧州における適格レベルを充足する為の基準として、EN 419 241-2 及び、EN 419 221-5 を策定している。



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

図 6　欧州のリモート署名の技術基準のスコープ

リモート QSCD、即ちコモンクライテリア認証を取得した SAM と HSM の利用は、SCAL2 の達成に必要とされている。認証取得製品は既に市場にあり、日本においても調達が可能であり、リモート署名サービスが達成したい保証レベルに応じて、構成を選択する必要がある。

プロファイルは、ある特定の製品やシステムの評価のために使用される。

[3] ISO/IEC 15408 は、情報セキュリティの評価基準である「コモンクライテリア（Common Criteria）」に関する国際規格である。コモンクライテリアは、異なる国や組織が開発した情報セキュリティ製品やシステムを評価するための共通の基準を提供することを目的としている

1.6　評価基準の文書における法助動詞

この評価基準においては，各評価基準項目への準拠性の対応内容を明確にするため英語の法助動詞を添えて下記の表現を用いている。
「するものとする」，(SHALL) 実施が義務付けられる
「しないものとする」，(SHALL NOT)実施しないことが義務付けられる
「すべきである」，(SHOULD) 実施しない場合、合理的な理由を示さなければならない
「すべきでない」，(SHOULD NOT) 実施する場合、合理的な理由を示さなければならない
「してもよい」，(MAY) 実施することが許容される
「する必要がない」，(NEED NOT) 実施することが求められていない

2.　用語と定義

英語表記	日本語表記	内容
authentication	認証	主張されたエンティティの同一性の保証の提供 （注） ISO/IEC 18014-2 で定義されているとおり。
authentication factor	認証ファクター	ある実体の同一性識別の認証、または検証のために使用される情報の断片および/またはプロセス
Coordinated Universal Time (UTC)	協定世界時	勧告 ITU-R TF.460-6 に定義されている秒を基準とした時間スケール。
data to be signed representation (DTBS/R)	署名対象データレプレゼンテーション	デジタル署名値を算出するために署名対象文書から生成されるデータ（ハッシュ値など）
(AdES)digital signature	デジタル署名	CAdES 署名、PAdES 署名、XAdES 署名のいずれかであり、デジタル署名値とその検証に必要な情報等を含んでいる電子データ。電子データの受信者が当該データの出所と完全性を証明し、受信者などによる偽造から保護できるようにするもの。
digital signature value	デジタル署名値	署名対象データのハッシュ値を署名者の秘密鍵により暗号変換して得られる値。
eIDAS Regulation	eIDAS 規則	EU 内部市場において、電子署名指令（1999/93/EC）を上書きする電子取引のための電子識別及びトラストサービスに関する欧州議会及び理事会の規則（EU）No 910/2014。
electronic identification (eID)	電子識別(eID)	自然人や法人、または法人を代表する自然人等を一意に表す電子的な個人識別データを用いて、オンライン・サービスなどで電子的に当該自然人等を識別するプロセス。
electronic identification means	電子識別手段（eID 手段）	個人識別データを含む電子形式のデータもしくは、それを格納した物理トークン。オンライン・ サービスの認証に使用されるもの。

electronic identification means reference	電子識別手段の参照	署名者を認証するために、電子識別手段の参照として SSASC で使用されるデータ。 （例） 電子識別手段が非対称鍵を使用する場合、公開鍵を参照とすることができる。 署名者の認証に成功した後に署名付きアサーションが生成される場合、アサーション署名者 ID およびユーザー ID を参照とすることができる。 電子識別手段が秘密鍵（ワンタイム・パスワード・ジェネレータなど）を使用する場合、秘密鍵を 参照とすることができる。
person identification data	個人識別データ	自然人もしくは法人、または法人を代表する自然人の身元を確認することを可能にするデータの集合。本人のみが所持または知りえる秘密情報を含む。
relying party	依拠当事者	電子証明書またはトラストサービスに依拠する自然人または法人をいう。 （注） 依拠当事者には、公開鍵証明書を使用してデジタル署名を検証する当事者が含まれる。
remote signature creation device	リモート署名生成装置	署名者の視点からリモートで使用され、署名者に代わって署名操作を制御する署名生成装置等。
server signing application (SSA)	サーバー署名アプリケーション	署名者に代わってデジタル署名値を生成するために署名生成装置等を使用するアプリケーション。
server signing application service component (SSASC)	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）	署名者に代わってデジタル署名値を生成するサーバー署名アプリケーションを管理・運用するサービスコンポーネント。
server signing application service provider (SSASP)	サーバー署名アプリケーションサービスプロバイダー（SSASP）	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を管理・運用する TSP。
signature activation data (SAD)	署名活性化データ	SAP が収集するデータのうち、署名者に代わって暗号モジュールによって実行される所定の署名操作を高レベルの信頼性で制御するために使用されるデータ。署名者の単独制御下にあるもの。
signature activation module (SAM)	署名活性化モジュール	署名鍵が署名者の単独制御で使用されることを高レベルの信頼性で保証するために、SAD を使用するよう構成されたソフトウェア。
signature activation protocol (SAP)	署名活性化プロトコル	署名者の署名鍵を用いて、DTBS/R の署名操作を制御するために使用される SAD を収集するプロトコル。
signature applicability rules	署名適用性規則	1 つまたは複数のデジタル署名に適用され、署名が特定のビジネス目的または法的目的に適しているかどうかを判断するための要件を定義する一連の規則。 （注） 署名適用可能性規則は、暗黙的である場合もあれば、人間が読み取り可能な文書および/または機械が処理可能な文書に記載されている場合もある。ETSI TS

		119 172-1 はこの目的に使用できる。
signature creation application (SCA)	デジタル署名生成アプリケーション	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。
signature creation application service component (SCASC)	署名生成アプリケーションサービスコンポーネント	デジタル署名生成アプリケーションを管理・運用するサービスコンポーネント。
signature creation application service provider (SCASP)	署名生成アプリケーションサービスプロバイダー	署名生成アプリケーションサービスコンポーネントを管理・運用する TSP。
signature creation constraint	署名生成制約	デジタル署名を生成する際に使用される規則。
signature creation device (SCDev)	署名生成装置等	署名者の署名鍵を保持し、デジタル署名値を生成するために使用されるソフトウェアまたはハードウェア。
signature creation policy	署名生成ポリシー	SCA によって処理される署名生成制約のセット。
signature policy	署名ポリシー	同一の署名または署名の集合に適用される、署名生成や検証に関わるポリシー。
signer	署名者	デジタル署名の生成者となるエンティティ（自然人または法人）
signer's interaction component	署名者インタラクションコンポーネント	署名者が SAP をサポートするために使用するソフトウェアおよび/またはハードウェアコンポーネント
signing key	署名鍵	デジタル署名値を生成するために使用される非対称暗号アルゴリズムにおける秘密鍵。
subscriber	加入者	トラストサービスプロバイダーとの契約により指定された加入者義務に拘束される法人または自然人
trust service practice statement	トラストサービス運用規程	TSP がトラストサービスを提供する際に採用する実務を記述したもの。
trust service provider (TSP)	トラストサービスプロバイダー	1 つ以上のトラストサービスを提供するエンティティ

3. 記号・略語

CA	Certification Authority（認証局）
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
CEN	Comité Européen de Normalization (European Committee for Standardization)
DTBS/R	Data To Be Signed Representation（署名対象データ表現）
EAL	Evaluation Assurance Level
eID	electronic Identification（電子識別）
ETSI	European Telecommunications Standards Institute
EUSCP	EU SSASC Policy
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISSS	Information Society Standardization System
LSCP	Lightweight SSASC Policy
NSCP	Normalized SSASC Policy
OID	Object Identifier（オブジェクト識別子）
SAD	Signature Activation Data （署名活性化データ）
SAM	Signature Activation Module（署名活性化モジュール）
SAP	Signature Activation Protocol（署名活性化プロトコル）
SCA	Signature Creation Application（署名生成アプリケーション）
SCAL	Sole Control Assurance Level（署名者唯一による署名鍵の制御。単独制御）
SCASC	Signature Creation Application Service Component（署名生成アプリケーションサービスコンポーネント）
SCASP	Signature Creation Application Service Provider（署名生成アプリケーションサービスプロバイダー）
SCDev	Signature Creation Device（署名生成装置等）
SCP	SSASC Policy
SD	Signer's Document（署名者のドキュメント）
SIC	Signer's Interaction Component
SLA	Service-Level Agreement（サービスレベルアグリーメント、サービス品質保証、サービスレベル合意書）
SSA	Server Signing Application
SSASC	Server Signing Application Service Component（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）

SSASP	Server Signing Application Service Provider（サーバー署名アプリケーションサービスプロバイダー）
TSA	Time-Stamping Authority（タイムスタンプ局）
TSP	Trust Service Provider

4. 参照規格

- ETSI EN 319 401 トラストサービスプロバイダーの一般的ポリシー要求
  General Policy Requirements for Trust Service Providers
- 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
- 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
- ETSI TS 119 431-1 リモート QSCD/SCDev のポリシー要求事項
  Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 AdES デジタル署名生成を提供する TSP のポリシー要求事項
  Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (remote signing)
- ETSI TS 119 432 リモートデジタル署名生成プロトコル
  Protocols for remote digital signature creation

リモート署名サービスの評価基準

― 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 を参考に作成）

目次

1　スコープ

本書は、リモート署名生成装置（以降 SCDev）を運用するサービスコンポーネントとして実装するトラストサービスプロバイダー（以降 TSP）に対して、一般的に適用されるポリシーとセキュリティ要件を規定する。

注： SCDev が一般的な暗号モジュールとしての評価や認定だけでなく、各国の電子署名関連法規制に従った追加の要件が必要となる場合がある。例えば、欧州における Qualified Electronic Signature 相当として受け入れられるためには、適格署名生成デバイス（以降 QSCD）に関する欧州規格に従って、Common Criteria で評価されることが求められるとともに、特定の要件が適用される。

サービスコンポーネントは、サーバー署名アプリケーション（以降 SSA）と QSCD/SCDev 等から構成される。本書では、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（以降 SSASC）という用語を用いる。

ポリシーおよびセキュリティ要件は、電子署名の作成に使用する署名鍵の作成、維持、ライフサイクル管理、使用に関する要件という観点から定義される。

本書では、このようなコンポーネントを実装する TSP の種類について特に制限を設けない。

本書は、リモート署名サービスを運営する TSP が信頼できることを示す適合性評価の基礎とし て、独立した適合性評価機関が使用することを目的としている。

注1： 限定的ではないが、本書は、電子署名、及び e シール（法人名義のデジタル署名）をサポートするデジタル署名生成機能を提供するトラストサービスプロバイダー向けである。附属書 A には、欧州の eIDAS 規則における SSASC に特有の要件が記載されている。

本書では、独立した適合性評価機関による要求事項の充足の評価方法、当該評価者が利用できる情報についての要求事項、または当該評価者に対する要求事項は規定されていない。

注 2： 本書は、ETSI 標準の対象となるすべての TSP サービスに共通する一般的なポリシー要件について、別途定める「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」を参照している

本書では、SSASC にアクセスするためのプロトコルは規定しない。

注 3： リモート電子署名生成のプロトコルは、ETSI TS 119 432 に定義されている。

本書では、リモート QSCD/SCDev 等を運用するサービスに関連するリスクに対処するために必要な特定の管理策を示す。また、いくつかの管理策はポリシーレベルに応じて複数の対策が示されており、レベルに応じた管理策への準拠性を SSASC の評価基準に用いることを可能としている。

2　参照規格

参照規格は、保健医療福祉分野におけるリモート署名サービスの評価基準を参照のこと。

3　用語と定義、記号・略称及び評価基準での表記

3.1　用語と定義、記号・略称

用語と定義及び記号・略称は、保健医療福祉分野におけるリモート署名サービスの評価基準を参照のこと。

3.2　評価基準での表記

本書で特定される要件には，次のものが含まれる：

a) SSASC のポリシーに適用される要件。このような要件は、追加記号を付けずに節で示す。

b) ある条件下で適用される要求事項。このような要件は、"[CONDITIONAL]"でマークされた条項で示される。

c) 適用される状況に応じてた選択肢を含む要件。このような要求事項は、"[CHOICE]"でマークされた節で示される。

d) SSASC ポリシーのもとで提供されるサービスに適用される要件。そのような要件は、以下のように該当する SSASC ポリシーでマークされた条項で示される。

- "[LSCP]"、"[NSCP]"および"[EUSCP]"。

本書における要求事項は、別表にて以下の要件番号により特定されている。

・ 要件番号＝<3 文字のサービスコンポーネント記号> - <節番号> - <2 桁の番号-増分>

SSASC サービスコンポーネント記号は以下の通り。

・ OVR:一般要件（1 つ以上のサービス要素に適用される要件）。
・ GEN:署名鍵生成サービス
・ LNK:証明書と電子識別手段を紐づけるリンクサービス
・ SIG:署名鍵活性化サービス
・ DEL:署名キー削除サービス
・ EID:eID 手段提供（オプション）

この文書の後続の版における要件番号の管理は，次のとおりである。

- 要件が節の末尾に挿入されると、上記の 2 桁の数字は次の利用可能な桁にインクリメントされる。
- 要件番号が既存の 2 つの要件番号の間に挿入される場合、新しい要件を区別するために、前の要件番号に付加された大文字が使用される。
- 削除された要件の要件番号は、"無効"と記述して残す。
- 変更された要件の要件番号は"無効"として残し、変更された要件は最初の要件番号に付与された大文字で識別される。

4 一般コンセプト

4.1 一般ポリシー要求事項のコンセプト

本書は、ETSI EN 319 411-1 にほぼ沿って構成されており、TSP がこれらの要件を独自のポリシーおよび運用規程に適用することを支援するものである。

本書は、「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」を参照することによりその要求事項を組み込んでいる。「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」は、単独制御（sole control）の保証レベルを定義している。「単独制御」という用語は、電子署名にのみ要求事項が適用されることを意味するものではない。要件は、しかるべき変更を加えた上で e シールに準用することができる（MAY）。すなわち、読者は、「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」 5.3 で説明されているように、「sole control：単独の制御」という用語を「control：制御」に置き換えることができる（MAY）。

注 1： 「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」の要件を参照し、SSASC を運用する TSP(以降 SSASP)に関連する要件を追加している。

本書は、参照により「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」の要件を組み込み、SSASP に関連する要件を追加している。ガイダンスとして「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」の 4 および IETF RFC 3647 の 3.1 と 3.4 を参照すること。

要件は、セキュリティの目的という観点から示され、その目的を達成するために必要と考えられる事項が存在する場合、その目的を満たすためのコントロールに関するより具体的な要件が示される。

注 2： 目的を満たすために要求される管理の詳細は、必要な信頼性を達成する一方で、TSP が署名生成装置を操作する際に採用できる技術の制限を最小にすることのバランスをとることである。場合によっては、より詳細な管理要件の参考として使用でき、より一般的な規格を参照する。これらの要因により、あるトピックで示される要求事項の具体性は異なる可能性がある。

本書では、鍵生成、署名鍵と証明書、電子識別手段（eID means、以下 eID 手段と呼ぶ）とのリンク、署名活性化、鍵削除、デバイス提供の各サービスに関する要件が含まれる（4.4 参照）。

4.2 証明書を発行するTSP（認証局）とSSASCとの関係性

SSASC は、証明書を発行する TSP が提供するサービスの一部である場合もあれば、別の TSP が提供するサービスの一部である場合もある。または SSASC のみをサポートする TSP によって提供される。すべての場合において、この TSP は SSASP として定義される。

注： SSASP が証明書を発行する TSP の一部 である場合、本書の一部の要件は、CA のサービスコンポーネントによって 満たされることがある。

4.3 SSASC適用文書

4.3.1 SSASC の運用規程

SSASP は、「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」6.1 に定義されるトラストサービス運用規程を SSASC 用に特化し、SSASC 運用規程を開発、実装、実施、更新する。

SSASC 運用規程は、SSASP がどのようにサービスを運用するかを記述し、SSASP に帰属されるものである。SSASC の運用は、TSP の組織構造、運用手順、施設、コンピューティング環境に合わせたものである。運用規程の開示先としては、監査人、加入者、依拠当事者が想定される。

注: 本書で要求されているように、いくつかの要素は SSASC 運用規程において必須であるが、本書は SSASC 運用規程の形式を制限していない;TSP が提供する他のサービスをカバーする一般的な TSP 運用規程に含まれることも、独立した文書として作成することも可能である。

本書は、4.3.2 で定義された SSASC ポリシーが、SSASP によって承認され、その運用規程に反映されるために必要な要件として特定されたものを提供するものである。

4.3.2 SSASC ポリシー

SSASC ポリシー**(以降 SCP)は、**提供される内容**を**記述し、SSASC の適用可能性を示すために、本書の範囲を超えて多様な情報を含むことができる。SCP は、SSASP の具体的な運用環境の詳細とは無関係に定義される。SCP の開示先は、監査人、加入者、依拠当事者とすることができる。

本書では、3 段階の SCP を定義している。

1) 軽量 SSASC ポリシー(以降 LSCP)は、リスクアセスメントが NSCP (次項)の全要件を満たすことによる追加的な負担を正当化できない場合に使用する。NSCP よりも負担の少ないサービス品質を提供する(要求されるポリシー要件がより少ない)ポリシーである(例:署名活性化モジュールの使用)。

2) 標準 SSASC ポリシー(以降 NSCP)は、あらゆる種類のトランザクションをサポートするために使用されるリモート SCDev を運用する TSP にとって、一般に認められたベストプラクティスを満たす標準的なポリシーである。

3) EU SSASC ポリシー(以降 EUSCP)は、NSCP と同じ品質を提供するが、QSCD 管理に関連する eIDAS 規則の特定の要件を備えたポリシーである。

注: EUSCP 固有の要件は付属書 A に定義されている。

SCP は必ずしも SSASP の文書の一部である必要はない(「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」に従えば、運用規程および利用規約で十分である);たとえば、SCP はコミュニティによって共有可能で、必ずしも SSASP に帰属しなくてもよい。また、本書は SCP の形式を制限していない。SCP は独立した文書であっても、運用規程内、もしくは一般的な利用規約の一部として提供されてもよい。

4.3.3 利用規約

SCP と SSASC 運用規定に加えて、またはその一部として、TSP は利用規約を発行する。利用規約は、広範な商業的条件または技術的条件をカバーすることができる。条件は、SSASP に固有のものである。利用規約の提示先は、加入者と依拠当事者である。

注: この文書で要求されているように、いくつかの要素の存在は諸条件に必須であるが, この文書は諸条件の形式 に制限を設けていない。利用規約参照者のための独立した文書とすることも, 加入者の契約や依拠当事者に対する情報 に分割することもできる。また, 約款の形式及び内容は, 国の規則等に準拠したものとすることができる。

4.4 SSASCサブコンポーネントサービス

注 1: 本書は、TSP のサービスの以下の分割を義務付けるものではない。要件は後続の節に記述される。

SSASC は、本書では要件分類のため、以下のサブコンポーネントサービスに分類される。

- **署名鍵生成サービス:**リモートデバイスで署名鍵を生成する。生成された署名鍵の所有証明は、関連する証明書を発行する TSP の登録サービ スに引き渡される。
- **証明書リンクサービス:**TSP の証明書生成サービスにより生成された証明書と対応する署名鍵をリンクさせる。
- **eID 手段リンクサービス:**eID 手段の参照情報と対応する署名鍵をリンクさせ、単独制御できるようにする。このサービスは、証明書を発行する TSP の ETSI EN 319 411-1 の要件 REG-6.3.1-01 をサポートするために使用することができる。

  例 1. 秘密鍵とリンクする署名者の認証のアサーションを提供することにより実現。
- **署名活性化サービス:**署名活性化データを検証し、対応する署名鍵を活性化し、デジタル署名を作成する。
- **署名鍵削除サービス:**署名鍵が使用できなくなるような方法で署名鍵を破棄する。
- **eID 手段提供サービス(オプション):**eID 手段を準備し、署名者に提供または利用可能にする。

  例 2. 認証キーを生成し、その鍵を証明書のサブジェクトに配布するサービス(「ソフト」鍵、すなわちソフトウェア環境で保護された鍵を含む);

  認証デバイスとイネーブルコードを準備し、証明書のサブジェクトに配布するサービス(ハードウェア環境で保護された鍵を含む)。

このサービスの細分化は、ポリシー要件を明確にするためのものであり、TSP のサービスの実装の細分化に何ら制限を加えるものではない。

図 1 は、本書のサービスサブコンポーネントと、署名証明書を発行する TSP の外部コンポーネントサービスとの相互関係を示したものである。

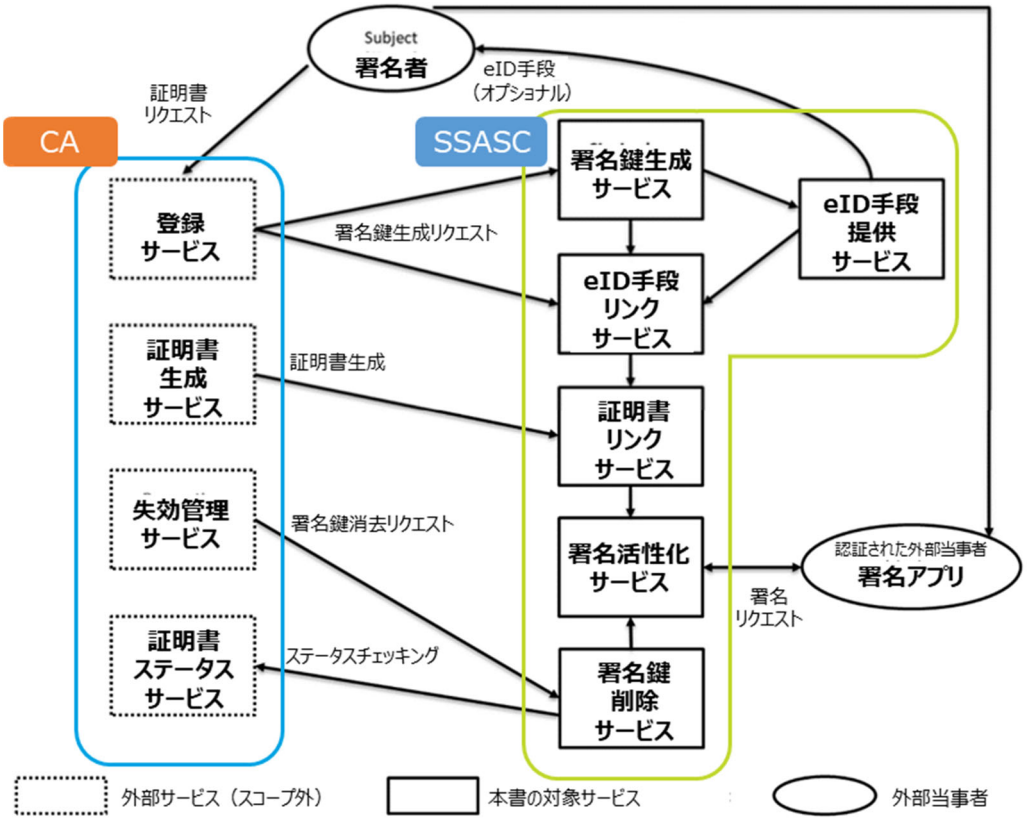


図1　SSASC サブコンポーネントの細分化

図 2 は、本書のサービス間の相互関係と、外部に委託された認証処理との関係を示したものである。

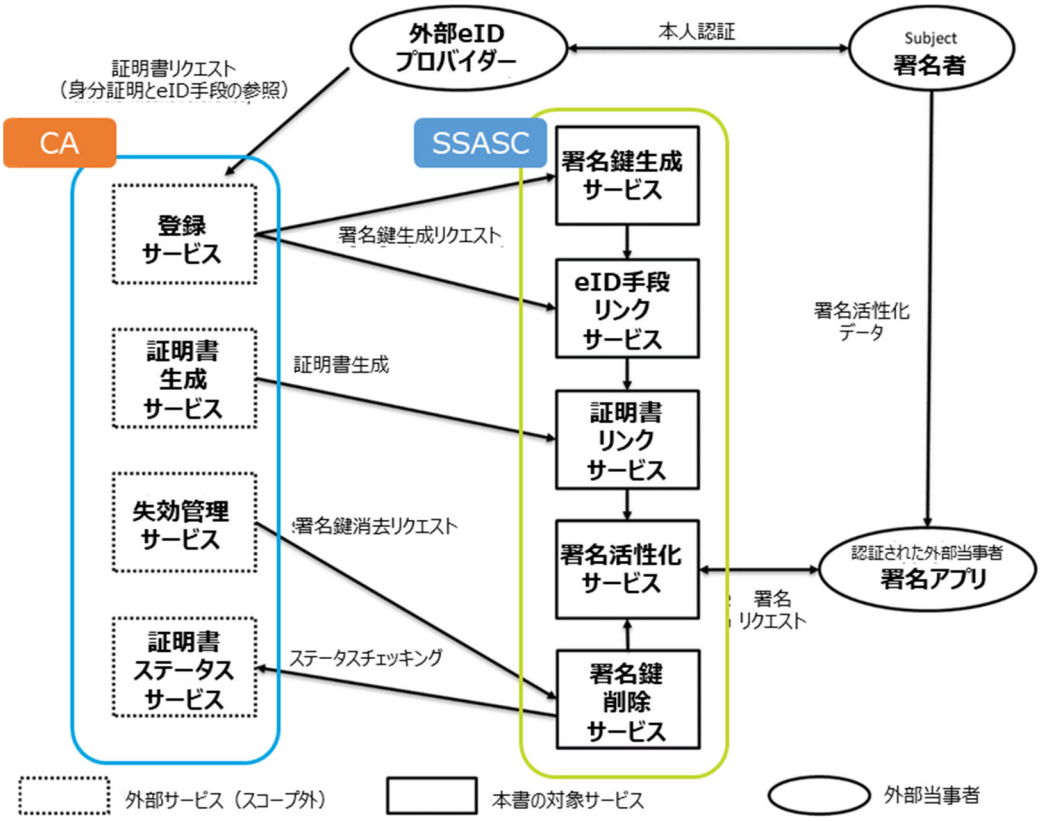


図2　SSASC サブコンポーネントの細分化と外部 eID プロバイダーへの認証委任

注 2:　図 1 および図 2 は説明のためのものであり、処理の流れを示すものではない。本書の 6 では、各サービスに対する具体的な要求事項を規定する。

5　運用規定とポリシーに関する一般規定

本章の詳細は「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」参照のこと

5.1 運用規定の要求事項

6　トラストサービスプロバイダーの運用

本章の詳細は「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」参照のこと

6.1 公開とリポジトリに対する責任

6.2 署名鍵の初期化

6.2.1 署名鍵の生成
6.2.2 電子識別手段のリンキング

6.2.3 証明書のリンキング
6.3 署名鍵のライフサイクル運用要件 6.3.1 署名鍵活性化
6.3.2 署名鍵の消去

6.4 施設、管理、および運用管理

6.4.1 一般事項
6.4.2 物理的セキュリティ管理
6.4.3 手続き上のコントロール
6.4.4 人的コントロール
6.4.5 監査の記録手順
6.4.6 記録保管
6.4.7 鍵更新
6.4.8 危殆化と災害復旧

6.5 技術的なセキュリティ管理

6.5.1 システム及びセキュリティ管理
6.5.2 システムと運用
6.5.3 コンピューターセキュリティコントロール
6.5.4 ライフサイクルセキュリティコントロール
6.5.5 ネットワークセキュリティコントロール

6.6 コンプライアンス監査およびその他の評価

6.7 その他のビジネスおよび法的事項

6.7.1 手数料
6.7.2 財政的責任
6.7.3 業務情報の守秘義務
6.7.4 個人情報の保護
6.7.5 知的財産権
6.7.6 表明と保証
6.7.7 保証の免責事項
6.7.8 責任の制限
6.7.9 免責事項
6.7.10 期間と終了
6.7.11 参加者への個別通知と連絡
6.7.12 修正
6.7.13 紛争解決手続き
6.7.14 準拠法
6.7.15 適用される法律の遵守

7　本書を基に構築された SSASC ポリシーを定義するためのフレームワーク

本章の詳細は「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」参照のこと

附属書 A (規定):

eIDAS 規則に関連する特定の要求事項

本章の詳細は「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」参照のこと

附属書 B（参考）:

リモート署名標準のスコープ

B.1　　リモート署名標準のスコープ

図 B.1 は、リモート署名作成サービスに適用されるさまざまな標準を示している。

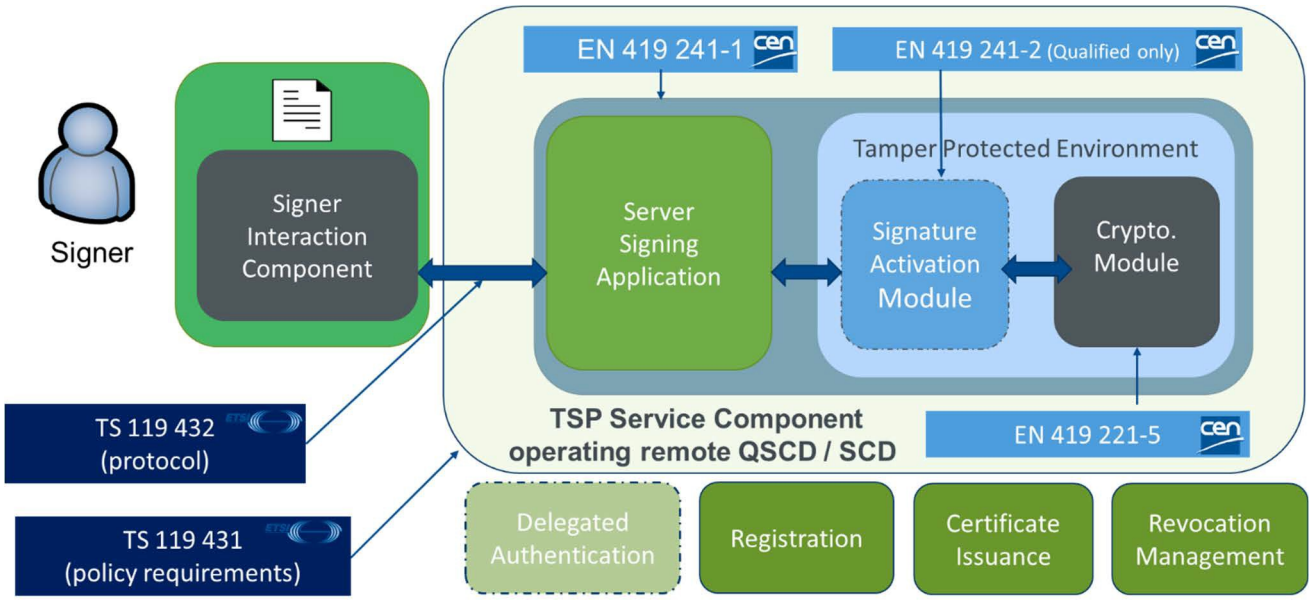


図 B.1: さまざまなリモート署名コンポーネントに関する規格の範囲

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

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
		Level 1	Level 2	Level 3	
5	**General provisions on practice statement and policies**				**運用規定とポリシーに関する一般規定**
5.1 Practice statement requirements					5.1 運用規定の要求事項
OVR-5.1-01	The general requirements specified in ETSI EN 319 401 , clause 6.1 shall apply. In addition, the following particular requirements apply: NOTE 1: A TSP can document practices relating to specific SSASC policy requirements separate from the main practice statement document.	○	○	○	「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」の 6.1 項に規定される一般要求事項を適用するものとする(SHALL)。加えて、以下の特定の要件を適用する。 注1:TSPは、特定のSSASCポリシー要件に関連する実務を、主要な運用規程とは別に文書化することができる。
OVR-5.1-02	The TSP's practice statement shall include the signature algorithms and parameters applied, the algorithms applied for key pair generation and any other algorithms and parameters that are critical to the security of the SSASC operation.	○	○	○	TSP の運用規程には、適用される署名アルゴリズムおよびパラメータ、鍵ペア生成に適用されるアル ゴリズム、ならびに SSASC 運用のセキュリティにとって重要なその他のアルゴリズムおよびパラメータを 含むものとする(SHALL)。
OVR-5.1-03	The TSP shall publicly disclose its practice statement through an online means that is available on a 24x7 basis. NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.	○	○	○	TSP は、24 時間 365 日利用可能なオンライン手段を通じて、自己の運用規程を公開するものとする(SHALL)。 注2: TSPは、機密情報を含むいかなる側面も開示する義務はない。
OVR-5.2-01	If any changes are made to a SCP as described in clause 4.3.2 which affects the applicability then the policy identifier should be changed.	○	○	○	SCP(SSASCのポリシー) に変更があり、適用性に影響がある場合は、ポリシー識別子を変更するべきである(SHOULD)。
OVR-5.3.1-01	The SSASP may make use of other parties to provide parts of the service, however, the SSASP always maintains overall responsibility and shall ensure that the policy requirements identified in the present document are met.	○	○	○	SSASP は、サービスの一部を提供するために他の当事者を利用することができるが(MAY)、SSASP は常に全体的な責任を維持し、本書で特定されるポリシー要件が満たされていることを保証するものとする(SHALL)。
6	**Trust Service Providers practice**				**6 トラストサービスプロバイダの運用**
6.1Publication and repository responsibilities					6.1 公開とリポジトリの責任
OVR-6.1-01	The TSP shall make available to subscribers and relying parties the applicable SCPs, practice statements and terms and conditions regarding the use of signing keys.	○	○	○	TSP は、署名鍵の使用に関して、適用される SCP群、運用規程、利用規約を加入者及び依拠当事者に提供 するものとする(SHALL)。
OVR-6.1-02	The applicable terms and conditions shall be readily identifiable for a given signing key or for the associated certificate.	○	○	○	適用される利用規約は、与えられた署名鍵または関連する証明書について容易に特定可能でなければならない(SHALL)。
OVR-6.1-03	The information identified in OVR-6.1-01 and OVR-6.1-02 above shall be available 24 hours per day,7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the SSASC practice statement.	○	○	○	上記OVR-6.1-01 及び OVR-6.1-02 で特定された情報は、24時間365日利用可能であるものとする(SHALL)。 システム障害、サービス、その他トラストサービスプロバイダーの管理下にない要因が発生した場合、トラストサービスプロバイダーは、SSASC運用規程に示される最長期間を超えてこの情報サービスが利用できないことがないよう最善の努力をするものとする(SHALL)。
OVR-6.1-04	The information identified in OVR-6.1-01 above should be publicly and internationally available.	○	○	○	上記**OVR-6.1-01で**特定された情報は、一般的に利用可能とすべきである(SHOULD)。
6.2Signing key initialization					6.2 署名鍵の初期化
6.2.1Signing key generation					6.2.1 署名鍵の生成
GEN-6.2.1-01 [LSCP]	Clause SRG_KM.1.1 of EN 419 241-1 [3] , specifying signing keys environment shall apply.	○	○	○	「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」の SRG_KM.1.1 項(署名鍵の環境に関する規定)を適用するものとする(SHALL)。
GEN-6.2.1-02 [NSCP]	Clause SRA_SKM.1.1 of EN 419 241-1 [3] , specifying signing keys environment shall apply.		○	○	「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」の SRA_SKM.1.1 項(署名鍵の環境に関する規定)を適用するものとする(SHALL)。
GEN-6.2.1-03	Clause SRG_KM.1.2 of EN 419 241-1 [3] , specifying cryptographic algorithms and key lengths, shall apply.	○	○	○	「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」の SRG_KM.1.2 項(暗号アルゴリズムと鍵長を規定)を適用するものとする(SHALL)。
GEN-6.2.1-04	Clause SRG_KM.1.3 of EN 419 241-1 [3] , specifying key protection shall apply.	○	○	○	「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」の SRG_KM.1.3 項(鍵の保護に関する規定)を適用するのとする(SHALL)。
GEN-6.2.1-05	Clause SRG_KM.1.4 of EN 419 241-1 [3] , specifying device initialization shall apply.	○	○	○	「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」の SRG_KM.1.4 項(デバイスの初期化に関する規定)を適用するのとする(SHALL)。
GEN-6.2.1-06	Clause SRC_SKS.1.1 of EN 419 241-1 [3] , specifying algorithm parameters shall apply.	○	○	○	「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」の SRC_SKS.1.1 項(アルゴリズムパラメータを規定)を適用するのとする(SHALL)。
GEN-6.2.1-07	Clause SRC_SKS.1.3 of EN 419 241-1 [3] , specifying time of generation shall apply.	○	○	○	「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」の SRC_SKS.1.3 項(生成時間に関する規定)を適用するものとする(SHALL)。
GEN-6.2.1-08 [CONDITIONAL]:	[CONDITIONAL]: If the SSASC and the certificate generation service component are managed separately, then the SSASC shall support the requirement defined in clause REG-6.3.1-01 of ETSI EN 319 411-1 [2]. EXAMPLE: By providing an assertion of the authentication of the signer that is linked to the private key.	○	○	○	SSASC と証明書生成サービスコンポーネントが別々に管理される場合、SSASC は ETSI EN 319 411-1 [2] の REG-6.3.1-01 項で定義された要件をサポートするものとする(SHALL)。 例:秘密鍵にリンクされた署名者の認証のアサーションを提供することによって。 EN 319 411-1 [2] の REG-6.3.1-01 サブジェクトの鍵ペアがCAによって生成されていない場合、証明書申請プロ セスは、サブジェクトが認証のために提示された公開鍵に関連する秘密鍵を所有または管理してい ることを確認するものとする。
GEN-6.2.1-09 [LSCP+] [CONDITIONAL]:		○	○	○	SSASC と証明書生成サービスコンポーネントが別々に管理される場合で、サブジェクトの鍵ペアがCAによって生成されている場合、SSASC は 国に認定された信頼できるCAから直接、安全に署名鍵をインポートするものとする(SHALL)。 (例)CAから直接安全に署名鍵をインポートする手段は、以下が考えられる ・インターネットとの接合点は持たないセキュアな回線を用いる
6.2.2 eID means linking					6.2.2 電子識別手段のリンキング
LNK-6.2.2-01	Clause SRC_SA.1.1 of EN 419 241-1 [3] , specifying enrolment shall apply.	○	○	○	「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」の SRC_SA.1.1 項(登録(enrolment))に関する規定)が適用されるものとする(SHALL)。
LNK-6.2.2-02 [NSCP] [CONDITIONAL]	If the signer is a natural person, clause SRA_SAP.1.1 of EN 419 241-1 [3] , specifying enrolment shall apply.	○	○	○	署名者が自然人の場合、「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」の SRA_SAP.1.1 項(登録(enrolment))に関する規定)を適用するものとする(SHALL)。 SRA_SAP.1.1: 署名者の登録の保証レベルは、別表AのA.1に規定される「十分」以上であるものとする(SHALL)。 電子識別手段の特性及び設計の保証レベルは、別表AのA.2.1に規定される「十分」以上であるものとする(SHALL)。 認証メカニズムの保証レベルは、別表AのA.2.2に規定される「十分」以上であるものとする(SHALL)。
LNK-6.2.2-03	The SSASP shall link signing keys with the appropriate signer's eID means reference.	○	○	○	SSASP は、署名鍵を適切な署名者の eID 手段の参照情報とリンクさせるものとする(SHALL)。
LNK-6.2.2-04	The SSASP may generate eID means reference and provide the corresponding eID means to the signer (see clause 6.2.4).	○	○	○	SSASP は eID 手段の参照情報を生成し、対応する eID 手段を署名者に提供することができる(MAY)。 (6.2.4項参照)。

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
LNK-6.2.2-05	The SSASP shall ensure that the person identification data linked to the eID means reference is the same as the one linked to the subject of the associated certificate. NOTE 1: When the eID means reference is provided by the TSP issuing certificates registration service, the conformance to this requirement can be assumed.	○	○	○	SSASP は、eID の手段参照にリンクされた人物識別データが、関連する証明書のサブジェクトにリンク されたものと同一であることを保証するものとする(SHALL)。 注1：電子識別手段のリファレンスが証明書登録サービス発行元の TSP である場合、本要件への適合性があると見なすことができる
LNK-6.2.2-06	The signer's eID means reference may be provided by an authorized (external) party.	○	○	○	署名者の eID手段の参照情報 は、権限のある（外部の）当事者が提供してもよい（MAY）。
LNK-6.2.2-07 [LSCP] [CONDITIONAL]	If all or part of the authentication process is delegated to an external party the SSASP shall ensure the external party meets the requirements specified in LNK-6.2.2-01. NOTE 2: If the external party uses an eID means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1], there is no need to demonstrate the conformance to the required level, conformance to the regulatory requirements can be assumed.	○	○	○	認証プロセスの全部または一部が外部に委任される場合、SSASP は、その外部が LNK-6.2.2-01 に規定される要件を満たすことを保証するものとする(SHALL)。 注2: 外部当事者が、公的個人認証法第17条の4号の届け出もしくは5号、6号の認定事業者の場合、国により認められた、もしくは国際的な評価基準への適合性が独立した監査機関により認められた事業者の場合要求されるレベルへの適合性を仮定することが可能である。
LNK-6.2.2-08 [NSCP] [CONDITIONAL]	If all or part of the authentication process is delegated to an external party the SSASP shall ensure that the external party meets the requirements specified in LNK-6.2.2-02 and LNK-6.2.2-03.	○	○	○	認証プロセスの全部または一部が外部に委任される場合、SSASP は、その外部が LNK-6.2.2-02 および LNK-6.2.2-03 に規定される要件を満たすことを保証するものとする(SHALL)。
LNK-6.2.2-09 [NSCP] [CONDITIONAL]	If all or part of the authentication process is delegated to an external party the SSASP shall ensure that: -the external party fulfils all the relevant requirements of the present document and the requirements for registration according to the applicable regulatory requirements; or NOTE 3: In the context of the European Union, the applicable regulatory requirements are defined in Regulation (EU) No 910/2014 [i.1]. -the authentication process delegated to the external party uses an eID means issued under a notified scheme in accordance with the applicable regulatory requirements. NOTE 4: In the context of the European Union, the list of electronic identification means, issued under notified schemes, is published by the European Commission pursuant to Article 9 of Regulation (EU) No 910/2014 [i.1].	○	○	○	認証プロセスのすべてまたは一部が外部に委譲される場合、SSASP は以下を確認するものとする(SHALL)。 -外部当事者が、本文書の関連する全ての要求事項及び適用される規制要件に従った登録の要求事項を満たしている事、又は 外部当事者に委任された認証プロセスが、公的個人認証サービスの下で発行された電子識別手段を使用すること。 注3: 外部当事者が、公的個人認証法第17条の4号の届け出もしくは5号、6号の認定事業者の場合、国により認められた、もしくは国際的な評価基準への適合性が独立した監査機関により認められた事業者の場合要求されるレベルへの適合性を仮定することが可能である。
LNK-6.2.2-10	The SSASP shall protect the integrity of links between signer's signing key and its eID means reference.	○	○	○	SSASP は、署名者の署名鍵とその eID の参照手段との間のリンクの完全性を保護するものとする(SHALL)。
6.2.3Certificate linking					6.2.3 証明書のリンキング
LNK-6.2.3-01	Clause SRC_SKS.1.2 of EN 419 241-1 [3] , specifying certificate linking shall apply to the SSASC.	○	○	○	「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」の SRC_SKS.1.2 項（証明書のリンキングに関する規定）は、SSASC に適用されるものとする(SHALL)。 SRC_SKS.1.2 SSASCは、署名者の署名鍵を、適切な署名者の公開鍵証明書とリンクさせるものとする（SHALL）。
LNK-6.2.3-02	Clause SRC_SKS.1.4 of EN 419 241-1 [3] , specifying certificate linking shall apply to the SSASC.	○	○	○	「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」の SRC_SKS.1.4 項、（証明書のリンキングに関する規程）は、SSASC に適用されるものとする(SHALL)。
LNK-6.2.3-03	Clause SRC_SKS.1.5 of EN 419 241-1 [3] , specifying links protection shall apply to the SSASC.	○	○	○	「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」の SRC_SKS.1.5 項（リンクの保護に関する吉衛）は、SSASC に適用されるものとする(SHALL)。
6.2.4eID means provision					6.2.4 電子識別手段の提供
EID-6.2.4-01 [CONDITIONAL]	If the SSASP provides the signer's eID means, the eID means shall be securely passed to the signer.	○	○	○	SSASP が署名者の eID 手段を提供する場合、eID 手段は署名者に安全に渡されるものとする(SHALL)。
EID-6.2.4-02 [CONDITIONAL]	If the SSASP personalizes the signer's eID means with an associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signer's eID means.	○	○	○	SSASP が署名者の eID 手段を関連するユーザ活性化データ（例：PIN コード）でパーソナライズする場合、活性化データは署名者の eID 手段とは別に安全に準備・配布されるものとする。
6.3Signing key life-cycle operational requirements					6.3 署名鍵のライフサイクル運用要件
6.3.1Signature activation					6.3.1 署名活性化
SIG-6.3.1-01	Clause SRC_SA.1.2 of EN 419 241-1 [3] , specifying authentication shall apply.	○	○	○	「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」の SRC_SA.1.2 項（認証に関する規定）が適用されるものとする(SHALL)。 SRC_SA.1.2 SSAは、署名鍵の単独制御に影響を与える可能性のある行為を許可する前に、各署名者の識別と認証に成功することを要求するものとする（SHALL）。
SIG-6.3.1-02	Clause SRC_SA.1.3 of EN 419 241-1 [3] , specifying protocol security shall apply.	○	○	○	「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」の SRC_SA.1.3 項（プロトコルセキュリティの規定）を適用する(SHALL)。
SIG-6.3.1-03	Clause SRC_SA.1.4 of EN 419 241-1 [3] , specifying access control shall apply.	○	○	○	「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」の SRC_SA.1.4 項（アクセス制御を規定）を適用するものとする(SHALL)。
SIG-6.3.1-04	Clause SRC_SA.1.5 of EN 419 241-1 [3] , specifying signing key control shall apply.	○	○	○	「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」の SRC_SA.1.5 項（署名鍵管理に関する規定）を適用するものとする(SHALL)。
SIG-6.3.1-05 [NSCP]	Clause SRA_SKM.2.1 of EN 419 241-1 [3] , specifying signing key activation shall apply.		○	○	「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」の SRA_SKM.2.1 項（署名鍵の活性化に関する規定）を適用するものとする(SHALL)。SRA_SKM.2.1 SSASCは、署名者を認証し、署名鍵を活性化するために、署名者がSAMに対してSADを提示することを要求するものとする（SHALL）。
SIG-6.3.1-06 [NSCP]	Clause SRA_SAP.1.2 of EN 419 241-1 [3] , specifying protocol security shall apply.		○	○	「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」の SRA_SAP.1.2 項（プロトコルセキュリティに関する規定）を適用するものとする(SHALL)。SRA_SAP.1.2 SADおよびSAD使用に関する以下の脅威（オンライン推測、オフライン推測、クレデンシャル複製、フィッシング、盗聴、リプレイ、セッションハイジャック、中間者、クレデンシャル盗難、スプーフィング、マスカレード攻撃）に対抗するため、リスクアセスメントにより必要とされるコントロールを提供するものとする（SHALL）。
SIG-6.3.1-07 [NSCP]	Clause SRA_SKM.2.5 of EN 419 241-1 [3] , specifying signing key control shall apply.		○	○	「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」の SRA_SKM.2.5 項（署名鍵の管理に関する規定）を適用するものとする(SHALL)。 SRA_SKM.2.5 活性化された署名鍵は、SAPによって認可されたDTBS/Rのみに署名するために使用されるものとする（SHALL）。

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
SIG-6.3.1-08	The SSASP should ensure that the public key certificate is valid before using the corresponding signing key. NOTE:valid = not expired not revoked not suspended, can be met by applying DEL-6.3.2-01 if suspension is not used.	○	○	○	SSASP は、対応する署名鍵を使用する前に、公開鍵証明書が有効であることを確認するべきである(SHOULD)。 注：有効＝有効期間切れでない、失効していない、一時停止していない、一時停止を使用しない場合は DEL-6.3.2-01 を適用することにより満たすことができる 。
SIG-6.3.1-09	Signing keys shall be usable in only those cases for which the signer's consent has been obtained.	○	○	○	署名鍵は、署名者の同意が得られた場合のみ使用できるものとする(SHALL)。
SIG-6.3.1-10	Clause SRC_DSC.1.1 of EN 419 241-1 [3] , specifying signature creation's algorithm parameters shall apply.	○	○	○	「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」の SRC_DSC.1.1 項(署名生成のアルゴリズムパラメータを規定)を適用するものとする(SHALL)。
6.3.2 Signing key deletion					6.3.2 鍵の消去
DEL-6.3.2-01	Clause SRG_KM.7.1 of EN 419 241-1 [3] shall apply. If the public key certificate is revoked, the corresponding signing key shall be destroyed.	○	○	○	「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」の SRG_KM.7.1 項を適用するものとする(SHALL)。公開鍵証明書が失効された場合、対応する署名鍵は破棄されるものとする(SHALL)。
DEL-6.3.2-02	The SSASP shall destroy a signing key when requested by the signer.	○	○	○	SSASP は、署名者から要求された場合、署名鍵を破棄するものとする(SHALL)。
DEL-6.3.2-03	Clause SRG_KM.7.2 of EN 419 241-1 [3] , specifying session management shall apply.	○	○	○	「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」の SRG_KM.7.2 項(セッション管理に関する規定)が適用されるものとする(SHALL)。
DEL-6.3.2-04	Clause SRG_KM.7.3 of EN 419 241-1 [3] , specifying key backup deletion shall apply.	○	○	○	「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」の SRG_KM.7.3 項(鍵のバックアップの削除を規定)が適用されるものとする(SHALL)。SRG_KM.7.3 署名鍵破壊の仕組みと手順では、破壊された署名鍵の全てのバックアップもまた破壊され、残っている情報が署名鍵を再構築するために使用できないことを確実にすべきである(SHOULD)。
6.4 Facility, management, and operational controls					6.4 施設、管理、および運用管理
6.4.1 General					6.4.1 概要
OVR-6.4.2-01	The requirements identified in ETSI EN 319 401 , clause 7.6 shall apply. In addition, the following particular requirements apply:	○	○	○	「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」の 7.6 項に規定される要求事項を適用するものとする(SHALL)。さらに、以下の特別な要件が適用される。
OVR-6.4.2-02	The requirements identified in ETSI EN 319 411-1 [2], clause OVR-6.4.2-02 to OVR-6.4.2-10 shall apply mutatis mutandis to signing key generation and activation management services.	○	○	○	ETSI EN 319 411-1 [2]の OVR-6.4.2-02 項から OVR-6.4.2-10 項(物理的セキュリティ管理)で規定される要件は、(しかるべき変更を加えた上で)署名鍵生成および活性化管理サービスに準用されるものとする(SHALL)。 OVR-6.4.2-02 証明書の生成および失効管理に関わる設備は、システムまたはデータへの不正なアクセスによる危殆化からサービスを物理的に保護する環境で運用されるものとする(SHALL)。 OVR-6.4.2-03 物理的に安全なエリアへのすべての立ち入りは、独立した監視の対象となるものとし、権限のない者は、安全なエリアにいる間は権限のある者が同行するものとする(SHALL)。 OVR-6.4.2-04 すべての入退室は記録されるものとする(SHALL)。 OVR-6.4.2-05 物理的保護は、証明書生成および失効管理サービスの周囲に明確に定義されたセキュリティ境界線(すなわち物理的障壁)を設けることにより達成されるものとする(SHALL)。 OVR-6.4.2-06 他の組織と共有する施設のいかなる部分も、証明書生成及び失効管理サービスの周囲の外にあるものとする(SHALL)。 OVR-6.4.2-07 システムリソースを収容する施設、システムリソース自体、及びその運用をサポートするために使用される施設を保護するために、物理的及び環境的なセキュリティ管理を実施するものとする(SHALL)。 OVR-6.4.2-08 証明書生成及び失効管理サービスに関連するシステムに対する TSPの物理的及び環境的セキュリテ ィポリシーは、物理的アクセスコントロール、自然災害対策、火災安全要因、サポートするユーティリティ(電力、通信など)の障害、構造物の崩壊、配管の漏れ、窃盗、不法侵入に対する保護、及び災害 回復に対処するものとする(SHALL)。 OVR-6.4.2-09 TSPのサービスに関連する機器、情報、メディア、及びソフトウェアが許可なくオフサイトに持ち出され ないように管理を行うものとする(SHALL)。 OVR-6.4.2-10 TSPの運用に関連する他の機能は、アクセスが許可された人員に限定されることを条件に、同じ保護区域内でサポートできる(MAY)。
6.4.3 Procedural controls					6.4.3 手続き上のコントロール
OVR-6.4.3-01	The requirements REQ-7.4-04 to REQ-7.4-09 in ETSI EN 319 401 shall apply.	○	○	○	「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」の要求事項 REQ-7.4-04 から REQ-7.4-09 が適用されるものとする(SHALL)。
6.4.4 Personnel controls					6.4.4 人的コントロール
OVR-6.4.4-01	The requirements identified in ETSI EN 319 401 , clause 7.2 shall apply.	○	○	○	「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」 7.2 項に規定される要求事項を適用するものとする(SHALL)。
6.4.5 Audit logging procedures					6.4.5 監査の記録手順
OVR-6.4.5-01	The requirements identified in ETSI EN 319 401 , clause 7.10 shall apply.	○	○	○	「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」 7.10 項に規定される要求事項が適用されるものとする(SHALL)。
OVR-6.4.5-02	All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and SSASC system access attempts.	○	○	○	セキュリティポリシーに関する変更、システムの起動・停止、システムクラッシュ及びハードウェア障害、ファイアウォール及びルータの動作、SSASCシステムアクセスの試行など、すべてのセキュリティイベントを記録するものとする(SHALL)。
OVR-6.4.5-03	Clause SRG_AA.1 of EN 419 241-1 [3] , specifying audit data generation shall apply.	○	○	○	「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」 SRG_AA.1項 (監査データ生成に関する規定)を適用するものとする(SHALL)。
OVR-6.4.5-04	Clause SRG_AA.2 of EN 419 241-1 [3] , specifying audit data availability shall apply.	○	○	○	「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」 SRG_AA.2項 (監査データの利用可能性に関する規定)を適用するものとする(SHALL)
OVR-6.4.5-05	Clause SRG_AA.3 of EN 419 241-1 [3] , specifying audit data parameters shall apply.	○	○	○	「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」 SRG_AA.3項 (監査データのパラメータに関する規定)を適用するものとする(SHALL)。
OVR-6.4.5-06	Clause SRG_AA.7 of EN 419 241-1 [3] , specifying audit data integrity shall apply.	○	○	○	「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」 SRG_AA.7項 (監査データの完全性に関する規定)を適用するものとする(SHALL)。
OVR-6.4.5-07	Clause SRG_AA.8 of EN 419 241-1 [3] , specifying audit data timing shall apply.	○	○	○	「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」の SRG_AA.8 項 (監査データのタイミングに関する規定)を適用するものとする(SHALL)。
6.4.6	Records archival				6.4.6 記録保管
OVR-6.4.6-01	The SSASP shall retain the audit data records for at least seven years after any certificate based on these records ceases to be valid and within the constraint of applicable legislation.	○	○	○	SSASP は、監査データの記録を、これらの記録に基づく証明書が効力を失った後、少なくとも 7 年間、適用される法律の制約の範囲内で、保持するものとする(SHALL)。
6.4.7	Key changeover				6.4.7 鍵更新
	No policy requirement.				規程しない
6.4.8	Compromise and disaster recovery				6.4.8 危殆化と災害復旧
OVR-6.4.8-01	The requirements identified in ETSI EN 319 401 , clauses 7.9 and 7.11 shall apply.	○	○	○	「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」の 7.9 項と 7.11 項で特定された要件が適用されるものとする(SHALL)。
6.5	Technical security controls				6.5 技術的なセキュリティ管理
6.5.1	Systems and security management				6.5.1 システム及びセキュリティ管理
OVR-6.5.1-01	The requirements identified in EN 419 241-1 [3] , clause SRG_M.1 shall apply.	○	○	○	「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」の SRG_M.1 項に規定された要件が適用されるものとする(SHALL)。
6.5.2	Systems and operations				6.5.2 システムと運用

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
OVR-6.5.2-01	The requirements identified in EN 419 241-1 [3] , clause SRG_SO.1 shall apply.	○	○	○	「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」の SRG_SO.1 項に規定された要求事項を適用するものとする(SHALL)。
OVR-6.5.2-02	The requirements identified in EN 419 241-1 [3] , clause SRG_SO.2 shall apply.	○	○	○	「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」、SRG_SO.2 項で特定された要求事項を適用するものとする(SHALL)。
6.5.3	Computer security controls				6.5.3 コンピューターセキュリティコントロール
OVR-6.5.3-01	The requirements REQ-7.4-01, REQ-7.4-02, REQ-7.4-03 and REQ-7.4-10 in ETSI EN 319 401 shall apply. NOTE:Requirements for the trustworthy systems can be ensured using, for example, systems conforming to EN 419 241-1 [3] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [i.6].	○	○	○	「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」の要件、REQ-7.4-01、REQ-7.4-02、REQ-7.4-03 および REQ-7.4-10 が適用されるものとする(SHALL)。 注:信頼できるシステムの要件は、例えば、「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」に準拠するシステム、またはISO/IEC 15408 [i.6]に従って定義される適切な保護プロファイル(またはプロファイル)を使用して確保することができる。
OVR-6.5.3-02	Clause SRG_AA.6.1 of EN 419 241-1 [3] , regarding system monitoring shall apply	○	○	○	「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」のSRG_AA.6.1項 (システム監視に関する規定)を適用するものとする(SHALL)。
6.5.4	Life cycle security controls				6.5.4 ライフサイクルセキュリティコントロール
OVR-6.5.4-01	The requirements identified in ETSI EN 319 401 , clause 7.7 shall apply for all service components.	○	○	○	「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」の 7.7 項で特定された要件が、すべてのサービス・コンポーネントに適用されるものとする(SHALL)。
6.5.5	Network security controls				6.5.5 ネットワークセキュリティコントロール
OVR-6.5.5-01	The requirements identified in ETSI EN 319 401 , clause 7.8 shall apply.	○	○	○	「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」の 7.8 項で特定された要件が適用されるものとする(SHALL)。
6.6	Compliance audit and other assessment				6.6 コンプライアンス監査およびその他の評価
	NOTE:See ETSI EN 319 403 [i.3].				注:ETSI EN 319 403 [i.3]を参照。
6.7	Other business and legal matters				6.7 その他のビジネスおよび法的事項
6.7.1	Fees				6.7.1 手数料
	These policy requirements are not meant to imply any restrictions on charging for TSP's services.				これらのポリシー要件は、TSP のサービスに対する課金に関する制限を意味するものではない。
6.7.2	Financial responsibility				6.7.2 財政的責任
OVR-6.7.2-01	Void NOTE:Financial responsibility is covered in clause 6.8.1 of the present document by OVR-6.8.1-01.				廃止 注:財務的責任については、本書 6.8.1 項の OVR-6.8.1-01 に記載されています。
6.7.3	Confidentiality of business information				6.7.3 業務情報の守秘義務
	No policy requirement.				規程しない
6.7.4	Privacy of personal information				6.7.4 個人情報の保護
OVR-6.7.4-01	The requirement REQ 7.13-05 identified in ETSI EN 319 401 shall apply.	○	○	○	「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」で特定された要件 REQ 7.13-05 が適用されるものとする(SHALL)。
6.7.5	Intellectual property rights				6.7.5 知的財産権
	No policy requirement				規程しない
6.7.6	Representations and warranties				6.7.6 表明と保証
OVR-6.7.6-01	The requirements REQ-6.3-05 and REQ-6.3-06 identified in ETSI EN 319 401 shall apply. NOTE:The SSASP has the responsibility for conformance with the procedures prescribed in this policy, even when the SSASP's functionality is undertaken by outsourcers.	○	○	○	「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」に規定されている要件 REQ-6.3-05 および REQ-6.3-06 が適用されるものとする(SHALL)。 注:SSASP は、SSASP の機能がアウトソーサーによって引き受けられる場合でも、本ポリシーに規定された手順への適合に責任を有する。
6.7.7	Disclaimers of warranties				6.7.7 保証の免責事項
	See clause 6.7.6.				6.7.6項を参照。
6.7.8	Limitations of liability				6.7.8 責任の制限
	Limitations on liability are covered in the terms and conditions as per clause 6.8.4.				責任の限定は、6.8.4 項のとおり、利用規約でカバーされます。
6.7.9	Indemnities				6.7.9 免責事項
	No policy requirement.				規程しない
6.7.10	Term and termination				6.7.10 期間と終了
	No policy requirement.				規程しない
6.7.11	Individual notices and communications with participants				6.7.11 参加者への個別通知と連絡
	No policy requirement.				規程しない
6.7.12	Amendments				6.7.12 修正
	No policy requirement.				規程しない
6.7.13	Dispute resolution procedures				6.7.13 紛争解決手続き
OVR-6.7.13-01	Void NOTE:Dispute resolution procedures is covered in clause 6.8.1 and 6.8.1 of the present document by OVR-6.8.1-01 and OVR-6.8.4-04.				無効 注:紛争解決手続きは、本書 6.8.1 項および 6.8.1 項の OVR-6.8.1-01 および OVR-6.8.4-04 でカバーされます。
6.7.14	Governing law				6.7.14 準拠法
	Not in the scope of the present document.				本文書の対象外
6.7.15	Compliance with applicable law				6.7.15 適用される法律の遵守
OVR-6.7.15-01	The requirements REQ-7.13-01 and REQ-7.13-02 identified in ETSI EN 319 401 shall apply.		○	○	「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」に規定される要件 REQ-7.13-01 および REQ-7.13-02 が適用されるものとする(SHALL)。
6.7.16	Miscellaneous provisions				6.7.16 雑則
	No policy requirement.				ポリシーの要件なし。
6.8	Other provisions				6.8 その他の規定
6.8.1	Organizational				6.8.1 組織的要件
OVR-6.8.1-01	The requirements identified in ETSI EN 319 401 , clause 7.1 shall apply.	○	○	○	「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」の 7.1 項に規定される要求事項を適用するものとする(SHALL)。
6.8.2	Additional testing				6.8.2 追加試験
	No policy requirement.				ポリシーの要件なし。
6.8.3	Disabilities				6.8.3 障害
OVR-6.8.3-01	The requirements REQ-7.13-03 and REQ-7.13-04 identified in ETSI EN 319 401 shall apply.	○	○	○	「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」で特定された要求事項 REQ-7.13-03 および REQ-7.13-04 が適用されるものとする(SHALL)。 「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」 REQ-7.13-03:提供されるトラストサービスおよびそれらのサービスの提供に使用されるエンドユーザー製品は、可能な場合には障害のある人もアクセスできるようにする必要がある。 REQ-7.13-04:アクセシビリティに関する規格を考慮する必要がある。
6.8.4	Terms and conditions				利用規約
OVR-6.8.4-01	The requirements identified in ETSI EN 319 401 , clause 6.2 shall apply.	○	○	○	「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」の 6.2 項に規定される要求事項を適用するものとする(SHALL)。
7	**Framework for definition of server signing application service component policy built on the present document**				**7. 本書を基に構築されたSSASCポリシーを定義するためのフレームワーク**
OVR-7-01 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 6.	○	○	○	本文書で定義された要求事項から SCP を構築する場合、ポリシーは条項 5 から 6 で特定されたすべての要求事項を組み込むか、さらなる制約条件を組み込むものとする(SHALL)。

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
OVR-7-02 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy shall identify any variances it chooses to apply.	○	○	○	本文書に定義された要求事項から SCP を構築する場合，ポリシーは，適用することを選択したあらゆる差異を特定するものとする(SHALL)。
OVR-7-03 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document.	○	○	○	本文書で定義された要件から SCP を構築する場合、契約者は、利用規約を締結する一環として、特定のポリシーが本文書で定義されたポリシーの要件に追加する、あるいはさらに制約する方法について知らされるものとする(SHALL)。
OVR-7-04 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy.	○	○	○	本文書で定義された要件から SCP を構築する場合、ポリシーを規定し承認する最終的な権限と責任を 持つ機関（例えば、ポリシー管理権限者）が存在するものとする(SHALL)。
OVR-7-05 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.	○	○	○	本文書で定義された要件から SCP を構築する場合、ビジネス要件を評価し、明記されたコミュニティ及び適用可能性のためにポリシーに含めるべきセキュリティ要件を決定するために、リスクアセスメントを実施するものとする(SHALL)。
OVR-7-06 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.	○	○	○	本文書で定義された要件から SCP を構築する場合、ポリシーを維持する責任を含む、定義されたレビュープロセ スに従って、ポリシーの承認と修正を行うべきである(SHOULD)。
OVR-7-07 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, a defined review process should exist to ensure that the policy is supported by the practices statements.	○	○	○	本文書で定義された要件から SCP を構築する場合，方針が実務の記述によって裏付けられていることを確 認するために，定義されたレビュープロセスが存在すべきである。
OVR-7-08 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, the TSP should make available the policies supported by the TSP to its user community.	○	○	○	本文書で定義された要件から SCP を構築する場合、TSP は、TSP がサポートするポリシーをその利用者コ ミュニティに公開すべきである(SHOULD)。
OVR-7-09 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, revisions to policies supported by the TSP should be made available to subscribers.	○	○	○	本文書に定義された要件から SCP を構築する場合、TSP がサポートするポリシーの改訂をサブスクライバに公開すべきである(SHOULD)。
OVR-7-10 [CONDITONAL]	[CONDITIONAL]: When building a SCP from requirements defined in the present document, a unique object identifier shall be obtained for the policy (e.g. OID or URI).	○	○	○	本文書で定義された要件から SCP を構築する場合，ポリシーについて一意のオブジェクト識別子（OID または URI など）を取得するものとする(SHALL)。
Annex A (normative):	**Specific requirements related to Regulation (EU) No 910/2014**				**eIDAS規則に関連する特定の要求事項**
A.1 SSASP as a Qualified TSP	The present annex specifies generally applicable policy and security requirements for a Qualified TSP implementing a service component operating a remote QSCD.			○	本付属書は、リモートQSCDを操作するサービス・コンポーネントを実装する適格TSPに一般的に適用されるポリシーおよびセキュリティ要件を規定する。
OVR-A.1-01 [EUSCP]:	[EUSCP]: The SSASP shall be a Qualified TSP as defined in Regulation (EU) No 910/2014 [i.1]. NOTE 1: The current general interpretation of Regulation (EU) No 910/2014 [i.1] is that the SSASP cannot be qualified for operating the server signing application service component (SSASC) only. The SSASP managing a QSCD, is required to be used as part of a qualified trust service as defined in Regulation (EU) No 910/2014 [i.1]. NOTE 2: See Regulation (EU) No 910/2014 [i.1] Article 3 (16) for trust service definitions.			○	[EUSCP]に準拠する。SSASP は、規則 (EU) No 910/2014 [i. 1] に定義される Qualified TSP であるものとする(SHALL)。 注1：規則（EU）No 910/2014[i.1]の現在の一般的な解釈は、SSASPは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）のみを操作するための資格を得ることはできないということである。QSCDを管理するSSASPは、規則（EU）No 910/2014[i.1]に定義されるように、適格トラストサービスの一部として使用することが要求される。 注2：トラストサービスの定義については、Regulation (EU) No 910/2014 [i.1] 第3条 (16) を参照のこと。
A.2 Policy name and identification [EUSCP]:	SSASPs following the present document can claim conformance to the present document via the following specific trust service policy OID: a)EUSCP: EU SSASC Policy itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)			○	本文書に従うSSASPは、以下の特定のトラストサービスポリシーOIDを介して、本文書への準拠を主張することができる。 a)EUSCP: EU SSASCポリシー itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)
A.3 General requirements					一般的要求事項
OVR-A.3-01 [EUSCP]:	[EUSCP]: All requirements specified for [NSCP] shall apply.		○	○	[EUSCP]:[NSCP]に規定された全ての要求事項を適用するものとする(SHALL)。
OVR-A.3-02 [EUSCP]:	[EUSCP]: The TSP's practice statement shall include the reference to the certification that the QSCD employed against the requirements of Regulation (EU) No 910/2014 [i.1], annex II.			○	[EUSCP]: TSP の運用規定には、規則(EU)No 910/2014[i.1]附属書Ⅱの要求事項に対して QSCD が採用した証明書への言及を含めるものとする(SHALL)。
A.4 Signing key generation					署名鍵の生成
GEN-A.4-01 [EUSCP]:	[EUSCP]: Signer's signing key shall be generated in a QSCD.			○	[ESCP]:署名者の署名鍵は、QSCD で生成されるものとする(SHALL)。
GEN-A.4-02 [EUSCP]:	[EUSCP]: The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.			○	[EUSCP]:QSCDは、適切な認証ガイダンス文書に記載された構成で、または同じセキュリティ目的を達成する同等の構成で運用されるものとする(SHALL)。
A.5 Signature activation					署名活性化
SIG-A.5-01 [EUSCP]:	[EUSCP]: Signer's signing key shall be used in a QSCD.			○	[EUSCP]:署名者の署名鍵は、QSCDで使用されるものとする(SHALL)。
SIG-A.5-02 [EUSCP]:	[EUSCP] The QSCD shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.			○	[EUSCP] QSCDは、適切な認証ガイダンス文書に記載された構成で、または同じセキュリティ目的を達成する同等の構成で運用されるものとする(SHALL)。

Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev(ETSI TS 119 431-1)を参考に作成

LSCP
NSCP
EUSCP

要求識別子	ETSI TS 119 431-1	監査項目			要求事項
SIG-A.5-03 [EUSCP]:	[EUSCP]: Clause SRA_SAP.1.3 of EN 419 241-1 [3] , specifying cryptographic strength shall apply.		○	○	[EUSCP]:「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」の SRA_SAP.1.3 項(暗号強度の規定)を適用するものとする(SHALL)。
SIG-A.5-04 [EUSCP]:	[EUSCP]: Clause SRA_SAP.1.4 of EN 419 241-1 [3] , specifying threats mitigation shall apply.		○	○	[Euscp]:「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」の SRA_SAP.1.4 項 (脅威の軽減に関する規定)を適用しするものとする(SHALL)。
SIG-A.5-05 [EUSCP]:	[EUSCP]: Clause SRA_SAP.1.5 of EN 419 241-1 [3] , specifying environment protection shall apply.		○	○	[EUSCP]:「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」の SRA_SAP.1.5 項(環境保護に関する規定)を適用するものとする(SHALL)。
SIG-A.5-06 [EUSCP]:	[EUSCP]: Clause SRA_SAP.1.6 of EN 419 241-1 [3] , specifying protection against tampering shall apply.		○	○	[EuscP]:「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」の SRA_SAP.1.6 項 (改ざんに対する保護規定)を適用するものとする(SHALL)。
SIG-A.5-07 [EUSCP]:	[EUSCP]: Clause SRA_SAP.1.7 of EN 419 241-1 [3] , specifying protection against attacker shall apply.		○	○	[EuscP]:「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」の SRA_SAP.1.7 項 (攻撃者に対する防御規定)を適用するものとする(SHALL)。
A.6 Signature activation data management					署名活性化データの管理
SIG-A.6-01 [EUSCP]:	[EUSCP]: Clause SRA_SAP.2.1 of EN 419 241-1 [3] , specifying signature activation data format shall apply.		○	○	[EUSCP]:「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」の SRA_SAP.2.1項 (署名活性化データ形式に関する規定)を適用するものとする(SHALL)。
SIG-A.6-02 [EUSCP]:	**[EUSCP]: Clause SRA_SAP.2.2 of EN 419 241-1 [3] , specifying signature activation data collection and generation shall apply.**		○	○	[EUSCP]:「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」の SRA_SAP.2.2 項(署名活性化データの収集と生成に関する規定)を適用するものとする(SHALL)。
SIG-A.6-03 [EUSCP]:	[EUSCP]: Clause SRA_SAP.2.3 of EN 419 241-1 [3] , specifying signature activation data parameters shall apply.		○	○	[EUSCP]:「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」の SRA_SAP.2.3項(署名活性化データのパラメータに関する規定)を適用するものとする(SHALL)。
SIG-A.6-04 [EUSCP]:	**[EUSCP]: Clause SRA_SAP.2.4 of EN 419 241-1 [3] , specifying signature activation data usage shall apply.**		○	○	[EUSCP]:「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」の SRA_SAP.2.4 項(署名活性化データの使用法に関する規定)を適用するものとする(SHALL)。
SIG-A.6-05 [EUSCP]:	[EUSCP]: Clause SRA_SAP.2.5 of EN 419 241-1 [3] , specifying signature activation data destination, shall apply.		○	○	[EUSCP]:「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」の SRA_SAP.2.5 項(署名活性化データの提出先に関する規定する)を適用するものとする。
SIG-A.6-06 [CONDITONAL] [EUSCP]:	**[EUSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.2.6 of EN 419 241-1 [3] , specifying signature activation data collection and protection shall apply.**		○	○	[EUSCP] :「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」 SRA_SAP.2.6項(署名者が自然人の場合の署名活性化データの収集と保護に関する規定)を適用するものとする(SHALL)。
SIG-A.6-07 [CONDITONAL] [EUSCP]:	[EUSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.2.7 of EN 419 241-1 [3] , specifying signature activation data submission under sole control shall apply.		○	○	[EUSCP] :「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」のSRA_SAP.2.7項(署名者が自然人の場合のソールコントロールの下での署名活性化データの提出に関する規定)を適用するものとする。
SIG-A.6-08 [EUSCP]:	**[EUSCP]: Clause SRA_SAP.2.8 of EN 419 241-1 [3] , specifying signature activation data protection after activation shall apply.**		○	○	[EUSCP]:「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」のSRA_SAP.2.8項(活性化後の署名活性化データ保護に関する規定)を適用するものとする(SHALL)。

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　別表A

A.1　登録

A.1.1　申請と登録

保証レベル	必要な要素
「低」	1. 電子識別手段の使用に関する条件を申請者が認識していることを確実にする。 2. 電子識別手段に関連する推奨されるセキュリティ上の注意事項を申請者が認識していることを確実にする。 3. 身元確認と検証に必要な関連する同一性識別情報を収集する。
「十分」	レベル「低」と同じ。
「高」	レベル「低」と同じ。

A.1.2　身元確認と検証（自然人）

保証レベル	必要な要素
「低」	1. 申請者は、主張された身元を示している証拠をその人物が所持していると仮定することができる。 2. 証拠が真正である、または信頼できる情報源によって存在すると仮定でき、その証拠は有効であるとみなせる。 3. 主張された身元が存在することが信頼できる情報源によって知られており、その身元を主張する人 が同一人物であると仮定することができる。
「十分」	レベル「低」に加えて、1〜4のいずれかの選択肢を満たす必要がある 1. 申請者は、主張された身元を示している証拠をその人物が所持していると検証されている かつ その証拠が真正であることを確認している、または信頼できる情報源によって、その証拠が存在し、実在の人物に関連するものであると知られている かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元ではないリスクを最小限に抑えるための措置が取られている または 2. 身元証明書が登録手続き中に提示され、その書類が提示した人物に関連するとみなせる かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元でないリスクを最小限に抑えるための措置が取られていること または 3. 電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠した適合評価機関又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 4. 電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行され、個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、保証レベル「十分」または「高」は、 適用される規制要件（注1参照）に準拠する適合性評価機関または同等の機関によって確認されなけ ればならない。

「高」	1または2のいずれかの要件を満たす必要がある 1.レベル「十分」、かつ、(a)～(c)に掲げる選択肢のうち1つを満たさなければならない (a) 申請者は、主張された身元を示している写真または生体識別証拠を所持していることが確認されている場合、その証拠が信頼できる情報源によって有効であると確認されている かつ 申請者が、1つまたは複数の身体的特徴を信頼できる情報源と比較することにより、主張された本人であると確認される または (b) 電子識別手段の発行以外の目的で，公的又は私的団体が以前に使用した手順が，保証レベル「高」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合性評価機関（注2参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ 以前の手順の結果が有効であることを証明するための措置を講じている または (c) 電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行され、 個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関または同等の機関によって、保証レベル「高」が確認されなければならない かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている または 2.申請者が認められた写真または生体識別証拠を提示しない場合、そのように認められた写真または生体識別証拠を取得するために、国レベルで使用されるものと全く同じ手順が適用される。

A.1.3 身元確認と検証（法人）

保証レベル	必要な要素
「低」	1. 法人の主張する身元は、証拠に基づいて証明される。 2. 証拠が有効であるとみなせ、かつ真正である、または信頼できる情報源に従って存在すると仮定できる。ただし、信頼できる情報源に法人が含まれることは任意であり、法人と信頼できる情報源の間の協定によって規制される。 3. その法人が、その法人として行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。

「十分」	レベル「低」に加えて、1〜3のいずれかの選択肢を満たす必要がある 1.電子識別手段の申請が行われた証拠に基づいて、主張された法人のアイデンティティが証明されている。ここには法人の名前、法人形態、登録番号(該当する場合)を含む。 かつ その証拠が真正であることを確認している、あるいは信頼できる情報源に従って既知かどうかが確認されていて、法人がその分野で活動するために信頼できる情報源に法人が含まれることが求められる かつ 例えば、紛失、盗難、停止、失効または期限切れの証憑書類のリスクを考慮し、法人のアイデンティティが主張するアイデンティティと異なるリスクを最小限に抑えるための措置が取られていること または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.3 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合評価機関（注1参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 3.電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、電子識別証明および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関 （注1参照）または同等の機関によって、保証レベル「十分」または「高」を確認する必要である。
「高」	レベル「十分」に加えて、1〜3のいずれかの選択肢を満たす必要がある 1.主張される法人のアイデンティティは証拠に基づいて証明される。ここには、法人の名前、法人形態、および国内で使用される法人を表す少なくとも 1 つの固有識別子が含まれる。 かつ その証拠が信頼できる情報源に基づき有効であることを確認する または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「高」について A.1.3 節に規定するものと同等の保証を提供する場合，その同等の保証が， 該当する規制要件に準拠する適合性評価機関（注2参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ この前の手順の結果が有効であることを証明するための措置がとられている または 3.電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関 （注2参照）または同等の機関によって、保証レベル「高」が確認されなければならない。 かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている。

A.1.4　自然人と法人の電子識別手段の紐づけ(バインディング)

保証レベル	必要な要素
「低」	1.法人を代表して行動する自然人の身元確認が、レベル「低」以上で行われたことが確認される。 2.バインディングは、国に認められた手順に基づいて確立されている。 3.自然人が、その人が法人を代表して行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。
「十分」	レベル「低」の3に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「十分」または「高」で行われたことが検証される。 2.バインディングは、国に認められた手続きに基づいて確立され、その結果、信頼できる情報源に登録されたものである。 3.バインディングは、信頼できる情報源からの情報に基づいて確認されている。
「高」	レベル「低」の3、レベル「十分」の2に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「高」で行われたことが検証される。 2.バインディングは、国内で使用される法人を表す固有の識別子、及び信頼できる情報源からの自然人を表す固有の情報に基づいて検証されている。

A.2　電子識別手段と認証

A.2.1　電子識別手段の特性と設計

保証レベル	必要な要素
「低」	1.電子識別手段は、少なくとも1つの認証要素を利用する。 2.電子識別手段が、その電子識別手段を携帯する者の制御下または所有下にある場合のみ使用されることを確認するための合理的な措置を、発行者が講じるように設計されていること。
「十分」	1.電子識別手段は、異なる種類から少なくとも2つの認証要素を利用する。 2.電子識別手段は、その電子識別手段を携帯する者の制御下または所有下にある場合にのみ使用されることが想定できるように設計されていること。
「高」	レベル「十分」に加えて、 1.電子識別手段は、複製や改ざん、さらには攻撃可能性が高い攻撃者から保護する。 2.電子識別手段は、他人の使用に対して、その電子識別手段を携帯する者が確実に保護することができるように設計されている。

A.2.2　認証メカニズム

保証レベル	必要な要素
「低」	1.個人識別データの開示は、電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムの一部として個人識別データが保存される場合、その情報は、紛失や、オフラインでの分析を含む侵害を防ぐために保護されている。 3.認証メカニズムは、基本的な攻撃能力を強化した攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低いように、電子識別手段の検証のためのセキュリティ制御を実装している。

「十分」	レベル「低」に加え、 1.個人識別データの開示は、動的認証による電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムは、中程度の攻撃力を持つ攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。
「高」	レベル「十分」に加え、 認証メカニズムは、攻撃力の高い攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。

リモート署名サービスの評価基準

― 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 を参考に作成）

目次

1　スコープ

1.1 概要

本書はデジタル署名を生成する、サーバー署名を支える信頼できるシステムとしての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（以降 SSASC）に対するセキュリティ要件と推奨事項を規定する。

SSASC は少なくとも 1 台のリモート署名アプリケーション（以降 SSA）と 1 台の署名生成装置（以降 SCDev）、または 1 台のリモート署名生成装置で構成される。

リモート SCDev は、改ざん防止環境で実行される署名活性化モジュール(以降 SAM)によって提供される拡張リモート制御 SCDev によって拡張されている。このモジュールは署名活性化プロトコル（以降 SAP）によりまとめられた署名活性化データ（以降 SAD）を使用し、署名鍵が署名者の単独制御下(sole control)で使用されていることを高い信頼性で保証する。

SSA は、承認された署名者のみの単独制御下で署名鍵を生成・維持・使用するために SCDev またはリモート SCDev を使用する。

そのため SSA がリモート SCDev を使用する場合、認可された署名者は高い信頼性をもって署名鍵をリモートで制御する。

SSASC は、署名対象データに基づいて作成されたデジタル署名を署名者または他アプリケーションに配信することを目的とする。

— 本標準は、SSASC の一般的に認識されている機能モデルを提供する。

— 機能モデルで識別された全てのサービスに適用される全体的な要件を規定する。

— SSASC で識別された各サービスに対するセキュリティ要件を規定する。

— SSASC が使用する可能性のある機密性の高いシステムコンポーネントのセキュリティ要件を規定する。本規格は技術およびプロトコルに中立的であり、セキュリティ要件に重点を置いている。

1.2 スコープの対象外

以下の点は、本書のスコープ外としている。

— 電子証明書発行サービス、署名検証サービス、タイムスタンプサービス、情報保存サービスなど、本サービスと共に利用される可能性のあるその他トラストサービス

— SSASC 以外のアプリケーションやシステム（特に、高度な署名フォーマットの作成を含む署名作成アプリケーション）

— 署名形式に関する法的解釈（デジタル署名、e シール、適格、その他）

1.3 想定読者

本規格は、以下のようなセキュリティ要件を規定している。

— SSASC システム提供会社

— 署名生成サービスを提供するトラストサービスプロバイダー(TSP)

— 署名生成サービスを提供するトラストサービスプロバイダー(TSP)の適合性評価を実施する独立機関

2 参照規格

参照規格は、リモート署名サービスの評価基準を参照のこと。

3 用語と定義

用語と定義は、リモート署名サービスの評価基準を参照のこと。

4 記号・略語

記号・略称は、リモート署名サービスの評価基準を参照のこと。

5 サーバー署名をサポートする信頼できるシステムの解説

5.1 概要

本節では、第 6 章のセキュリティ要件がどのように実装されるべきかを明確にするため、サーバー署名 のさまざまな概念について記述する。

本標準のすべての要求事項は明確に記述され、以下のようになる：

— 必須（SHALL(NOT)で示す）

— オプション（SHOULD（NOT）で示す）

— 許可（MAY（NOT）で示す）

（法助動詞の使い分けの詳細は、「リモート署名サービスの評価基準」1.6 評価基準の文書における法助動詞、参照）

5.2 署名生成とサーバー署名の目的

SSASC の目的は、DTBS/R を受け取り、署名者のコントロール下でデジタル署名を生成することである。

※(Data To Be Signed Representation：署名対象データ(ハッシュ値))

5.3 自然人の電子署名または法人のeシール

デジタル署名は、電子署名やeシールを表すために使用することができる。

署名鍵の管理に関する信頼度は、デジタル署名がシールを表す場合と電子署名を表す場合とで、必ずしも同じであることは期待できない。

本規格に準拠して作成されたデジタル署名は、自然人または法人の管理下で生成することができる。

本規格では便宜上、自然人または法人を対象とし、署名者という用語を使用する。

本規格では便宜上、署名生成装置や e シール生成装置も含めて SCDev という用語を使用する。

5.4 署名者唯一による署名鍵の制御(Sole control)の保証レベル

本書では、単独制御のための 2 つの保証レベルを定めている:

— 単独制御保証レベル 1 (Sole control assurance level 1：SCAL1):

- 署名鍵は、署名者の単独制御のもとで、低い信頼度で使用される。
- 認可された署名者が署名のためにその鍵を使用することは、署名者を認証する SSA によって強制される。

— 単独制御保証レベル 2（Sole control assurance level 2 :SCAL2):

- 署名鍵は、署名者の唯一の管理下で、高い信頼性をもって使用される。
- 承認された署名者が署名のためにその鍵を使用することは、対応する署名鍵の使用を可能にするために、署名者が SAP を使用して提供する SAD により、SAM によって強制される。

単独制御保証レベル 1 または 2 を使用するかどうかは、署名ポリシーと適用される法的要件に依存する。

5.5 バッチサーバー署名

発出元証明に用いる e シールのように、署名者が各文書を閲覧し明示的に承認することを必要とせず、また署名前に閲覧する機会を与えることなく、一括して署名することが可能なところもある。

このことは、署名者は、個々の文書ではなく、バッチの署名プロセスに対してのみ、唯一のコントロールを適用すればよいことを意味する。

（注）EU との電子署名の相互運用にリモート署名を用いる場合は、EU 加盟国の中には、一括署名を認めていない国もあることに留意すべきである。この場合、この禁止があらゆる種類の先進電子署名に盲目的に適用されるのか、それとも適格署名のみに適用されるのかを確認する必要がある。

一括署名の法的適用性は法的およびアプリケーション環境に依存するため、SSASC は電子署名の一括署名を許可または不許可とする設定プロファイルを持つべきである (SHOULD)。

5.6 署名鍵と暗号化モジュール

SCAL1 での電子署名は、高い柔軟性を保証するために、署名鍵(非対称鍵ペアの秘密鍵など)は必ずしも暗号モジュール(ハードウェアセキュリティデバイスやスマートカードなど)内で生成・保存・使用する必要はない。署名鍵はファイルに保存し、そのファイルを用いて SCDev をソフトウェア化することも可能である。

ファイルを使用する場合、ファイル自体を改ざん(削除、変更)から保護することに加え、特定の外部セキュリティ対策を実施するべきである(SHOULD)。

しかしながら、本基準は、SSASC が電子署名を作成するために、改ざん防止環境で保護された署名鍵を使用することを推奨する。すなわち、SCDev は暗号モジュール(例えば、EN 419211 シリーズまたは CEN/TS 419221 シリーズに準拠したハードウェアセキュリティデバイス)であるべきである(SHOULD)。

5.7 署名者の認証

＜概要＞ （EN419 241-2 4.4 TOE Overview から抜粋、加筆）

SSA は、署名者の署名鍵が、意図された目的のために署名者の単独制御のもとでのみ使用されることを保証する。SSA は暗号モジュールを使用してデジタル署名値を生成する。

SCAL2 では、署名操作は署名活性化プロトコル（SAP）を使用して実行され、署名活性化データ（SAD）がローカル環境で提供される必要がある。SAD は、署名鍵を指定する情報、当該署名鍵に対する署名者認証、署名対象データのハッシュ値（DTBS/R(s)）の 3 つの要素を結合し、DTBS/R が署名者が指定したデータのものであること、および、それらの真正性が保証され、署名活性化モジュール（SAM）によって検証されなければならない。SAM は SAD を検証することにより、暗号モジュール内で署名鍵を活性化することができる。暗号モジュールと SAM はともに、耐タンパー保護環境内に配置される。SAD の検証とは、SAM が 3 つの SAD エレメント間のバインディングをチェックし、署名者が認証されていることを確認することである。

3 つの SAD 要素の 1 つは署名者認証である。EU と同等の適格電子署名を行う場合、署名者認証は本書の SCAL2 のすべての要件に従って実施されるものとする。すなわち、署名者認証は以下のいずれかの方法で実施できる:

— SAM が直接行う。この場合、SAM は署名者の認証要素を検証する。

— SAM による間接的なもの。この場合、SSA の一部、または委託された認証サービスが、署名者の認証要素を検証し、署名者が認証されたというアサーションを発行する。SAM はアサーションを検証するものとする。

— 署名者認証の一部が SAM によって直接行われ、別の一部が SAM によって間接的に行われる。

図 1 に、ローカル環境とリモート TSP の保護環境、耐タンパー保護環境の概要を示す。本基準の Level3 では SAM は SCDev(QSCD)の耐タンパー保護環境(図1の青の破線部分)に含めるものとし、Level2 では SAM はリモート TSP の保護環境内に設置し、SCDev の耐タンパー保護環境(赤の実線部分)には CM(Cryptographic Module:暗号モジュール)を設置するものとする。

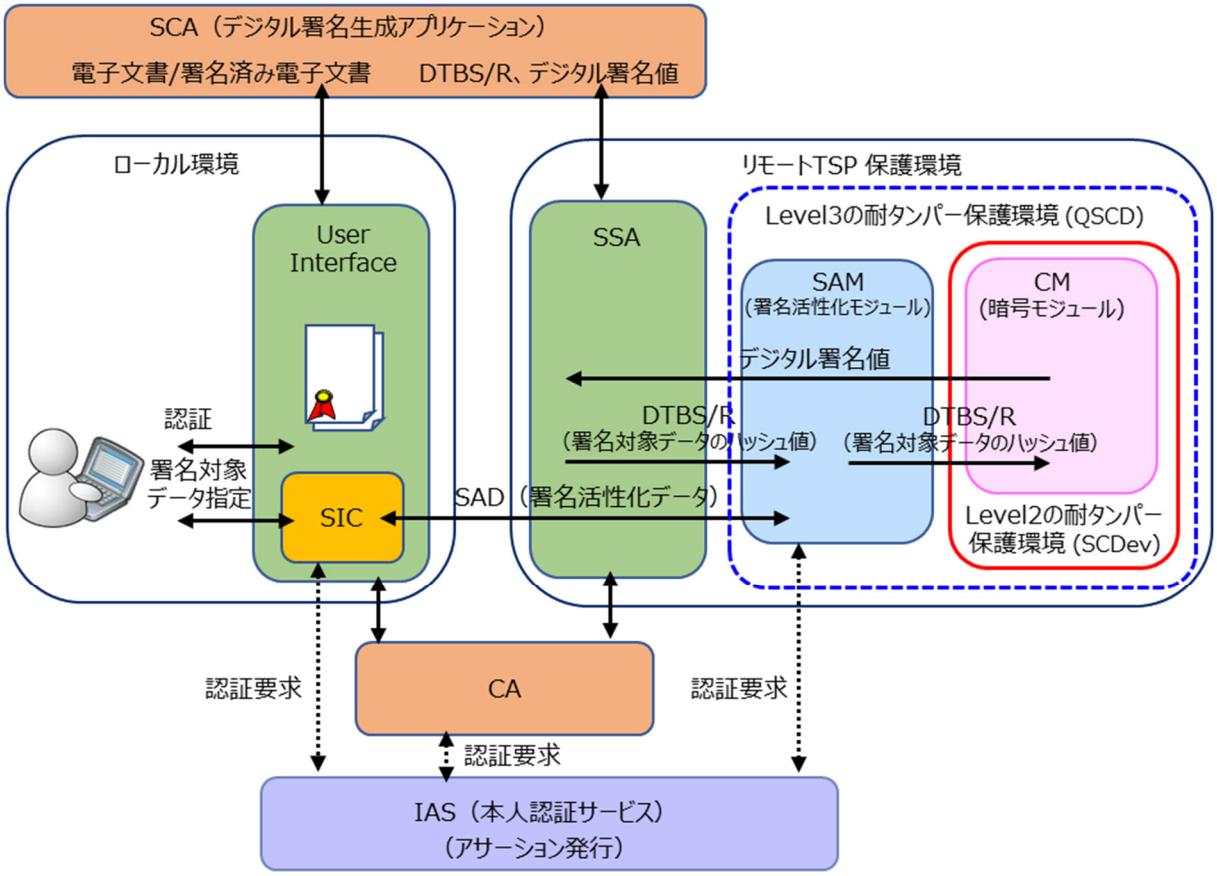


図 1 ローカル環境とリモート TSP の保護環境の概要

(EN 419 241-2 より抜粋加筆)

5.7.1 電子識別手段

5.7.1.1 SCAL1

署名者の登録と電子識別手段の特性および設計要件は、SRC_SA.1.1 に定義される。

5.7.1.2 SCAL2

署名者の登録と電子識別手段の特性および設計要件は、SRA_SAP.1.1 に定義される。

5.7.2 Authentication Mechanism

5.7.2.1 SCAL1
認証機構の要件は、SRC_SA.1.1 に定義される。

5.7.2.2 SCAL2
認証機構の要件は、SRA_SAP.1.1 に定義される。

5.7.3 認証ターゲット

5.7.3.1SCAL1
— 署名操作へのアクセスを許可するために、署名者は SSA に対する認証に成功しなければな らない。

— 署名者の署名鍵は、SSA によって署名者の認証要素にリンクされなければならない。

5.7.3.2SCAL2
— SCDev 内の署名操作を許可するために、SAD は設定され、計算され、または SSA を通して SAM と SIC の間の安全なやりとりの結果となるものとする(SHALL)。

— SAD は、専用 DTBS/R の SCDev 内での署名操作を許可するために、SSA を通して SAM に送信されるものとする(SHALL)。

5.7.4 外部機関への認証の委任

5.7.4.1 概要
TSP は、認証プロセスを外部当事者(例えば、ID プロバイダー)に委任できる(MAY)。

5.7.4.2 SCAL1
TSP は、外部当事者に委任された認証プロセスが SRC_SA.1.1 に規定される要件を満たすことを保証するものとする(SHALL)。

注） 外部当事者が、公的個人認証法第 17 条の 4 号の届け出もしくは 5 号、6 号の認定事業者の場合、国により認められた、もしくは国際的な評価基準への適合性が独立した監査機関により認められた事業者の場合要求されるレベルへの適合性を仮定することが可能である。

5.7.4.3 SCAL2
TSP は、外部当事者に委任された認証プロセスが SRA_SAP.1.1 に規定される要件を満たすことを保証するものとする(SHALL)。

TSP は、以下を保証するものとする(SHALL):

— 外部当事者が、本基準の関連するすべての要求事項及び適用される規制要件に従った登録の要求事項を満たしていること、又は

— 外部当事者に委任された認証プロセスが、公的個人認証サービスの下で発行された電子識別手段を使用すること。

注 1） 外部当事者が、公的個人認証法第 17 条の 4 号の届け出もしくは 5 号、6 号の認定事業者の場合、もしくは国や、国により認められた国内外の基準への適合性が独立した監査機関の監査で確認された事業者の場合、要求されるレベルへの適合性を仮定することが可能である。

注 2） 公的個人認証法に基づき、地方公共団体情報システム機構（J-LIS）により運営されている、個人認証サービスで利用者のマイナンバーカードの IC チップ内に当該利用者の電子証明書を発行する。

5.8 署名活性化データ（SAD）

SCAL2 に到達するために、署名者の鍵の管理を確実にするために SAD を使用することは、SAM によって強制されるものとする。

SCAL2 での署名の有効化は、署名者の認証と署名者の署名操作要求の真正性といういくつかの条件を満たすことを必要とする(詳細は 5.7 で示される)。

両特性は SAD によって直接与えられてもよい。しかし、例えば、認証の委任を使用するなどして、SAD 生成前に署名者認証を実行することも可能である。

SAD は、データセットである場合もあれば、同じ情報を導き出すことができる暗号操作の結果（詳細は SRA_SAP.2 に記載されている）である場合もある。

SAD は、署名者を直接または間接的に認証するために寄与する。

署名者の認証が SAD の収集前に行われる場合、SAD は、既知のソースから主張された署名者を識別する項目を 含まなければならない。このアサーションは、SIC または信頼できる e ID プロバイダーのいずれかから得てもよい。アサーションのソースは、認証されるものとする。

5.9 署名活性化プロトコル（SAP）

SAP は、署名者に代わって暗号モジュールが実行する電子署名の生成のために、署名鍵の安全な 使用を可能にするように設計されなければならない。

SAP は、署名者（SIC 経由）と SSASC が SAD を生成するために通信するプロトコルである。

SAP の設計は、最低限以下の検証を含むものとする:

— 署名鍵を使用する際の署名者の認証

— SAD を使用した署名要求の真正性の確保

— 選択された署名鍵が有効かつアクティブであること

— SAD の全エレメントを安全に転送すること

署名鍵を、証明書取得のための証明書発行要求の鍵の所持証明に使用しない場合、SAP は以下の検証を含むべきで ある:

— 署名鍵に関連する有効な証明書が存在すること

5.10 署名者のインタラクションコンポーネント（SIC）

SIC は、署名者の環境において、署名者の単独制御で動作するソフトウェアおよび/またはハードウェアの一部である。

このコンポーネントの使用は、SAP プロセスおよび SCDev による電子署名の作成に不可欠である。

SIC は、署名者を認証するため、または SAD を生成するために、常に SAP を使用する:

— SIC は、直接 SAD を生成することができる。もしくは

— SIC は署名者を認証するために使用することができ、署名者を識別するアサーションは SAD 生成に使用される

このコンポーネントは、たとえば次のようなもの（またはその組み合わせ）である：

— ブラウザで実行されるアプリケーション（例：TLS 上の HTTP POST フォーム）

— モバイルデバイス（スマートフォン、タブレットなど）により実行されるアプリケーション

— 携帯電話のセキュアエレメント

— 署名者が所有する暗号化装置（eID トークン、eToken、FIDO-Token など）

— [...]

SIC は、署名者と SAP 内の署名操作の間のリンクを強制する。

5.11 署名活性化モジュール（SAM）

SAM は、SCAL2 の署名鍵が署名者のみの管理下で使用されることを高い信頼性で保証するために、SAD を使用するソフトウェアである。

SAM は、耐タンパー環境(改ざん防止環境)下で使用することが要求される。

SAM が SCDev と同じ耐タンパー環境(改ざん防止環境)で使用されない場合、耐タンパー環境(改ざん防止環境)間双方の安全なチャネルが必要である。

5.12 環境

注） 図 1 で表す、3 つの異なる環境が定義されている。

5.12.1 耐タンパー環境

耐タンパー環境（改ざん防止環境）は、TSP 保護環境内で運用され、インターネットからの直接アクセスから保護される。この環境内で実行されるコードの完全性を保証する。

コードは署名鍵の使用を保護し、署名の有効化を署名者の制御下に置くことを強制する。

耐タンパー環境(改ざん防止環境)は、署名鍵と署名者の間のリンクも保護する（リンクは署名作成に必要なときに作成され、チェックされる）。

SCAL1 では、秘密鍵は耐タンパー環境(改ざん防止環境)で生成され使用されることが推奨される。

SCAL2 の場合は、秘密鍵の生成と耐タンパー環境(改ざん防止環境)下での使用が必須となる。また、SAM のソフトウェアは、改ざん防止された環境で使用されることが要求される。

5.12.2 TSP により保護された環境

TSP 保護環境は、サーバー署名システムの安全な運用のための要件に従って監査される。

この環境は、インターネットからの攻撃から保護し、外部環境（署名者、SCA、RA など）との間のインター ネット接続を処理する。

この環境は、保護された形式で、署名鍵、および鍵と署名者の間のリンクを保存できる。

TSP は、SAD および SAP の要件を満たし、RA 環境に（登録に関する）義務を課すために、この環境を保護する。仕様は、例えば、ETSI EN 319 411-1:2015, 6.2.2 および ETSI EN 319 411-2:2015, 6.2.2 で示される。

また、単独制御を証明するための証明書登録の要件も満たす必要がある（RA が必要とする）。これらの要件は、例えば ETSI EN 319 411-1:2015, 6.3.1 a および 6.3.3 d に規定されている。

5.12.3 署名者の環境

署名者の環境は、署名者のローカルなものである。

署名者は、その環境を保護する責任がある。署名者が第三者によって提供された環境を使用する場合，第三者は署名者の環境の保護に責任を負う。

署名者環境は、SIC と同様に、署名される文書の準備と文書署名のフォーマット化に使用される一般的な要素からなる。

SIC は署名者が使用し、署名者と SAP を通じて起動される署名操作全体との間のリンクを作成するために使用される。

この規格に関して、SIC に対する直接的な認証要件はない。しかし、SIC の設計および実装において、SAD の伝送/計算に関する要件、および署名者の認証を含む SAP を介した SIC と SAM の相互作用を考慮することが必要である。

5.13 機能モデル

5.13.1 概要

SSASC のスコープ、構成要素及び起動メカニズムを示すために、SSASC の概念的なアーキテクチャーを示す。

実際には、負荷分散や冗長性のために複数のサーバーやデバイスを使用することになるが、これは物理的なアーキテクチャーを表すものではない。

署名者の環境は、SSASC にとって未知である。例えば、信頼できるソフトウェアのみをインストールし、悪意のあるソフトウェアに対する保護を使用することで、保護する必要がある。

署名生成サービスを提供する TSP は、SSASC の環境を保護する。SSASC は、一般的な物理的、人的、手続き的、文書的なセキュリティ要件と、署名生成サービスを提供する TSP に対する特定の要件が組み込まれたセキュリティポリシーで運用される。

要件の定義は、例えば、「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」に記載されている。

SCAL2 では、署名鍵および SAM は、改ざん防止環境（例：EN 419211 シリーズまたは CEN/TS 419221 シリーズに準拠した暗号モジュール）により保護されている。

5.13.2 要求事項のスコープ

SSASC は、署名者の署名鍵の安全なリモート管理、およびリモート管理された署名鍵による電子署名の作成を提供する。

本標準は、サーバーおよび署名者システムを 1 つまたは複数のコンポーネントに分割する方法について、何ら制限を課さない。署名生成アプリケーション（SCA）は本標準の適用範囲外であり（図 2 参照）、証明書発行に関連する TSP の信頼できるシステムの要件は適用範囲外である（CEN/TS 419 261 参照）。

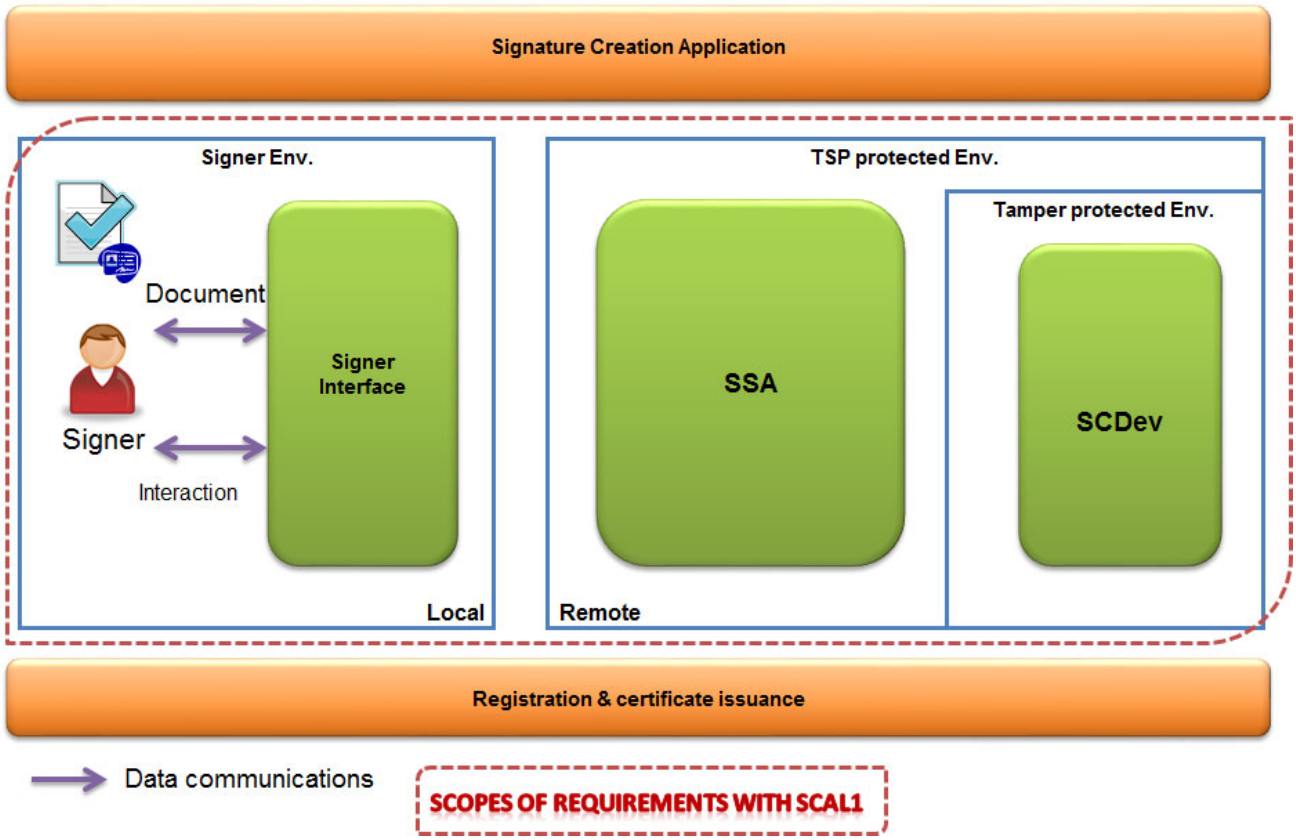


図 2 – 要求事項のスコープ

注　認証の委任(5.7.4 参照)を使用する場合、要求事項の範囲を外部当事者に拡張することができる(MAY)。

5.13.3 署名の活性化メカニズム

5.13.3.1 概要

電子署名を作成するための署名活性化のためのいくつかの推奨モデルを示す。6 章に準拠した他のアーキテクチャーを実装してもよい(MAY)。

SSASC は通常、署名者のセットによって使用され、各署名者は 1 つまたは複数の署名鍵を所有し、SSASC は署名操作を実行するために 1 つまたは複数の SCDev を含むことができる。

署名鍵は SCDev の外部に安全に保管し、動的にロードすることができる。ただし、署名鍵に SCDev 内に保管する場合と同じセキュリティを確保するための制御が適用されることが条件である。署名鍵の保護に採用される鍵のロード／アンロード機構は、本標準の範囲外である。

5.13.3.2 SCAL1 での署名活性化

署名鍵の機密性及び完全性は SCDev によって保証される。SCDev は SSA によって起動される。

SSA によって起動することができる。この起動は、所定の期間および/または所定の数の署名に対して維持することができる。

署名鍵の活性化には、署名者が SSA によって認証されることが必要である(図 3 参照)。署名者の認証が成功した場合、対応する署名鍵は、ある期間内および/またはある量の署名操作の中で、署名者に代わって署名操作に使用されてもよい(MAY)。これにより、SSA はバルク/バッチ署名の目的で使用することができる。

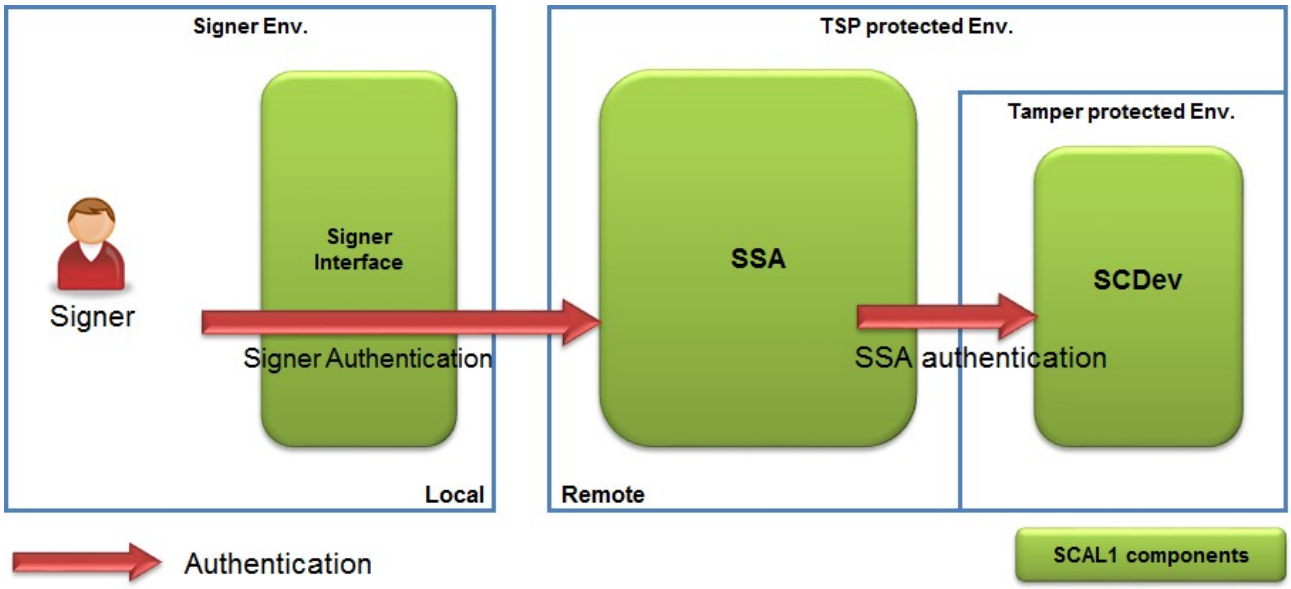


図 3 – SCAL1 を用いた署名活性化システム

注　このアーキテクチャーは、認証の委任(5.7.4 参照)を使用する場合、外部のパーティに拡張することができる。

　このアーキテクチャーは、制御の保証が低いデジタル署名値(例えば、署名者の秘密鍵を使用して暗号化したハッシュ)を作成するために使用することができる。

5.13.3.3 SCAL2 での署名活性化

署名鍵の機密性と完全性は、リモート SCDev によって保証される。リモート SCDev は、SSA の管理下にある。

リモート SCDev は SAP に参加し、署名操作が正当な署名者の管理下にあることを保証する。

SSA は安全なチャネルを介してリモート SCDev の SAM に接続し、対応する署名キーを有効にするために SAD を検証する(図 4 参照)。

署名者認証は、所定の期間および/または所定の署名数まで維持することができる。しかし、SAD の計算は、署名操作ごとに行われなければならない(SHALL)。SAD は DTBS/R のセットとリンクしてもよく、これにより SSA をバルク/バッチ署名の目的で使用することができる。

署名者の認証は、SAD の一部として署名者と署名の間のリンクを作成するために使用される SSIC を使用して行うことができる。

SAD の使用は、SAM の責任の下にある:

— SAD が SIC によって生成される場合、検証のために SIC から SAM に安全に転送されなければならない。

— SAD が SIC によって生成される場合、SAD は SIC を使用した署名者の認証に成功した際/中に生成され、検証のために SAM に安全に転送されるものとする(SHALL)。

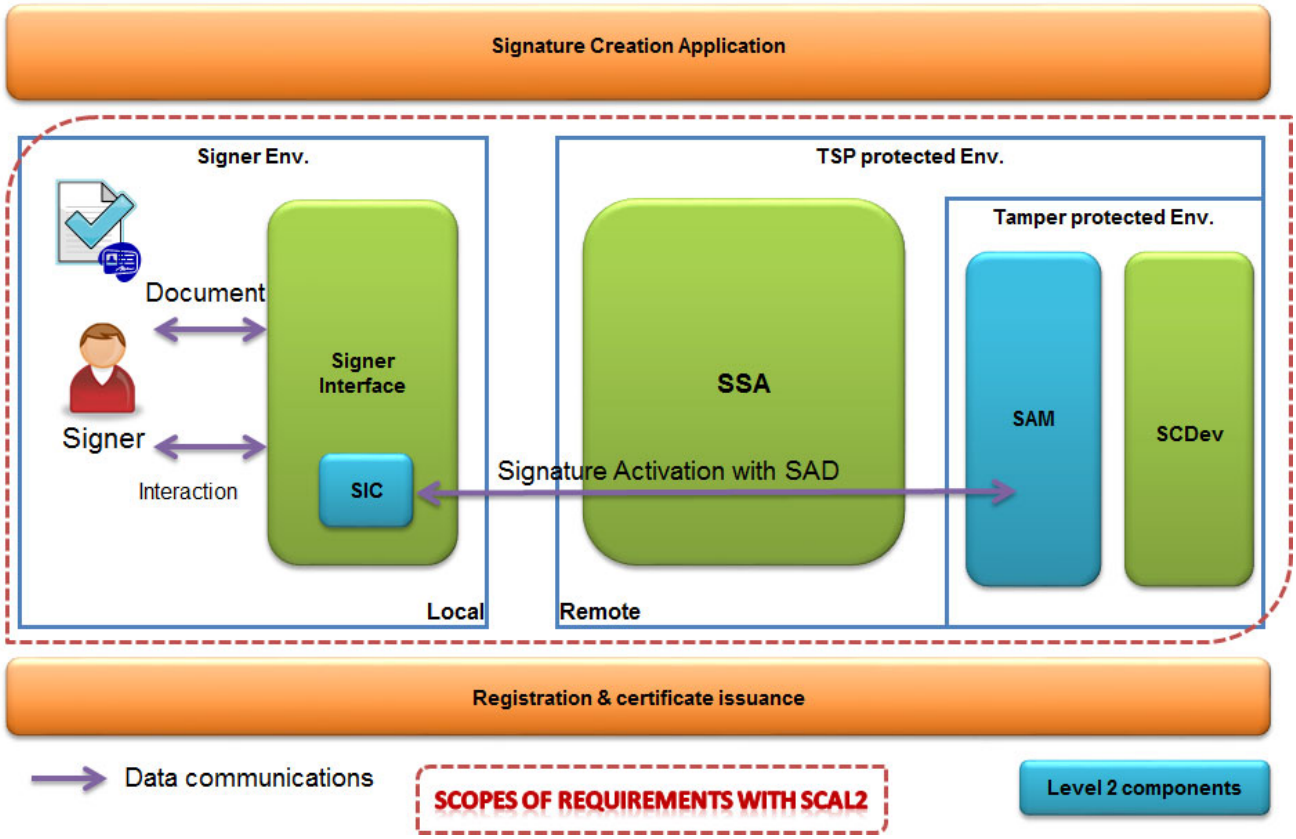


図 4 – SCAL2 を用いた署名活性化システム

注 1 このアーキテクチャーは、認証の委任(5.7.4 参照)を使用する場合、外部のパーティに拡張することができる。

注 2 認証の委任(5.7.4 参照)を使用する場合、要求事項の範囲を外部のパーティに拡張することができる。

このアーキテクチャーは、より高い管理保証を持つデジタル署名値(例えば、署名者の秘密鍵で暗号化されたハッシュ)を作成するために使用することができる。

5.13.4 サーバー署名アプリケーションサービスの各コンポーネントの役割

本標準が要件を規定する SSASC の中核部分は、一連の機能コンポーネントである:

— 署名鍵の設定 – SCDev 内で署名キーを生成し、許可された署名者が使用できるように割り当てる。

— 署名鍵管理 – SCDev 内で署名鍵を削除、バックアップ、復元する。

— 署名者認証 – 署名者による署名鍵の使用を許可する。

— 電子署名の作成 – SCDev 内で電子署名を作成するために、承認された署名者のインターフェイスとなる。

— 保証レベルを向上させるため、SCAL2 に到達するためには追加コンポーネントが必須となる。

— SIC – SAP 内で署名者と署名操作の間のリンクを作成する。SIC は署名者の環境で SAD を生成してもよい(MAY)。

— SAM - 耐タンパー環境(改ざん防止環境)で保護され、SAP の実行に責任を負う。SAM は一連のコンポーネントを提供する。

— SAD 生成 – SAD が SIC によって生成されない場合、耐タンパー環境(改ざん防止環境)において SAD を 生成する。

— 署名鍵の有効化 – SAD の検証を管理し、署名鍵を有効化する。

— 署名鍵生成 – 署名鍵にバインドされる認証要素を管理する。

6 セキュリティ要求事項

本章の詳細は別紙「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」参照

6.1 一般事項

6.2 一般的なセキュリティ要件 (SRG)

6.2.1 管理 (SRG_M)

6.2.1.1 一般事項
6.2.1.2 システムとセキュリティ管理 (SRG_M.1)
6.2.2 システムと運用 (SRG_SO)

6.2.2.1 運用管理 (SRG_SO.1)
6.2.2.2 時刻同期 (SRG_SO.2)
6.2.3 識別と認証 (SRG_IA)

6.2.3.1 一般事項
6.2.3.3 認証失敗 (SRG_IA.2)
6.2.4 システムアクセス制御 (SRG_SA)

6.2.4.1 一般事項
6.2.4.2 権限管理 (SRG_SA.1)
6.2.5 鍵管理 (SRG_KM)

6.2.5.1 一般事項
6.2.5.2 鍵生成 (SRG_KM.1)
6.2.5.3 鍵の保管、バックアップ、リカバリー (SRG_KM.2)

附属書 A（規定）

電子識別手段、特性および設計に対する要件

注記 本附属書に概説する技術仕様及び手順の要素は、保証レベル「低」、「十分」又は「高」に関して、(EU)2015/1502 [6] ANNEX Clauses 2.1, 2.2.1 及び 2.3.1 で規定する要求事項と同等である。

A.1 登録

A.1.1 申請と登録

保証レベル	必要な要素
「低」	1. 電子識別手段の使用に関する条件を申請者が認識していることを確実にする。 2. 電子識別手段に関連する推奨されるセキュリティ上の注意事項を申請者が認識していることを確実にする。 3. 身元確認と検証に必要な関連する同一性識別情報を収集する。
「十分」	レベル「低」と同じ。
「高」	レベル「低」と同じ。

A.1.2 身元確認と検証（自然人）

保証レベル	必要な要素
「低」	1. 申請者は、主張された身元を示している証拠をその人物が所持していると仮定することができる。 2. 証拠が真正である、または信頼できる情報源によって存在すると仮定でき、その証拠は有効であるとみなせる。 3. 主張された身元が存在することが信頼できる情報源によって知られており、その身元を主張する人 が同一人物であると仮定することができる。

保証レベル	必要な要素
「十分」	レベル「低」に加えて、1～4 のいずれかの選択肢を満たす必要がある 1. 申請者は、主張された身元を示している証拠をその人物が所持していると検証されている かつ その証拠が真正であることを確認している、または信頼できる情報源によって、その証拠が存在し、実在の人物に関連するものであると知られている かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元ではないリスクを最小限に抑えるための措置が取られている または 2. 身元証明書が登録手続き中に提示され、その書類が提示した人物に関連するとみなせる かつ 例えば、紛失、盗難、停止、失効または期限切れの証拠のリスクを考慮し、申請人の身元が主張された身元でないリスクを最小限に抑えるための措置が取られていること または 3. 電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠した適合評価機関又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 4. 電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行され、個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、保証レベル「十分」または「高」は、適用される規制要件（注 1 参照）に準拠する適合性評価機関または同等の機関によって確認されなけ ればならない。

保証レベル	必要な要素
「高」	1 または 2 のいずれかの要件を満たす必要がある 1.レベル「十分」、かつ、(a)～(c)に掲げる選択肢のうち 1 つを満たさなければならない (a) 申請者は、主張された身元を示している写真または生体識別証拠を所持していることが確認されている場合、その証拠が信頼できる情報源によって有効であると確認されている かつ 申請者が、1 つまたは複数の身体的特徴を信頼できる情報源と比較することにより、主張された本人であると確認される または (b) 電子識別手段の発行以外の目的で，公的又は私的団体が以前に使用した手順が，保証レベル「高」について A.1.2 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合性評価機関（注 2 参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ 以前の手順の結果が有効であることを証明するための措置を講じている または (c) 電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行され、個人識別データの改変のリスクを考慮する場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関または同等の機関によって、保証レベル「高」が確認されなければならない かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている または 2.申請者が認められた写真または生体識別証拠を提示しない場合、そのように認められた写真または生体識別証拠を取得するために、国レベルで使用されるものと全く同じ手順が適用される。

A.1.3 身元保証と検証(法人)

保証レベル	必要な要素
「低」	1.法人の主張する身元は、証拠に基づいて証明される。 2.証拠が有効であるとみなせ、かつ真正である、または信頼できる情報源に従って存在すると仮定できる。ただし、信頼できる情報源に法人が含まれることは任意であり、法人と信頼できる情報源の間の協定によって規制される。 3.その法人が、その法人として行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。
「十分」	レベル「低」に加えて、1～3 のいずれかの選択肢を満たす必要がある 1.電子識別手段の申請が行われた証拠に基づいて、主張された法人のアイデンティティが証明されている。ここには法人の名前、法人形態、登録番号(該当する場合)を含む。 かつ その証拠が真正であることを確認している、あるいは信頼できる情報源に従って既知かどうかが確認されていて、法人がその分野で活動するために信頼できる情報源に法人が含まれることが求められる かつ 例えば、紛失、盗難、停止、失効または期限切れの証憑書類のリスクを考慮し、法人のアイデンティティが主張するアイデンティティと異なるリスクを最小限に抑えるための措置が取られていること または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「十分」について A.1.3 項に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合評価機関（注 1 参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない または 3.電子識別手段が、保証レベル「十分」または「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、電子識別証明および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関（注 1 参照）または同等の機関によって、保証レベル「十分」または「高」を確認する必要である。

保証レベル	必要な要素
「高」	レベル「十分」に加えて、1～3 のいずれかの選択肢を満たす必要がある 1.主張される法人のアイデンティティは証拠に基づ いて証明される。ここには、法人の名前、法人形態、および国内で使用される法人を表す少なくとも 1 つの固有識別子が含まれる。 かつ その証拠が信頼できる情報源に基づき有効であることを確認する または 2.電子識別手段の発行以外の目的で，公的又は私的機関が以前に使用した手順が，保証レベル「高」について A.1.3 節に規定するものと同等の保証を提供する場合，その同等の保証が，該当する規制要件に準拠する適合性評価機関（注 2 参照）又は同等の機関によって確認されていれば，登録に責任を負う機関は，以前の手順を繰り返す必要がない かつ この前の手順の結果が有効であることを証明するための措置がとられている または 3.電子識別手段が、保証レベル「高」を有する有効な通知済み電子識別手段に基づいて発行される場合、身元確認および検証プロセスを繰り返す必要はない。根拠となる電子識別手段が通知されていない場合、適用される規制要件に準拠した適合性評価機関（注 2 参照）または同等の機関によって、保証レベル「高」が確認されなければならない。 かつ 通知された電子識別手段の前の発行手続きの結果が有効であることを証明するための措置がとられている。

A.1.4 自然人と法人の電子識別手段の紐づけ(バインディング)

自然人の電子識別手段と法人の電子識別手段との間のバインディングについては、該当する場合、以下の条件が適用される

a)バインディングの停止及びまたは失効を可能とするものとする。バインディングのライフサイクル（活性化，停止，更新，失効など）は，国に認められた手続きに基づいて管理されるものとする。

b) 電子識別手段が法人の電子識別手段とバインドしている自然人は，国に認められた手続きに基づき，バインディングを他の自然人に委任することができる。ただし、委任した自然人は、引き続き説明責任を負うものとする。

c) バインディングは、以下の方法で行うものとする。

保証レベル	必要な要素

「低」	1.法人を代表して行動する自然人の身元確認が、レベル「低」以上で行われたことが確認される。 2.バインディングは、国に認められた手順に基づいて確立されている。 3.自然人が、その人が法人を代表して行動することを妨げるような状態にあることを、信頼できる情報源から知らされていないこと。
「十分」	レベル「低」の 3 に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「十分」または「高」で行われたことが検証される。 2.バインディングは、国に認められた手続きに基づいて確立され、その結果、信頼できる情報源に登録されたものである。 3.バインディングは、信頼できる情報源からの情報に基づいて確認されている。
「高」	レベル「低」の 3、レベル「十分」の 2 に加え、 1.法人を代表して行動する自然人の身元確認が、レベル「高」で行われたことが検証される。 2.バインディングは、国内で使用される法人を表す固有の識別子、及び信頼できる情報源からの自然人を表す固有の情報に基づいて検証されている。

A.2 電子識別手段と認証

A.2.1 電子識別手段の特性と設計

保証レベル	必要な要素
「低」	1.電子識別手段は、少なくとも 1 つの認証要素を利用する。 2.電子識別手段が、その電子識別手段を携帯する者の制御下または所有下にある場合のみ使用されることを確認するための合理的な措置を、発行者が講じるように設計されていること。
「十分」	1.電子識別手段は、異なる種類から少なくとも 2 つの認証要素を利用する。 2.電子識別手段は、その電子識別手段を携帯する者の制御下または所有下にある場合にのみ使用されることが想定できるように設計されていること。
「高」	レベル「十分」に加えて、 1.電子識別手段は、複製や改ざん、さらには攻撃可能性が高い攻撃者から保護する。 2.電子識別手段は、他人の使用に対して、その電子識別手段を携帯する者が確実に保護することができるように設計されている。

A.2.2 認証メカニズム

保証レベル	必要な要素
「低」	1.個人識別データの開示は、電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムの一部として個人識別データが保存される場合、その情報は、紛失や、オフラインでの分析を含む侵害を防ぐために保護されている。 3.認証メカニズムは、基本的な攻撃能力を強化した攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低いように、電子識別手段の検証のためのセキュリティ制御を実装している。
「十分」	レベル「低」に加え、 1.個人識別データの開示は、動的認証による電子識別手段とその有効性を確実に確認した上で行う。 2.認証メカニズムは、中程度の攻撃力を持つ攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。
「高」	レベル「十分」に加え、 認証メカニズムは、攻撃力の高い攻撃者による推測、盗聴、再生、通信操作などの行為が認証メカニズムを破壊する可能性が極めて低くなるように、電子識別手段の検証のためのセキュリティ制御を実装している。

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
Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements (EN 419 241-1) を参考に作成

要求識別子	EN 419 241-1	監査項目			要求事項
		Level 1	Level 2	Level 3	
6 Security requirements					6 セキュリティ要件
6.1 General					6.1 一般事項
6.2 General security requirements (SRG)					6.2 一般的なセキュリティ要件 (SRG)
6.2.1 Management (SRG_M)					6.2.1 管理 (SRG_M)
6.2.1.1 General					6.2.1.1 一般事項
6.2.1.2 Systems and security management (SRG_M.1)					6.2.1.2 システムとセキュリティ管理 (SRG_M.1)
SRG_M.1.1	TW4S SHALL support roles with different privileges.	○	○	○	SSASCは異なる特権を持つロールをサポートするものとする(SHALL)。
SRG_M.1.2	As a minimum the TW4S SHALL support the following roles:	○	○	○	SSASCは最低限、下記のロールをサポートするものとする(SHALL):
	Security Officers: having overall responsibility for administering the implementation of the security policies, practices and have access to security related information.	○	○	○	セキュリティオフィサー: セキュリティポリシー、セキュリティプラクティスの実施を管理する全体的な責任を持ち、セキュリティ関連情報へアクセスできるロール。
	System Administrators: are authorized to install, configure and maintain the TW4S but with controlled access to security-related information.	○	○	○	システム管理者:SSASCのインストール、設定、保守を行う権限を持つが、セキュリティ関連情報へのアクセスは制御されるロール。
	System Operators: are responsible for operating the TW4S on a day-to-day basis and are authorized to perform system backup and recovery.	○	○	○	システムオペレーター:SSASCの日常的な運用に責任を持ち、システムのバックアップとリカバリーを実行する権限を持つロール。
	System Auditors: are authorized to view archives and audit logs of the TW4S for the purposes of auditing the operations of the system in line with security policy.	○	○	○	システム監査人:セキュリティポリシーに沿ったシステムの運用を監査する目的で、SSASCのアーカイブや監査ログの閲覧の権限を持つロール。
	Security officers and system administrators are privileged system users.	○	○	○	セキュリティオフィサーとシステム管理者は特権システムユーザーである。
	System operators and system auditors have privileged roles but are not able to administer or configure the TW4S.	○	○	○	システムオペレーターとシステム監査人は特権を持つが、SSASCを管理や設定はできない。
SRG_M.1.3	As a minimum the TW4S SHALL support the following non-privileged roles:	○	○	○	SSASCは最低限、下記の非特権ロールをサポートするものとする(SHALL):
	Signer: is authorized to use the TW4S by passing the SAD as part of the SAP in order to sign the document or the DTBS/R, which potentially can be passed through the SAP as well.	○	○	○	署名者: 文書またはDTBS/Rに署名するために、SADを渡すことにより、SSASCを使用する権限を持つロール。
	SCA: is authorized to send the DTBS/R request to the TW4S in order to be signed by a signer.	○	○	○	SCA: 署名者が署名するために、SSASCにDTBS/R要求を送信する権限を有するロール。
	RA: is authorized to send the public key certificate to the TW4S in response of a certificate signing request.	○	○	○	RA: 証明書発行要求に応じて公開鍵証明書をSSASCに送信する権限を持つロール。
SRG_M.1.4	One privileged user SHALL NOT be able to take on all the privileged roles and SHOULD NOT take on more than one of the privileged roles.	○	○	○	一人の特権ユーザーが全ての特権ロールを担えないものとし(SHALL NOT)、一つ以上の特権ロールを担えるべきではない(SHOULD NOT)。
SRG_M.1.5	Users associated with privileged roles SHALL NOT be associated with non-privileged role.	○	○	○	特権ロールを割り当てられたユーザには、非特権ロールを割り当てないものとする(SHALL NOT)。
	Users associated with non-privileged roles SHALL NOT be associated with privileged role.	○	○	○	非特権ロールを割り当てられたユーザには、特権ロールを割り当てないものとする(SHALL NOT)。
SRG_M.1.6	TW4S SHALL be capable of ensuring that a user authorized to assume a Security Officer role is not authorized to assume a System Auditor role.	○	○	○	SSASCは、セキュリティオフィサーのロールを担う権限を持つユーザが、システム監査人のロールを担う権限を持たないことを確実にすることができるものとする(SHALL)。
SRG_M.1.7	TW4S SHALL be capable of ensuring that a user authorized to assume a System Administrator role and/or a System Operator role is not authorized to assume a System Auditor role and/or a Security Officer role.	○	○	○	SSASCは、システム管理者及び/又はシステムオペレータのロールを担う権限を持つユーザが、システム監査人及び/又はセキュリティオフィサーのロールを担う権限を持たないことを確実にすることができるものとする(SHALL)。
SRG_M.1.8	Individuals that are part of a group of privileged system users SHALL be named and trained persons.	○	○	○	特権システムユーザのグループの一員である個人は、指名され、訓練された要員であるものとする(SHALL)。
SRG_M.1.9	Only privileged system users SHALL have physical access to the hardware and can administer the TW4S.	○	○	○	特権システムユーザーのみが、ハードウェアへ物理的にアクセスでき、SSASCを管理することができるものとする(SHALL)。
SRG_M.1.10	Only privileged system users SHALL have extensive privileges to administer the TW4S	○	○	○	特権システムユーザのみが、関連する全てのアプリケーションとインタフェースを通してSSASCを管理する広範な特権を持つものとする(SHALL)。
6.2.2 Systems and operations (SRG_SO)					6.2.2 システムと運用 (SRG_SO)
6.2.2.1 Operations management (SRG_SO.1)					6.2.2.1 運用管理 (SRG_SO.1)
SRG_SO.1.1	TW4S manufacturers SHALL ensure instructions are provided to allow the TW4S to be:	○	○	○	SSASC構築事業者は、SSASC が下記が実施できるための指示事項が提供されることを確実にするものとする(SHALL):
	– correctly and securely operated;	○	○	○	– 正しく、安全に運用する。
	– deployed in such a way that the risk of systems failure is minimized;	○	○	○	– システム障害リスクを最小化する方法でデプロイする。
	– protected against viruses and malicious software to ensure the integrity of the systems and the information they process.	○	○	○	– システムと処理する情報の完全性を確実にするためにウィルスや悪意のあるソフトウェアに対して保護する。
SRG_SO.1.2	TW4S manufacturers SHALL provide system documentation covering the responsibilities of the four privileged roles mentioned in SRG_M.1.2. It SHOULD include:	○	○	○	SSASC構築事業者は、SRG_M.1.2で言及した4つの特権ロールの責任をカバーするシステム文書を提供するものとする(SHALL)。それは以下を含むべきである(SHOULD):
	– Installation Guidance;	○	○	○	– インストールガイド
	– Administration Guidance;	○	○	○	– 管理ガイド
	– User Guidance.	○	○	○	– ユーザーガイド
6.2.2.2 Time synchronization (SRG_SO.2)					6.2.2.2 時刻同期 (SRG_SO.2)

SRG_SO.2.1	TW4S manufacturers SHALL state the time accuracy of TW4S and how this is ensured.	○	○	○	SSASC構築事業者は、SSASCの時刻精度とそれを確実にする方法を表明するものとする(SHALL)。
SRG_SO.2.2	In order to ensure time accuracy of audited events, a time source suitably synchronized with a standard time source SHOULD be used.	○	○	○	監査対象事象の時刻精度を確保するため、標準時と適切に同期した時刻ソースを使用するべきである(SHOULD)。
SRG_SO.2.3	In order to check whether a certificate has expired, a time source suitably synchronized with the UTC SHALL be used.	○	○	○	証明書が有効期限切れかどうかを確認するために、協定世界時UTCと適切に同期した時刻ソースを使用するものとする(SHALL)。
6.2.3 Identification and authentication (SRG_IA)					6.2.3 識別と認証 (SRG_IA)
6.2.3.1 General					6.2.3.1 一般事項
6.2.3.2 Authentication for privileged and non-privileged roles other than signer (SRG_IA.1)					6.2.3.2 署名者以外の特権および非特権ロールのための認証 (SRG_IA.1)
SRG_IA.1.1	TW4S SHALL require each user to identify him/herself and be successfully authenticated before allowing any action on behalf of that user or role assumed by the user.	○	○	○	SSASCは、各ユーザが、そのユーザまたはそのユーザが担う役割を代表して行う行動を許可する前に、自身を識別し、認証が成功することを要求するものとする(SHALL)。
SRG_IA.1.2	Re-authentication SHALL be mandatory after log out.	○	○	○	ログアウト後の再認証は必須であるものとする(SHALL)。
SRG_IA.1.3	Combination of authentication data, where used, SHALL be unpredictable.	○	○	○	認証データの組み合わせを使用する場合、予測不可能であるものとする(SHALL)。
SRG_IA.1.4	For privileged users mechanisms SHALL be implemented to reduce the risk of an authenticated user session being taken over if the user's input device is left unattended, for example by terminating a user session after a given idle period.	○	○	○	特権ユーザに対して、ユーザの入力デバイスが放置された場合、認証されたユーザセッションが乗っ取られるリスクを低減するためのメカニズム(例えば、所定のアイドル時間後にユーザセッションを終了させるなど)が実装されるものとする(SHALL)。
6.2.3.3 Authentication failure (SRG_IA.2)					6.2.3.3 認証失敗 (SRG_IA.2)
SRG_IA.2.1	If the number of unsuccessful authentication attempts from the same user reaches the maximum number of allowed attempts, the TW4S SHALL prevent further user authentication attempts within a certain time frame or until an administrative role unblock the user.	○	○	○	同一ユーザーからの認証失敗回数が最大許容回数に達した場合、SSASC は、一定時間内または管理者がユーザーのブロックを解除するまで、さらなるユーザー認証試行を防止するものとする(SHALL)。
6.2.4 System access control (SRG_SA)					6.2.4 システムアクセス制御 (SRG_SA)
6.2.4.1 General					6.2.4.1 一般事項
6.2.4.2 Right management (SRG_SA.1)					6.2.4.2 権限管理 (SRG_SA.1)
SRG_SA.1.1	TW4S SHALL provide the capability of controlling and limiting access for identified individuals to the system or user objects which they own or are responsible for.	○	○	○	SSASCは、識別された個人が所有または責任を負うシステムまたはユーザーオブジェクトへのアクセスを制御し、制限する機能を提供するものとする(SHALL)。
SRG_SA.1.2	TW4S SHALL ensure it provide access control to sensitive residual information.	○	○	○	SSASCは、機密性の高い残留情報へのアクセス制御を確実に提供するものとする(SHALL)。
6.2.5 Key management (SRG_KM)					6.2.5 鍵管理 (SRG_KM)
6.2.5.1 General					6.2.5.1 一般事項
6.2.5.2 Keys generation (SRG_KM.1)					6.2.5.2 鍵生成 (SRG_KM.1)
SRG_KM.1.1	Private or secret keys SHOULD be generated and used in a SCDev.	○	○	○	秘密鍵もしくは共通鍵はSCDev内で生成し使用すべきである(SHOULD)。
	The SCDev used SHOULD:				使用されるSCDev(SHOULD)。
	— be a trustworthy system which is ensured to EAL 4 or higher, augmented by AVA_VAN.5 in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security. This SHALL be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non- technical security measures; or	○	○	○	— 使用されるSCDevは、AVA_VAN.5で補強されたISO/IEC 15408 EAL 4以上が確実にされた、もしくは同等の国内もしくは国際的に認知されたITセキュリティの評価基準が確保された信頼できるシステムであるべきである(SHOULD)。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要求事項を満たすセキュリティターゲットもしくはプロテクションプロファイルであるものとする(SHALL)。
	— meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3.	○	○	○	— 使用されるSCDevは、ISO/IEC 19790 またはFIPS PUB 140-2レベル3で識別される要件を満たすべきである(SHOULD)。
SRG_KM.1.2	The SCDev SHALL support cryptographic algorithms and key lengths corresponding to the appropriate level of security, which fulfils the security needs identified during the system design.	○	○	○	SCDevは、システム設計中に識別されたセキュリティ要求を満たす適切なセキュリティレベルに対応する暗号アルゴリズム及び鍵長をサポートするものとする(SHALL)。
	Wherever confidentiality or integrity protection services are required (e.g. for backup of signing keys), only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.	○	○	○	(例えば署名鍵のバックアップなど)機密性または完全性保護サービスが必要な場合には、同等以上の暗号強度を持つ暗号アルゴリズムおよびアルゴリズムパラメータのみを使用するものとする(SHALL)。
SRG_KM.1.3	When the private or secret keys (including signer's signing key, Infrastructure and Control Keys) are held outside the SCDev, these keys SHALL be protected to ensure the confidentiality and integrity of the keys.	○	○	○	(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)秘密鍵または共通鍵がSCDevの外部で保持される場合、これらの鍵は鍵の機密性と完全性を確実にするために保護されるものとする(SHALL)。
SRG_KM.1.4	SCDev SHALL be initialised, before generating or containing any signing key, with technical mechanisms that requires at least two operators in the SCDev.	○	○	○	SCDevは、署名鍵を生成または格納する前に、少なくとも2人のオペレータを必要とするSCDev内の技術的な仕組みで初期化されるものとする(SHALL)。
6.2.5.3 Keys storage, backup and recovery (SRG_KM.2)					6.2.5.3 鍵の保管、バックアップ、リカバリ (SRG_KM.2)
SRG_KM.2.1	All private or secret keys (including signer's signing key, Infrastructure and Control Keys) SHALL be securely stored, i.e. never be stored in an unprotected state.	○	○	○	全ての秘密鍵または共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)、安全に保管されるものとする(SHALL)。即ち、保護されていない状態で保管してはならない。
SRG_KM.2.2	If any private or secret key (including signer's signing key, Infrastructure and Control Keys), is exported from that SCDev, it SHALL be protected to ensure its confidentiality and integrity to the same or higher security level as within the SCDev.	○	○	○	(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)任意の秘密鍵もしくは共通鍵が当該SCDevからエクスポートされる場合、SCDev内と同等以上のセキュリティレベルで機密性と完全性を確実にするために、その鍵は保護されるものとする(SHALL)。
	Wherever the private/secret key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.	○	○	○	秘密鍵/共通鍵が暗号化により保護される場合は、同等以上の暗号強度を持つ暗号アルゴリズムおよびアルゴリズムパラメータのみを使用するものとする(SHALL)。

SRG_KM.2.3	TW4S SHALL ensure that backup, storage and restoration of private or secret keys (including signer's signing key, Infrastructure and Control Keys) are only performed by authorized personnel. Master keys used to protect both user and working keys SHALL be backed up, stored and reloaded under at least dual control. Such master keys SHALL only be held outside the SCDev in protected form.	○	○	○	SSASCは、(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)秘密鍵もしくは共通鍵のバックアップ、保管、リカバリが、認可された要員によってのみ行われることを確実にするものとする(SHALL)。ユーザー鍵および作業鍵の両方を保護するために使用するマスター鍵は、少なくとも複数人制御の下でバックアップ、保管、リロードされるものとする(SHALL)。SCDevの外部では、当該マスターキーは、保護された形でのみ保有されるものとする(SHALL)。
6.2.5.4 Key usage (SRG_KM.3)					6.2.5.4 鍵の利用 (SRG_KM.3)
SRG_KM.3.1	Private or secret key (including signer's signing key, Infrastructure and Control Keys) SHALL only be used for its intended purpose.	○	○	○	秘密鍵と共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)その意図された目的のためだけに使用されるものとする(SHALL)。
SRG_KM.3.2	Private or secret keys (including signer's signing key, Infrastructure and Control Keys) SHALL NOT be shared except as required to meet their purpose.	○	○	○	秘密鍵と共通鍵は(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)その目的に満たすために必要な場合を除いて、共有はされないものとする(SHALL NOT)。
SRG_KM.3.3	Access controls SHALL be in place to protect the access and usage of the keys (including signer's signing key, Infrastructure and Control Keys).	○	○	○	アクセス制御は、(署名者署名鍵、インフラストラクチャ鍵、制御鍵を含め)鍵のアクセスと利用が保護された場所で行われるものとする(SHALL)。
SRG_KM.3.4	A signing key SHALL be linked to only one signer and only one public key certificate.	○	○	○	署名鍵は唯一の署名者および、唯一の公開鍵証明書に紐付けられるものとする(SHALL)。
6.2.5.5 Key distribution (SRG_KM.4)					6.2.5.5 鍵の配布 (SRG_KM.4)
SRG_KM.4.1	Private or secret keys (including Infrastructure and Control Keys) SHALL be transmitted securely when they have to be transmitted.	○	○	○	(インフラストラクチャ鍵及び制御鍵を含む)秘密鍵もしくは共通鍵は、送信する必要がある場合、安全に送信されるものとする(SHALL)。
SRG_KM.4.2	All the keys used to protect other private/secret keys during transmission SHALL be (at least) as strong as keys transmitted.	○	○	○	送信中に他の秘密鍵/共通鍵を保護するために使用される全ての鍵は、送信される鍵と(少なくとも)同程度の強度であるものとする(SHALL)。
6.2.5.6 Key renewal/update/change (SRG_KM.5)					6.2.5.6 鍵の更新と変更 (SRG_KM.5)
SRG_KM.5.1	Infrastructure and Control Keys SHOULD be changed on a regular basis, with a frequency based on risk assessment.	○	○	○	インフラストラクチャ鍵および制御鍵は、リスク評価に基づく頻度で定期的に変更すべきである(SHOULD)。
SRG_KM.5.2	If any of the key algorithms or length is considered to have become unsuitable, keys based on those algorithms SHALL be changed immediately.	○	○	○	鍵アルゴリズムもしくは鍵長が不適切になったと判断した場合、そのアルゴリズムに基づく鍵は直ちに変更されるものとする(SHALL)。
SRG_KM.5.3	If any of the keys is compromised or suspected to be compromised, they SHOULD be changed immediately.	○	○	○	鍵の危殆化、もしくは危殆化が疑われる場合、直ちにその鍵を変更するべきである(SHOULD)。
6.2.5.7 Key archiving (SRG_KM.6)					6.2.5.7 鍵のアーカイブ (SRG_KM.6)
SRG_KM.6.1	A signing key SHALL NOT be archived.	○	○	○	署名鍵はアーカイブされないものとする(SHALL NOT)。
6.2.5.8 Key deletion (SRG_KM.7)					6.2.5.8 鍵の削除 (SRG_KM.7)
SRG_KM.7.1	A signing key SHALL be destroyed after the expiration of the public key certificate or if the signing key is useless for the signer.	○	○	○	署名鍵は、公開鍵証明書の有効期限が切れた後、もしくは署名者にとって不必要になった場合、破棄されるものとする(SHALL)。
SRG_KM.7.2	If the link between the signing key and the signer is not maintained after the signing operations session, then the signing key SHALL be destroyed at the end of the signing operations session.	○	○	○	署名鍵と署名者の間のリンクが署名操作セッションの後に維持されない場合、署名鍵は署名操作セッションの終了時に破棄されるものとする(SHALL)。
SRG_KM.7.3	Signing key destruction mechanism and procedure SHOULD ensure that all backups of the destroyed signing key are also destroyed and that no residual information can be used to reconstruct the signing key.	○	○	○	署名鍵破壊の仕組みと手順では、破壊された署名鍵の全てのバックアップもまた破壊され、残っている情報が署名鍵を再構築するために使用できないことを確実にすべきである(SHOULD)。
	NOTE this recommendation does not apply if deleting of single keys in backup is practically not feasible.				注: この推奨事項は、バックアップ中の一つの鍵を指定した削除が現実的ではない場合には適用されない。
6.2.6 Auditing (SRG_AA)					6.2.6 監査(SRG_AA)
6.2.6.1 Audit data generation (SRG_AA.1)					6.2.6.1 監査データの生成(SRG_AA.1)
	Each service has additional specific auditing requirements that SHALL be addressed in addition to these general requirements.				各サービスには、これらの一般的な要件に加え、さらに特定の監査要件があり、これに対処するものとする(SHALL)。
SRG_AA.1.1	As a minimum, the following events SHALL be logged: — significant TW4S environmental, key management events (generation, usage and destruction); — user signing events (e.g. successful signing with a signer's signing key and DTBS/R request management); — user authentication during SAP; — signer's SAD management by TW4S; — start up and shut down of the audit data generation function; — changes of the audit parameters. User signing events SHALL include associate certificate to the signing key. All access attempts to TW4S SHOULD be logged.	○	○	○	最低限、以下のイベントは記録されるものとする(SHALL): - 重要なSSASCの環境に関わる鍵管理イベント(生成、使用、破棄); - ユーザ署名イベント(例:署名者の署名鍵による署名成功、DTBS/Rリクエスト管理など); - SAPを利用する場合、SAPにおけるユーザー認証; - SSASCによる署名者のSAD管理; - 監査データ生成機能の起動・停止; - 監査パラメータの変更。 ユーザーの署名イベントには、署名鍵に関連する証明書を含めるものとする(SHALL)。SSASCへのすべてのアクセスの試みは、ログに記録されるべきである(SHOULD)。
SRG_AA.1.2	The TSP SHALL specify what is done (i.e. actions taken) in case of failure of passing audit information to any external storage.	○	○	○	TSPは、外部ストレージへの監査情報の転送が失敗した場合に何を行うか(すなわち、取られる措置)を明示するものとする(SHALL)。
6.2.6.2 Guarantees of					6.2.6.2 監査データの利用可能性の保証(SRG_AA.2)
SRG_AA.2.1	TW4S SHALL maintain audit data and ensure that measures are taken for all audit data to be stored.	○	○	○	SSASCは、監査データを維持し、すべての監査データを保存するための措置を講じることを確実にするものとする(SHALL)。
SRG_AA.2.2	The audit function SHALL only append information.	○	○	○	監査機能は、情報を追加するだけであるものとする(SHALL)。
SRG_AA.2.3	TW4S SHALL protect the stored audit records in the audit trail from unauthorized deletion.	○	○	○	SSASCは、監査証跡に保存された監査記録を、権限を伴わない削除から保護するものとする(SHALL)。
SRG_AA.2.4	Audit records MAY be deleted when archived to an external storage.	○	○	○	監査記録は、外部ストレージにアーカイブされる場合には、内部からは削除できる(MAY)。
6.2.6.3 Audit data parameters (SRG_AA.3)					6.2.6.3 監査データパラメータ (SRG_AA.3)

SRG_AA.3.1	All audit records (including service specific audit logging) SHALL contain the following parameters: — Date and time of event; — Type of event; — Identity of the entity (e.g. user, administrator, process) responsible for the action; — Success or failure of the audited event.	○	○	○	すべての監査記録(サービス固有の監査ログを含む)は、以下のパラメータを含むものとする(SHALL): - イベントの日時 - イベントのタイプ - アクションに責任を持つエンティティ(ユーザー、管理者、プロセスなど)のアイデンティティ; - 監査イベントの成否。
6.2.6.4 Selectable					6.2.6.4 選択可能な監査レビュー(SRG_AA.4)
SRG_AA.4.1	TW4S SHALL allow searching for events in the audit log based on the date of event, the type of event and/or the identity of the user.	○	○	○	SSASCは、イベントの日付、イベントのタイプ、及び/又はユーザーのアイデンティティに基づいて、監査ログ内のイベントを検索できるようにするものとする(SHALL)。
SRG_AA.4.2	The audit records SHALL be in a format that can be processed and be presented in such a way that is suitable for the system auditors to interpret the information.	○	○	○	監査記録は、処理可能な形式であり、システム監査人が情報を解釈するのに適した方法で提示されるものとする(SHALL)。
6.2.6.5 Restricted audit review (SRG_AA.5)					6.2.6.5 制限された監査レビュー (SRG_AA.5)
SRG_AA.5.1	TW4S SHALL by default deny all user read access to the audit records, except for users that have been granted explicit read access (e.g. those with System Auditor role).	○	○	○	SSASCは、デフォルトで、明示的に読み取り権限を付与されたユーザー(例:システム監査の役割を持つユーザー)を除き、監査記録への全てのユーザーの読み取りアクセスを拒否するものとする(SHALL)。
6.2.6.6 Generation of warning (SRG_AA.6)					6.2.6.6 警告の生成(SRG_AA.6)
SRG_AA.6.1	TW4S SHALL generate a warning notifying in a timely manner unusual events which can have impact on the ability of the signing server system to meet the security requirements identified in this standard. A mechanism that issues a warning whenever an unusual event is detected SHOULD be implemented. The warning SHOULD trigger a notification to relevant administrator personnel. A warning MAY also trigger further actions to react to possible attacks such as cutting off the path of potential attack. Examples of unusual events related to user activities can be (but not limited to): — User actions outside of standard usage hours. — User actions executed with an abnormal speed (in order to detect non-human interventions). — User actions skipping standard activities within defined processes. — Duplicated user sessions.	○	○	○	SSASCは、署名サーバーシステムは、本規定で特定されるセキュリティ要件を満たす能力に影響を及ぼしうる異常なイベントを、適時に通知する警告を生成するものとする(SHALL)。 異常なイベントが検出されるたびに警告を発する機構を実装すべきである(SHOULD)。警告は、関連する管理者に通知するトリガーとなるべきである(SHOULD)。 警告は、攻撃される可能性のある経路を遮断するなど、攻撃の可能性に対応するためのさらなる行動のトリガーとすることができる(MAY)。 ユーザー活動に関連する異常事態の例としては、以下のようなものが考えられる(ただし、これらに限定されない): - 標準的な利用時間外のユーザーの行為。 - 異常な速度で実行されるユーザーアクション(人間以外の介入を検出するため)。 - 定義されたプロセス内の標準的なアクティビティをスキップするユーザーアクション。 - 重複するユーザーセッション。
6.2.6.7 Guarantees of audit data integrity (SRG_AA.7)					6.2.6.7 監査データの完全性の保証(SRG_AA.7)
SRG_AA.7.1	TW4S SHALL ensure the integrity of the audit data.	○	○	○	SSASCは、監査データの完全性を確実にするものとする(SHALL)。
SRG_AA.7.2	TW4S SHALL provide a function to verify the integrity of the audit data.	○	○	○	SSASCは、監査データの完全性を検証する機能を提供するものとする(SHALL)。
6.2.6.8 Guarantees of audit timing (SRG_AA.8)					6.2.6.8 監査時刻の保証 (SRG_AA.8)
SRG_AA.8.1	To ensure time accuracy of audited events requirement SRG_SO.2.2 applies.	○	○	○	監査対象イベントの時刻の精度を確実にするため、要求事項SRG_SO.2.2を適用する。
6.2.7 Archiving (SRG_AR)					6.2.7 アーカイビング(SRG_AR)
6.2.7.1 Archive data generation (SRG_AR.1)					6.2.7.1 アーカイブデータ生成 (SRG_AR.1)
SRG_AR.1.1	TSP SHALL be capable of generating an archive on an external media. The media SHOULD be appropriate for storage and subsequent processing, and be able to provide the necessary legal evidence in support of digital signatures. NOTE These policy requirements will be moved into the appropriate standard when available.	○	○	○	TSPは、外部メディア上にアーカイブを生成することができるものとする(SHALL)。 このメディアは、保存とその後の処理に適切であり、デジタル署名のサポートに必要な法的証拠を提供できるものであるべきである(SHOULD)。 注 これらのポリシー要件は、適切な規格が利用可能になった時点でその規格に移行される予定である。
SRG_AR.1.2	All audit logs SHALL be archived.	○	○	○	すべての監査ログは、アーカイブされるものとする(SHALL)。
SRG_AR.1.3	Each archive entry SHALL include the time at which the archiving occurred.	○	○	○	各アーカイブエントリは、アーカイブが発生した時刻を含むものとする(SHALL)。
SRG_AR.1.4	The archive SHALL NOT include any sensitive security parameters, such as TW4S user passwords	○	○	○	アーカイブは、SSASCユーザーパスワードのような機密性の高いセキュリティパラメータを含まないものとする(SHALL NOT)。
6.2.7.2 Integrity of archived data (SRG_AR.2)					6.2.7.2 アーカイブデータの完全性 (SRG_AR.2)
SRG_AR.2.1	Unauthorized modifications of each entry in the archive SHALL be prevented. A mechanism to verify the integrity SHALL be in place to detect unauthorized modifications.	○	○	○	アーカイブの各エントリーの権限を伴わない改変を防止するものとする(SHALL)。権限を伴わない改変を検出するために、完全性を検証する機構を設けるものとする(SHALL)。
6.2.8 Backup and recovery (SRG_BK)					6.2.8 バックアップとリカバリー(SRG_BK)
6.2.8.1 General					6.2.8.1 一般事項
6.2.8.2 Integrity and confidentiality of backup information (SRG_BK.1)					6.2.8.2 バックアップ情報の完全性及び機密性 (SRG_BK.1)
SRG_BK.1.1	Backups SHALL be protected against modification by a mechanism that allows verifying the integrity of the backup information.	○	○	○	バックアップは、バックアップ情報の完全性を検証することができるメカニズムによって、変更から保護されるものとする(SHALL)。
SRG_BK.1.2	Sensitive security parameters and other confidential information SHALL be stored in a protected form in order to ensure confidentiality and integrity.	○	○	○	機密性の高いセキュリティパラメータやその他の機密情報は、機密性と完全性を確実にするために、保護された形で保存されるものとする(SHALL)。
6.2.8.3 Recovery (SRG_BK.2)					6.2.8.3 リカバリー(SRG_BK.2)
SRG_BK.2.1	The TW4S SHALL include a recovery function that is able to restore the state of the system from a backup.	○	○	○	SSASCは、バックアップからシステムの状態を復元することができるリカバリー機能を含むものとする(SHALL)。

SRG_BK.2.2	A user linked to a role with sufficient privileges SHALL be capable of invoking the recovery function on demand from a backup.	○	○	○	十分な権限を持つロールにリンクされたユーザは、バックアップからオンデマンドで復旧機能を呼び出すことが可能であるものとする(SHALL)。
6.3 Core components security requirements (SRC)					6.3 コアコンポーネントのセキュリティ要求事項(SRC)
6.3.1 Signing key setup (SRC_SKS) – Cryptographic key (SRC_ SKS.1)					6.3.1 署名鍵設定(SRC_SKS) – 暗号鍵(SRC_SKS.1)
SRC_SKS.1.1	Algorithm parameters to be used for signature creation by trustworthy systems SHALL be chosen so that can resist during the life time of the signer's certificate. NOTE Standardization bodies, security agencies and supervisory authorities of the Member States, cooperate on the harmonization of suitable algorithms [5], and provide cryptographic suites recommendations (e.g. ETSI/TS 119 312 [10], SOG-IS-CRYPTO [18]).	○	○	○	信頼できるシステムによる署名生成に使用するアルゴリズムパラメータは、署名者証明書の有効期間において、耐えられるよう選択されるものとする(SHALL)。 (CRYPTREC電子政府推奨暗号リストおよび暗号強度要件を参照する。)
SRC_SKS.1.2	TW4S SHALL link signer's signing keys with the appropriate signer's public key certificate.	○	○	○	SSASCは、署名者の署名鍵を、適切な署名者の公開鍵証明書とリンクさせるものとする(SHALL)。
SRC_SKS.1.3	Signer's signing key MAY be generated in advance (i.e. not linked to a public key certificate).	○	○	○	署名者の署名鍵は、事前に生成することができる(MAY)(すなわち、公開鍵証明書とリンクしない)。
SRC_SKS.1.4	A signing key SHOULD NOT be used before its public key certificate is linked by the TW4S. NOTEthis recommendation does not apply when the signing key is used to sign a proof of possession in order to obtain a certificate.	○	○	○	署名鍵は、その公開鍵証明書がSSASCによってリンクされる前に使用されるべきではない(SHOULD NOT)。 注:この勧告は、署名鍵が証明書を取得するための所有証明の署名に使用される場合は適用されない。
SRC_SKS.1.5	TW4S SHALL protect the integrity of links between signer's signing key and public key	○	○	○	SSASCは、署名者の署名鍵と公開鍵の間のリンクの完全性を保護するものとする(SHALL)。
6.3.2 Signer authentication (SRC_SA)					6.3.2 署名者認証(SRC_SA)
6.3.2.1 Signer authentication for SCAL1 (SRC_SA.1)					6.3.2.1 SCAL1 の署名者認証(SRC_SA.1)
SRC_SA.1.1	The enrolment of the signer SHALL be as specified in Annex A, A.1, for assurance level low or higher. The electronic identification means characteristics and design SHALL be as specified in Annex A, A.2.1, for assurance level low or higher. The authentication mechanism SHALL be as specified in Annex A, A.2.2, for assurance level low or higher.	○	○	○	署名者の登録の保証レベルは、別表AのA.1に規定される「低」あるいはそれ以上であるものとする(SHALL)。 電子識別手段の特性および設計の保証レベルは、別表AのA.2.1に規定される「低」あるいはそれ以上であるものとする(SHALL)。 認証メカニズムの保証レベルは、別表AのA.2.2に規定される「低」あるいはそれ以上であるものとする(SHALL)。
SRC_SA.1.2	SSA SHALL require each signer to be successfully identified and authenticated before allowing any actions that can impact the sole control of any signing key.	○	○	○	SSASCは、署名鍵の単独制御に影響を与える可能性のある行為を許可する前に、各署名者の識別と認証に成功することを要求するものとする(SHALL)。
SRC_SA.1.3	Protocols in use SHALL prevent man-in-the-middle attacks, replay attacks, and more generally any form of attacks where a malicious user can use authentication credentials which do not belong to him/her.	○	○	○	使用するプロトコルは、中間者攻撃、リプレイ攻撃、より一般的には悪意のあるユーザが自分のものではない認証情報を使用することができるあらゆる形態の攻撃を防止するものとする(SHALL)。
SRC_SA.1.4	Access controls SHALL ensure that a signer does not have access to sensitive system objects and any functions which gives the user control over another's signing key.	○	○	○	アクセス制御は、署名者が機密性の高いシステムオブジェクトや、他の署名鍵の制御をユーザに与える機能へのアクセス権を持たないことを確実にするものとする(SHALL)。
SRC_SA.1.5	The TW4S SHALL ensure that the DTBS/R provided under control of the signer is only signed by the signing key belonging to this signer.	○	○	○	SSASCは、署名者の制御下で提供されるDTBS/Rが、この署名者に属する署名鍵によってのみ署名されることを確実にするものとする(SHALL)。
6.3.2.2 Authentication failure handling (SRC_SA.2)					6.3.2.2 認証失敗時の対応(SRC_SA.2)
SRC_SA.2.1	For a given signer, TW4S SHALL detect when a defined number of consecutive unsuccessful authentication attempts occurs.	○	○	○	与えられた署名者について、SSASCは、定義された回数の連続した認証失敗が発生した場合、それを検知するものとする(SHALL)。
SRC_SA.2.2	For a given signer, when the defined number of unsuccessful authentication attempts is met, the TW4S SHALL block this user's access for a reasonable amount of time or until an administrative role unblock the user.	○	○	○	所定の署名者について、定義された認証失敗回数に至った場合、SSASCは、妥当な期間、または管理者の役割によりユーザーのブロックを解除するまで、このユーザーのアクセスをブロックするものとする(SHALL)。
6.3.2.3 Signer authentication delegated to external system (SRC_SA.3)					6.3.2.3 外部システムに委任された署名者認証(SRC_SA.3)
SRC_SA.3.1	If the signer authentication is delegated to an external system, the TSP SHALL ensure that requirements specified in Clauses SRC_SA.1 and SRC_SA.2 are met by the external system.	○	○	○	署名者認証が外部システムに委任される場合、TSPは、SRC_SA.1節およびSRC_SA.2節に規定される要件が外部システムによって満たされることを確実にするものとする(SHALL)。
6.3.3 Digital signature creation (SRC_DSC) –					6.3.3 電子署名生成(SRC_DSC) – 暗号操作(SRC_DSC.1)
SRC_DSC.1.1	Algorithm parameters for being used for signature creation by trustworthy systems SHALL be chosen so that can resist during the life time of the signer's certificate. NOTE Standardization bodies, security agencies and supervisory authorities of the Member States, cooperate on the harmonization of suitable algorithms [5], and provide cryptographic suites recommendations (e.g. ETSI/TS 119 312 [10], SOG-IS-CRYPTO [18]).	○	○	○	信頼できるシステムによる署名生成に使用されるアルゴリズムパラメータは、署名者証明書の有効期間において耐えられるよう選択されるものとする(SHALL)。 (CRYPTREC電子政府推奨暗号リストおよび暗号強度要件を参照する。)
6.4 Additional security requirements for SCAL2 (SRA)					6.4 SCAL2に対する追加セキュリティ要求事項(SRA)
6.4.1 General					6.4.1 一般事項
6.4.2 Signature activation protocol and signature activation data (SRA_SAP)					6.4.2 署名活性化プロトコル及び署名活性化データ (SRA_SAP)
6.4.2.1 Threat resistance (SRA_SAP.1)					6.4.2.1 脅威への耐性(SRA_SAP.1)

SRA_SAP.1.1	The enrolment of the signer SHALL be as specified in Annex A, subclause A.1, for assurance level substantial or higher. The electronic identification means characteristics and design SHALL be as specified in Annex A, subclause A.2.1, for assurance level substantial or higher. The authentication mechanism SHALL be as specified in Annex A, subclause A.2.2, for assurance level substantial or higher.	○	○	○	署名者の登録保証レベルは別表AのA.1に規定される「十分」以上であるものとする（SHALL）。 電子識別手段の特性及び設計の保証レベルは、別表AのA.2.1に規定される「十分」以上であるものとする（SHALL）。 認証メカニズムの保証レベルは、別表AのA.2.2に規定される「十分」以上であるものとする（SHALL）。
SRA_SAP.1.2	Controls SHALL be provided, as determined necessary by a risk assessment, in order to counter the following threats on SAD and SAD use: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing and masquerading attacks.		○	○	SADおよびSAD使用に関する以下の脅威（オンライン推測、オフライン推測、クレデンシャル複製、フィッシング、盗聴、リプレイ、セッションハイジャック、中間者、クレデンシャル盗難、スプーフィング、マスカレード攻撃）に対抗するため、リスクアセスメントにより必要とされるコントロールを提供するものとする（SHALL）。
SRA_SAP.1.3	SAP SHALL provide cryptographic strength mechanisms that protect the authentication factors against compromise by the protocol threats as well as trusted third party impersonation attacks.		○	○	SAPは、プロトコルの脅威や信頼できる第三者のなりすまし攻撃による侵害から認証要素を保護する暗号強度のメカニズムを提供するものとする（SHALL）。
SRA_SAP.1.4	The SAP SHALL be protected against replay, bypass and forgery attack between signer and the remote SCDev (e.g. with a nonce, timestamp or session token).			○	SAPは、署名者とリモートSCDev間のリプレイ、バイパス、偽造攻撃に対して保護される（例えば、ノンス、タイムスタンプ、セッショントークンを使用）ものとする（SHALL）。
SRA_SAP.1.5	The SAM SHALL be used in a tamper protected environment that: — is a trustworthy system which is ensured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security. This SHALL be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or NOTE 1 Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 are currently under development within CEN as CEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, or EN 419221-5. — meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3. NOTE 2 With the general availability of devices which meet ISO/IEC 15408, it is expected that ISO/IEC 19790 or FIPS 140-2 level 3 will no longer be acceptable.			○	SAMは、以下のような耐タンパー保護環境で使用されるものとする（SHALL）： - これは、ISO/IEC 15408、またはITセキュリティに関する国内もしくは国際的に認知された同等の評価基準に従い、EAL 4以上が確保された信頼できるシステムである。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要件を満たすセキュリティターゲット又はプロテクションプロファイルに対するものとする（SHALL）。 注 1 ISO/IEC 15408に準拠したTSP暗号モジュールのコモンクライテリア プロテクションプロファイルを規定する規格は、現在CEN内でCEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, または EN 419221-5 として開発中である。 - あるいは、ISO/IEC 19790またはFIPS PUB 140-2レベル3で特定される要件を満たす。 注2 ISO/IEC 15408を満たす機器が一般に普及したことで、ISO/IEC 19790やFIPS 140-2のレベル3は通用しなくなることが予想される。
SRA_SAP.1.6	The SAP SHALL be designed such that it can be assumed that the SAD is always reliably protected against duplication or tampering against an attacker with high attack potential.		○	○	SAPは、攻撃可能性の高い攻撃者に対して、SADが複製や改ざんから常に確実に保護されていると仮定できるように設計されるものとする（SHALL）。
SRA_SAP.1.7	The SAP SHALL be designed such that the signer can always reliably protect the signing key activation by the SAD against an attacker with high attack potential.		○	○	SAPは、攻撃可能性の高い攻撃者に対して、署名者がSADによる署名鍵の活性化を常に確実に保護できるように設計されるものとする（SHALL）。
6.4.2.2 SAD Management (SRA_SAP.2)					6.4.2.2 SAD管理（SRA_SAP.2）
SRA_SAP.2.1	The SAD MAY be a set of data or be a result of cryptographic operations using mandatory parameters listed below.	○	○	○	SADは、データの集合とすることもできるし、以下に示す必須パラメータを用いた暗号操作の結果とすることもできる（MAY）。
SRA_SAP.2.2	The SAD MAY be collected or generated in the signer's environment by the SIC or remotely using the SIC under control of signer.	○	○	○	SADは、署名者の環境の中のSICにより、または署名者の制御下にあるSICを使用して遠隔に収集または生成できる（MAY）。
SRA_SAP.2.3	The SAD SHALL link with a high level of confidence at least the following parameters: — a given DTBS/R or a set of DTBS/R, — items to identify the authenticated signer, and — default or selected signing key. If supported, it SHALL be possible to disable use of more than one DTBS/R in contexts where it is not legally permitted.		○	○	SADは、少なくとも以下のパラメータを高い信頼性でリンクするものとする（SHALL）： - 与えられたDTBS/RまたはDTBS/Rの集合、 - 認証された署名者を識別するための項目、および - デフォルトまたは選択された署名鍵 サポートされている場合、法的に許可されていない文脈では、複数のDTBS/Rの使用を無効化することが可能であるものとする（SHALL）。
SRA_SAP.2.4	The SAD SHALL be used to activate signing key only if signer authentication succeeds. (by e.g. computing SAD after successful authentication, or by other cryptographic means).	○	○	○	署名者認証に成功した場合のみ、SADを使用して署名鍵を活性化するものとする（SHALL）。 （認証に成功した後にSADを計算すること、または他の暗号化の手段によって）。
SRA_SAP.2.5	The SAD SHALL be passed to the SAM in the SAP.		○	○	SADは、SAPのSAMに渡されるものとする（SHALL）。

SRA_SAP.2.6	The SAD SHALL: — be collected in a way that is under the control of the signer with a high level of confidence, — be protected so that any keys held within devices are secure, and — protect any secret used (one time or long term one) as defined in SRA_SAP.1.4		○	○	SADは、以下をすべて満足するものとする(SHALL): - 署名者の管理下にある方法で、高い信頼性をもって収集されること、 - デバイス内に保持される鍵が安全であるように保護されていること、そして - SRA_SAP.1.4 で定義されているように、使用される秘密(一回限りまたは長期的なもの)を保護すること。
SRA_SAP.2.7	The SAP SHALL be designed such that if SAD are received by the SAM, it can be assumed that the SAD were submitted under sole control of the signer by means that are in possession of the signer.		○	○	SAPは、SAMがSADを受領した場合、SADが署名者の単独制御のもと、署名者が所有する手段により提出されたと想定できるように設計されるものとする(SHALL)。
SRA_SAP.2.8	The SAD SHALL be verified such that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication for signature activation.		○	○	SADは、攻撃可能性の高い攻撃者による推測、盗聴、リプレイ、通信操作などの行為によって、署名活性化のための認証が破られる可能性が極めて低いことを検証するものとする(SHALL)。
6.4.3 Signing key management (SRA_SKM)					6.4.3 署名鍵管理(SRA_SKM)
6.4.3.1 Signing key generation (SRA_SKM.1)					6.4.3.1 署名鍵生成 (SRA_SKM.1)
SRA_SKM.1.1	Signer's signing key SHALL be generated and used in a SCDev that: — is a trustworthy system which is ensured to EAL 4 or higher, augmented by AVA_VAN.5 in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security. This SHALL be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non- technical security measures; or NOTE 1 Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408, are currently under development within CEN as CEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, or EN 419221-5. — meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3. NOTE 2 With the general availability of devices which meet ISO/IEC 15408, it is expected that ISO/IEC 19790 or FIPS 140-2 level 3 will no longer be acceptable.		○	○	署名者の署名鍵を以下のSCDevで生成し使用するものとする(SHALL): - ISO/IEC 15408に準拠したAVA_VAN.5で補強されたEAL 4以上、またはITセキュリティに関する国内もしくは国際的に認知された同等の評価基準で確保された信頼できるシステムである。これは、リスク分析に基づき、物理的及びその他の非技術的なセキュリティ対策を考慮した上で、本文書の要求事項を満たすセキュリティターゲット又はプロテクションプロファイルに対するものであるものとする(SHALL)。 注 1 ISO/IEC 15408 に準拠した TSP暗号モジュールのコモンクライテリアプロテクションプロファイルを規定する規格は、現在CEN内で CEN/TS 419221-2, CEN/TS 419221-3, CEN/TS 419221-4, または EN 419221-5 として開発中である。 - あるいは、ISO/IEC 19790 または FIPS PUB 140-2 レベル 3で識別される要件を満たす。 注2ISO/IEC 15408に適合する機器の一般的な普及に伴い、ISO/IEC 19790またはFIPS 140-2のレベル3は受け入れられなくなることが予想される。
SRA_SKM.1.2	This SCDev SHALL be dedicated to supporting the cryptographic functions required by the signature creation service (i.e. including random number generation and possibly even encryption in support of the server signing).	○	○	○	このSCDev は、署名生成サービスに必要な暗号機能(乱数生成や、場合によってはサーバー署名をサポートする暗号化も含む)のサポート専用であるものとする(SHALL)。
SRA_SKM.1.3	When the SCDev used to generate signing keys is different from the SCDev used for signature operations, the transmission of signing keys SHALL requirement SRG_KM.4.1.		○	○	署名鍵の生成に使用するSCDevが署名操作に使用するSCDevと異なる場合、署名鍵の転送はSRG_KM.4.1を要求するものとする(SHALL)。
SRA_SKM.1.4	SCDev MAY contain several signing keys for the same signer and for different signers. Where several signing keys for the same signer or for different signers are contained within the SCDev, separation of control over the use of the keys SHALL be ensured.	○	○	○	SCDevは、同じ署名者及び異なる署名者のための複数の署名鍵を含むことができる(MAY)。 同一署名者または異なる署名者の複数の署名鍵がSCDevに含まれる場合、鍵の使用に関する管理の分離を確実にするものとする(SHALL)。
SRA_SKM.1.5	Signer's signing key SHALL be linked with a high level of confidence to its signer by a means provided by the SAP.		○	○	署名者の署名鍵は、SAPが提供する手段により、その署名者に高い信頼性でリンクされるものとする(SHALL)。
SRA_SKM.1.6	Signer's signing key SHALL NOT be used before its signer is linked by the TW4S.	○	○	○	署名者の署名鍵は、その署名者がSSASCによってリンクされる前に使用されないものとする(SHALL NOT)。
SRA_SKM.1.7	TW4S MAY support several different SAP and SAD mechanisms to activate signing keys. However, a signing key SHALL be linked to only one SAD and SAP mechanism.		○	○	SSASCは、署名鍵を活性化するために、いくつかの異なるSAPとSADのメカニズムをサポートしてもよい(MAY)。 ただし、1つの署名鍵は、1つのSADおよびSAP機構にのみリンクされるものとする(SHALL)。
6.4.3.2 Signing key activation (SRA_SKM.2)					6.4.3.2 署名鍵の活性化 (SRA_SKM.2)
SRA_SKM.2.1	The TW4S SHALL require the signer to present a SAD to the SAM in order to be authenticated and to activate the signing key.		○	○	SSASCは、署名者を認証し、署名鍵を活性化するために、署名者がSAMに対してSADを提示することを要求するものとする(SHALL)。
SRA_SKM.2.2	The SAP SHALL manage the transmission of SAD to SAM in a way that guarantees that the signing key is under control of signer with high level of confidence.		○	○	SAPは、署名鍵が高い信頼性で署名者の制御下にあることを保証する方法で、SADのSAMへの転送を制御するものとする(SHALL)。
SRA_SKM.2.3	Signer's signing key SHALL be activated for a use in a remote SCDev only.	○	○	○	署名者の署名鍵は、リモートSCDevでの使用のためにのみ活性化されるものとする(SHALL)。
SRA_SKM.2.4	Signer's signing key SHALL be activated by the SAD generated with the signer's authentication factors with the correct key reference.	○	○	○	署名者の署名鍵は、署名者の認証要素を用いて生成されたSADにより、正しい鍵へのリファレンスで活性化されるものとする(SHALL)。
SRA_SKM.2.5	Activated signing key SHALL be used to sign only DTBS/R authorized by the SAP.		○	○	活性化された署名鍵は、SAPによって認可されたDTBS/Rのみに署名するために使用されるものとする(SHALL)。
SRA_SKM.2.6	Where DTBS/R for a SAD comes from a SCA, the source SHALL be authenticated.	○	○	○	SADのDTBS/RがSCAから来る場合、そのソースは認証されるものとする(SHALL)。 ※ SCAを認証しているかどうか不明。 ※ 本来必要な要件で、他の対策等でカバーできるかどうかを確認する必要がある。
SRA_SKM.2.7	Privileged users SHALL not be able to use signing key allocated to a signer.	○	○	○	特権ユーザは、署名者に割り当てられた署名鍵を使用することができないものとする(SHALL NOT)。

SRA_SKM.2.8	After signing key activation and digital signature creation, signer’s SAD SHALL NOT be stored unprotected anywhere by TW4S.	○	○	○	署名鍵の活性化とデジタル署名の生成後、署名者のSADをSSASCが保護されない状態で保存しないものとする（SHALL NOT）。

リモート署名サービスの評価基準

― 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を参考に作成）

目次

1 スコープ

本書は、デジタル署名生成をサポートするサービスコンポーネントを実装しているトラストサービスプロバイダ(TSP)のポリシーとセキュリティ要件を規定する。デジタル署名生成アプリケーション(SCA)を含むこのコンポーネントをデジタル署名生成アプリケーションサービスコンポーネント(SCASC)と呼ぶ。しかし、SCASCはSCA以外の機能を含む場合もある。SCASCには、ETSI TS 119 102-1およびETSI TS 119 101で定義されている駆動アプリケーション(署名対象文書等をはじめ、署名を生成するための様々なパラメータ(使用する署名アルゴリズム、署名の意図、署名者の役割、など)を設定・入力し、署名生成のトリガーをかけるコンポーネント)の一部を実装するためのサービスエレメントを含む場合がある。本書は、SCASCによって実行される機能がデジタル署名生成アプリケーション内に存在するか外部に存在するかについては制限を加えない。

本書は、このようなサービスコンポーネントを実装するTSPのタイプ(TSPが提供するサービスのタイプ。CA、TSAなど)について制限を加えない。

本書は、デジタル署名の生成において信頼できる組織であることを確認するための根拠として、管轄機関が使用することができる。

注1： TSPプロセスおよびサービスの評価に関するガイダンスについては、ETSI EN 319 403を参照のこと。

SCASCは、例えば署名に含まれる情報を提供するために接続可能な外部(トラスト)サービスとの接続を有する。本書は、そのような外部サービスによって適用されるトラストサービスポリシーに関する要件を提示しない。

本書は、SCASCにアクセスするために使用されるプロトコルや、SCACSが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)や署名生成デバイス(SCDev)に接続する方法を規定しない。

注2： SCASCまたはSSASCにコンタクトするためのプロトコルは、ETSI TS 119 432に定義されている。

本書は、デジタル署名生成を提供するサービスに関連するリスクに対処するために必要な管理策を特定する。

2 参照規格

参照規格は、リモート署名サービスの評価基準を参照のこと。

3 用語と定義、記号・略称及び評価基準での表記

3.1 用語と定義

用語と定義は、リモート署名サービスの評価基準を参照のこと。

3.2 記号

なし。

3.3 略称

略称は、リモート署名サービスの評価基準を参照のこと。

3.4 評価基準での表記

「デジタル署名生成サービスの一般ポリシー要求事項」で示される要件には，次のものが含まれる：

a) 本書に適合するあらゆるTSPに適用される要件。このような要件は，付加的な表示をせずに示す。

b) 特定の条件下で適用される要件。このような要件は、"[CONDITIONAL]"を付与して示す。

「デジタル署名生成サービスの一般ポリシー要求事項」における要求事項は，次のような要求識別子で識別される：

<サービスの要素を識別する3文字> - <条項番号> - <2桁の番号-増分>。

サービスの要素は次の通り：

- OVR：一般要件（1つ以上の構成要素に適用される要件）
- ASI：デジタル署名インタフェース

この次版以降における要求識別子の管理は、以下の通りである：

- 要件が条項の末尾に挿入される場合、上記の2桁の数字は、利用可能な次の数字にインクリメントされる。
- 要件が既存の2つの要件の間に挿入される場合、新しい要件を区別するために、以前の要件識別子に大文字が付加される。
- 削除された要件の要件識別子は残され、"VOID" で示さ れる。
- 変更された要件の要件識別子は空白にされ、変更された要件は、最初の要件番号に付加された大文字で識別される。

4 一般的な概念

4.1 一般的なポリシー要件の概念

本書は、ETSI EN 319 401に沿って構成されている。ETSI EN 319 401の要求事項を参照により組み込み、SCASPに関連する要求事項を追加している。

一般的なポリシー要件に関するガイダンスについては、ETSI EN 319 401の第4章を参照のこと。

4.2 デジタル署名生成サービスコンポーネントの関連文書

4.2.1 デジタル署名生成サービスコンポーネント運用規定

デジタル署名生成サービスプロバイダー(SCASP)は、ETSI EN 319 401に定義されるトラストサービス運用規定を、デジタル署名生成サービスコンポーネント向けに特化したSCASC運用規定として開発、実装、実施、更新する。「デジタル署名生成サービスの一般ポリシー要求事項」を参照のこと。

SCASC運用規定は、SCASPがサービスをどのように運用するかを記述し、SCASPが所管する。SCASCの運用は、TSPの組織構造、運用手順、設備、およびコンピューティング環境に合わせて調整される。運用規定の受領者としては、監査人、加入者、および依拠当事者等があげられる。

注： 本書で要求されるように、SCASC運用規定にはいくつかの要素の存在が必須であるが、本書はSCASC運用規定の形式に制限を設けない。

本書は、SCASPによって承認され、その運用規定に反映される、高レベルのSCASCポリシーをサポートするために必要と認められた要件を提供する。

4.2.2 デジタル署名生成サービスコンポーネントポリシー

SCASCのポリシーは何が提供されるかを記述するものであり、サービスの適用可能性を示すために本書のスコープを超えた多様な情報を含むことができる。SCASCポリシーは、SSASPの具体的な運用環境の詳細とは無関係に定義される。サービスポリシーの受領者は、監査人、加入者、依拠当事者である。

本書はSCASCポリシーによって参照され、サービスレベルに関する情報を提供する。

SCASCポリシーは必ずしも4.2で示されるSCASPの関連文書の一部である必要はない(ETSI EN 319 401に従えば、運用規定と利用規約だけで十分である)。例えば、SCASCポリシーはコミュニティ内で共有され、個々のSCASPが独自に所有しないこともあり得る。また、本書はSCASCポリシーの形式について制約を設けていない。SCASCポリシーは独立した文書とすることもできるし、運用規定および／または利用規約の一部として提供することもできる。

本書はSCASCポリシーの内容にいかなる制限も加えるものではないが、SCASPは提供するサービスに関する最低限の情報を提供することが要求される(「デジタル署名生成サービスの一般ポリシー要求事項」参照)。

4.2.3 利用規約

SCASC運用規定及びSCASPが発行する場合はSCASCポリシーに加え、SCASPは「デジタル署名生成サービスの一般ポリシー要求事項」を参照して利用規約を発行する。利用規約は、必ずしも利用者等に通知されない広範な商業的条件または技術的条件を包含することができる。取引条件は個々のSCASPにとって特有のものである。利用規約の受領者は、契約者および依拠当事者である。

注： 本書で要求されているように、いくつかの要素の存在は利用規約に必須であるが、本書は利用規約の形式に制限を設けていない。利用規約の形式および内容は、法令等にも依存しうる。

4.2.4 デジタル署名生成に関するその他の文書

SCASPがデジタル署名生成サービスを提供するために採用した運用規定の記述に加え、署名が生成される基準を文書化することが重要であり、その上で特定のビジネスニーズに適合しているかを判断することができる。

これらの目的のために、2つの文書を使用することができる：

- SCAが処理する署名生成制約の集合である署名生成ポリシー。署名生成ポリシーはOIDによって識別される。
- 署名適用性規則は、ETSI TS 119 172-1に従い構成され、SCAが適用する署名生成制約を含む署名生成ポリシー、および特定のビジネスニーズに対する生成された署名の適用性を示すその他の基準を含むことができる。

注： 署名適用性規則の使用は本書のスコープ外であるが、本書の記載範囲内であるデジタル署名生成サービスの拡張として適用することができる。

SCASC運用規定、署名生成ポリシー、および署名適用性規則は異なるタイプの文書である。SCASCの運用規定はSCASPがサービスを運用する方法を記述し、署名生成ポリシーは署名を生成する際にSCAが処理すべき制約を記述する。署名適用性規則は、署名生成ポリシーのスコープを超えて、これらのルールに従って生成された署名が目的に適合しているかどうかを判断するためにユーザーが使用するルールと仮定を記述する。

SCASC運用規定の所有者はSCASPであり、署名適用性規則の所有者は、通常、署名者である。

4.3 アーキテクチャ

デジタル署名生成をサポートするTSPサービスコンポーネント(SCASC)は、署名される文書および/または文書のハッシュ、およびオプションでいくつかの署名パラメータを受け取り、署名生成に必要なすべての情報を収集し、署名対象のデータ表現(DTBS/R)を生成して、これをSCDevに送信する。ETSI TS 119 431-1に記載されているように、SCDevがユーザーの環境にある場合と、リモートに存在して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)によって管理される場合がある。本書では、SCDevが認証とユーザーによる署名することへの合意を処理し、デジタル署名値を返すと仮定する。SCDev内で署名鍵を使用するための認可は、SCASCを経由することもできるが、署名者とSCDev間の通信によって直接行うこともできる。デジタル署名値はSCASCによってデジタル署名に含められる。

注： SCASCはEN 419241-1における署名生成アプリケーションを表す。

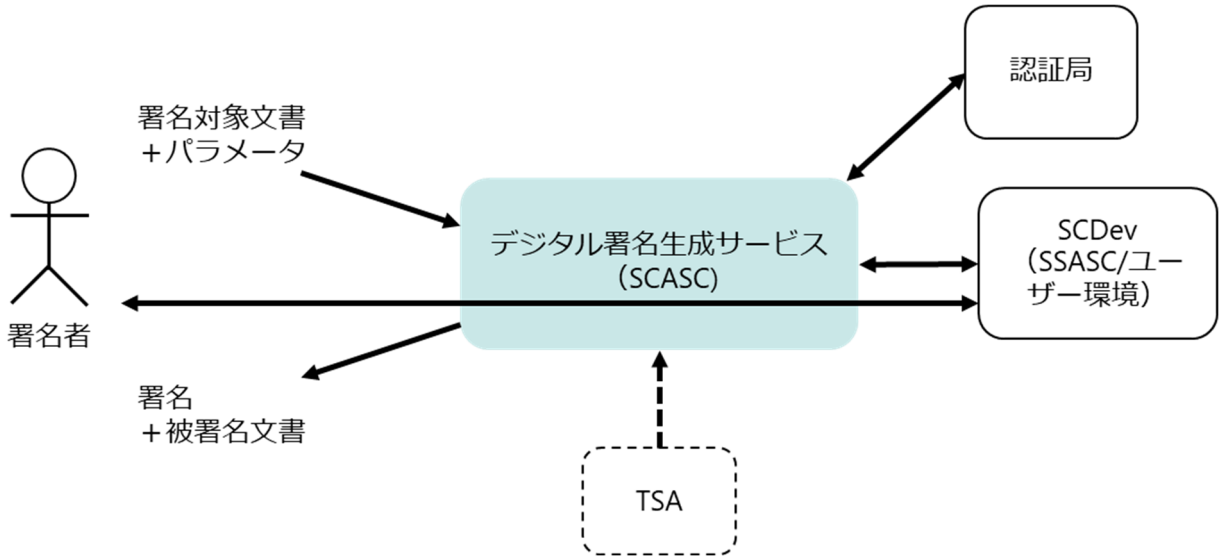


図１：デジタル署名生成のためのTSP**サービスコンポーネントの関係**

5 リスクアセスメント

「デジタル署名生成サービスの一般ポリシー要求事項」参照

6 ポリシーと運用規程

「デジタル署名生成サービスの一般ポリシー要求事項」参照

7 デジタル署名生成サービスの管理と運用

「デジタル署名生成サービスの一般ポリシー要求事項」参照

8 デジタル署名生成サービスコンポーネントの技術的要件

「デジタル署名生成サービスの一般ポリシー要求事項」参照

9 本書を基に構築された署名生成アプリケーションサービスコンポーネントポリシーの定義のためのフレームワーク

「デジタル署名生成サービスの一般ポリシー要求事項」参照

デジタル署名生成サービスの一般ポリシー要求事項			
Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation(ETSI TS 119 431-2 V1.2.1)を参考に作成			
		監査対象(全レベル共通)	
5 Risk assessment			5 リスクアセスメント
OVR-5-01	The requirements specified in ETSI EN 319 401 [9], clause 5 shall apply.	○	「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」の5に規定されている要件が適用されるものとする(SHALL)。
6 Policies and practices			6 ポリシーと運用規程
6.1 Trust service practice statement			6.1 トラストサービス運用規程
OVR-6.1-01	The requirements specified in ETSI EN 319 401 [9], clause 6.1 shall apply. In addition, the following particular requirements apply:	○	「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」の6.1に規定されている要件が適用されるものとする(SHALL)。さらに、以下の特定の要件が適用される。
OVR-6.1-02 [CONDITIONAL]	When the SCASC supports the inclusion of time-stamp tokens in the AdES digital signature, the SCASC practice statement shall list which TSA are used.	○	SCASCがデジタル署名にタイムスタンプトークンを含めることをサポートしている場合、SCASC運用規程はどのTSAが使用されているかを列挙するものとする(SHALL)。
OVR-6.1-03	The SCASC practice statement shall specify all the supported signature creation polices.	○	SCASC運用規程は、サポートされているすべての署名生成ポリシーを指定するものとする(SHALL)。
OVR-6.1-04	The SCASC practice statement shall specify all the supported signature formats.	○	SCASC運用規程は、サポートされているすべての署名フォーマット(CAdES/XAdES/PAdES/JAdESなど)を指定するものとする(SHALL)。
OVR-6.1-05	The SCASC practice statement shall specify all the supported signature classes. NOTE: ETSI TS 119 102-1 [2] describes different signature classes.	○	SCASC運用規程は、サポートされているすべての署名クラス(B、T、LT、LTA)を指定するものとする(SHALL)。
OVR-6.1-06	The SCASP shall identify in the SCASC practice statements the obligations of all external organizations supporting its services including the applicable policies and practices	○	SCASPは、適用可能なポリシーと実務を含む、そのサービスを支援するすべての外部組織の義務をSCASC運用規程の中で識別するものとする(SHALL)。
6.2 Terms and Conditions			6.2 利用規約
OVR-6.2-01	The requirements specified in ETSI EN 319 401 [9], clause 6.2 shall apply. In addition, the following particular requirements apply:	○	OVR-6.2-01：「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」の6.2に規定されている要件を適用するものとする(SHALL)。加えて、以下の特定の要件が適用される。
OVR-6.2-02	To specify the trust service policy being applied, the SCASC terms and conditions shall list or make reference to (e.g. through OIDs), and briefly describe, the supported SCASC policies it conforms to.	○	適用されているトラストサービスポリシーを特定するために、SCASC利用規約は、それが準拠するSCASCポリシーを列挙または参照し(例えばOIDを通して)、そして簡潔に説明するものとする(SHALL)。
OVR-6.2-06	The terms and conditions shall indicate the rights and obligations of the SCASP and the signer.	○	利用規約はSCASPと署名者の権利と義務を示すものとする(SHALL)。
OVR-6.2-07	The terms and conditions shall describe the options supported by the service. At least:	○	利用規約は、サービスによってサポートされているオプションを記述するものとする(SHALL)。少なくとも以下を記述するものとする(SHALL)：
a)	the supported signature formats, EXAMPLE: CAdES [3], [4], XAdES [5], [6] or PAdES [7],[8].	○	a) サポートされている署名フォーマット 例： CAdES、XAdES、またはPAdES。
b)	the supported signature parameters	○	サポートされている署名パラメータ
c)	if the to be signed document can be provided only as a hash, and	○	署名対象の文書がハッシュとしてのみ提供される場合
d)	the supported signature creation devices (SCDev) in the user's environment or the supported SSASCs creating the digital signature value for the signer.	○	サポートされている利用者の環境の署名生成装置(SCDev)、またはサポートされている署名者のデジタル署名値を生成するSSASC。
OVR-6.2-08	The terms and conditions shall include Service-Level Agreement (SLA) elements for the availability of the service and when applicable, other SLA information such as response times.	○	利用規約は、サービス可用性に関するサービスレベル合意(SLA)の要素、および該当する場合は応答時間などの他のSLA情報を含むものとする(SHALL)。
OVR-6.2-09	The terms and conditions shall provide a notice that the SLA can be affected by the practices, policies and SLAs of other TSPs, not under the control of the SCASP like the CA issuing the certificate used for the signature or a TSA used for a time-stamp.	○	利用規約は、SLAが、署名に使用される証明書を発行するCAやタイムスタンプに使用されるTSAのようなSCASPの管理下にない他のTSPの運用、ポリシー、SLAによって影響を受ける可能性があることを通知するものとする(SHALL)。
OVR-6.2-10	The terms and conditions shall explain how the SCASP processes personal data.	○	利用規約はSCASPがどのように個人データを処理するかを説明するものとする(SHALL)。
6.3 Information security policy			6.3 情報セキュリティポリシー

OVR-6.3-01	The requirements specified in ETSI EN 319 401 [9], clause 6.3 shall apply. In addition, the following particular requirement apply:	○	「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」の6.3に規定されている要件を適用するものとする(SHALL)ことに加えて、以下の特定の要件が適用される。
OVR-6.3-02	The security policy should document the security and privacy controls implemented to protect personal data. NOTE: If the SCASP has access to the to be signed data, then this can contain confidential information as well as personal data	○	セキュリティポリシーは、個人データを保護するために実装されたセキュリティとプライバシーの管理策を文書化するべきである(SHOULD)。 注： SCASPが署名対象のデータにアクセスできる場合、これには個人情報だけでなく機密情報も含まれる可能性がある。
7 Signature creation application service management and operationon			7 デジタル署名生成サービスの管理と運用
7.1 Internal organization			7.1 内部組織
OVR-7.1-01	The requirements specified in ETSI EN 319 401 [9], clause 7.1 shall apply.	○	「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」の7.1に規定されている要件が適用されるものとする(SHALL)。
7.2 Human resources			7.2 人的資源
OVR-7.2-01	The requirements specified in ETSI EN 319 401 [9], clause 7.2 shall apply	○	「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」の7.2に規定されている要件が適用されるものとする(SHALL)。
7.3 Asset managemen			7.3 資産管理
OVR-7.3-01	The requirements specified in ETSI EN 319 401 [9], clause 7.3 shall apply.	○	「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」の7.3に規定されている要件が適用されるものとする(SHALL)。
7.4 Access control			7.4 アクセス制御
OVR-7.4-01	The requirements specified in ETSI EN 319 401 [9], clause 7.4 shall apply.	○	「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」の7.4に規定されている要件が適用されるものとする(SHALL)。
7.5 Cryptographic controls			7.5 暗号制御
OVR-7.5-01	The requirements specified in ETSI EN 319 401 [9], clause 7.5 shall apply.	○	「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」の7.5に規定されている要件が適用されるものとする(SHALL)。
7.6 Physical and environmental security			7.6 物理的および環境的安全
OVR-7.6-01	The requirements specified in ETSI EN 319 401 [9], clause 7.6 shall apply. In addition the following particular requirement apply:	○	「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」の7.6に規定されている要件に加えて、以下の特定の要件が適用されるものとする(SHALL)。
OVR-7.6-02	The following requirement specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: GSM 1.4. GSM 1.4: Cryptographic libraries tested against the corresponding standard shall be used. Established libraries should be used.	○	ETSI TS 119 101の5.2に規定されている以下の要求事項がSCAに適用されるものとする(SHALL)：GSM 1.4。 GSM 1.4： 対応する標準に対してテストされた暗号ライブラリを使用すること。確立されたライブラリを使用すべきである(SHOULD)。
7.7 Operation security			7.7 運用セキュリティ
OVR-7.7-01	The requirements specified in ETSI EN 319 401 [9], clause 7.7 shall apply. In addition, the following particular requirements apply:	○	「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」の7.7に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。
OVR-7.7-02	The following requirements specified in ETSI TS 119 101 [1], clause 5.2 should apply to the SCA:GSM 1.2 and GSM 1.3 GSM 1.2: The latest application environment (managed software environments) should be used including up to date security fixes. GSM 1.3: Well-tested and reviewed implementations of standardized protocol(s) and libraries shall be used.	○	ETSI TS 119 101の5.2に規定されている以下の要求事項がSCAに適用されるべきである(SHOULD)：GSM 1.2およびGSM 1.3。 GSM 1.2：最新のアプリケーション環境(管理されたソフトウェア環境)は、最新のセキュリティフィックスを含めて使用されるべきである(SHOULD)。 GSM 1.3:：標準化されたプロトコルとライブラリの実装は、十分にテストされ、レビューされたものを使用するものとする(SHALL)。
OVR-7.7-03	The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SCA: GSM 2.4. GSM 2.4: The SCA/SVA/SAA shall maintain integrity and confidentiality of all information supplied by the user and of any data flowing between the application and the user, even in the case of a public application environment.	○	ETSI TS 119 101の5.2に規定されている以下の要求事項がSCAに適用されるものとする(SHALL)：GSM 2.4。 GSM 2.4：SCA/SVA/SAAは、公開アプリケーション環境の場合であっても、ユーザーから提供された全ての情報、およびアプリケーションとユーザーの間を流れる全てのデータの完全性と機密性を維持するものとする(SHALL)。
7.8 Network security			7.8 ネットワークセキュリティ
OVR-7.8-01	The requirements specified in ETSI EN 319 401 [9], clause 7.8 shall apply.	○	「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」の7.8に規定されている要件が適用されるものとする(SHALL)。
7.9 Incident management			7.9 インシデント管理
OVR-7.9-01	The requirements specified in ETSI EN 319 401 [9], clause 7.9 shall apply.	○	「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」の7.9に規定されている要件が適用されるものとする(SHALL)。
7.10 Collection of evidence			7.10 証拠の収集

OVR-7.10-01	The requirements specified in ETSI EN 319 401 [9], clause 7.10 shall apply. In addition the following particular requirements apply:	○	「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」の7.10に規定されている要件に加えて、以下の特定の要件が適用されるものとする(SHALL)。
OVR-7.10-02	Any AdES digital signature creation operation shall be logged, together with identification of the subscriber when this information is known.	○	この情報が知られているときは、デジタル署名生成操作は、加入者の識別とともに記録されるものとする(SHALL)。
OVR-7.10-03	Event logs shall be marked with the time of the event.	○	イベントログはイベントの発生時刻でマーク付けされるものとする(SHALL)。
OVR-7.10-04	The frequency of processing, the retention period, the protection, the back-up procedures of the collection system, the archiving procedures and the vulnerability assessment of the event logs shall be documented in the SCASC practice statement	○	処理頻度、保存期間、保護、収集システムのバックアップ手順、アーカイブ手順、およびイベントログの脆弱性評価は、SCASC運用規程に文書化されるものとする(SHALL)。
OVR-7.10-05	The implementation of requirements OVR-7.10.1 and OVR-7.10.2 shall take the applicable privacy requirements into account.	○	要件OVR-7.10.1およびOVR-7.10.2の実装は、適用されるプライバシー要件を考慮に入れるものとする(SHALL)。
OVR-7.10-06	Event logs should include the type of the event, the event success or failure, and an identifier of the person and/or component at the origin for such an event.	○	イベントログには、イベントの種類、イベントの成功または失敗、およびそのようなイベントの発生源となる人物および/またはコンポーネントの識別子を含めるものとする(SHALL)。
7.11 Business continuity management			7.11 事業継続マネジメント
OVR-7.11-01	The requirements specified in ETSI EN 319 401 [9], clause 7.11 shall apply. In addition, in order to provide business continuity as specified in the terms and conditions the following particular requirements apply:	○	「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」の7.11に規定されている要件が適用されるものとする(SHALL)。さらに、利用規約に指定されているとおりに事業継続性を提供するために、以下に示す要件が適用される。
OVR-7.11-02	Measures should be implemented to avoid interruptions of the service due to intentional or unintentional behaviour of users or third parties.	○	ユーザーまたは第三者の意図的または意図的でない行動によるサービスの中断を回避するための対策が実施されるべきである(SHOULD)。
OVR-7.11-03 [CONDITIONAL]	When adding time-stamps to the signature, the SLA of the SCASP should take the SLA of the corresponding TSA into account.	○	署名にタイムスタンプを追加するとき、SCASPのSLAは対応するTSAのSLAを考慮に入れるべきである(SHOULD)。
7.12 Termination and termination plans			7.12 終了および終了計画
OVR-7.12-01	The requirements specified in ETSI EN 319 401 [9], clause 7.12 shall apply.	○	「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」の7.12に規定されている要件が適用されるものとする(SHALL)。
7.13 Compliance and legal requirements			7.13 コンプライアンスと法的要件
OVR-7.13-01	The requirements specified in ETSI EN 319 401 [9], clause 7.13 shall apply. In addition, the following particular requirements apply:	○	「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」の7.13に規定されている要件に加え、以下の特定の要件が適用されるものとする(SHALL)。
OVR-7.13-02	When personal data is processed by a third party, if needed by the law, an appropriate agreement shall be made with third party processors of personal data in order to ensure that they do comply with the legal requirements, including the implementation of technical, organizational and legal measures to protect the personal data. NOTE 1: The data to be signed is to be considered as personal data.	○	個人データが第三者によって処理される場合、法律等により必要とされる場合は、個人データの第三者処理者が個人データを保護するための技術的、組織的および法的措置の実施を含む法的要件を遵守することを確実にするために、個人データの第三者処理者と適切な契約を結ぶものとする(SHALL)。 注1：署名対象データは個人データと見なされる。
OVR-7.13-03	The SCASC shall not store the SD after processing when not necessary. NOTE 2: If the SCASP works in combination of a preservation service there can be a need to keep such data.	○	SCASCは、不要なときはSD(署名者のドキュメント)を処理後に保存しないものとする(SHALL NOT)。 注2：SCASPが保存サービスと組み合わせて機能する場合、そのようなデータを保存する必要があり得る。
OVR-7.13-04	The SCASP shall have the overall responsibility for meeting the requirements defined in clauses 5 to 8 even when some or all of its functionalities are undertaken by sub-contractors.	○	SCASPは、その機能の一部または全部が下請け業者によって行われている場合でも、5から8に定義された要件を満たすことに対して全体的な責任を負うものとする(SHALL)。
8 Signature creation application service component technical requirements			8 デジタル署名生成サービスコンポーネントの技術的要件
8.1 Interface			8.1 インターフェース
ASI-8.1-02	The connection between the SCASC and the SCDev used for creation of the digital signature value shall be secured.	○	デジタル署名値の生成に使用されるSCASCとSCDevの間の接続は保護されるものとする(SHALL)。
ASI-8.1-03 [CONDITONAL]	When the SCASC presents the document to the signer, it shall describe in its SCASC practice statement how it guarantees that What You See Is What You Sign (WYSIWYS).	○	SCASCがその文書を署名者に提示するとき、SCASC運用規程の中で、「見たものが署名したもの」であること(WYSIWYS)を保証する方法を記述するものとする(SHOULD)。

ASI-8.1-04 [CONDITONAL]	When the SCASC presents the document to the signer in an interpreted way, the SCASC practice statement shall clearly state how it interprets specific data. EXAMPLE: The document to be signed is XML format, and the practice statement states which software is used for the presentation or which rules are followed to present the different XML tags.	○	SCASCが文書を変換して署名者に提示するとき、SCASC運用規程はそれが特定のデータをどのように変換するかを明記するものとする(SHALL)。 例：署名される文書はXMLフォーマットであり、運用規程は、プレゼンテーションにどのソフトウェアが使用されるか、または異なるXMLタグを提示するために従うべき規則を述べている。
ASI-8.1-05 [CONDITONAL]	When the SCASC presents the document to the signer, the SCASC practice statement or the terms and conditions shall state which content types can be correctly presented.	○	SCASCが文書を署名者に提示するときには、SCASC運用規程または諸条件は、どのコンテンツタイプを正しく提示できるかを述べるものとする(SHALL)。
ASI-8.1-06 [CONDITONAL]	When the SCASC presents the document to the signer, the interface shall warn the signer if it cannot accurately present all parts of the SD according to the data content type.	○	SCASCが文書を署名者に提示するとき、データ内容の種類に従ってSDのすべての部分を正確に提示できない場合、インタフェースは署名者に警告するものとする(SHALL)。
ASI-8.1-07 [CONDITONAL]	When the SCASC provides a graphical user interface to the client the requirements UI 1 and UI 2 from ETSI TS 119 101 [1] should apply. UI 1: The user interface should: a) provide unambiguous user guidance on how to use the SCA/SVA/SAA, and, if applicable, to install and configure the system; b) be self-descriptive to the extent that each dialogue step is easy to understand through feedback from the system or is explained to the user upon request; c) be error tolerant if, despite evident errors in input, the intended result can be achieved with minimal corrective action; d) deliver informative error reporting to lead the user forward; e) provide feedback to confirm that the action carried out by the user is correct (or incorrect); f) when using colour indication, use red for errors and green for go/proceed; g) be able, at any time, to cancel the current operation and return to the main menu; or, to exit the system completely;	○	SCASCがクライアントにグラフィカルユーザインタフェースを提供するときは、ETSI TS 119 101の要件UI 1とUI 2が適用されるべきである(SHOULD)。 UI 1：ユーザーインターフェースは以下の通りであるべきである(SHOULD)： a) SCA/SVA/SAA の使用方法、および該当する場合、システムのインストールと設定に関する明確なユーザーガイダンスを提供すること； b) 各ダイアログステップがシステムからのフィードバックによって容易に理解できる程度に自己記述的であるか、またはユーザーの要求に応じて説明がなされること； c) 明らかな入力エラーがある場合でも、最小限の修正措置で意図した結果が得られる場合は、入力エラーに対して寛容であること； d) ユーザーの作業を先に進めるために、有益なエラー報告を行う； e) 利用者が行った操作が正しい(または正しくない)ことを確認するためのフィードバックを提供する； f) 色表示を使用する場合、エラーには赤色を、正常/成功には緑色を使用する； g) いつでも、現在の操作をキャンセルしてメインメニューに戻れるか、システ ムを完全に終了することができること；
	h) protect privacy for the individual, e.g. by making the information not accessible to others at the user interface; and i) ask for confirmation of the key decisions and choices of the user. UI 2: The SCA/SVA/SAA shall provide a detailed user's guide leading first time users through the process of generating, augmenting and validating a signature.		h) 例えば、ユーザーインターフェイスにおいて、情報を他人がアクセスできないようにするなど、個人のプライバシーを保護すること； そして i) ユーザの重要な決定や選択について確認を求める。 UI 2：SCA/SVA/SAAは、初めてのユーザーをガイドし、署名の生成、拡充、および検証のプロセスを詳細に説明するユーザーズガイドを提供するものとする(SHALL)。
ASI-8.1-08 [CONDITONAL]	When the SCASC presents the document to the signer, it shall have a workflow where it is clear to the signer that the signer consents to the signing of the document.	○	SCASCが文書を署名者に提示するときには、署名者が文書の署名に同意することが署名者に明白であるワークフローであるものとする(SHALL)。
ASI-8.1-09 [CONDITONAL]	When the SCASC presents the document to the signer, SCP 13 and SCP 47 of ETSI TS 119 101 [1] shall apply. SCP 13:When the SD presented to the signer, the SCA shall ensure that the SD presented to the signer is the same as the one that will be signed in the signature process. SCP 47:If the business process contains the presentation of the DTBS or the SD to the signer, the SCA shall compute the signature only after the DTBS or SD was presented to the signer. NOTE: In the case of bulk signer may not get all the signer.	○	SCASCが文書を署名者に提示するとき、ETSI TS 119 101のSCP 13とSCP 47が適用されるものとする(SHALL)。 SCP 13：SDが署名者に提示された場合、SCAは署名者に提示されたSDが署名プロセスで署名される SDと同一であることを保証するものとする(SHALL)。 SCP 47：ビジネスプロセスに署名者へのDTBS(署名対象データ)またはSDの提示が含まれる場合、SCAはDTBSまたはSDが署名者に提示された後にのみ署名を計算するものとする(SHALL)。 注：一括署名の場合、署名者に全てのSDやDTBSが提示されるとは限らない
ASI-8.1-10 [CONDITONAL]	When the SCASC presents the document to the signer, the SCASC should allow to download the document to be signed.	○	SCASCが文書を署名者に提示するとき、SCASCは署名される文書のダウンロードを許可すべきである(SHOULD)。
ASI-8.1-11 [CONDITONAL]	When the SCASC presents the document to the signer, the SCASC should log for how long the document was presented to the signer.	○	SCASCが文書を署名者に提示するとき、SCASCは文書が署名者に提示された期間を記録するものとする(SHALL)。
ASI-8.1-12 [CONDITONAL]	When the SCASC presents the document to the signer and the document was downloaded, the SCASC should log such an event.	○	SCASCが文書を署名者に提示し、文書がダウンロードされたとき、SCASCはそのようなイベントをログに記録するべきである(SHOULD)。
8.2 AdES digital signature creation			8.2 デジタル署名の生成

OVR-8.2-01	The SCASC shall guarantee the integrity and confidentiality of the received information.	○	SCASCは受け取った情報の完全性と機密性を保証するものとする(SHALL)。
OVR-8.2-02	The cryptographic algorithms used should be selected from algorithms recommended by ETSI TS 119 312 [i.5]. NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.5] can be superseded by national recommendations.	○	使用される暗号アルゴリズムは、Cryptrecの「電子政府推奨暗号リスト」によって推奨されているアルゴリズムから選択されるべきである(SHOULD)。
OVR-8.2-03	The cryptographic algorithms applied shall be as defined in signature creation policy.	○	適用される暗号アルゴリズムは、運用規程や利用規約などで定義されているとおりであるものとする(SHALL)。
OVR-8.2-04	SCP 14, SCP 31, SCP 37 and SCP 61 of ETSI TS 119 101 [1] shall apply. SCP 14: The DA shall ensure that the SD selected by the signer for signing is the same as the one provided to the SCA for the signature. SCP 31: When more than one signing certificate is available to be used by the signer, the DA shall allow the signer to select the certificate to be used for creating the signature. The DA may provide a default selection for the user. If there is only a single choice possible, this step may be omitted. SCP 37: The SCA shall protect the reference to or copy of the signing certificate within the signature from undetected replacement after the signature has been created. NOTE 3: This typically is realized by signing this data along with the document and by putting it in e.g. the authenticated attributes section of the signature format. SCP 61: When the signer's authentication data transits through the SCA, the SCA shall maintain the confidentiality and integrity of the authentication data and shall securely erase it as soon as it is no longer needed (e.g. they are substituted or the signer's enrolment is removed).	○	ETSI TS 119 101のSCP 14、SCP 31、SCP 37およびSCP 61が適用されるものとする(SHALL)。 SCP 14：DA(駆動アプリケーション)は、署名のために署名者が選択したSDが、署名のためにSCAに提供されたSDと同一であることを保証するものとする(SHALL)。 SCP 31：署名者が複数の署名証明書を使用できる場合、DAは署名者が署名を生成するために使用する証明書を選択できるものとする(SHALL)。DAは、ユーザにデフォルトの選択を提供することができる。選択可能なものが 1 つしかない場合、このステップを省略してもよい(MAY)。 SCP 37：SCAは、署名が生成された後、署名内の署名証明書への参照または署名証明書のコピーが検知されずに置き換えられないように保護するものとする(SHALL)。 注3：これは通常、このデータを文書とともに署名し、署名フォーマットの認証済み属性セクションなどに格納することで実現される。 SCP 61：署名者の認証データがSCAを通過する際、SCAは認証データの機密性と完全性を維持し、不要になり次第(例えば、署名者の代替や署名者の登録が削除された場合)、安全に消去するものとする(SHALL)。
OVR-8.2-05	The SCASC shall inform the signer of the commitment type. NOTE 2: This information can be given within the signature policy.	○	SCASCは、署名者にコミットメントタイプ(署名の意図や目的等)を知らせるものとする(SHALL)。 注2：この情報は署名ポリシー、運用規程、利用規約の中で与えることができる。
OVR-8.2-06	The SCASC should include the signing certificate chain into the signature.	○	SCASCは、署名証明書チェーンを署名に含めるべきである(SHOULD)。
OVR-8.2-07	The signer shall be able to know which signature creation policy will be applied.	○	署名者は、どの署名生成ポリシーが適用されるのかを知ることができるものとする(SHALL)。
OVR-8.2-08	The signer shall be able to know which signature creation policy was applied when creating a specific the signature. EXAMPLE 1: The information on which signature creation policy will or was applied for a specific signature can be known from the user account of the signer. EXAMPLE 2: The signature creation policy can be added as a signed attribute to the signature. EXAMPLE 3: The SCASP has only one signature creation policy in force at each time, and from the time of signature it is clear which version applies.	○	署名者は、特定の署名を生成するときにどの署名生成ポリシーが適用されたかを知ることができるものとする(SHALL)。 例1：どの署名生成ポリシーが特定の署名に適用されるか、または適用されたかに関する情報は、署名者のユーザーアカウントから知ることができる。 例2：署名生成ポリシーを署名済み属性として署名に追加できる。 例3：SCASPは各時点で有効な署名生成ポリシーを1つだけ持ち、署名の時点からどのバージョンが適用されるのかが明確になる。 例4：運用規程や利用規約などによって署名生成ポリシーを示すことができる。
OVR-8.2-08A	The SCASC should provide the signature to the signer.	○	SCASCは署名者に署名を提供するべきである(SHOULD)。
OVR-8.2-09 [CONDITIONAL]	If the SCASC has access to the signed data, it should provide the signed data together with the signature to the signer. NOTE 3: In case the signature is enveloped in or enveloping the signed data, OVR-8.2-09 follows directly from OVR-8.2-08.	○	SCASCが被署名データにアクセスできる場合、被署名データと署名を署名者に提供すべきである(SHOULD)。 注3：署名が被署名データ内に収められているEnveloped署名、または被署名データを収めているEnveloping署名の場合、OVR-8.2-09はOVR-8.2-08Aをそのまま踏襲するものである。
9 Framework for definition of signature creation application service component policy built on the present document			9 本書を基に構築された署名生成アプリケーションサービスコンポーネントポリシーの定義のためのフレームワーク
OVR-9-01A [CONDITIONAL]	When building a SCASC policy on a trust service policy defined in the present document, the SCASC policy shall identify which of the trust service policies defined in the present document it adopts as the basis.	○	本書で定義されたトラストサービスポリシーの上にSCASCポリシーを構築する場合、SCASCポリシーは、本書で定義されたトラストサービスポリシーのどの項目を採用したかを示すものとする(SHALL)。
OVR-9-02 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; the policy shall identify any variances it chooses to apply.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーは、適用することを選択したあらゆるバリエーションを明らかにするものとする(SHALL)。

OVR-9-03 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document.	○	本書で定義された要件に基づきSCASCポリシーを構築する場合、契約者は、利用規約の実施の一部として、特定のポリシーが本書で定義されたポリシーの要件をどのように追加または制約するかについて通知されるされるものとする(SHALL)。
OVR-9-04 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy.	○	本書で定義された要件に基づきSCASCポリシーを構築する場合、ポリシーの規定と承認について最終的な権限と責任を持つ機関(例えばポリシー管理権限者)が存在するものとする(SHALL)。
OVR-9-05 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ビジネス要件を評価し、対象と適合範囲を示すポリシーに含むべきセキュリティ要件を決定するために、リスクアセスメントを実施すべきである(SHOULD)。
OVR-9-06 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; the policy shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーを維持するための責任を含め、定義されたレビュープロセスに従ってポリシーの承認と修正を行うものとする(SHALL)。
OVR-9-07 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; a defined review process shall exist to ensure that the policy is supported by the practices statements.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、ポリシーが運用規程に裏付けられていることを確実にするために、定義されたレビュープロセスが存在するものとする(SHALL)。
OVR-9-08 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; the TSP should make available the policies supported by the TSP to its user community.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、TSPは、TSPがサポートするポリシーをそのユーザーコミュニティに公開すべきである(SHOULD)。
OVR-9-09 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; revisions to policies supported by the TSP should be made available to subscribers.	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、TSPがサポートするポリシーの改訂は加入者が利用できるようにすべきである(SHOULD)。
OVR-9-10 [CONDITIONAL]	When building a SCASC policy built on requirements defined in the present document; a unique object identifier shall be obtained for the policy (e.g. OID or URI).	○	本書で定義された要件に基づいてSCASCポリシーを構築する場合、そのポリシーに対して一意なオブジェクト識別子(OIDやURIなど)を取得するものとする(SHALL)。

リモート署名サービスの評価基準

― 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 を参考に作成）

目次

1. スコープ

この文書は、トラストサービスプロバイダー(TSP)の種類を問わず、TSP の運用とマネジメントの実践に関する一般的なポリシー要件を定義する。

トラストサービスには、電子証明書の発行、登録サービス、タイムスタンプサービス、長期保存サービス、電子配信サービス、署名検証サービス及びリモート署名サービス等が含まれる。

この文書のポリシー要件は、TSP のサービスの課金に対する制限を意味するものではない。
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場合がある。この文書では、評価者に対する要件、評価者が利用できる情報の要件、評価の方法等については規定しない。

2. 概要

要件は、セキュリティ目標の観点から示される。続いて、それらの目標の達成に必要な管理に関する、より具体的な要件が示される。
なお、「TSP のマネジメントと運用」の管理を実施する場合、ISO/IEC 27002:2013、あるいは ISO/IEC27002:2022 を適用する必要がある。

3. 参照規格

参照規格は、リモート署名サービスの評価基準概説を参照のこと。

4. 用語と定義、記号・略称及び評価基準での表記

4.1 用語と定義、記号・略称

用語と定義及び記号・略称は、リモート署名サービスの評価基準概説を参照のこと。

4.2 評価基準での表記

本書における要求事項は、「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」にて以下のように要件識別子によって特定されている。
<3 文字の REQ> - <章節番号> - <2 桁の連番の番号>

要求事項の記述において要件識別子と要求事項が「・」(黒丸点)の箇条書きで示されているものは、その前の黒丸点のない要求事項に関連して特に要求する詳細な要求事項である。

このドキュメントの以降の版全体にわたる要件識別子の管理は次のとおりである。

- 要件が句の最後に挿入されると、上記の 2 桁の数字の次に使用可能な値にされる。
- 要件が 2 つの既存の要件の間に挿入される場合、前の要件識別子に大文字を追加したものを新しい要件の要件識別子とする。
- 削除された要件の要件識別子は残され、「廃止」と示される。
- 変更された要件の要件識別子は「廃止」とされ、変更された要件は最初の要件番号に大文字を追加して変更後の要求識別しとされる。

5. リスク評価

「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」を参照のこと。

6. 方針と実践

6.1 トラストサービス業務規程

「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」を参照のこと。

6.2 利用規約

「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」を参照のこと。

6.3 情報セキュリティポリシー

「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」を参照のこと。

7. TSP の管理と運用

7.1 内部組織

7.1.1 組織の信頼性

「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」を参照のこと。

7.1.2 職務の分離

「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」を参照のこと。

7.2 人材

「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」を参照のこと。

7.3 資産管理

7.3.1 一般要件

「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」を参照のこと。

7.3.2 メディアの取り扱い

「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」を参照のこと。

7.4 アクセス制御

「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」を参照のこと。

7.5 暗号コントロール

「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」を参照のこと。

7.6 物理的および環境的セキュリティ

「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」を参照のこと。

7.7 運用上のセキュリティ

「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」を参照のこと。

7.8 ネットワークセキュリティ

「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」を参照のこと。

7.9 インシデント管理

「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」を参照のこと。

7.10 証拠の収集

「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」を参照のこと。

7.11 事業継続管理

「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」を参照のこと。

7.12 TSP の終了と終了計画

「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」を参照のこと。

7.13 コンプライアンス

「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」を参照のこと。

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

General Policy Requirements for Trust Service Providers (ETSI EN 319 401 V2.3.1 (2021-05)) を参考に作成

要件識別子	原文	監査対象	要求事項
5 Risk Assessment			5 リスク評価
REQ-5-01	The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.	○	TSPは、ビジネスおよび技術的な問題を考慮して、トラストサービスのリスクを特定、分析、評価するためのリスクアセスメントを実施するものとする。[SHALL]
REQ-5-02	The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk. NOTE: See ISO/IEC 27005:2011 [i.5] for guidance on information security risk management as part of an information security management system.	○	TSPは、当該リスクアセスメント結果を考慮して、適切なリスク対応策を選択するものとする。リスク対応策は、セキュリティのレベルがリスクの程度に見合ったものであることを保証するものとする。[SHALL] 注:情報セキュリティマネジメントシステムの一部としての情報セキュリティリスクマネジメントに関するガイダンスについては、ISO/IEC 27005:2018 [i.5]を参照のこと。
REQ-5-03	The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).	○	TSPは、情報セキュリティポリシーおよびトラストサービス運用規程(第6章を参照)に文書化されているように、選択したリスク対応策を実装するために必要なすべてのセキュリティ要件と運用手順を決定するものとする。[SHALL]
REQ-5-04	The risk assessment shall be regularly reviewed and revised.	○	当該リスクアセスメントは定期的に見直され、改訂されるものとする。[SHALL]
REQ-5-05	The TSP's management shall approve the risk assessment and accept the residual risk identified.	○	TSPの経営陣は当該リスクアセスメントを承認し、特定された残留リスクを受け入れるものとする。[SHALL]
6 Policies and practices			6 方針と実践
6.1 Trust Service Practice statement			6.1 トラストサービス業務規程
REQ-6.1-01	The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.	○	TSPは、提供するトラストサービスに適した一連のポリシーと業務を指定するものとする。[SHALL]
REQ-6.1-02	The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.	○	一連のポリシーと業務は、経営陣によって承認され、公開され、関連する従業員や外部関係者に伝達されるものとする。[SHALL]
• REQ-6.1-03	Void.		廃止
• REQ-6.1-03A	The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP. NOTE 1: The present document makes no requirement as to the structure of the trust service practice statement.	○	TSPは、TSPが特定した適用可能なトラストサービスポリシーのすべての要件に対処するために使用される業務と手順の記述を持つものとする。 [SHALL] 注1:この文書は、トラストサービス運用規程の構造に関していかなる要件も設けていない。
• REQ-6.1-04	The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.	○	TSPのトラストサービス運用規程は、適用されるポリシーと業務を含む、TSPのサービスをサポートするすべての外部組織の義務を特定するものとする。[SHALL]
• REQ-6.1-05	Void.		廃止
• REQ-6.1-05A	The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy. NOTE 2: The TSP need not disclose any aspects containing sensitive information in the documentation that is made available to subscribers and relying parties.	○	TSPは、トラストサービスポリシーへの準拠を証明するために必要に応じて、その運用規程およびその他の関連文書を利用者および依拠当事者が利用できるようにするものとする。[SHALL] 利用者に対し、書類の交付その他の適切な方法により、トラストサービスの利用に関する重要な事項について説明を行うこと又は運用規程の記載事項以外の注意事項があれば別途明示するものとする。[SHALL] 注2:TSPは、利用者および依拠当事者に提供されるドキュメント内の機密情報を含む側面を全て開示する必要はない。

要件識別子	原文	監査対象	要求事項
• REQ-6.1-06	The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.	○	TSPは、TSPの運用規程を承認する最終権限を持つ、TSPに対する全体的な責任を負う管理機関を持つものとする。[SHALL]
• REQ-6.1-07	The TSP's management shall implement the practices.	○	TSPの管理者は規程を実装するものとする。[SHALL]
• REQ-6.1-08	The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement. NOTE 3: The due notice does not need to provide the details of the changes. The due notice can be published on the TSP's repository.	○	TSPは、TSPの運用規程を維持する責任を含む業務のレビュープロセスを定義するものとする。[SHALL] 注3:運用規程の変更の予告には変更の詳細を記載する必要はない。予告はTSPのリポジトリで公開できる。
• REQ-6.1-09	Void.		廃止
• REQ-6.1-09A [CONDITIONAL]	When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties. NOTE 3: The due notice does not need to provide the details of the changes. The due notice can be published on the TSP's repository.	○	TSPが、対象者、利用者、または依拠当事者によるサービスの受け入れに影響を与える可能性のあるトラストサービス運用規程の変更を行う場合、利用者および依拠当事者に変更について適切に通知するものとする。 注3:変更予告通知には変更の詳細を記載する必要はない。通知はTSPのリポジトリで公開できる。[SHALL]
• REQ-6.1-10	The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above.	○	TSPは、上記REQ-6.1-06の承認後、上記REQ-6.1-05の要求に応じて、修正されたトラストサービス運用規程を直ちに利用できるようにするものとする。[SHALL]
• REQ-6.1-11	The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).	○	TSPは、サービスの終了に関する規定をその運用規程の中で明記するものとする(第7章第12項を参照)。[SHALL]
6.2 Terms and Conditions			6.2 利用規約
REQ-6.2-01	TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.	○	TSPは、サービスに関する契約条件をすべての利用者および依拠当事者が利用できるようにするものとする。[SHALL]
REQ-6.2-02	The terms and conditions shall at least specify for each trust service policy supported by the TSP the following: a) the trust service policy being applied; b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations; EXAMPLE 1: The expected life-time of public key certificates. c) the subscriber's obligations, if any; d) information for parties relying on the trust service; EXAMPLE 2: How to verify the trust service token, any possible limitations on the validity period associated with the trust service token. e) the period of time during which TSP's event logs are retained; f) limitations of liability; g) the applicable legal system; h) procedures for complaints and dispute settlement; i) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme; j) the TSP's contact information; and k) any undertaking regarding availability.	○	利用規約では、TSPによってサポートされる各トラストサービスポリシーについて少なくとも次の内容を指定するものとする。 [SHALL] a)適用されているトラストサービスポリシー。 b)サービスの制限を超えたサービスの使用から生じる損害（賠償）の制限を含む、提供されるサービスの使用に関する制限。 例1:公開鍵証明書の有効期間。 c)利用者の義務（ある場合）。 d)トラストサービスに依存する依拠当事者向けの情報。 例2:トラストサービストークンを検証する方法、トラストサービストークンに関連付けられた有効期間に関する制限の可能性。 e)TSPのイベントログが保持される期間。 f)責任の制限。 g)適用される法制度。 h)苦情および紛争解決の手順。 i)TSPのトラストサービスに関する当該ポリシーの準拠性評価の有無と、(該当する場合)当該準拠性評価スキーム。 j)TSPの連絡先情報。 k)可用性に関するあらゆる保証。
REQ-6.2-03	Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.	○	利用者およびトラストサービスに依存する依拠当事者は、契約を締結する前に、上記の項目を含む正確な契約条件を知らされるものとする。[SHALL]

要件識別子	原文	監査対象	要求事項
REQ-6.2-04	Terms and conditions shall be made available through a durable means of communication.	○	利用規約は、耐久性のある通信手段を通じて入手できるものとする。[SHALL]
REQ-6.2-05	Terms and conditions shall be available in a readily understandable language.	○	利用規約は、容易に理解できる言語で提供されるものとする。[SHALL]
REQ-6.2-06	Terms and conditions may be transmitted electronically.	○	利用規約は電子的に送信される場合があってもよい。[MAY]
6.3 Information security policy			6.3 情報セキュリティポリシー
REQ-6.3-01	The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.	○	TSPは、情報セキュリティを管理する組織のアプローチを規定する経営陣によって承認された情報セキュリティポリシーを定義するものとする。[SHALL]
REQ-6.3-02	Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.	○	情報セキュリティポリシーの変更は、該当する場合、第三者に通知されるものとする。これには、利用者、依拠当事者、評価機関、監督機関、またはその他の規制機関が含まれるものとする。[SHALL]
	In particular:		特に:
• REQ-6.3-03	A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.	○	TSPの情報セキュリティポリシーは、サービスを提供するTSPの施設、システム、情報資産のセキュリティ管理と運用手順を含め、文書化、実装、維持されるものとする。[SHALL]
• REQ-6.3-04	The TSP shall publish and communicate the information security policy to all employees who are impacted by it. NOTE 1: See clause 5.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPは、情報セキュリティポリシーを公開し、当該ポリシーの影響を受けるすべての従業員に伝達するものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2013の5.1.1、あるいは、ISO/IEC 27002:2022の5.1を参照のこと。
• REQ-6.3-05	The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers.	○	TSPは、TSPの機能が委託先によって引き受けられる場合でも、情報セキュリティポリシーに規定された手順への準拠について全体的な責任を負うものとする。[SHALL]
• REQ-6.3-06	TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP.	○	TSPは委託先の責任を定義し、委託先がTSPから要求されるあらゆる管理を実施する義務を負うことを保証するものとする。[SHALL]
• REQ-6.3-07	The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	○	TSPの情報セキュリティポリシーおよび情報セキュリティ資産の目録(第7.3項を参照)は、計画された間隔で、または重大な変更が発生した場合に、継続的な適合性、適切性、および有効性を確保するために見直されるものとする。[SHALL]
• REQ-6.3-08	Any changes that will impact on the level of security provided shall be approved by the management body referred to in REQ-6.1-07.	○	提供されるセキュリティのレベルに影響を与える変更は、REQ-6.1-07で参照される管理機関によって承認されるものとする。[SHALL]
• REQ-6.3-09	The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.	○	TSPシステムの構成は、TSPのセキュリティポリシーに違反する変更がないか定期的にチェックされるものとする。[SHALL]
• REQ-6.3-10	The maximum interval between two checks shall be documented in the trust service practice statement. NOTE 2: Further specific recommendations are given in the CA/Browser Forum network security guide [i.7], item 1.	○	2つの定期的チェック間の最大間隔は、トラストサービス業務規程に文書化されるものとする。[SHALL] 注2:さらに具体的な推奨事項は、CA/Browser Forumのネットワークセキュリティガイドの項目1に記載されている。
7 TSP management and operation			7 TSPの管理と運用
7.1 Internal organization			7.1 内部組織
7.1.1 Organization reliability			7.1.1 組織の信頼性

要件識別子	原文	監査対象	要求事項
REQ-7.1.1-01	The TSP organization shall be reliable.	○	TSP組織は信頼できるものでなければならないものとする。[SHALL]
	In particular:		特に
• REQ-7.1.1-02	Trust service practices under which the TSP operates shall be non-discriminatory.	○	TSPが運営するトラストサービスの業務は、差別的であってはならないものとする。[SHALL]
• REQ-7.1.1-03	The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.	○	TSPは、TSPが宣言した事業分野に該当し、TSPの利用規約に指定された義務を遵守することに同意するすべての申請者が当該サービスにアクセスできるようにするべきである。[SHOULD]
• REQ-7.1.1-04	The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities. NOTE: For liability of TSPs operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.2].	○	TSPは、運用および/または活動から生じる責任をカバーするために、適用法に従って、十分な財源を維持し、および/または適切な賠償責任保険を利用するものとする。[SHALL] 注：EU域内で活動するTSPの責任については、EU規則No 910/2014の第13条を参照のこと。
• REQ-7.1.1-05	The TSP shall have the financial stability and resources required to operate in conformity with this policy.	○	TSPは、当該ポリシーに従って運営するために必要な財務的安定性とリソースを備えているものとする。[SHALL]
• REQ-7.1.1-06	The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.	○	TSPは、サービスの提供またはその他の関連事項に関して顧客または他の依拠当事者から受け取った苦情および紛争を解決するためのポリシーと手順を持つものとする。[SHALL]
• REQ-7.1.1-07	The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.	○	TSPは、サービスの提供に下請け、外部委託、またはその他の第三者の取り決めが含まれる場合、文書化された合意および契約関係を整備するものとする。[SHALL]
• REQ-7.1.1-08 [CONDITIONAL]	When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for meeting the requirements defined in the trust service policy.	○	TSPが、下請け、外部委託、またはその他の第三者の取り決めを通じてサービスの一部を提供するために、トラストサービスコンポーネントプロバイダーを含む他の第三者を利用する場合、TSPは、トラストサービスポリシーにおいて規定された要件に適合するための全体的な責任を維持するものとする。[SHALL]
• REQ-7.1.1-09 [CONDITIONAL]	When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.	○	TSPが別の当事者によって提供されたトラストサービスコンポーネントを利用する場合、当該コンポーネントインターフェイスの使用が当該コンポーネントプロバイダーによって指定された要件を満たすことを保証するものとする。[SHALL]
• REQ-7.1.1-10 [CONDITIONAL]	When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component are meeting the appropriate requirements of the applicable policy and practices.	○	TSPが別の当事者によって提供されたトラストサービスコンポーネントを利用する場合、当該コンポーネントによって要求されるセキュリティと機能が、該当するポリシーの適切な要件を満たしていることを保証するものとする。[SHALL]
7.1.2 Segregation of duties			7.1.2 職務の分離
REQ-7.1.2-01	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.	○	TSPの資産に対する不正または意図しない変更または悪用の機会を減らすために、職務および責任領域は適切に分離されるものとする。[SHALL]
7.2 Human resources			7.2 人材
REQ-7.2-01	The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations. NOTE 1: See clauses 6.1.1 and 7 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPは、従業員と請負業者がTSPの業務の信頼性をサポートすることを保証するものとする。[SHALL] 注1:ガイダンスとしてISO/IEC 27002: 2013の6.1.1および7、あるいは、ISO/IEC 27002: 2022の6.2および5.4、6.1～6.5を参照のこと。
	In particular:		

要件識別子	原文	監査対象	要求事項
• REQ-7.2-02	The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.	○	TSPは、必要な専門知識、信頼性、経験、資格を有し、提供されるサービスと職務に適切なセキュリティと個人データ保護規則に関するトレーニングを受けたスタッフを雇用し、場合によっては下請け業者を使用するものとする。[SHALL]
• REQ-7.2-03	TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.	○	TSPの担当者は、正式なトレーニングと資格、実務経験、またはその2つの組み合わせを通じて、「専門の知識、経験、資格」要件を満たすべきである。[SHOULD]
• REQ-7.2-04	This should include regular (at least every 12 months) updates on new threats and current security practices. NOTE 2: Personnel employed by a TSP include individual personnel contractually engaged in performing functions in support of the TSP's services. Personnel who can be involved in monitoring the TSP's services need not be TSP's personnel.	○	これには、新しい脅威と現在のセキュリティ慣行に関する定期的(少なくとも12か月ごと)の更新が含まれるべきである。[SHOULD] 注2:TSP雇用要員には、TSPサービスをサポートする機能の履行に契約上従事する要員が含まれる。TSPサービスの監視に関与できる要員は、TSPの要員である必要はない。
• REQ-7.2-05	Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures. NOTE 3: See clause 7.2.3 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPのポリシーまたは手順に違反した要員には、適切な懲戒処分が適用されるものとする。[SHALL] 注3:ガイダンスについては、ISO/IEC 27002:2013の7.2.3、あるいは、ISO/IEC 27002:2022の6.4を参照のこと。
• REQ-7.2-06	Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.	○	TSPの情報セキュリティポリシーで指定されているセキュリティの役割と責任は、職務記述書または関係者全員が利用できる文書に文書化されているものとする。[SHALL]
• REQ-7.2-07	Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.	○	TSPの運用に依拠するセキュリティに関する信頼された役割は、明確に特定されるものとする。[SHALL]
• REQ-7.2-08	Void.		廃止
• REQ-7.2-09	Void.		廃止
	NOTE 4: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in establishing roles and responsibilities.	○	注4:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2013の7.2.1を参照のこと。あるいは、ISO/IEC 27002:2022の5.4を参照のこと。
• REQ-7.2-10	TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.	○	TSPの要員(臨時職員と正社員の両方)は、職務の分離と最小限の権限(7.1.2を参照)、職務とアクセスレベルに基づくポジションの機密性の決定、身元調査、従業員の研修と意識向上の観点から定義された職務記述書を持つものとする。[SHALL]
• REQ-7.2-11	Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements. NOTE 5: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in establishing roles and responsibilities.	○	必要に応じて、職務記述書は一般的な職務とTSPの特定の特有職務を区別するものとする。[SHALL] 特有職務これらには、スキルと経験の要件を含めるべきである必要がある。[SHOULD] 注5:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2013の7.2.1、あるいは、ISO/IEC 27002:2022の5.4を参照のこと。[SHALL]
• REQ-7.2-12	Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures. NOTE 6: See clause 7.2.1 of ISO/IEC 27002:2013 [i.3] for further guidance on management responsibilities in establishing roles and responsibilities.	○	要員担当者は、TSPの情報セキュリティ管理手順に沿った管理、および管理手順およびプロセスを実行するものとする。[SHALL] 注6:役割と責任を確立する際の管理責任に関する詳細なガイダンスについては、ISO/IEC 27002:2013の7.2.1、あるいは、ISO/IEC 27002:2022の5.4を参照のこと。

要件識別子	原文	監査対象	要求事項
• REQ-7.2-13	Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.	○	管理者は、提供されるトラストサービスに関する経験または研修、セキュリティ責任を負う担当者のセキュリティ手順に精通し、管理機能を実行するのに十分な情報セキュリティとリスクアセスメントの経験を有しているものとする。[SHALL]
• REQ-7.2-14	All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations. NOTE 7: See clause 6.1.2 of ISO/IEC 27002:2013 [i.3] for guidance.	○	信頼される役割にあるすべてのTSP要員職員は、TSPの運営の公平性を損なう可能性のある利益相反を起こさないものとする。[SHALL] 注7:ガイダンスについては、ISO/IEC 27002:2013の6.1.2、あるいは、ISO/IEC 27002:2022の5.3を参照のこと。
• REQ-7.2-15	Trusted roles shall include roles that involve the following responsibilities: a) Security Officers: Overall responsibility for administering the implementation of the security practices. b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management. NOTE 8: This includes recovery of the system. c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup. d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems. NOTE 9: Additional application specific roles can be required for particular trust services.	○	信頼された役割には、次の責任を伴う役割が含まれるものとする。 [SHALL] a)セキュリティ責任者:セキュリティ業務の実施を管理する全体的な責任。 b)システム管理者:サービス管理のためにTSPの信頼できるシステムをインストール、構成、保守する権限を与えられる。 注8:これにはシステムのリカバリが含まれる。 c)システムオペレータ:TSPの信頼できるシステムを日常的に運用する責任を負う。システムバックアップを実行する権限を与えられる。 d)システム監査人:TSPの信頼できるシステムのアーカイブと監査ログを表示する権限を与えられる。 注9:特定のトラストサービスには、追加のアプリケーション固有の役割が必要になる場合がある。
• REQ-7.2-16	Void.		廃止
• REQ-7.2-16A	TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.	○	TSPの要員は、セキュリティを担当する上級管理者によって信頼される役割に正式に任命されるものとする。[SHALL]
• REQ-7.2-16B	Trusted roles shall be accepted by the appointed person to fulfil the role.	○	信頼された役割は、その役割を果たすために任命された要員大によって受け入れられるものとする。[SHALL]
• REQ-7.2-17	Personnel shall not have access to the trusted functions until the necessary checks are completed. NOTE 10:In some countries it is not possible for TSP to obtain information on past convictions without the collaboration of the candidate employee.	○	要員は、必要なチェックが完了するまで、信頼された機能にアクセスしないものとする。[SHALL] 注10:一部の国では、TSPが従業員候補者の同意なしに過去の有罪判決に関する情報の入手ができないことに留意すること。
7.3 Asset management			7.3 資産管理
7.3.1 General requirements			7.3.1 一般要件
REQ-7.3.1-01	The TSP shall ensure an appropriate level of protection of its assets including information assets. NOTE 1: See clause 8 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPは、情報資産を含む資産の適切なレベルの保護を確保するものとする。 注1:ガイダンスについては、ISO/IEC 27002:2013の8、あるいは、ISO/IEC 27002:2022の5.9~5.13、7.10を参照のこと。 [SHALL]
	In particular:		特に：
• REQ-7.3.1-02	The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment. NOTE 2: See clause 8.1.1 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPは、すべての情報資産の目録を維持し、リスクアセスメントと一致する分類を割り当てるものとする。 [SHALL] 注2:ガイダンスについては、ISO/IEC 27002:2013の8.1.1、あるいは、ISO/IEC 27002:2022の5.9を参照のこと。
7.3.2 Media handling			7.3.2 メディアの取り扱い
REQ-7.3.2-01	All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.	○	すべてのメディアは、情報分類スキームの要件に従って安全に取り扱われなければならない。機密データを含むメディアは、不要になった場合は安全に廃棄するものとする。 [SHALL]

要件識別子	原文	監査対象	要求事項
REQ-7.3.2-02	Media used within the TSP's systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.	○	TSPのシステム内で使用されるメディアは、メディアを損傷、盗難、不正アクセス、陳腐化から保護するために安全に取り扱うものとする。[SHALL]
REQ-7.3.2-03	Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained. NOTE:See clause 8.3 of ISO/IEC 27002:2013 [i.3] for guidance.	○	メディア管理手順は、記録を保持する必要がある期間内のメディアの陳腐化および劣化を防止するものとする。 [SHALL] 注:ガイダンスについては、ISO/IEC 27002:2013の8.3、あるいは、ISO/IEC 27002:2022の7.10を参照のこと。
7.4 Access control			7.4 アクセス制御
REQ-7.4-01	The TSP's system access shall be limited to authorized individuals.	○	TSPのシステムへのアクセスは、許可された個人に限定するものとする。[SHALL]
	In particular:		特に：
• REQ-7.4-02	Void.		廃止
• REQ-7.4-03	Void.		廃止
• REQ-7.4-04	Void.		廃止
• REQ-7.4-04A	The TSP shall administer user access of operators, administrators and system auditors applying the principle of "least privileges" when configuring access privileges. NOTE 1: This generally applies to personnel appointed to trusted roles as per REQ-7.2-16.	○	TSPは、アクセス権限を設定する際に「最小限の権限」の原則を適用して、オペレータ、管理者、およびシステム監査人のユーザーアクセスを管理するものとする。[SHALL] 注1:これは通常、REQ-7.2-16に従って信頼された役割に任命された担当者に適用される。
• REQ-7.4-05	The administration shall include user account management and timely modification or removal of access.	○	管理には、ユーザーアカウントの管理と、アクセスへの適時変更または削除が含まれるものとする。[SHALL]
• REQ-7.4-06	Access to information and application system functions shall be restricted in accordance with the access control policy.	○	情報およびアプリケーションシステム機能へのアクセスは、アクセス制御ポリシーに従って制限されるものとする。 [SHALL]
• REQ-7.4-07	The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.	○	TSPのシステムは、セキュリティ管理機能と運用機能の分離を含め、TSPの業務で特定された信頼された役割を分離するための十分なコンピュータセキュリティ制御を提供するものとする。 特に、システムユーティリティプログラムの使用を制限、管理するものとする。[SHALL]
• REQ-7.4-08	TSP's personnel shall be identified and authenticated before using critical applications related to the service.	○	TSPの要員は、サービスに関連する重要なアプリケーションを使用する前に識別および認証されるものとする。[SHALL]
• REQ-7.4-09	TSP's personnel shall be accountable for their activities. • EXAMPLE:By retaining event logs.	○	TSPの要員は、自らの活動に対して責任を負うものとする。 [SHALL] ・例:イベントログを保持する。
• REQ-7.4-10	Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or media (see clause 7.3.2) being accessible to unauthorized users. NOTE 2: See clause 9 of ISO/IEC 27002:2013 [i.3] for guidance. NOTE 3: Further recommendations regarding authentication are given in the CA/Browser Forum network security guide [i.7], clause 2.	○	機密データは、権限のないユーザーがアクセスできる再利用されたストレージオブジェクト(削除されたファイルなど)またはメディア(7.3.2を参照)を通じて漏洩しないように保護されるものとする。 [SHALL] 注2:ガイダンスについては、ISO/IEC 27002:2013の9、あるいは、ISO/IEC 27002:2022の5.15～5.18、8.2～8.5を参照のこと。 注3:認証に関するさらなる推奨事項は、CA/Browser Forumのネットワークセキュリティガイドの2に記載されている。
7.5 Cryptographic controls			7.5 暗号コントロール
REQ-7.5-01	Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle. NOTE:See clause 10 of ISO/IEC 27002:2013 [i.3] for guidance.	○	ライフサイクル全体を通じて、あらゆる暗号鍵キーおよびあらゆる暗号デバイスを管理するために、適切なセキュリティ管理を実施するものとする。[SHALL] 注:ガイダンスについては、ISO/IEC 27002:2013の10、あるいは、ISO/IEC 27002:2022の8.24を参照のこと。

要件識別子	原文	監査対象	要求事項
7.6 Physical and environmental security			7.6 物理的および環境的セキュリティ
REQ-7.6-01	The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security. NOTE 1: See clause 11 of ISO/IEC 27002:2013 [i.3] for guidance.	○	TSPは、セキュリティが信頼トラストサービスの提供にとって重要であるTSPシステムのコンポーネントへの物理的アクセスを制御し、物理的セキュリティに関連するリスクを最小限に抑えるものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2013の11、あるいは、ISO/IEC 27002:2022の7、8.1を参照のこと。
	In particular:		特に：
• REQ-7.6-02	Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals. NOTE 2: Criticality is identified through risk assessment, or through application security requirements, as requiring a security protection.	○	セキュリティがトラストサービスの提供にとって重要であるTSPシステムのコンポーネントへの物理的アクセスは、許可された個人に限定されるものとする。[SHALL] 注2:重要度は、リスクアセスメントを通じて、またはアプリケーションのセキュリティ要件を通じて、セキュリティ保護を必要とするものとして特定される。
• REQ-7.6-03	Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.	○	資産の損失、損傷、侵害、および事業活動の中断を回避するために管理を実施するものとする。[SHALL]
• REQ-7.6-04	Controls shall be implemented to avoid compromise or theft of information and information processing facilities.	○	情報および情報処理施設の侵害または窃取を回避するための制御を実装するものとする。[SHALL]
• REQ-7.6-05	Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion. NOTE 3: See ISO/IEC 27002:2013 [i.3], clause 11.1 for guidance on secure areas.	○	トラストサービスの安全な運用に重要なコンポーネントは、侵入に対する物理的保護、セキュリティ境界を介したアクセスの制御、および侵入を検出するアラームを備えた保護されたセキュリティ境界に配置されるものとする。 [SHALL] 注3:安全な領域に関するガイダンスについては、ISO/IEC 27002:2013、11.1、あるいは、ISO/IEC 27002:2022、 7 、8.1を参照のこと。
7.7 Operation security			7.7 運用上のセキュリティ
REQ-7.7-01	The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. NOTE 1: See clause 12 of ISO/IEC 27002:2013 [i.3] for guidance. NOTE 2: See clause 14 of ISO/IEC 27002:2013 [i.3] for guidance on systems acquisition, development and maintenance. NOTE 3: See clause 15 of ISO/IEC 27002:2013 [i.3] for guidance on supplier relationship.	○	TSPは、改変から保護された信頼できるシステムと製品を使用し、それらによってサポートされるプロセスの技術的安全性と信頼性を確保するものとする。 [SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2013の12、あるいは、ISO/IEC 27002:2022の5.37、8.6～8.8、8.13、8.15、8.17、8.19、8.31、8.32、8.34を参照のこと。 注2:システムの取得、開発、および保守に関するガイダンスについては、ISO/IEC 27002:2013の14、あるいは、ISO/IEC 27002:2022の5.8、8.25～8.33を参照のこと。 注3:サプライヤーとの関係に関するガイダンスについては、ISO/IEC 27002:2013の15、あるいは、ISO/IEC 27002:2022の5.19～5.22を参照のこと。
• REQ-7.7-02	An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.	○	セキュリティ要件の分析は、ITシステムにセキュリティが組み込まれていることを確認するために、TSPまたはTSPの代理で実施されるシステム開発プロジェクトの設計および要件仕様の段階で実行されるものとする。[SHALL]
	In particular:		特に：

要件識別子	原文	監査対象	要求事項
• REQ-7.7-03	Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.	○	変更管理手順は、運用ソフトウェアのリリース、修正、緊急ソフトウェア修正、およびTSPのセキュリティポリシーを適用する構成の変更に適用されるものとする。[SHALL]
• REQ-7.7-04	The procedures shall include documentation of the changes. • NOTE 4: See clause 14 of ISO/IEC 27002:2013 [i.3] for guidance.	○	手順には変更の文書化が含まれるものとする。 [SHALL] 注4:ガイダンスについては、ISO/IEC 27002:2013の14、あるいは、ISO/IEC 27002:2022の5.8、8.25～8.33を参照のこと。
• REQ-7.7-05	The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.	○	TSPのシステムと情報の完全性は、ウイルス、悪意のあるソフトウェア、および無許可のソフトウェアから保護されるものとする。[SHALL]
• REQ-7.7-06	Void.		廃止
• REQ-7.7-07	Void.		廃止
• REQ-7.7-08	Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.	○	サービスの提供に影響を与えるすべての信頼され~~できる~~管理された役割に対して手順を確立し、実施するものとする。 [SHALL]
• REQ-7.7-09	The TSP shall specify and apply procedures for ensuring that: a) security patches are applied within a reasonable time after they come available; b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and c) the reasons for not applying any security patches are documented. NOTE 5: Further specific recommendations are given in the CA/Browser Forum network security guide [i.7], item 1 l.	○	TSPは、以下を確実にするための手順を指定し、適用するものとする。 [SHALL] a)セキュリティパッチは、入手可能になってから適切な期間内に適用される。 b)セキュリティパッチを適用するメリットを上回る追加の脆弱性または不安定性が導入される場合、セキュリティパッチは適用されない。 c)セキュリティパッチを適用しない理由が文書化されている。 注5:さらに具体的な推奨事項は、CA/Browser Forumのネットワークセキュリティガイド、"1l."に記載されている。
7.8 Network security			7.8 ネットワークセキュリティ
REQ-7.8-01	The TSP shall protect its network and systems from attack.	○	TSPは、そのネットワークとシステムを攻撃から保護するものとする。[SHALL]
	In particular:		特に：
• REQ-7.8-02	The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.	○	TSPは、信頼できるシステムとサービス間の機能的、論理的、物理的(場所を含む)関係を考慮したリスクアセスメントに基づいて、システムをネットワークまたはゾーンに分割するものとする。[SHALL]
• REQ-7.8-03	The TSP shall apply the same security controls to all systems co-located in the same zone.	○	TSPは、同じゾーン内に同じ場所にあるすべてのシステムに同じセキュリティ制御を適用するものとする。[SHALL]
• REQ-7.8-04	The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.	○	TSPは、ゾーン間のアクセスおよび通信を、TSPの運営に必要なものに制限するものとする。[SHALL]
• REQ-7.8-05	The TSP shall explicitly forbid or deactivate not needed connections and services.	○	TSPは、不要な接続およびサービスを明示的に禁止または非アクティブ化するものとする。[SHALL]
• REQ-7.8-06	The TSP shall review the established rule set on a regular basis.	○	TSPは、確立された規程類を定期的にレビューするものとする。[SHALL]
• REQ-7.8-07	The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.9]).	○	TSPは、TSPの運営にとって重要なすべてのシステムを1つ以上のセキュアゾーンに保持するものとする。[SHALL] （例 ルートCAシステム、ETSI EN 319 411-1参照））
• REQ-7.8-08	The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.	○	TSPは、ITシステム管理用の専用ネットワークとTSPの運用ネットワークを分離するものとする。[SHALL]

要件識別子	原文	監査対象	要求事項
• REQ-7.8-09	The TSP shall not use systems used for administration of the security policy implementation for other purposes.	○	TSPは、セキュリティポリシー実装の管理に使用されるシステムを他の目的で使用しないものとする。[SHALL]
• REQ-7.8-10	The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).	○	TSPは、TSPのサービスのための実稼働システムを、開発およびテストで使用されるシステム(例:開発、テスト、ステージングシステム)から分離するものとする。[SHALL]
• REQ-7.8-11	Void.		廃止
• REQ-7.8-11A	The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.	○	TSPは、他の通信チャネルから論理的、暗号的、または物理的に分離され、エンドポイントの確実な識別とチャネルデータの変更または開示からの保護を提供する信頼できるチャネルを通じてのみ、別個の信頼できるシステム間の通信を確立するものとする。[SHALL]
• REQ-7.8-12	If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.	○	トラストサービスへの外部アクセスの高レベルの可用性が必要な場合、単一障害の場合でもサービスの可用性を確保するために、外部ネットワーク接続を冗長化するものとする。[SHALL]
• REQ-7.8-13	The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.	○	TSPは、リスクアセスメントを実施したうえで必要に応じTSPによって特定されたパブリックおよびプライベートIPアドレスに対して定期的な脆弱性スキャンを受けるかまたは実行し、各脆弱性スキャンが信頼できる報告書を提供するために必要な、スキル、ツール、熟練度、倫理規範、 および独立性を有する個人または事業体によって実行された証拠を記録するものとする。[SHALL] 注:認証局においては、電子署名法に基づくGPKI接続する認定認証事業者の認証業務用設備は認証事業者が利用者秘密鍵を生成するセンター発行方式が中心で、発行CAがルートCAの構造を持ち、高セキュリティゾーンに配置され、外部ネットワークからエアギャップされている。海外CA/B Forumではルート CAとは異なるセキュアゾーンに発行システム等が維持される階層構造モデルが前提であり、リスクアセスメントの結果により、脆弱性スキャンの実施についての要件が異なるべきと考えられる。 一方、電子署名法では利用者鍵生成のモデルも存在し、発行CAがセキュアゾーンに配置される構造も考えられるため、これをTSPのリスクアセスメントの結果及びTSPが重要であると判断した範囲で脆弱性スキャンを実施するものとする。
• REQ-7.8-13A	The vulnerability scan requested by REQ-7.8-13 should be performed once per quarter.	○	REQ-7.8-13によって要求された脆弱性スキャンは四半期に1回実行されるべきである。[SHOULD]
• REQ-7.8-14	The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.	○	TSPは、セットアップ時、およびTSPが重要であると判断したインフラストラクチャまたはアプリケーションのアップグレードまたは変更後に、TSPのシステムに対して~~侵入~~ペネトレーションテストを受けるものとする。[SHALL]
• REQ-7.8-14A	The penetration test requested by REQ-7.8-14 should be performed at least once per year.	○	REQ-7.8-14で要求されるペネトレーションテストは、少なくとも年に1回実行するべきである。[SHOULD]
• REQ-7.8-15	The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.	○	TSPは、信頼できるレポートを提供するために必要なスキル、ツール、習熟度、倫理規範、および独立性を備えた個人または団体によって各ペネトレーションテストが実行された証拠を記録するものとする。[SHALL]
• REQ-7.8-16	Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.	○	制御(ファイアウォールなど)は、TSPの内部ネットワークドメインを利用者や第三者によるアクセスを含む不正アクセスから保護するものとする。[SHALL]

要件識別子	原文	監査対象	要求事項
• REQ-7.8-17	Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.	○	TSPの運営に必要のないすべてのプロトコルとアクセスを防止するようにファイアウォールを構成するべきである。[SHOULD]
7.9 Incident management			7.9 インシデント管理
REQ-7.9-01	System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored. NOTE 1: See clause 16 of ISO/IEC 27002:2013 [i.3] for guidance.	○	ITシステムへのアクセス、ITシステムの使用、およびサービス要求に関するシステム活動アクティビティは監視されるものとする。[SHALL] 注1:ガイダンスについては、ISO/IEC 27002:2013の16、あるいは、ISO/IEC 27002:2022の5.24～5.28、6.8を参照のこと。
In particular	In particular:		特に：
• REQ-7.9-02	Monitoring activities should take account of the sensitivity of any information collected or analysed.	○	モニタリング活動では、収集または分析される情報の機密性を考慮するべきである。[SHOULD]
• REQ-7.9-03	Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms. NOTE 2: Abnormal network system activities can comprise (external) network scans or packet drops.	○	TSPのネットワークへの侵入を含む、潜在的なセキュリティ違反を示す異常なシステム活動は、検出され、警告として報告されるものとする。[SHALL] 注2:異常なネットワークシステムアクティビティには、(外部)ネットワークスキャンやパケットドロップが含まれる場合がある。
• REQ-7.9-04	The TSP shall monitor the following events: a) start-up and shutdown of the logging functions; and b) availability and utilization of needed services with the TSP's network.	○	TSPは次のイベントを監視するものとする。[SHALL] a)ロギング機能の起動と停止。 b)TSPのネットワークに必要なサービスの稼働率と使用率。
• REQ-7.9-05	The TSP shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.	○	TSPは、インシデントに迅速に対応し、セキュリティ侵害の影響を制限するために、適時かつ協調的な方法で対応するものとする。[SHALL]
• REQ-7.9-06	The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.	○	TSPは、潜在的な重大セキュリティイベントの警告をフォローアップし、関連インシデントがTSPの手順に従って確実に報告されるように、信頼できる担当者を任命するものとする。[SHALL]
• REQ-7.9-07	The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified. NOTE 3: TSPs operating within the European Union can contact the appropriate supervisory body and/or other competent authorities for further guidance on implementing notification procedures as per article 19.2 of Regulation (EU) No 910/2014 [i.2].	○	TSPは、侵害が特定されてから24時間以内に提供されるトラストサービスおよび当該サービスで維持される個人データに重大な影響を与えるセキュリティ違反または完全性の喪失について、該当する規制法令に従って適切な関係者に通知する手順を確立するものとする。[SHALL] 注3：EU域内で活動するTSPは、規則（EU）No 910/2014の19.2に従った届出手続の実施に関するさらなるガイダンスについて、適切な監督機関および／または他の所轄当局に問い合わせることができる。
• REQ-7.9-08	Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.	○	セキュリティの侵害または完全性の喪失が、トラストサービスが提供されている自然人または法人に悪影響を与える可能性がある場合、TSPはまた、当該自然人または法人に過度な遅延なくセキュリティの侵害または完全性を失うことを通知するものとする。[SHALL]
• REQ-7.9-09	The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.	○	TSP のシステムは、悪意のある活動の証拠を特定するため、監査ログの監視または定期的な見直しを含めて監視され、監査ログを処理する自動メカニズムを導入して重要なセキュリティ・イベントの可能性を担当者に警告されるものとする。[SHALL]

要件識別子	原文	監査対象	要求事項
• REQ-7.9-10	The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.	○	TSPは、TSPが以前に対処していない重大な脆弱性を発見後遅滞なく対処するものとする。[SHALL] 注4: 重大な脆弱性を生む可能性のあるHSMの脆弱性対策はHSMベンダーからの対応となるが遅滞なく対処するものとする。
• REQ-7.9-11	For any vulnerability, given the potential impact, the TSP shall [CHOICE]: - create and implement a plan to mitigate the vulnerability; or - document the factual basis for the TSP's determination that the vulnerability does not require remediation. EXAMPLE: The TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation. NOTE 4: Further recommendations are given in the	○	あらゆる脆弱性について、潜在的な影響を考慮して、TSPは以下を少なくとも一つ選択するものとする。[SHALL] -脆弱性を軽減する計画を作成して実装する。 -脆弱性は修復する必要がないとTSPが判断した事実に基づく根拠を文書化する。 例:TSPは、潜在的な影響のコストが軽減のコストを正当化できない場合、脆弱性を修復する必要がないと判断できる。 注5:さらなる推奨事項は、CA/Browser Forumのネットワークセキュリティガイドの4 f)に記載されている。
• REQ-7.9-12	Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.	○	インシデントの報告と対応手順は、セキュリティインシデントや機能不全による損害が最小限に抑えられるような方法で が採用されるものとする。[SHALL]
7.10 Collection of evidence			7.10 証拠の収集
REQ-7.10-01	The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. NOTE: See requirement REQ-7.13-05.	○	TSP は、TSP の活動停止後を含む適切な期間、TSP が発行および受領したデータに関するすべての関連情報を、特に法的手続における証拠提供の目的およびサービスの継続性を確保する目的で、記録し、アクセス可能な状態に保つものとする。[SHALL] 注:要件REQ-7.13-05を参照のこと。
	In particular:		特に：
• REQ-7.10-02	The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.	○	サービスの運用に関する現在およびアーカイブされた記録の機密性と完全性は維持されるものとする。[SHALL]
• REQ-7.10-03	Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.	○	サービスの運用に関する記録は、開示された事業規程に従って完全かつ機密にアーカイブされるものとする。[SHALL]
• REQ-7.10-04	Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.	○	サービスの運用に関する記録は、法的手続きの目的でサービスの正しい運用の証拠を提供する目的で必要な場合に利用可能とされるものとする。[SHALL]
• REQ-7.10-05	The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.	○	重要なTSPの環境イベント、鍵管理イベント、およびクロック同期イベントの正確な時刻が記録されるものとする。[SHALL]
• REQ-7.10-06	The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.	○	監査ログに必要なイベントの記録に使用される時刻は、少なくとも1日に1回UTCと同期されるものとする。[SHALL]
• REQ-7.10-07	Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.3).	○	サービスに関する記録は、必要な法的証拠を提供するために適切な期間、TSPの利用規約で通知されているとおりに保持されるものとする(6.3を参照)。[SHALL]
• REQ-7.10-08	The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held. EXAMPLE: This can be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup or by parallel storage of the information at several (e.g. 2 or 3) independent sites.	○	イベントは、保持が必要な期間内に安易に削除または破棄できない方法で記録されるものとする(長期メディアに確実に転送される場合を除く)。[SHALL] 例:これは、たとえば、書き込み専用メディアの使用、使用された各リムーバブルメディアの記録、およびオフサイトバックアップの使用、または複数(たとえば2つまたは3つ)の独立した場所における情報のパラレルストレージなどの手段によって実現できる。
7.11 Business continuity management			7.11 事業継続管理

要件識別子	原文	監査対象	要求事項
REQ-7.11-01	The TSP shall define and maintain a continuity plan to enact in case of a disaster.	○	TSPは、災害時に実施する継続計画を定義および維持するものとする。[SHALL]
REQ-7.11-02	In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures. NOTE 1: See clause 17 of ISO/IEC 27002:2013 [i.3] for guidance in the event of a disaster. NOTE 2: Other disaster situations include failure of critical components of a TSP's trustworthy system, including hardware and software.	○	秘密鍵の漏洩やTSPのその他のクレデンシャルの漏洩などの災害が発生した場合、災害の原因に対処した上で、再発する可能性（セキュリティ上の脆弱性など）に対して適切な修復手段を講じ、継続計画で定められた遅延時間内に運用を復元するものとする。[SHALL] 注1:災害時のガイダンスについては、ISO/IEC 27002:2013 、あるいは、ISO/IEC 27002:2022 5.29、8.14を参照のこと。 注2:その他の災害状況には、ハードウェアやソフトウェアを含む、TSPの信頼できるシステムの重要なコンポーネントの障害が含まれる。
7.12 TSP termination and termination plans			7.12 TSP の終了と終了計画
REQ-7.12-01	Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.	○	TSPのサービス停止の影響による利用者および依拠当事者に対する潜在的な混乱を最小限に抑え、特にトラストサービスの正確性を検証するために必要な情報の継続的な保守が提供されるものとする。[SHALL]
	In particular:		特に：
• REQ-7.12-02	The TSP shall have an up-to-date termination plan. Before the TSP terminates its services at least the following procedures apply:	○	TSPは最新の終了計画を持っているものとする。[SHALL] TSPがサービスを終了する前に、少なくともREQ-7.12-03からREQ-7.12-08の手順が適用される。
- REQ-7.12-03	Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.	○	TSPがサービスを終了する前に、TSPは以下に終了を通知するものとする:すべての利用者およびTSPと契約またはその他の形式の確立された関係を結んでいる他のエンティティ(依拠当事者、TSPおよび監督機関などの関連当局)。[SHALL]
- REQ-7.12-04	Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.	○	TSPがサービスを終了する前に、TSPは他の依拠当事者が終了に関する情報を利用できるようにするものとする。[SHALL]
- REQ-7.12-05	Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.	○	TSPがサービスを終了する前に、TSPは、トラストサービストークンの発行プロセスに関連する機能をTSPに代わって実行するすべての下請け業者の権限を終了するものとする。[SHALL]
- REQ-7.12-06	Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.	○	TSPがサービスを終了する前に、TSPは、そのような情報を保持していないことを示さない限り、TSPの運用の証拠を提供するために必要なすべての情報を合理的な期間維持する義務を信頼できる当事者に移転するものとする。[SHALL]
- REQ-7.12-07	Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.	○	TSPがそのサービスを終了する前に、バックアップコピーを含むTSPの秘密鍵は、取り出されないようにするために、復元できないような方法で破棄されるか回収されるものとする。[SHALL]
- REQ-7.12-08	Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.	○	TSPがサービスを終了する前に、可能な場合、TSPは既存の顧客に対するトラストサービスの提供を別のTSPに移管する手配を行うべきである。[SHOULD]

要件識別子	原文	監査対象	要求事項
• REQ-7.12-09	The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.	○	TSPは、TSPが破産した場合、またはその他の理由により自力で費用を賄えない場合に備えて、破産に関する法律の適用される制約の範囲内で可能な限り、これらの最低要件を満たすための費用を賄う取り決めを持つものとする。[SHALL]
• REQ-7.12-10	The TSP shall state in its practices the provisions made for termination of service. This shall include: a) notification of affected entities; and b) where applicable, transferring the TSP's obligations to other parties.	○	TSPは、サービスの終了について定められた条項をその規程類に明記するものとする。これには以下が含まれる。 [SHALL] a)影響を受けるエンティティへの通知。 b)該当する場合、TSPの義務に関する他の当事者への移転。
• REQ-7.12-11	The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.	○	TSPは、公開鍵またはトラストサービストークンを妥当な期間、依拠当事者に利用可能にする義務を維持するか、信頼できる当事者に譲渡するものとする。[SHALL]
7.13 Compliance			7.13 コンプライアンス
REQ-7.13-01	The TSP shall ensure that it operates in a legal and trustworthy manner.	○	TSPは、合法かつ信頼できる方法で運営することを保証するものとする。[SHALL]
	In particular:		特に：
• REQ-7.13-02	The TSP shall provide evidence on how it meets the applicable legal requirements.	○	TSPは、適用される法的要件をどのように満たしているかに関する証拠を提供するものとする。[SHALL]
• REQ-7.13-03	Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.	○	提供されるトラストサービスおよび当該サービスの提供に使用されるエンドユーザー製品は、可能な場合には障害者もアクセスできるようにするものとする。[SHALL]
• REQ-7.13-04	Applicable standards on accessibility such as ETSI EN 301 549 [i.10] should be taken into account.	○	ETSI EN 301 549などのアクセシビリティに関する規格を考慮するべきである。[SHOULD]
• REQ-7.13-05	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. NOTE 1: TSPs operating in Europe are required to ensure that personal data is processed in accordance with Directive 95/46/EC [i.1] until 25 May 2018, and from 25 May 2018 in accordance with Regulation (EU) 2016/679 [i.12] that repeals the Directive 95/46/EC [i.1]. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online. NOTE 2: See ISO/IEC 27701:2019 [i.14] for requirements and guidance on the extension to 27002 for privacy	○	個人データの無許可または違法な処理、および個人データの偶発的な紛失または破壊、損傷に対して、適切な技術的および組織的措置を講じるものとする。[SHALL] 注1：欧州で事業を行うTSPは、2018年5月25日までは指令95/46/ECに従って、2018年5月25日からは指令 95/46/ECを廃止するEU規則2016/679に従って、個人データが処理されることを保証する必要がある。この点で、オンライン・サービスの認証は、オンライン・サービスへのアクセスを許可するために適切で、関連性があり、過剰でない識別データのみの処理に関係する。 注2:プライバシー情報管理のための27002の拡張に関する要件とガイダンスについては、ISO/IEC 27701:2019を参照のこと。

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

－リモート電子署名基準の検討－

最終報告書

2024 年 3 月 22 日

一般社団法人デジタルトラスト協議会（JDTF）

リモート電子署名基準調査 TF

1 背景と目的

リモート署名とは、「リモート署名とは、一般に、事業者のサーバーに利用者（エンドエンティティ）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）であり、近年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利用が拡大している。

上記調査報告書では、「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。」とされている。

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」という。）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の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（5.参照規格、参照）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こととした。
- 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た。

2.2 国内のサービス事業者へアンケート調査

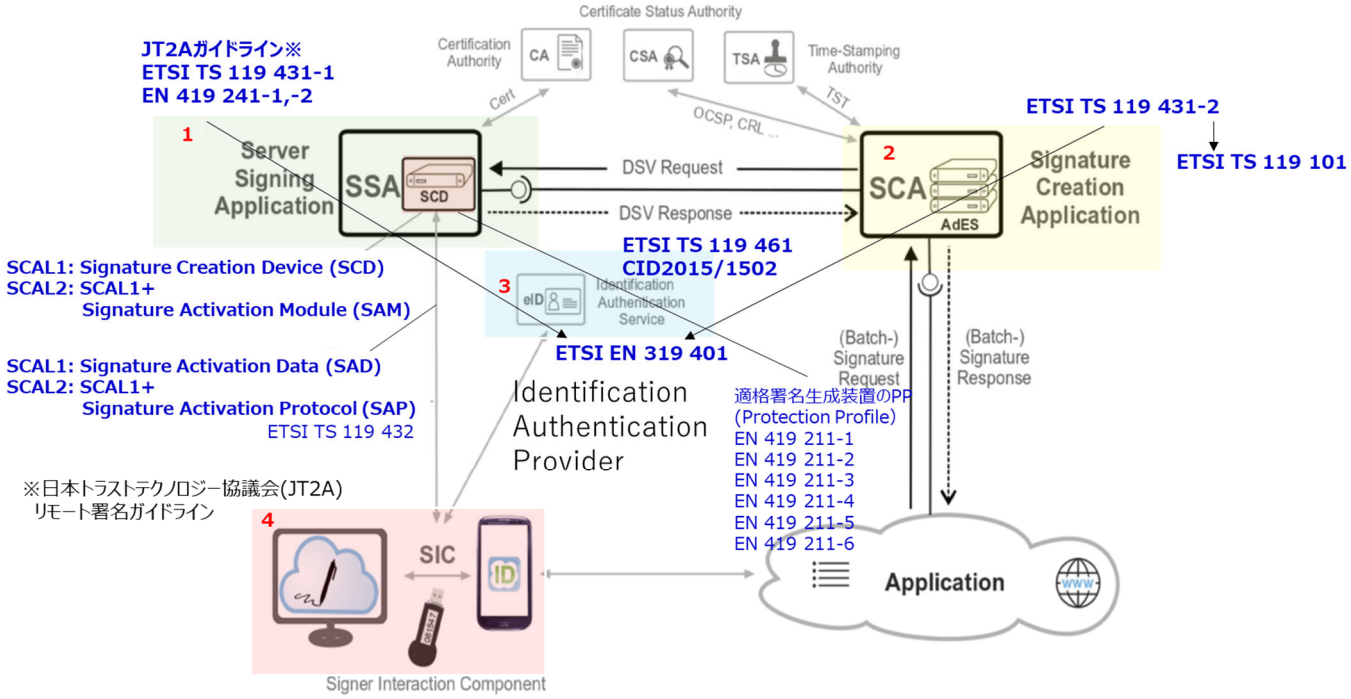
国内のサービス事業者へアンケート調査を行い、利用事例や課題の洗い出しを併せて実施し（付録1 アンケート結果報告 参照）、リモート署名サービスの評価基準を検討する際に必要と考えられる事項を以下のとおり整理した。

- 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を合わせて実施している。

3 リモート署名サービスの評価基準の作成

上記 2.1 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した。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に対応して、国内外のリモート署名サービスに関する基準を対応付けると以下の図のようになる。



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 とも記す)

図1 リモート署名サービスのアーキテクチャー
(ETSI TS 119 432 V1.1.1 Figure3 より抜粋加筆)

構成要素となる各コンポーネントは以下が挙げられる

1. サーバー署名アプリケーション(SSA: Server Signing Application)
   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、署名者の認証情報や署名に用いる署名鍵を特定する情報、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。電子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、リモート署名値生成装置等と呼ぶ場合がある。
   SSASC は、署名対象データのハッシュ値に基づいて生成された署名値を署名者または他アプリケーションに配信することを目的とする。

2. デジタル署名生成アプリケーション（SCA: Signature Creation Application）

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取り、SSA に署名者、署名鍵、署名対象文書等を特定する情報（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と呼ぶ。

3. 本人認証サービス（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 カードなどのデバイスなど)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。

従って、リモート署名サービスの基準案の対象は
・サーバー署名アプリケーション（SSA）
・デジタル署名生成アプリケーション（SCA）
の 2 つのアプリケーションに対し作成することとした。

3.1 リモート署名サービスの評価基準の文書構成

リモート署名サービスの評価基準は、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、デジタル署名生成アプリケーション（SCA）に対して適用するものとし、下図の（1）「リモート署名サービスの評価基準概説」（本書）及び、次の（2）から（5）の文書群により構成される。

また、リモート署名サービスの評価基準は、1つの保証レベルだけではなく、簡易なレベル（Level 1）、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 2）、国際相互運用が可能なレベル(Level 3)の 3 つの保証レベルに応じた評価が可能となるよう、各要求事項に対して対象となる保証レベルを示した。尚、Level3 では、EU で規定する QSDC の要件を含むすべての要件を満たすものとし、Level2 では、QSCD、および署名活性化モジュール（SAM）を耐タンパー保護環境内に含める要件を除外した。

リモート署名サービスの監査に用いる具体的な要求事項は、（2）から（5）の各保証レベルに応じた要求事項の欄に〇印が付けられている項目である。

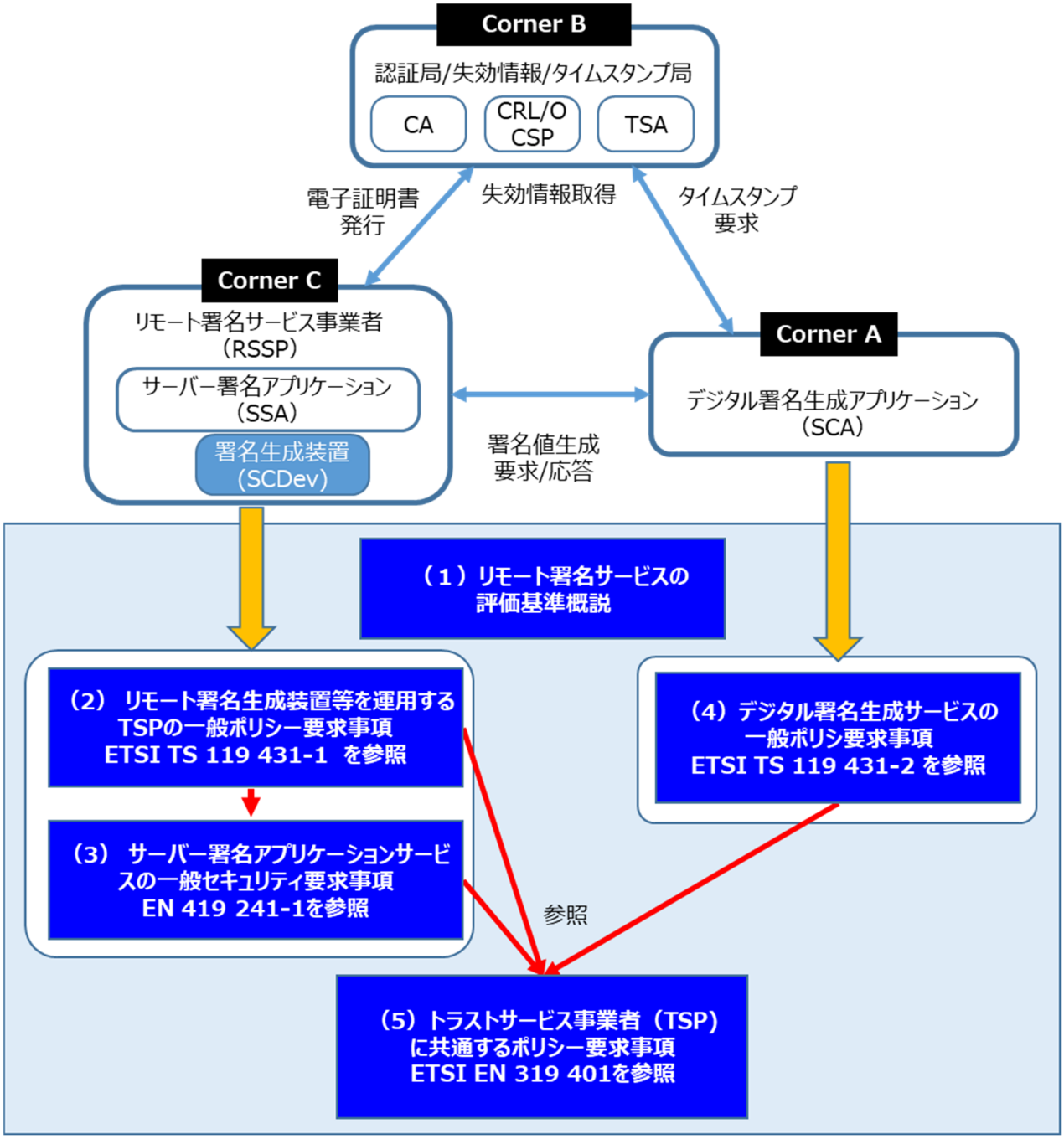


図 2 リモート署名サービスコンポーネントと評価基準の文書構成

注： 対象文書の重要度に応じて〇印の項目を再評価し、署名鍵の漏洩リスクを物理的な SCDev などを用いて十分に低減するか、または、たとえ漏洩した場合であっても署名者以外が署名できないような必要な管理策を検討すべきである。

（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構成を説明する文書。下記(2)から(5)の用語定義、記号・略語、参照規格はここに記載する。

（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、および
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 を参考に作成）

ここでは、リモート署名生成装置（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“トラストサービスプロバイダー（TSP）”に対して、適用されるポリシーとセキュリティ要件を規定した。この SSASC に対するセキュリティ要件の一部は次の（3）を引用している。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、すなわち簡易的な″LSCP″、標準的な″NSCP″および欧州の適格レベルを満たす″EUSCP“の 3 レベルに加え、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+″を規定した。

（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、および
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 を参考に作成）

ここでは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した。

SSA は、承認された署名者の制御下で SCDev を使用するため、認可（Authorization）された署名者による独占的な制御（単独制御）が保証されなければならない。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 つの基準が示されている。

（４） デジタル署名生成サービスの一般ポリシー要求事項、および
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 を参考に作成）

ここでは、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した。

（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、および
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 を参考に作成）

ここでは、トラストサービスプロバイダー(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定義する。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場合がある。

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、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、後述する図 3 の電子署名法令基準のモダナイズ調査検討チームに素案を提示し合同で改定案の作成を行った。

検討に当たり、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。

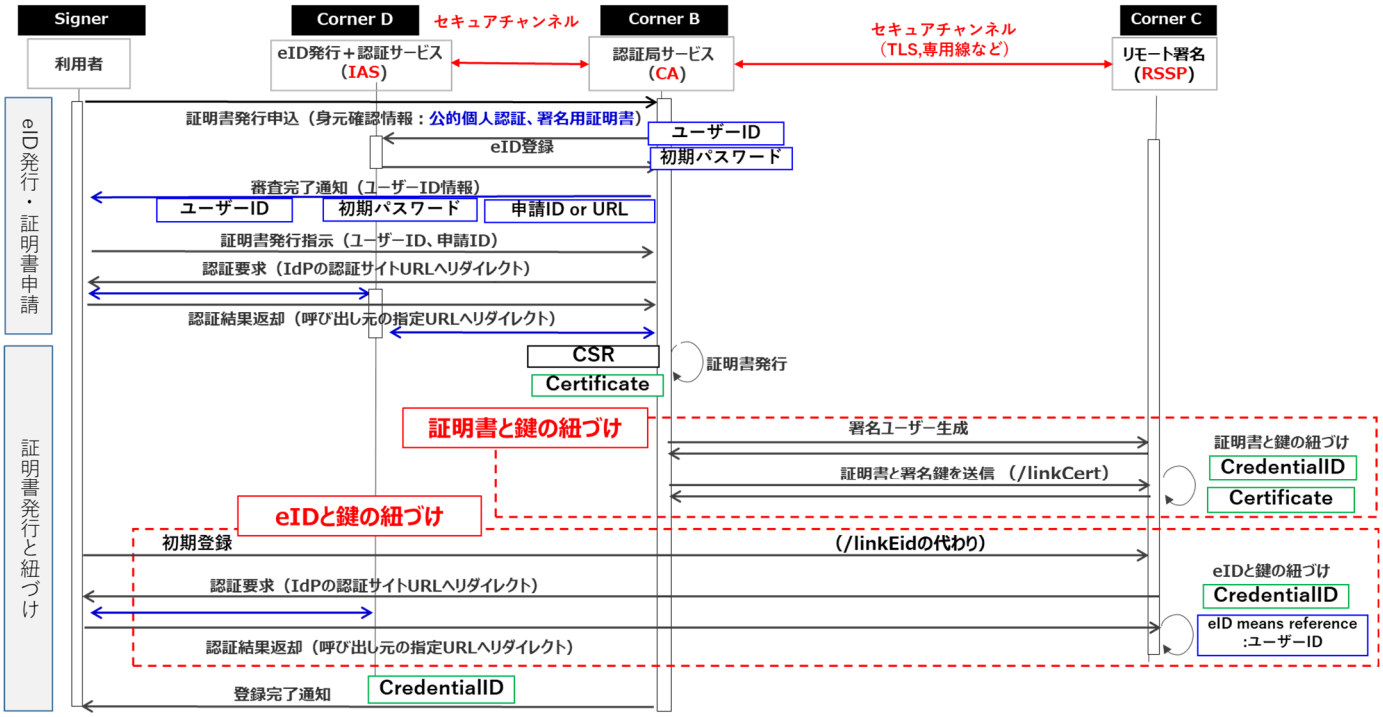


図 3　利用申請からサービス開始までの登録フロー例（CA、IAS、RSSP が別会社の場合）

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

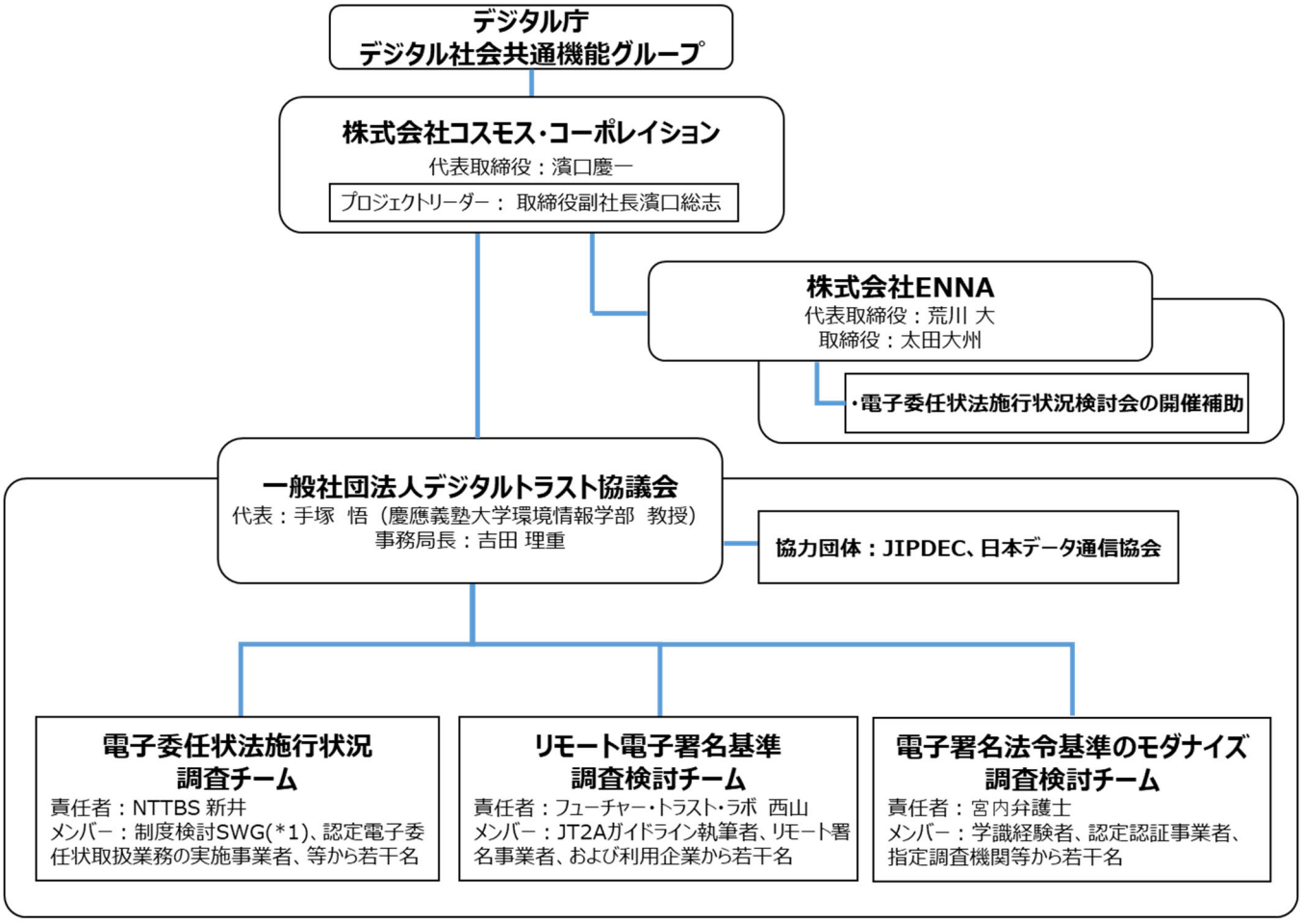
Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (remote signing)

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

6 検討体制

本、調査研究業務の実施体制を、「図 4 実施体制」に示す。本報告書、リモート電子署名基準の検討については、リモート電子署名基準調査検討チームにて実施した。



＊1 総務省：個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会 制度検討サブワーキンググループ
https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber-card/02tsushin01_04000468.html

図 4 実施体制