認証から見たリモート署名
利用認証 と 鍵認可

LangEdge,Inc.
有限会社 ラング・エッジ

プログラマ/取締役
宮地直人（miyachi@langedge.jp）

2020年7月29日

電子署名方式の概要

電子署名方式		本人性	非改ざん性	補足
本人型電子署名	ローカル署名	PKI証明書	デジタル署名	全てをローカル処理 （秘密鍵はローカル管理）
	クライアント署名	PKI証明書	デジタル署名	署名値計算はローカル処理 その他はリモート処理 （秘密鍵はローカル管理）
	リモート署名	PKI証明書 （認証結果）	デジタル署名	全てをリモート処理 （秘密鍵はリモート管理）
立会人型電子署名		認証結果 （立会人保証）	デジタル署名	認証結果にて本人性を保証 立会人はPKI証明書で保証
エビデンス保管型電子署名 （認証型電子署名）		認証結果 （事業者保証）	（別途）	米国のクラウド署名で 多かった方式

- リモート署名と立会人型は似た方式だが、認証後のデジタル署名が本人か立会人かが異なる。立会人型では認証結果を証拠として残す必要があるが、本人の秘密鍵を管理をする必要が無いので簡易な運用が可能となる。リモート署名は検証情報が署名文書に含まれるので検証が簡易に行える。
- 立会人型はエビデンス保管型に立会人のデジタル署名を追加した方式となる。最近では米国のクラウド署名も立会人型に移行またはオプションにてリモート署名も利用可能になっている。

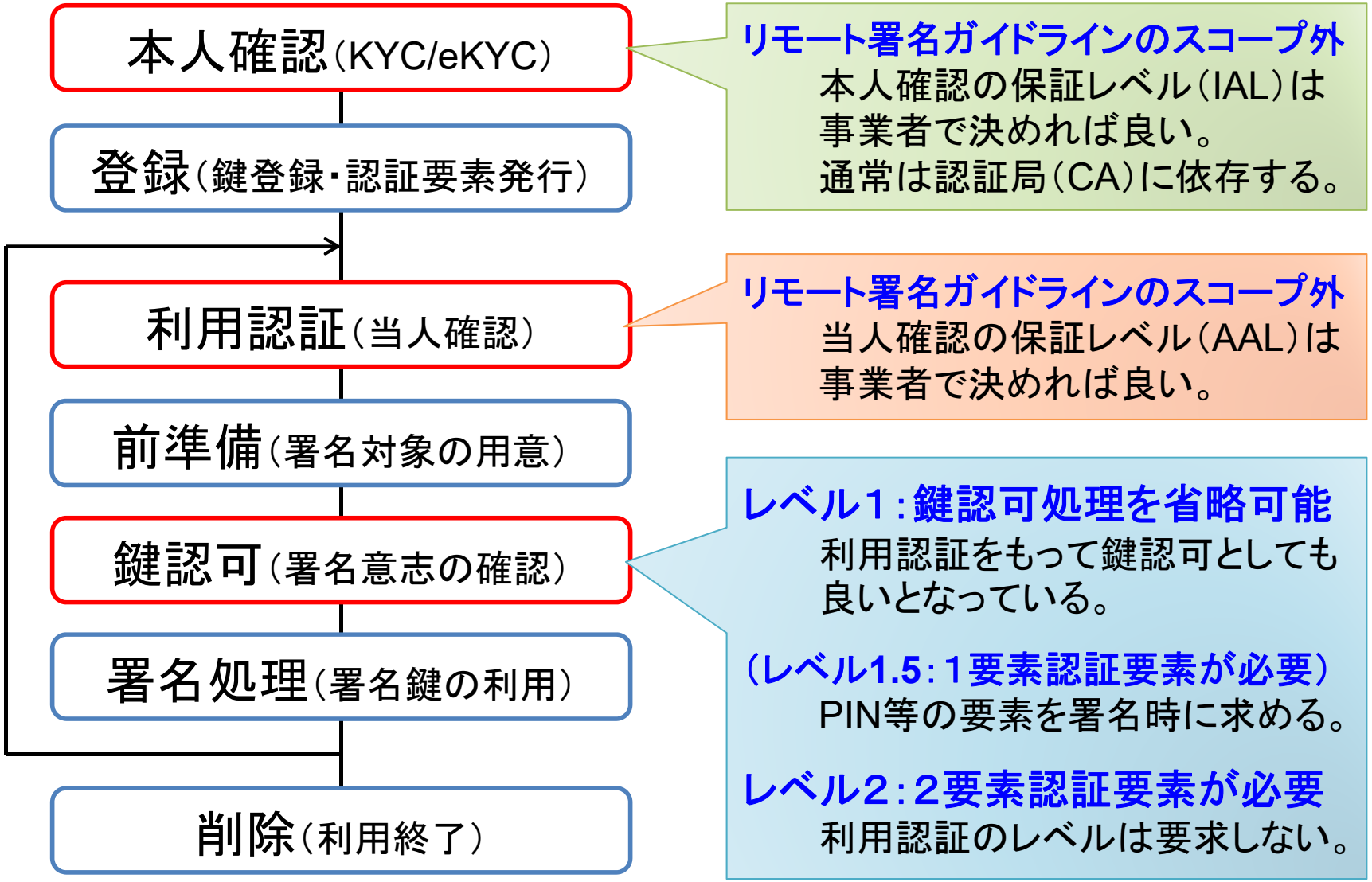
リモート署名ガイドライン

JT2A（日本トラストテクノロジー協議会）より2020年4月公開。
https://www.jnsa.org/result/jt2a/2020/index.html

3つのレベルに分けて解説している。

レベル	概要
レベル1	電子署名に利用する署名者の署名鍵を安全に管理するために最低限必要な対策を施したレベル
レベル2	電子署名法における認定認証業務において発行する電子証明書に基づいたリモート署名サービスが認定認証業務の信頼性と同等の信頼性を達成するために必要なレベル
レベル3	リモート署名サービスが欧州eIDAS規則における適格電子署名と同等の信頼性を達成するために必要なレベル

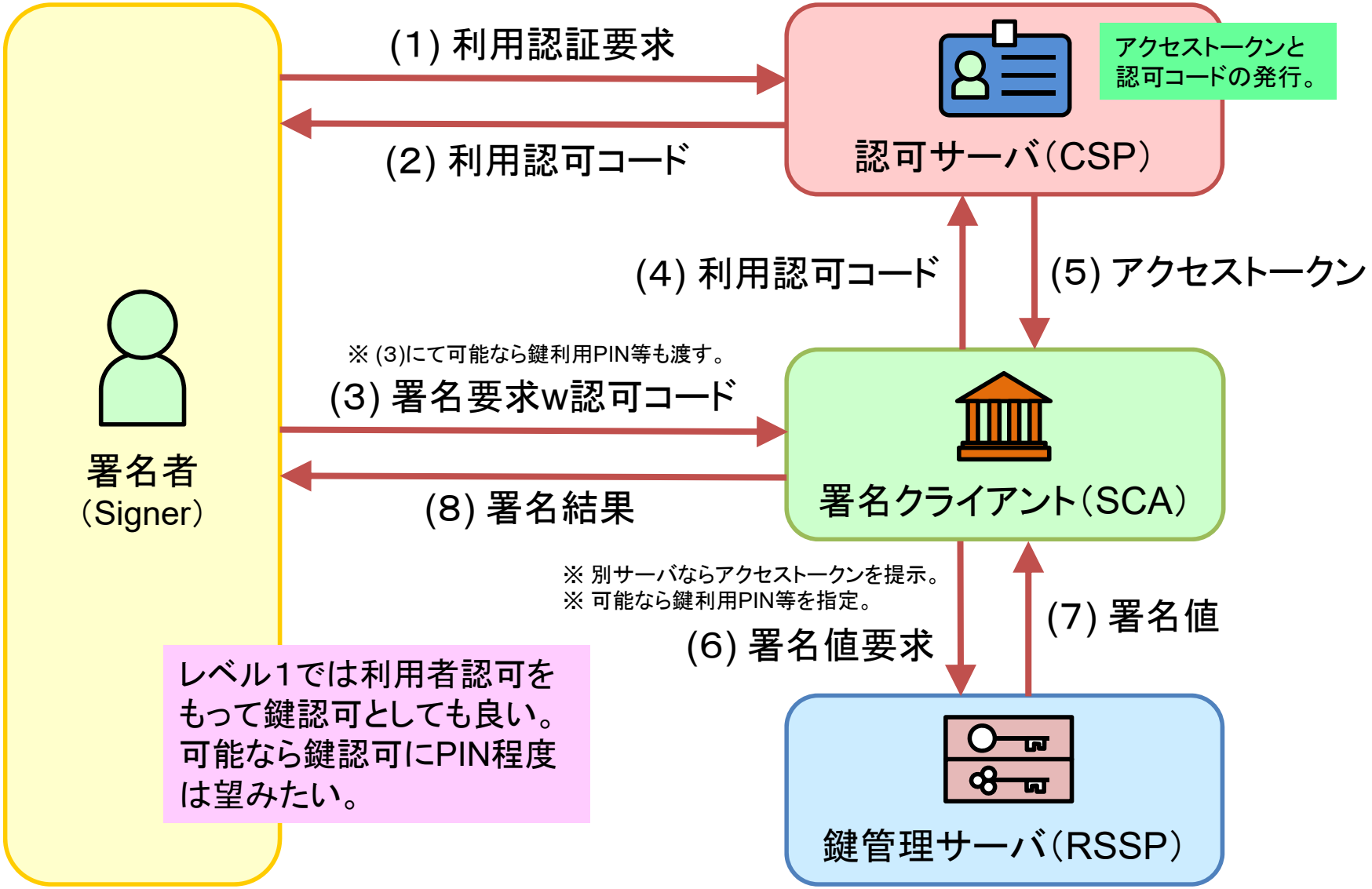
リモート署名利用の流れ



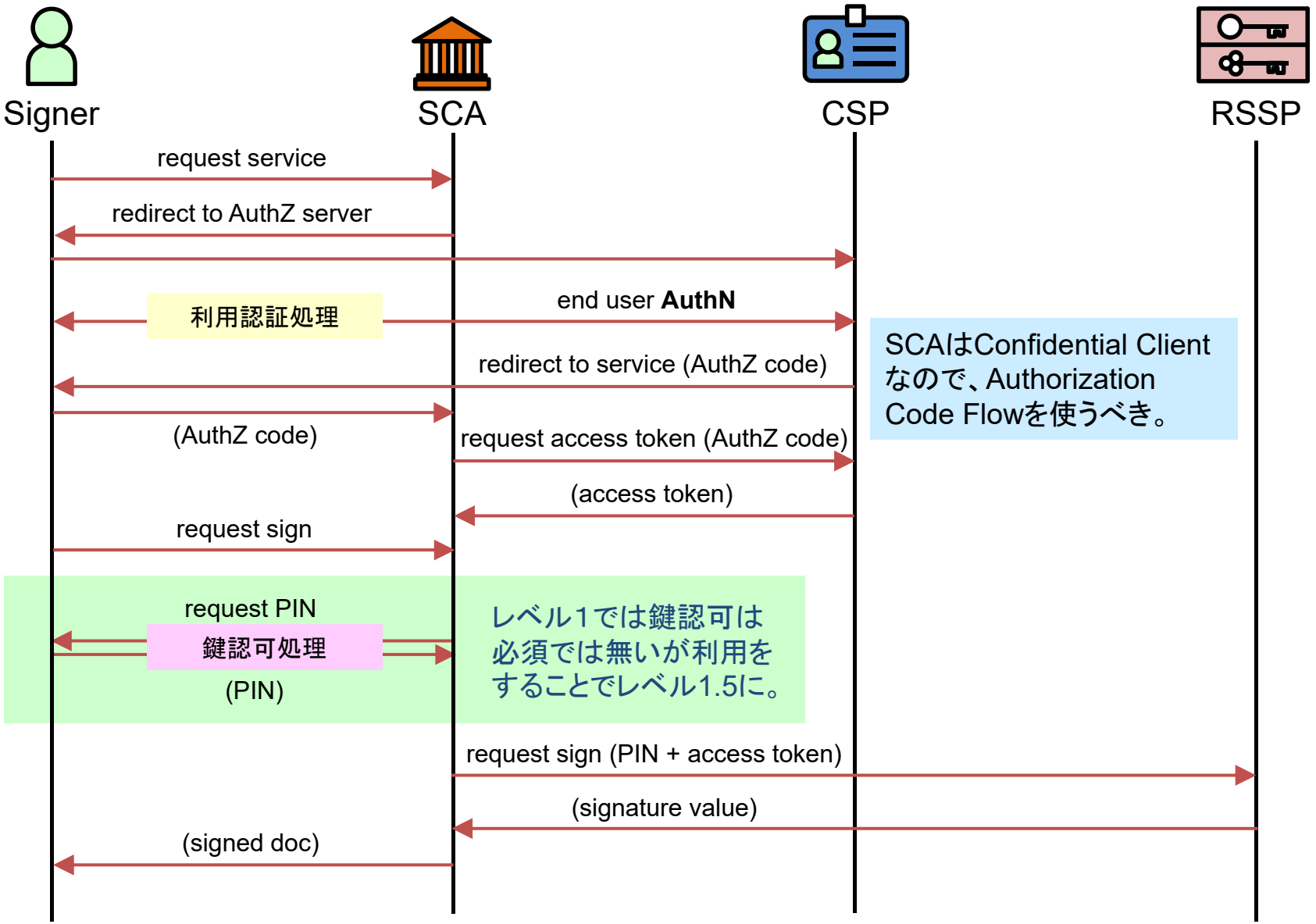
リモート署名 登場人物(ロール)

1. **Signer**(署名者/エンドユーザ)
   - リモート署名ではエンティティが人間なのでエンドユーザ。
2. **SCA**(署名クライアント/署名サービス)
   - 署名者の認可を受けて、署名を付与するサーバ。
3. **RSSP**(鍵管理サーバ/鍵リソースサーバ)
   - SCAからの要求により署名鍵にて署名値を計算して返す。
   - 別サーバの場合にはアクセストークンを要求する。
   - レベル2では署名者からクレデンシャル認可を受け取り、SADトークン(鍵認可トークン)の発行を行う。
4. **CSP**(クレデンシャル発行者/認可サーバ/OP)
   - 署名者(利用者)管理を行いOAuth/OIDC等の認証認可によりアクセストークンを発行するサーバ。

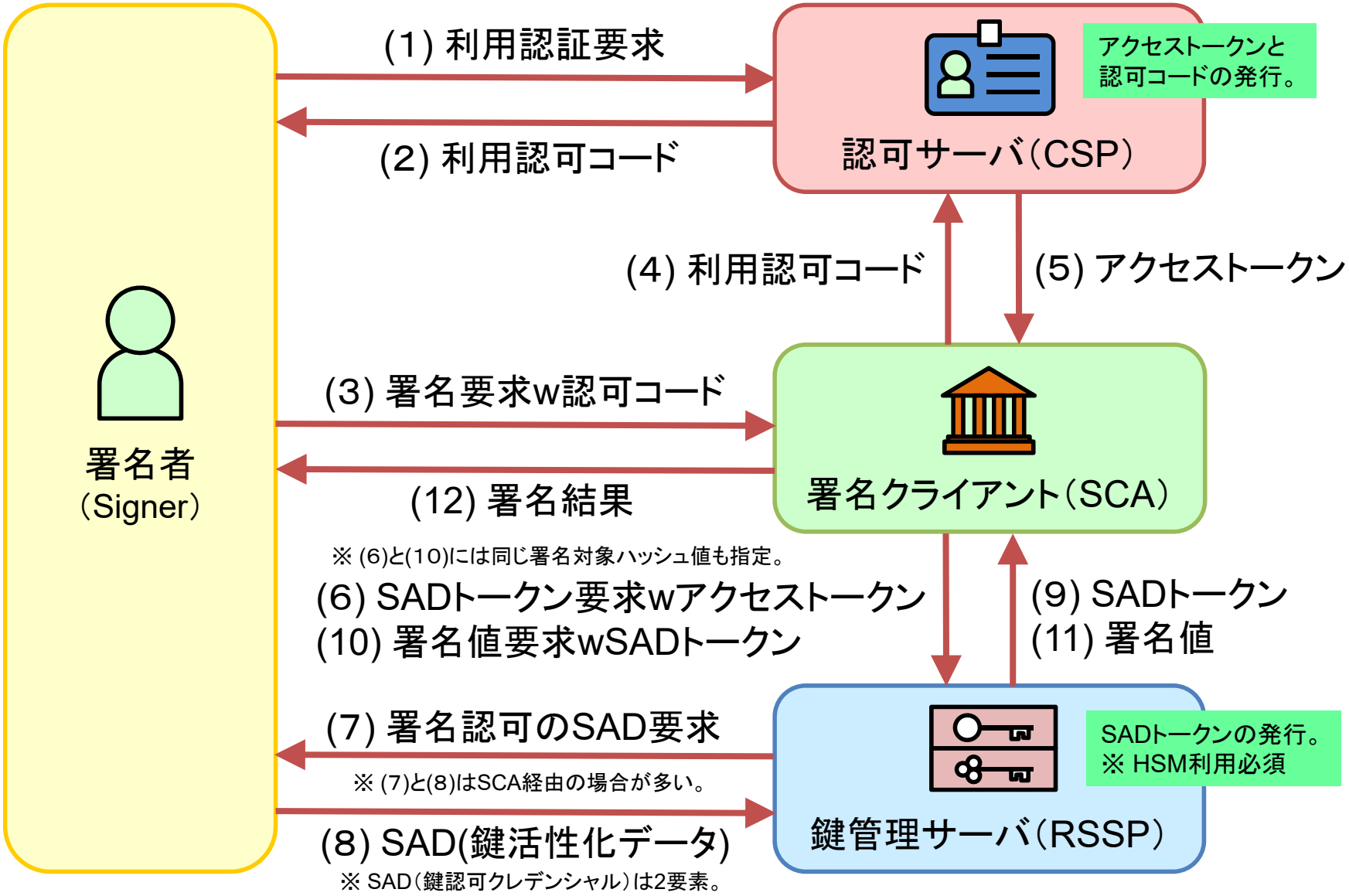
レベル1 リモート署名 登場人物(ロール)の関係



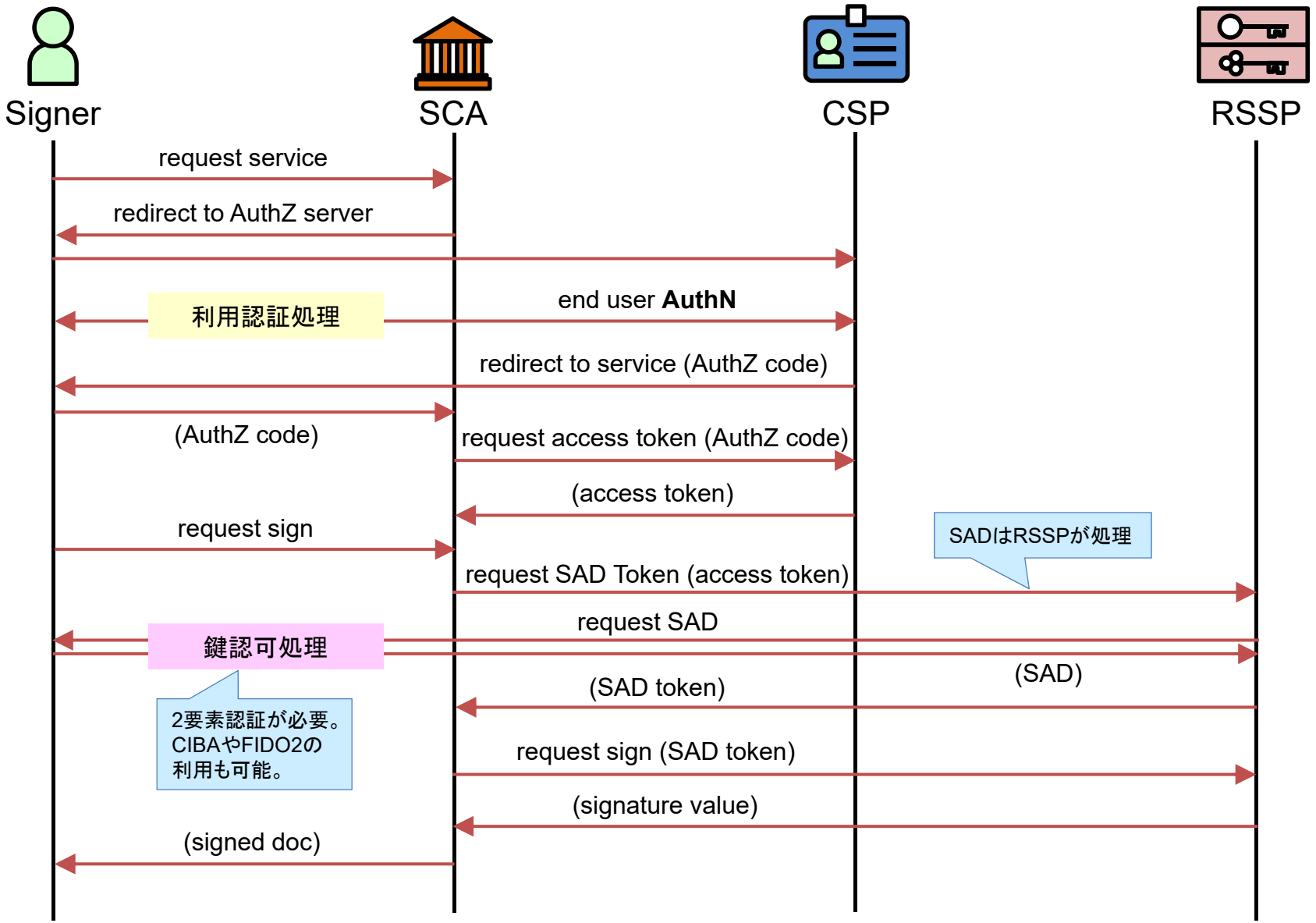
レベル1 リモート署名（Authorization Code Flow）



レベル2 リモート署名 登場人物(ロール)の関係



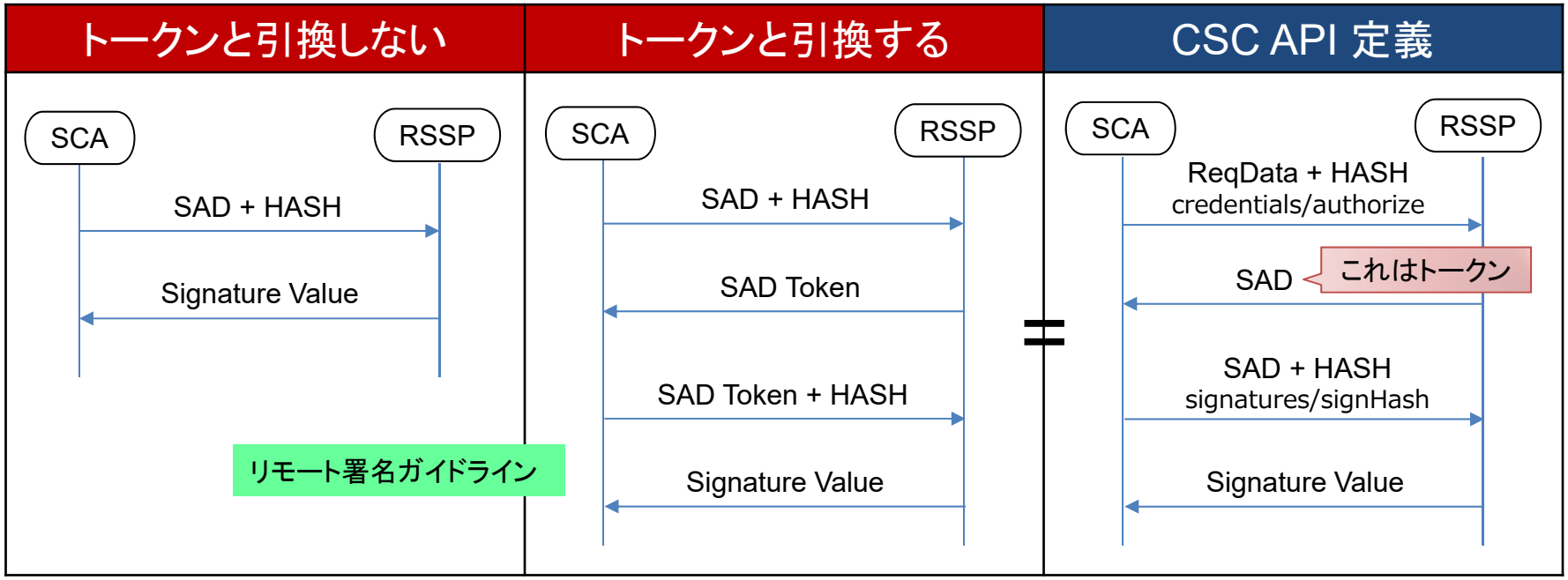
レベル2 リモート署名（Authorization Code Flow）



SAD（鍵活性化データ）とSADトークン

SAD：Signature Activation Data

署名鍵を活性化するデータ（クレデンシャル）だが、トークンとして引換する場合にそのトークン自体をSADと呼ぶ場合がある。
ガイドラインでは「SAD」と「SADトークン」として分けている。
SADトークン（鍵認可トークン）は署名１回のみで有効であり、複数署名する場合にはSADトークンを更新して行く。

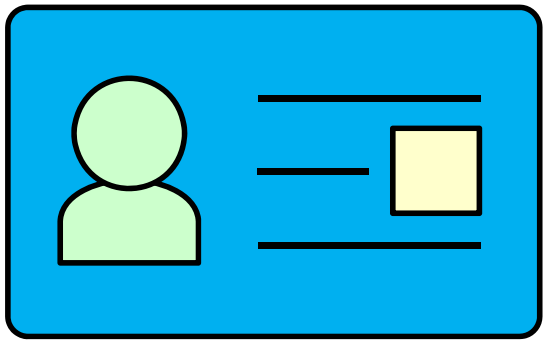


考察:ローカル署名の認証レベル(AAL)

ローカル署名では、手元に保有する秘密鍵(ICカードや証明書ストア格納)を利用して署名を付与する。これを認証的なレベル(AAL)のローカル認証として考えるとどうなるか？

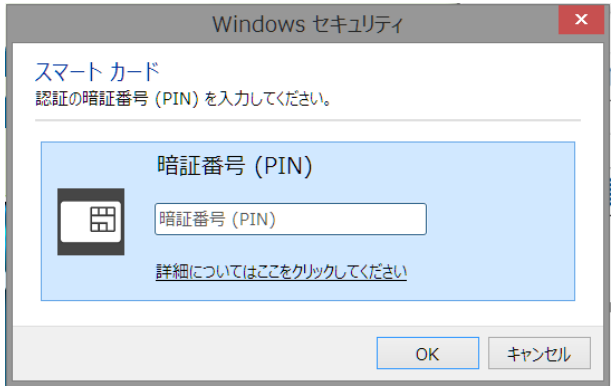
- 秘密鍵の「所有」で1要素は満たす。
- PINが必要であれば「知識」の2要素目も満たす。

つまり2要素認証と言えるのではないか。リモート署名に同等のレベルを要求するなら2要素認証(AAL2/AAL3)が必要となる。



所有

＋



知識

参考：電子署名・電子シールとデジタル署名技術

名称（用途）	電子署名	電子シール（eシール）	タイムスタンプ
英語名称	eSignature (Electronic Signature)	eSeal (Electronic Seal)	Timestamp
署名者 （証明書）	自然人	法人（組織・部署）	時刻認証局（TSA） ※ 信頼済みの第三者
説明	署名者は自然人であり 「本人性」を保証する 例：電子契約書	署名者は法人等であり 「発行元」を保証する 例：レシート	時刻認証局による サーバ署名であり 「日時」を保証する
デジタル署名 フォーマット （署名形式）	CAdES/XAdES/PAdES Digital Siganature Format ISO 14533-1/2/3 プロファイル ※ 電子署名と電子シールの違いは署名証明書のみ		タイムスタンプトークン RFC 3161 ※ デジタル署名の一種

- 電子署名・電子シール・タイムスタンプにデジタル署名の技術・標準を利用することで完全性も保証することが出来る。
- デジタル署名は暗号技術による電子署名・電子シール・タイムスタンプの実現方法の１つであり、他の方法により実現することも可能である（例：立会人型署名）。
- デジタル署名は「本人性」「非改ざん性」「日時」をまとめてパッケージ化できる利点がある。またデジタル署名には検証方法も標準化されている利点もある。