JNSA電子署名WG春祭り２０１８

クラウド署名とCSC対応について

2018年5月23日

セイコーソリューションズ株式会社
デジタルトランスフォーメション営業統括部
クロノトラスト営業部クロノトラストソリューション課
村尾　進一

自己紹介

職歴：

2003年　セイコーインスツルメンツ(株)入社　クロノトラスト事業に配属

2008年　長期署名システム「NiXAdES」の開発を担当
・省庁、医療、国税e文書における長期署名システムの提供

2011年　長期署名クラウドサービス「eviDaemon」をリリース

2013年　セイコーソリューションズ(株)に（クロノトラスト事業ごと）異動

2014年　NSF 2014「タイムスタンプ活用の動向」について発表

2015年　PKI Day 2015「トラストリストと信頼のグローバル化」について発表

2016年　JNSA電子署名WG五月祭「電子署名入門」について発表

2017年　弊社クラウド署名サービスをクラウド署名コンソーシアム（CSC）規格に対応
10月26日　アドビ システムズ社様のAdobe Signとの連携を発表

2017年　JNSA電子署名WG秋祭「 J-LIS公開のAPIを読み解くなど」について発表

・・・現在に至る

アジェンダ

- リモート署名とクラウド署名について
- クラウド署名の活用シーン
- クラウドHSMサービスのCSC仕様対応
- まとめ

リモート署名とクラウド署名について

リモート署名の定義※

**リモート署名事業者のサーバに利用者（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上で電子署名を行うこと。**

※電子署名法研究会（METI/経済産業省）
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html

リモート署名とクラウド署名について

リモート署名のメリット

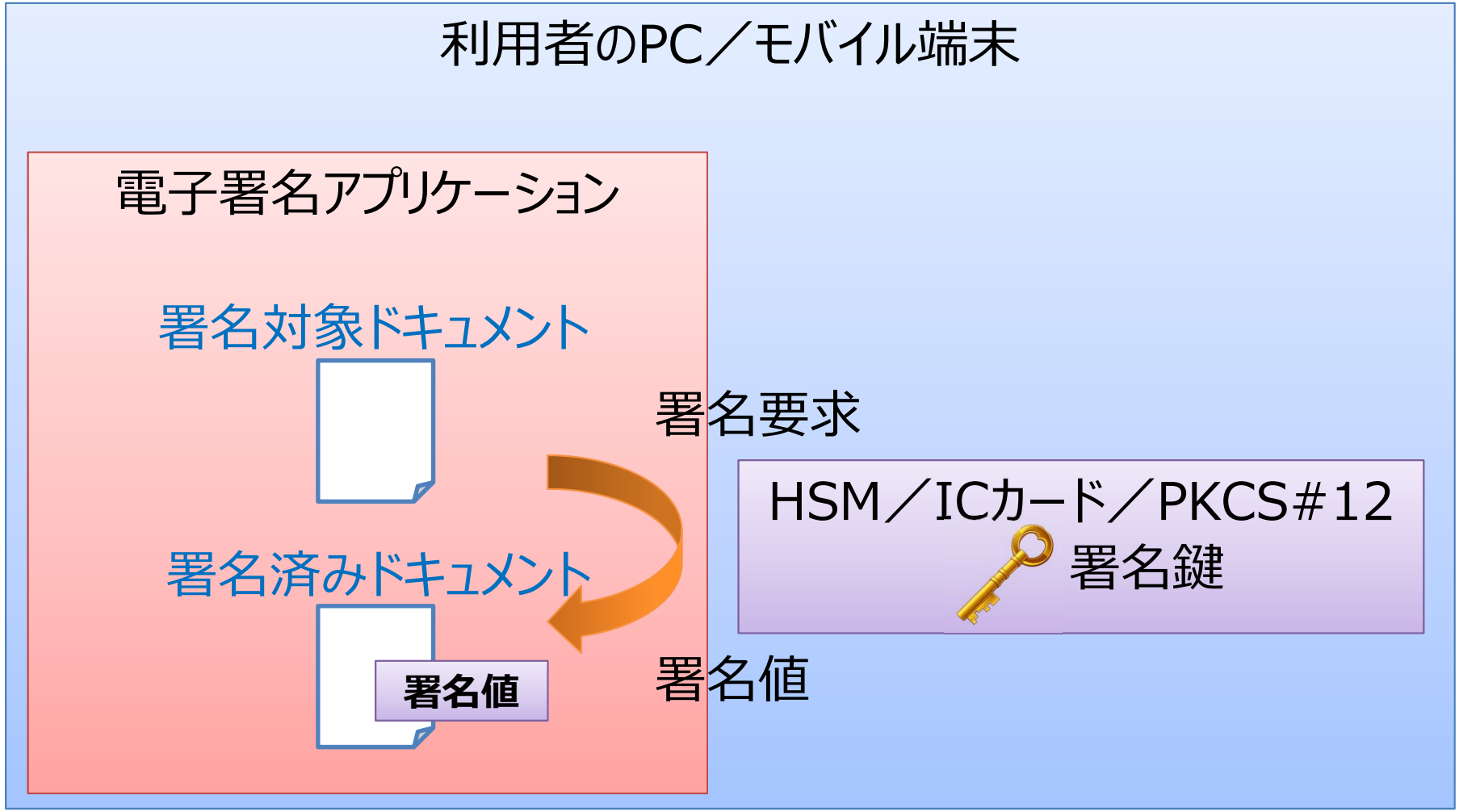
・ICカード/ICカードリーダやUSBトークンなどの
ドライバソフトウェアをインストールする必要が無い

・リモート署名事業者が提供する認証局との連携機能により
証明書申請や登録が簡単になる（発行自動化）

・リモート署名事業者が提供する鍵管理（HSM）機能により
安全に鍵が保管される（証明書更新管理サービス等）

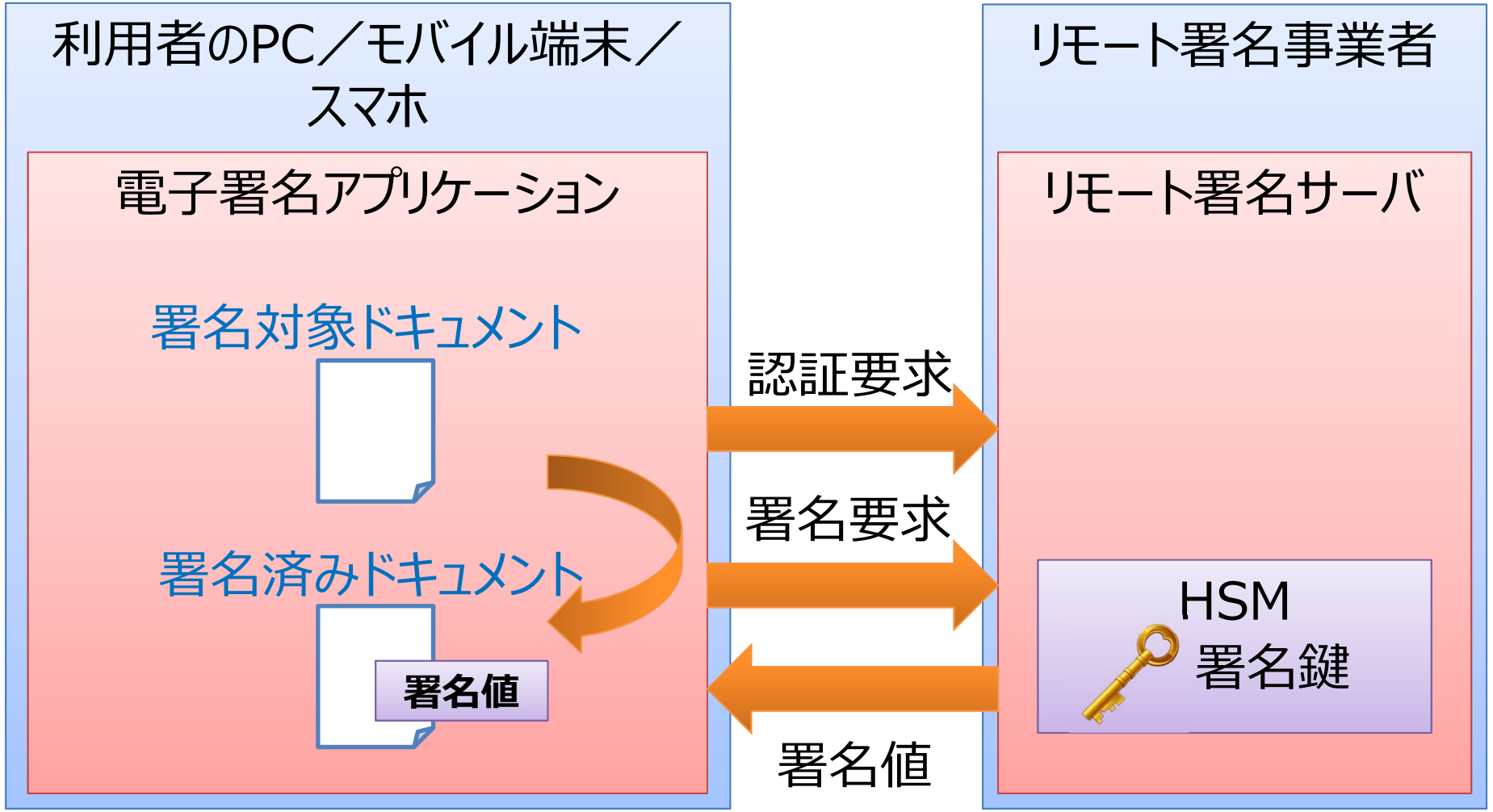
リモート署名とクラウド署名について

ローカル署名のイメージ図



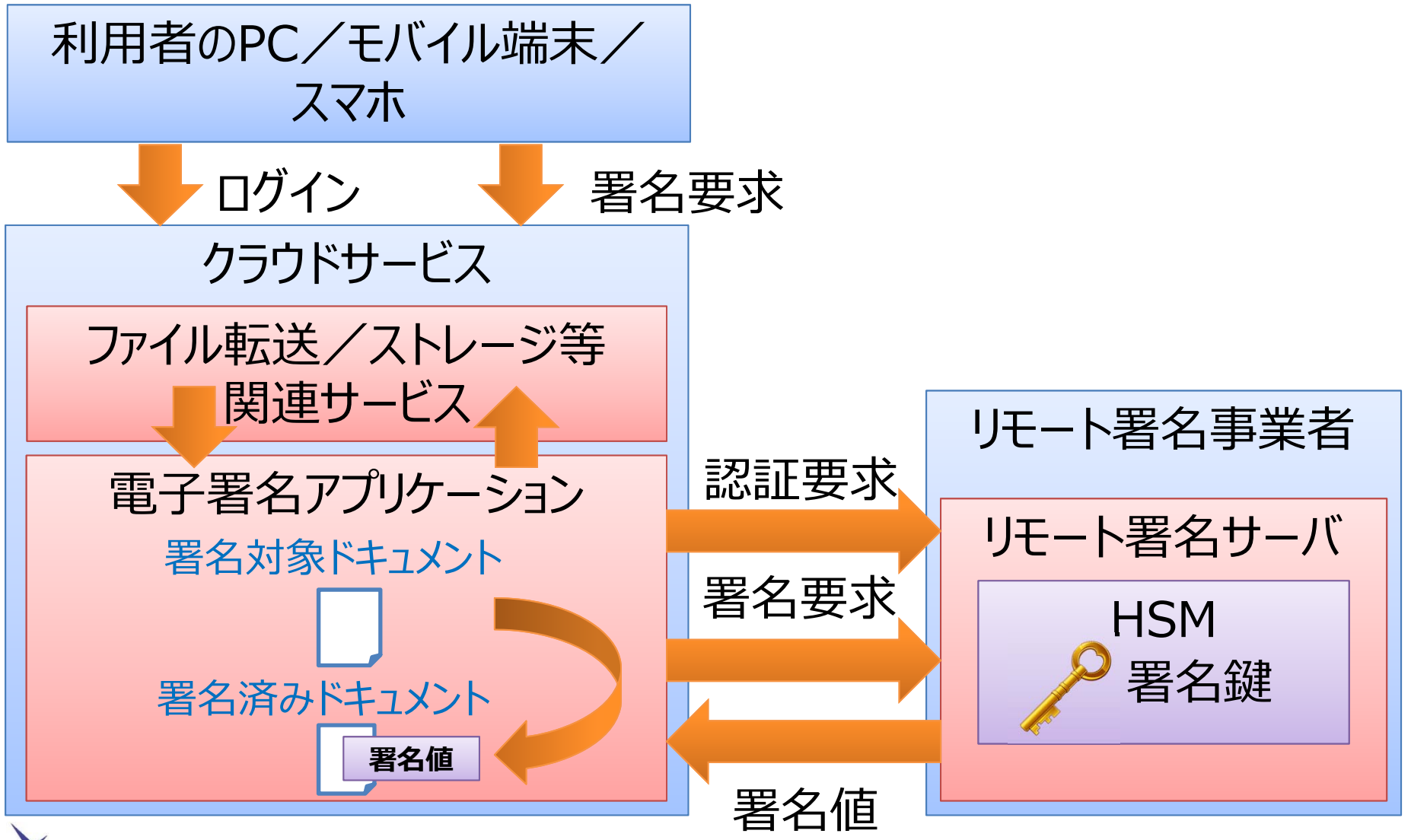
リモート署名とクラウド署名について

リモート署名のイメージ図



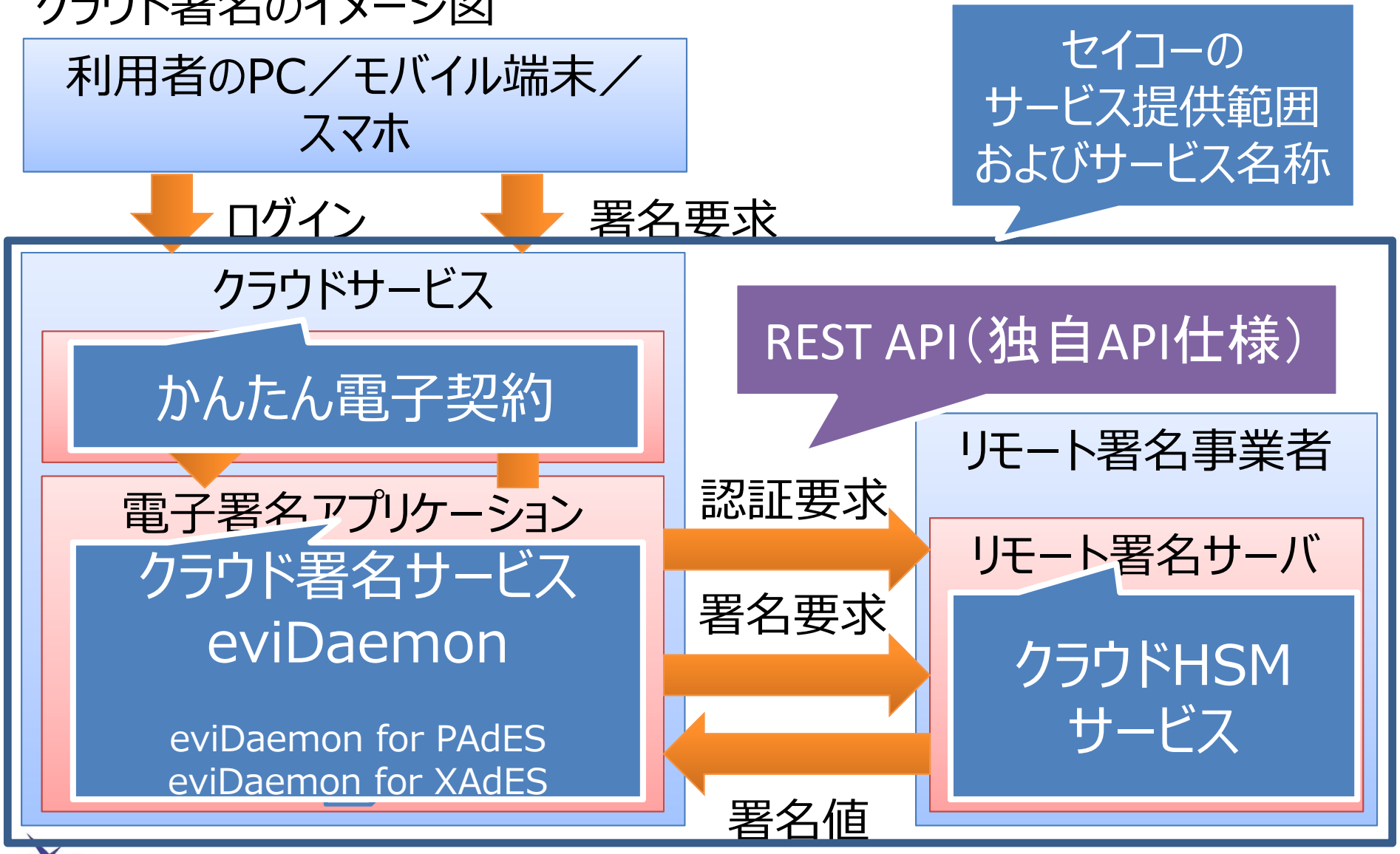
リモート署名とクラウド署名について

クラウド署名のイメージ図



リモート署名とクラウド署名について

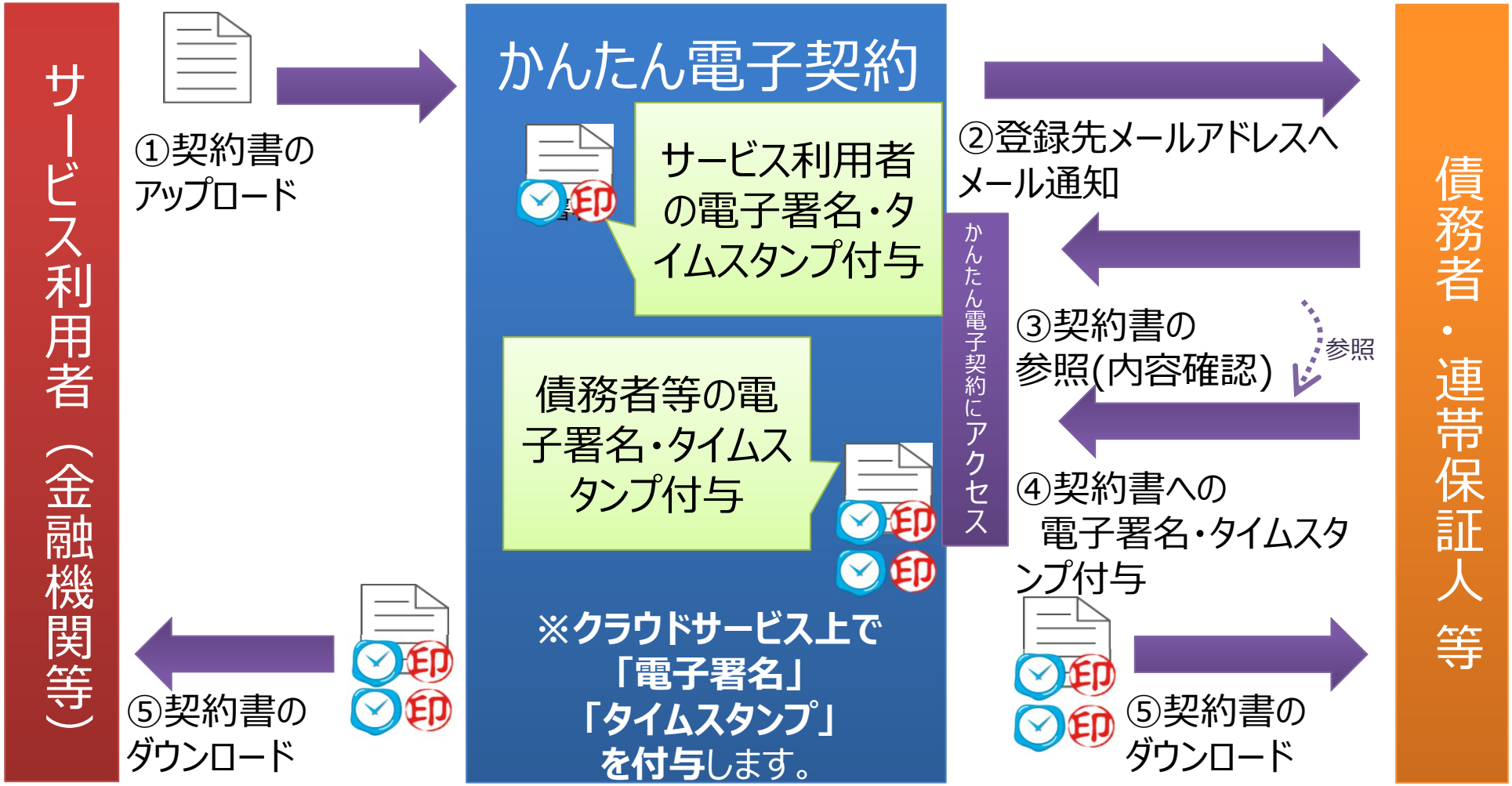
クラウド署名のイメージ図



クラウド署名の活用シーン

かんたん電子契約を利用した住宅ローン契約の電子化事例

電子署名・タイムスタンプを付与することのできる電子ファイル受渡サービス



クラウド署名コンソーシアム（Cloud Signature Consortium 以下 CSC）とは

2016年初め、ソリューション、テクノロジー、トラストサービスプロバイダを含む業界や学術界の専門家から成る国際的な協力グループによって設立された団体で、以下を目的として活動。

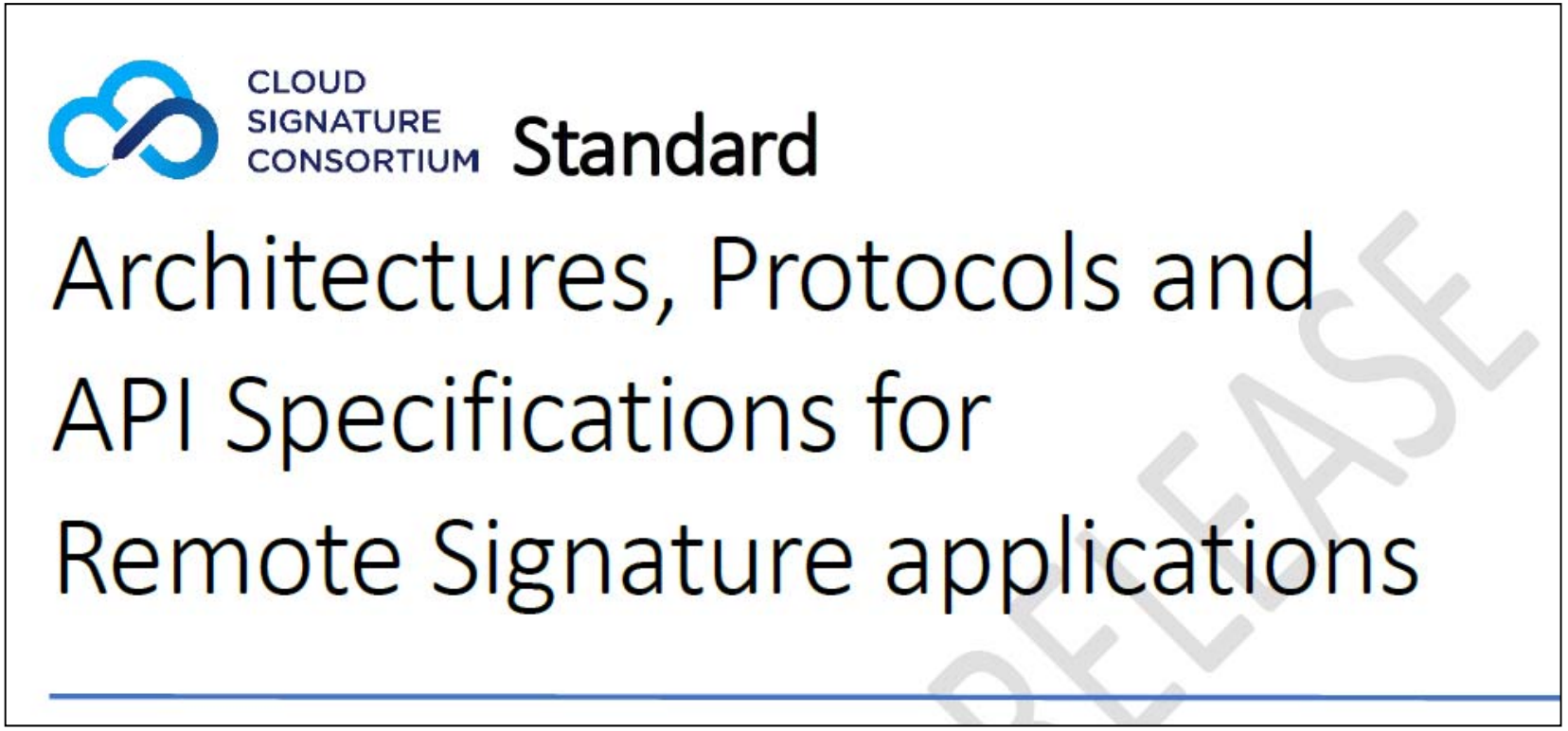
- **共通のアーキテクチャ設計と構成要素構築によって、ソリューション、テクノロジー、トラストサービスプロバイダ間の相互運用性を実現**
- **サービス間の連携を相互運用可能にするべくプロトコルとAPIの技術仕様開発**
- **オープンスタンダードとしてAPI仕様を公開**
- **クラウド署名のコンセプトを促進**

出典：https://itc.jipdec.or.jp/event/20170704.html（Cloud signature consortiumの概要）

クラウドHSMサービスのCSC仕様対応

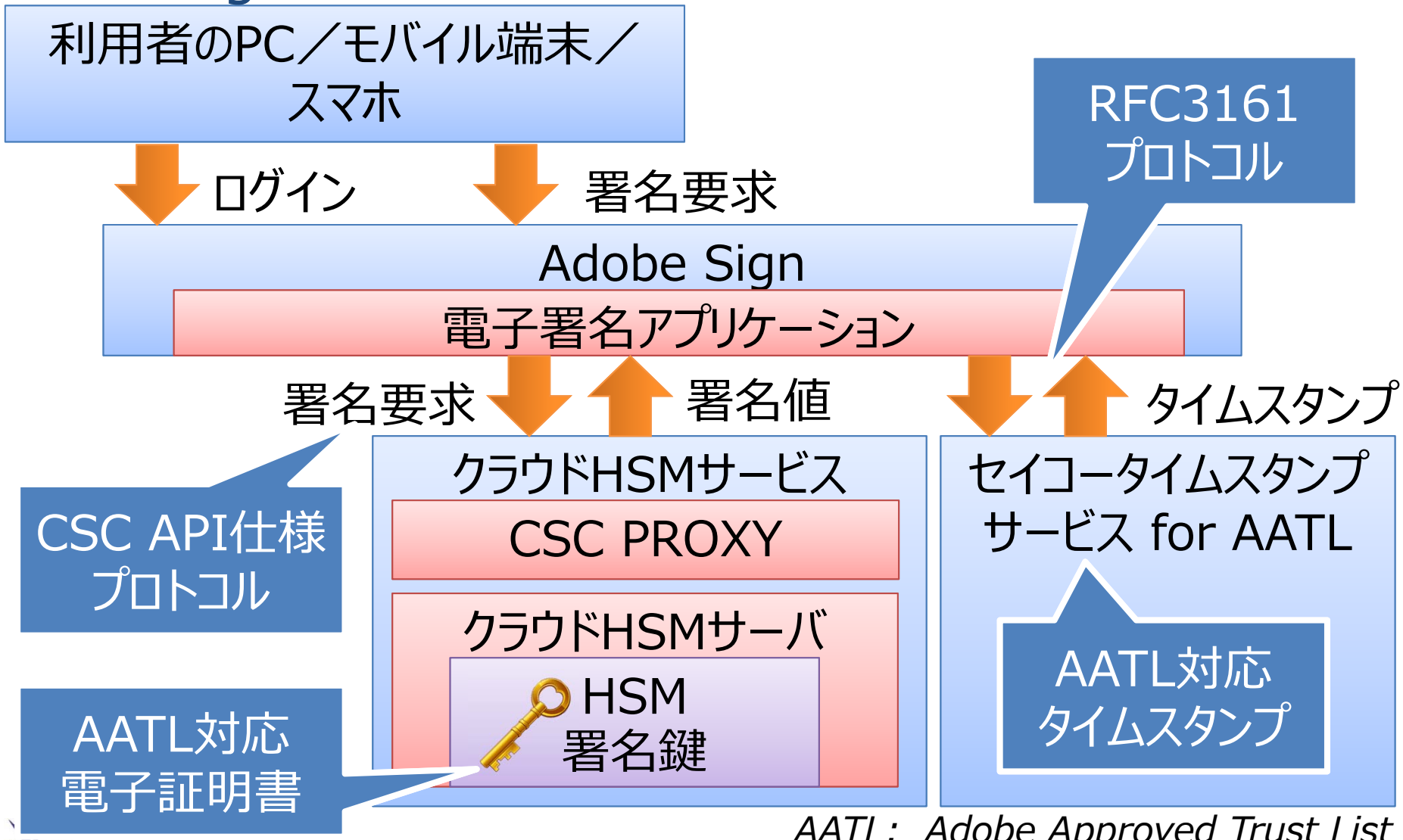
CSCのAPI仕様は下記URLから取得可能

http://www.cloudsignatureconsortium.org/specifications/



クラウドHSMサービスのCSC仕様対応

Adobe SignとクラウドHSMサービスの連携イメージ



AATL： Adobe Approved Trust List

クラウドHSMサービスのCSC仕様対応

実装API一覧

サービスURL形式：
https:// <CSC PROXYサーバ> /csc/v0/ <メソッドパス>

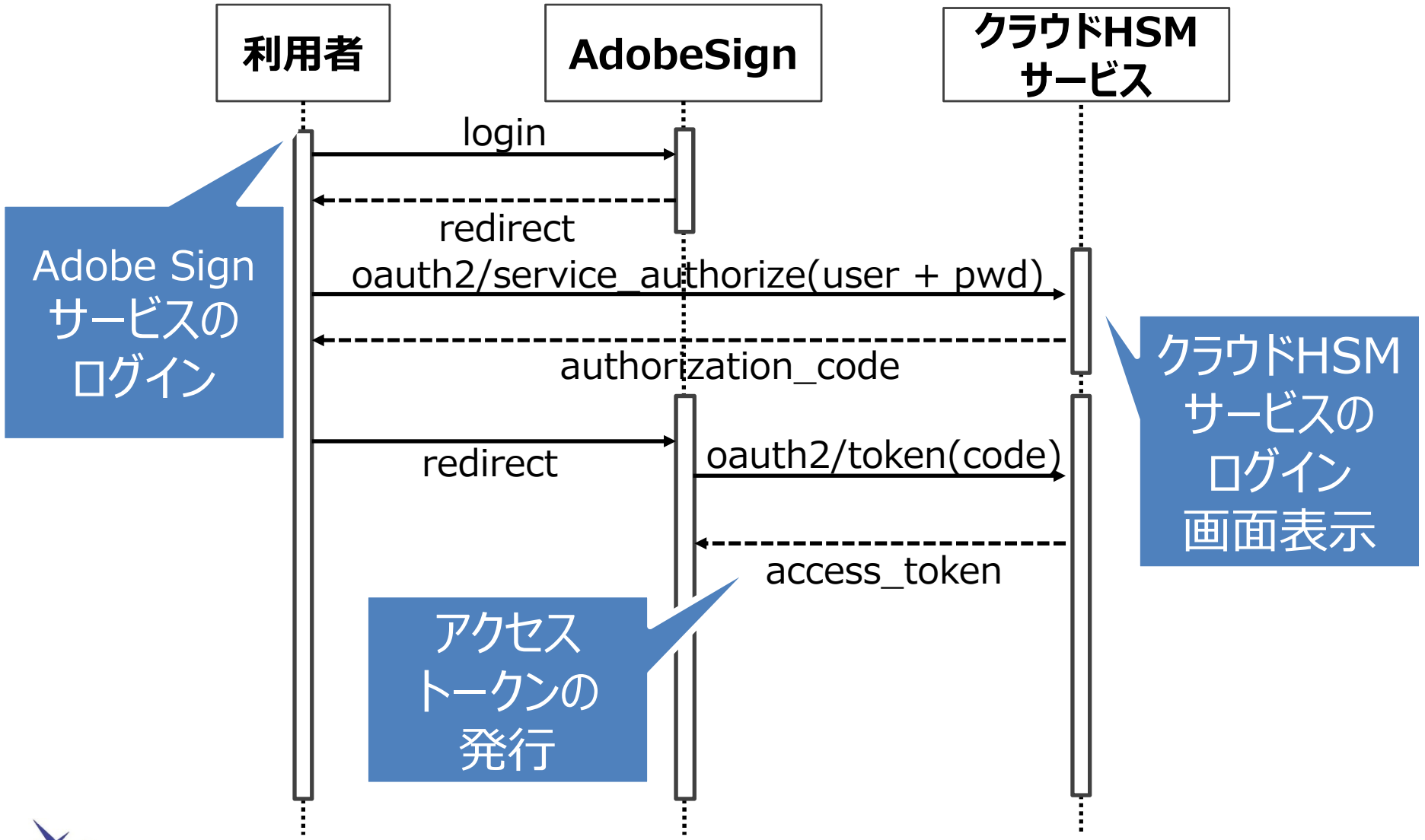
	メソッドパス	概要
1	info	サーバの基本情報を返します。このパスのみ認証不要です。
2	oauth2/authorize	サービスユーザまたは署名鍵に対するOAuth2「Authorization Code flow」認証を行います。認証に成功したら認可コードをクライアントサービスに返します。
3	oauth2/token	認可コードをアクセストークン（認証済みチケット）に変換します。 アクセストークンは、 (1)サービスユーザの場合Bearerで、これ以降のリクエストに「Authorization: Bearer」ヘッダとして付加します。 (2)署名鍵の場合SADで、署名実行時に使用します。
4	auth/login	直接ユーザIDおよびパスワードからBearerを取得します。
5	auth/revoke	Bearer/SAD/リフレッシュトークンを無効にします。
6	credentials/list	現在のエンドユーザの所有する署名鍵エイリアス一覧を返します。
7	credentials/info	指定された署名鍵エイリアスに対応する証明書およびその他の情報を返します。
8	credentials/authorize	直接PINをSADに変換します。
9	credentials/extendTransaction	既存のSADをもとに新しいSADを発行します。
10	signatures/signHash	署名を実行します。※PINではなくSADを入力します。
11	signatures/timestamp	タイムスタンプを取得します。

タイムスタンプもJSON形式でリクエスト可能

クラウドHSMサービスのCSC仕様対応

①認証処理

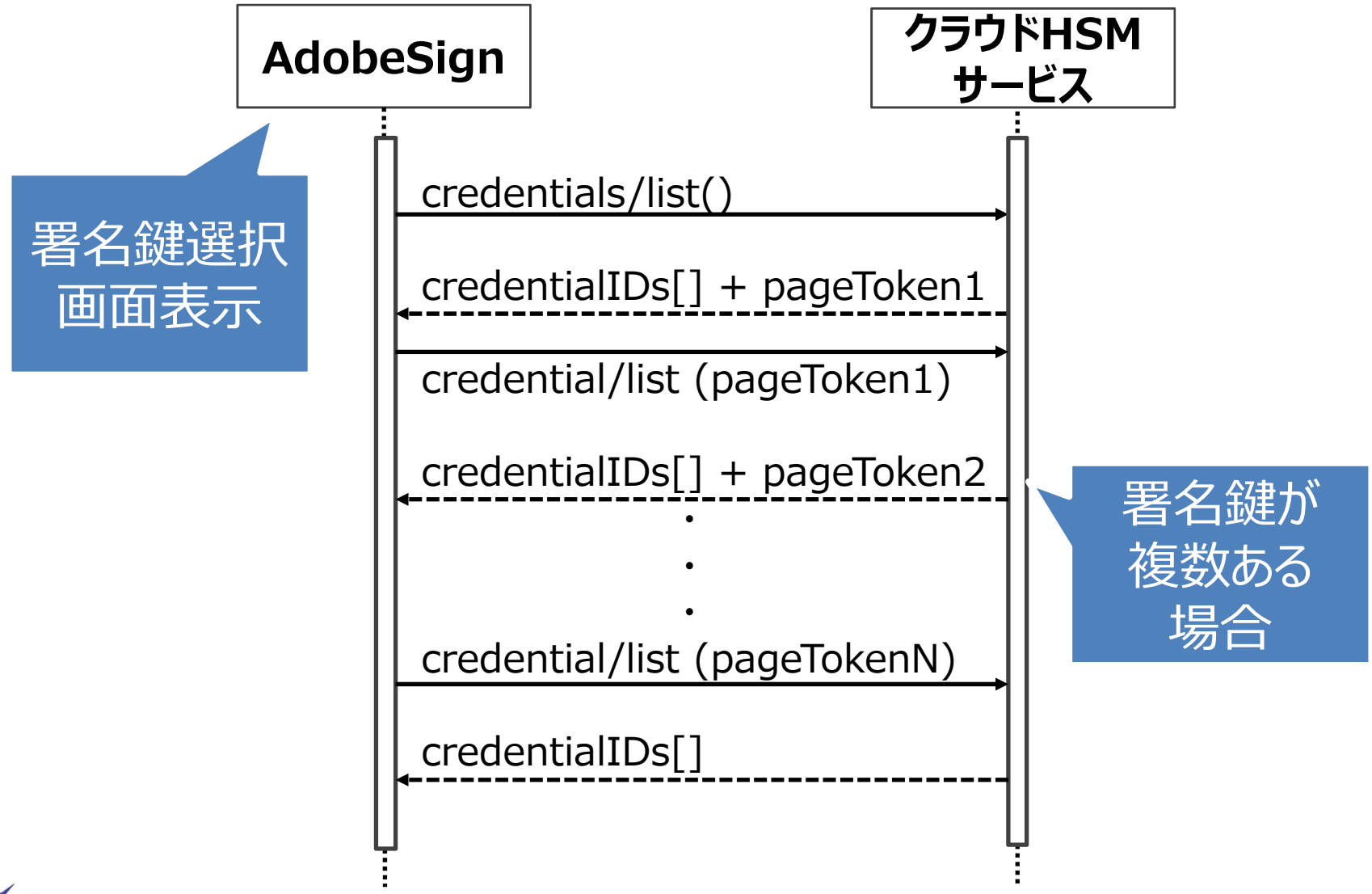
CSC_0.1.7.9_PR 13.3章に対応



クラウドHSMサービスのCSC仕様対応

②証明書リスト取得処理

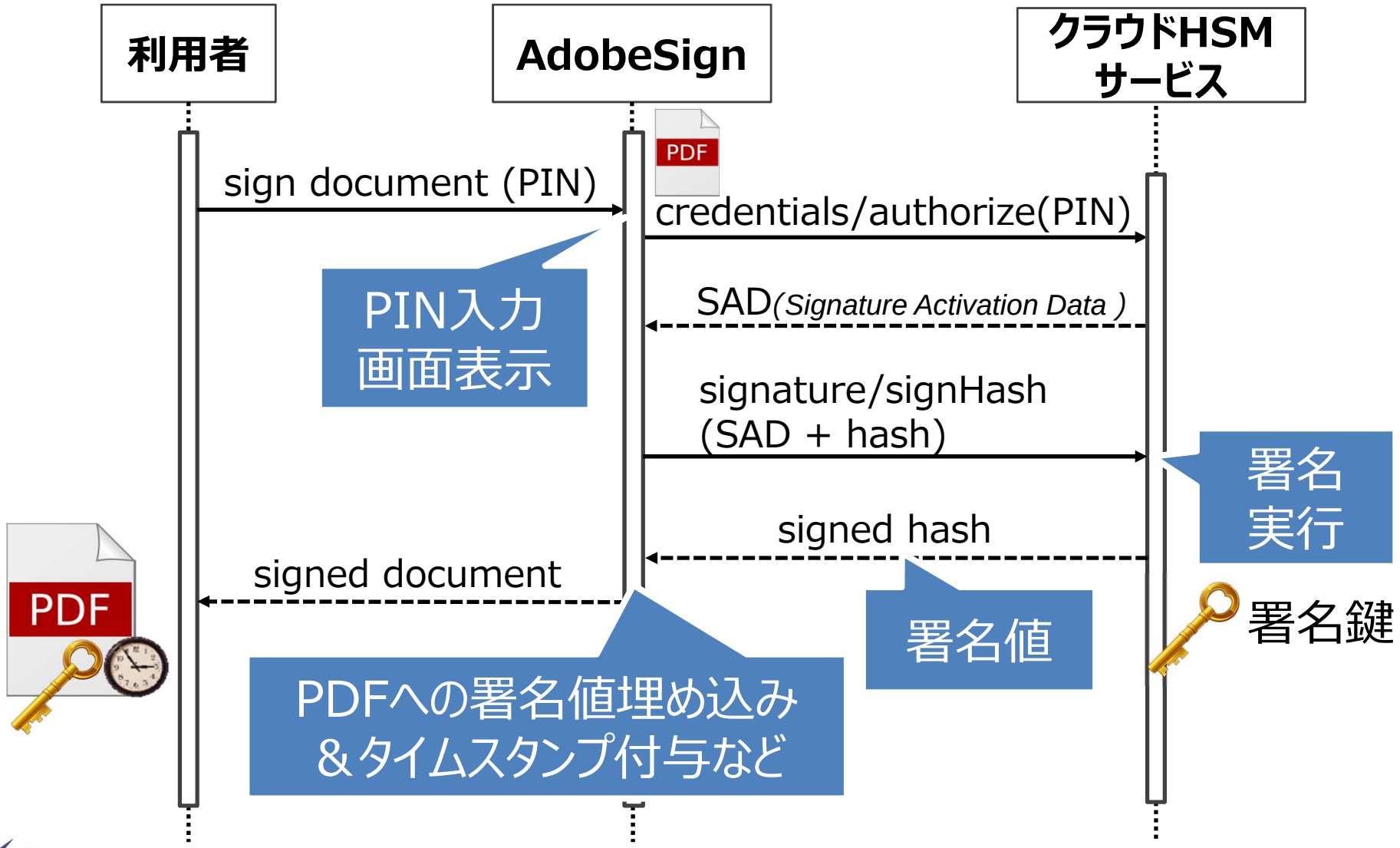
CSC_0.1.7.9_PR 13.6章に対応



クラウドHSMサービスのCSC仕様対応

③署名処理

CSC_0.1.7.9_PR 13.8章に対応



まとめ

・リモート署名／クラウド署名の実現により、PC・スマホを問わず、ブラウザのみでかんたんに電子署名ができる環境に

・リモート署名事業者に求められる安全性および信頼性についての指標についてJT2Aのリモート署名TFで検討しガイドラインを作成中

ご清聴ありがとうございました。