NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

PKI Day 2014

新しい電子署名

～クラウド/モバイル署名と非PKI署名～

宮地 (miyachi@langedge.jp)
電子署名WGサブリーダー/スキルアップTFリーダー
（有限会社ラング・エッジ）

2014 年 3 月 13 日

最初に:電子署名とは？

JNSA

http://ja.wikipedia.org/wiki/電子署名 より

電子署名とは、電磁的記録（電子文書）に付与する、電子的な徴証であり、紙文書における印やサイン（署名）に相当する役割をはたすものである。主に本人確認、偽造・改竄(かいざん)防止のために用いられる。

つまり以下２項目を目的とした技術であると言える。

１:否認防止（本人確認）→「誰が」
２:改ざん防止（真正性確認）→「何に」

PKIを利用した電子署名は電子署名の一種に過ぎない。
本日は初心に戻り電子署名を見直してみる。

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

もう1つ：利用環境の変化

JNSA

ご存知のように近年ITの利用環境が激変している。

クライアント環境：

PC利用からモバイル端末を含んだ環境へ広がった。
別の見方としてスマートフォンは個人端末となった。

サーバ環境：

オンプレミスからクラウドへ環境が広がった。
単独サービスから複数サービスのマッシュアップへ。
認証技術の標準化により認証レベルの明確化。

クラウドとモバイルの2つの環境変化が同時に進行中。
本日は利用環境の変化から電子署名を見直してみる。

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

新しい電子署名：本日のアジェンダ

JNSA

1）全体の説明（宮地）
電子署名の技術分析と分類他

2）最新トレンドの紹介（亀田さん）
クラウド署名：AWS CloudHSM
非PKI署名：OCRAワンタイムパスワード

3）クラウド署名とモバイル署名（宮地）

4）電子署名WGの活動計画（宮地）

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

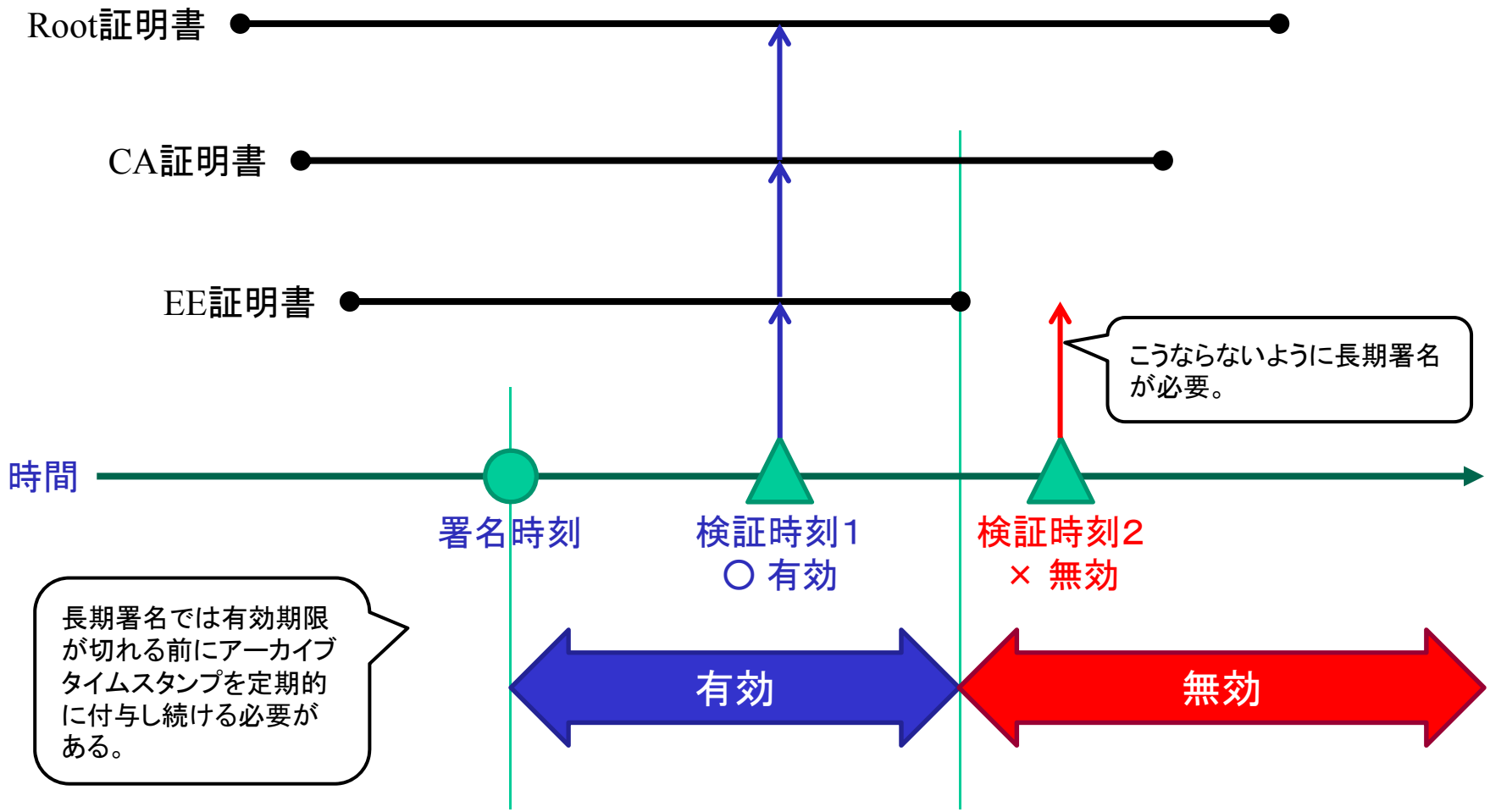
電子署名の技術分析と分類

JNSA

大分類	小分類	特徴	補足
PKI電子署名	従来のPKI電子署名（日本署名法型）	Shell model により有効期限が切れる前に再タイムスタンプが必要	間違い無いが面倒クラウドやモバイルへの対応が望まれている
	新しいPKI電子署名（ドイツ署名法型）	Chain model によりアルゴリズムが危殆化しない限り再タイムスタンプは不要	最近PKIモデルが日本と異なる事が判明運用が日本型より楽でも相互運用性は？
非PKI電子署名	ハッシュ応用やワンタイムパスワード	ガードタイム方式やハッシュツリー応用等の新技術	用途限定では普及している分野もあり事例もある
	エビデンス保管型（米国署名法型）	証拠を残す事で本人確認や真正性を担保	米国型クラウド署名で採用されている（クラウド署名で説明）

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

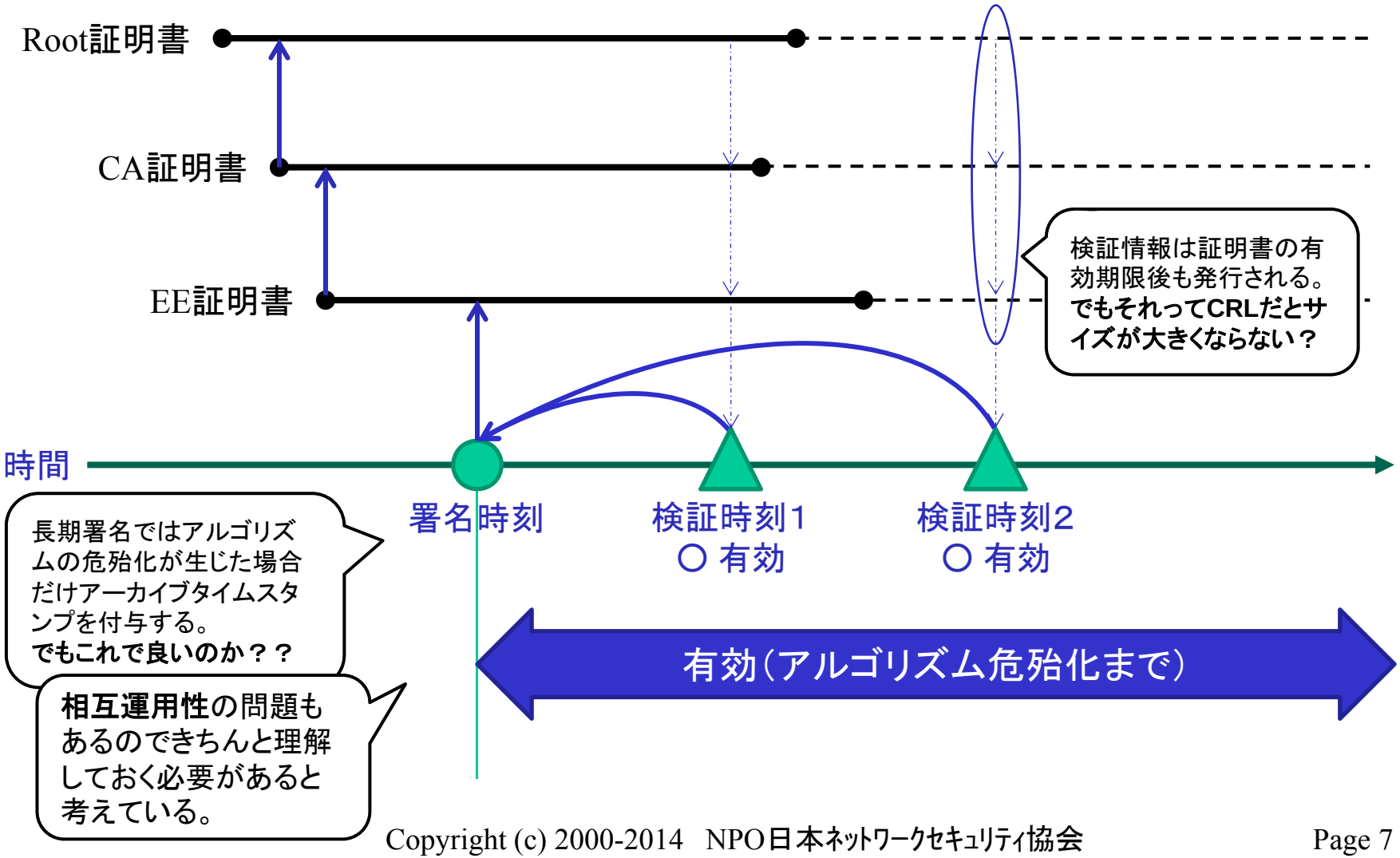
PKI電子署名：Shell model（日本他）



PKI電子署名：Chain model（ドイツ採用）

JNSA

※ 要調査！電子署名WGで調査予定。



非PKI電子署名：ガードタイム方式

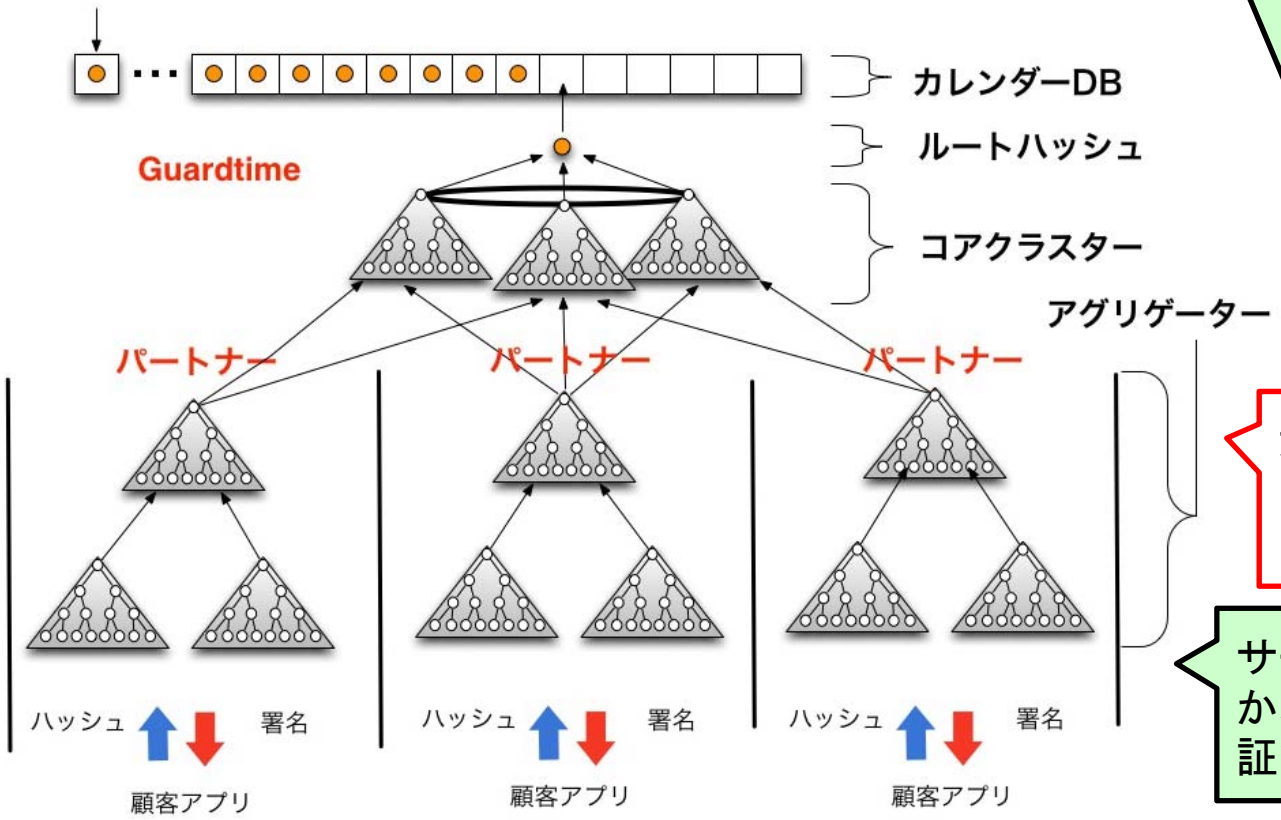
公表コード：カレンダーを結合して毎月１個のハッシュ値を生成し公文書館に保管される新聞に掲載。

検証カレンダー：複数のデータから生成したハッシュ値を結合し世界で毎秒１個のハッシュ値を生成しネット上に公開。

検証：オリジナルデータ・取得したキーレス署名・カレンダーを使って計算したハッシュ値を新聞に公表されたハッシュ値と照合し、データの非改ざん性を検証。

1970 January 1st 00:00:00

http://www.guardtime.com/



非PKIの根拠は、証明書等の信頼チェーンでは無く、新聞に公開されたハッシュ値を利用して信頼性を確保する為。単独で検証が可能。

全て数学的な仕組みの為にハッシュアルゴリズム危殆化まで有効である。

ガードタイム社はシンガポールに本社があり欧米で使われている。標準化が望まれる。

サーバ署名やタイムスタンプのかわりに使えるが「誰が」は保証できない。

非PKI電子署名：電子証拠 (Digital Evidence)

JNSA

米国の電子署名法はPKI電子署名は要求していない。

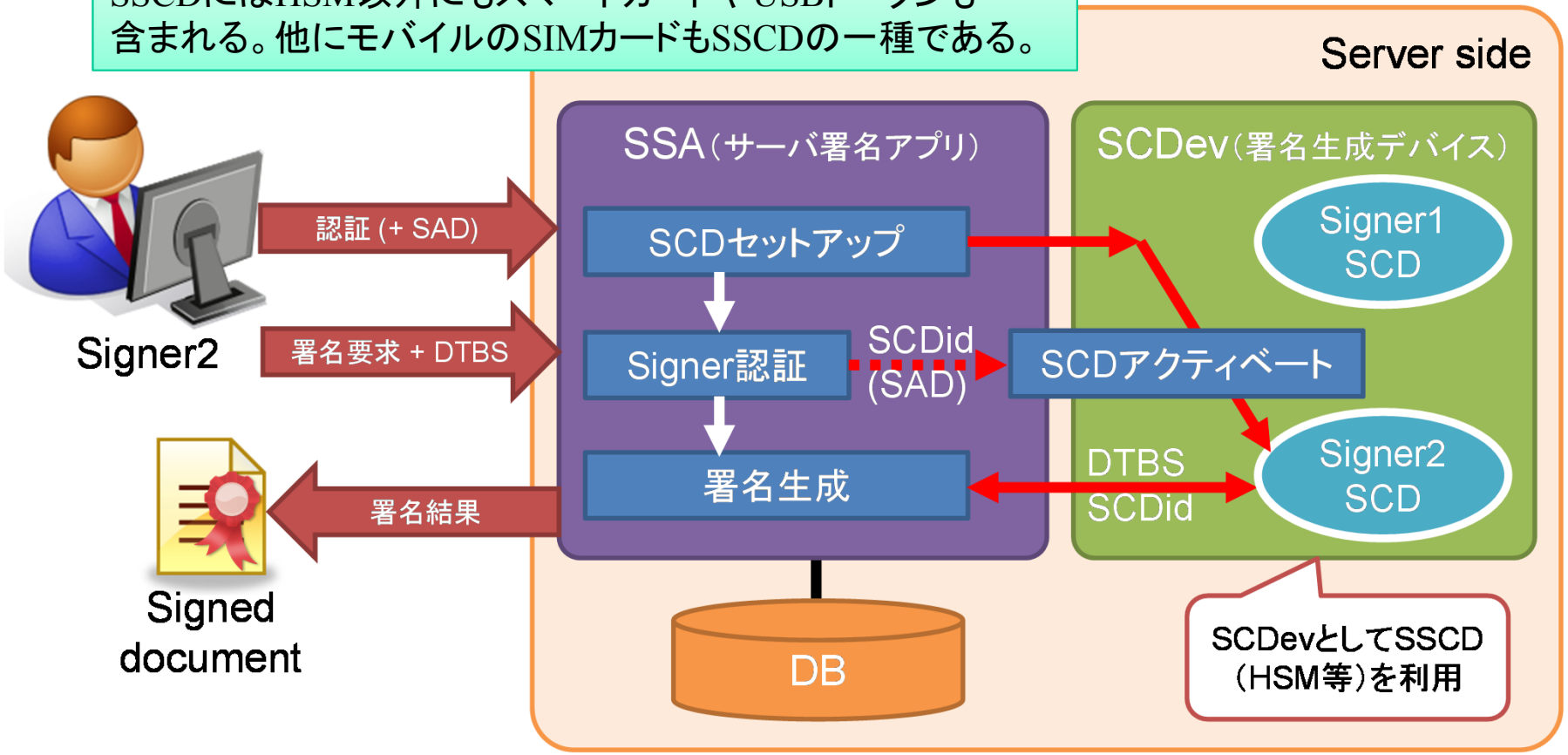
米国電子署名法の電子署名の定義：
「契約に添付された、あるいは論理的にその契約と関連づけられる電子音、電子的記号、または電子的プロセス」

つまり何らかの電子的なエビデンス（証拠）があれば良い。
電子的プロセスと言う意味ではクリックによる同意の証拠を保管。
電子的な同意プロセスとその電子証拠（Digital Evidence）が重要。
電子証拠の一種としてPKI電子署名も含まれるがより広く捉える。

※ 米国/英国ではDigital Evidenceのガイドラインやルールがある。
http://en.wikipedia.org/wiki/Digital_evidence Digital Evidence (Electronic Evidence)
http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

秘密鍵を守る：SSCD（Secure Signature Creation Device）

SSCDにはHSM以外にもスマートカードやUSBトークンも含まれる。他にモバイルのSIMカードもSSCDの一種である。



DTBS	Data to be Signed
SAD	Signer's Activation Data
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCDid	Signature Creation Data Identifier
SSA	Server Signing Application
HSM	Hardware Security Module
SSCD	Secure Signature Creation Device

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

最新トレンドの紹介

JNSA

JIPDEC客員研究員／日本セーフネット株式会社
亀田 治伸 氏

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

クラウド署名とモバイル署名

JNSA

クラウドとモバイルは表裏一体の関係。
主なクラウド署名サービスはモバイルに対応済み。

クラウド:

- クラウドは単にサービスをクラウド上に置くだけでは無い。
- REST API によりマッシュアップ可能であることが重要。
- 本日はクラウド署名をAPIから分析する。

モバイル:

- モバイル(スマートフォン等)の利用は今や大前提になった。
- PCと異なりモバイルはパーソナル端末と言う特徴がある。
- 本日はサーバ(クラウド)との連携した署名利用を分析する。

主なクラウド署名サービスの現状

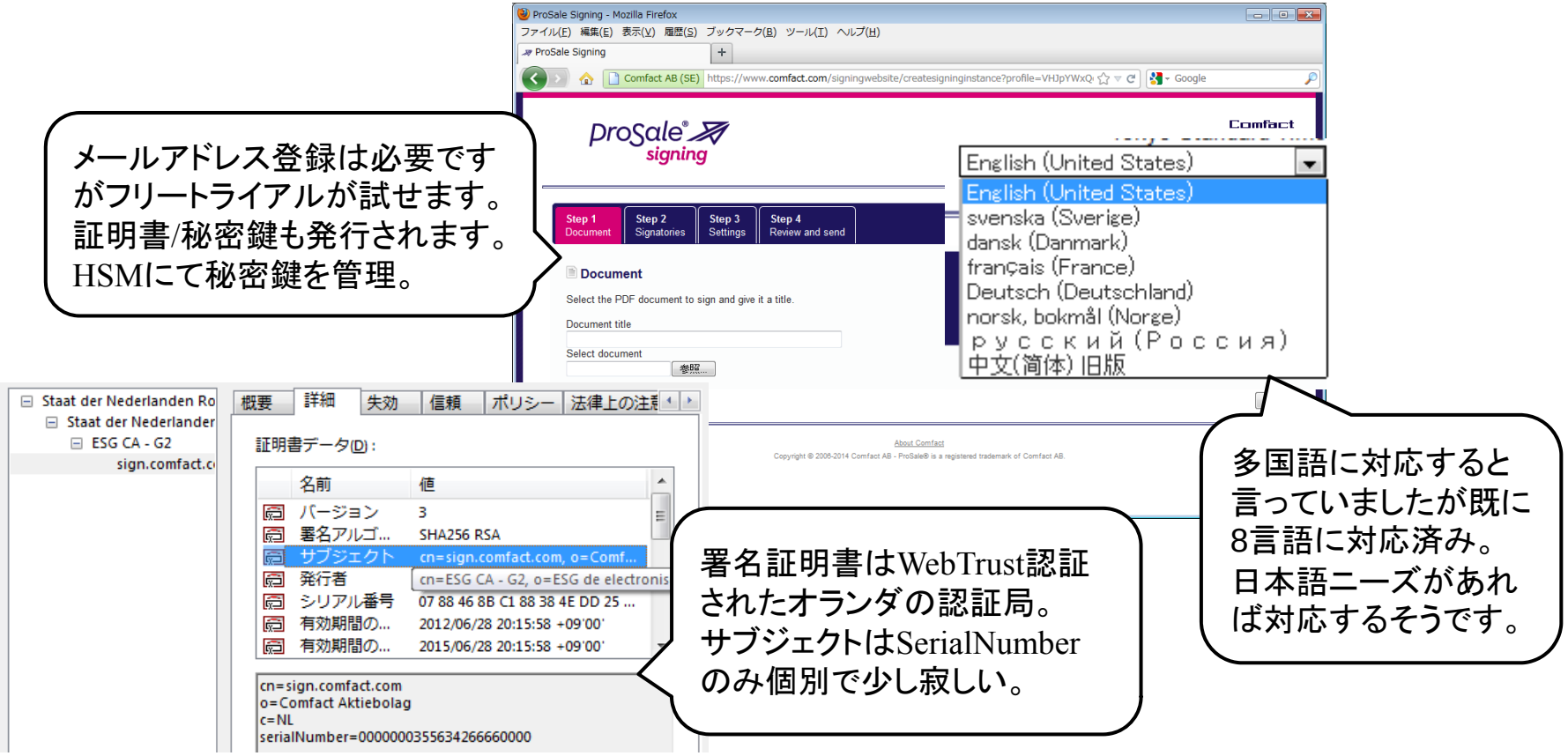
サービス名	種類	入出力	API他
ProSale Signing (Comfact AB) スウェーデンの会社	PKI電子署名	入出力：PDF形式	API利用可能（OASIS DSS可能） 認証は独自とSAMLに対応 証明書と秘密鍵は自動作成される モバイルアプリはまだ無いようだ 欧州ETSI標準に準拠予定
EchoSign (Adobe Systems)	PKIサーバ署名	入出力：PDF形式	REST API利用可能 認証は独自か？（OAuthっぽいが…） PC/MacOSのAdobe Readerで利用可能 iOS/AndroidのAdobe Readerでも対応 米国署名法に対応？
SignNow (Barracuda Networks)	非PKI電子署名 （合意システム）	入力：doc/docx/pdf/png 出力：PDF形式	REST API利用可能（シンプルなAPI） 認証は独自とOAuth2.0に対応 iOS/Androidアプリ公開中 米国署名法に対応？
DocuSign (DocuSign, Inc.) - MSと提携 -	PKIサーバ署名	入出力：MS-Office文書 及びPDF形式 ※Office365と連携可能 OneDriveに保存	SOAPのAPIも提供（RESTへ移行中？） REST API利用可能（API数が多い！） 認証はOAuth2.0に対応 Windows Azure Active Directoryも対応 iOS/Androidアプリ公開中 米国署名法に対応？

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

クラウド署名１：ProSale Sigining

https://www.comfact.com/Product/Signing/

スウェーデン Comfact社が開始したPKIクラウド署名サービス。
Comfact社はETSI Plugtestにも参加している会社。
電子署名以外にe-Seal（法人電子署名）やHSM等も扱っている。



メールアドレス登録は必要ですがフリートライアルが試せます。証明書/秘密鍵も発行されます。HSMにて秘密鍵を管理。

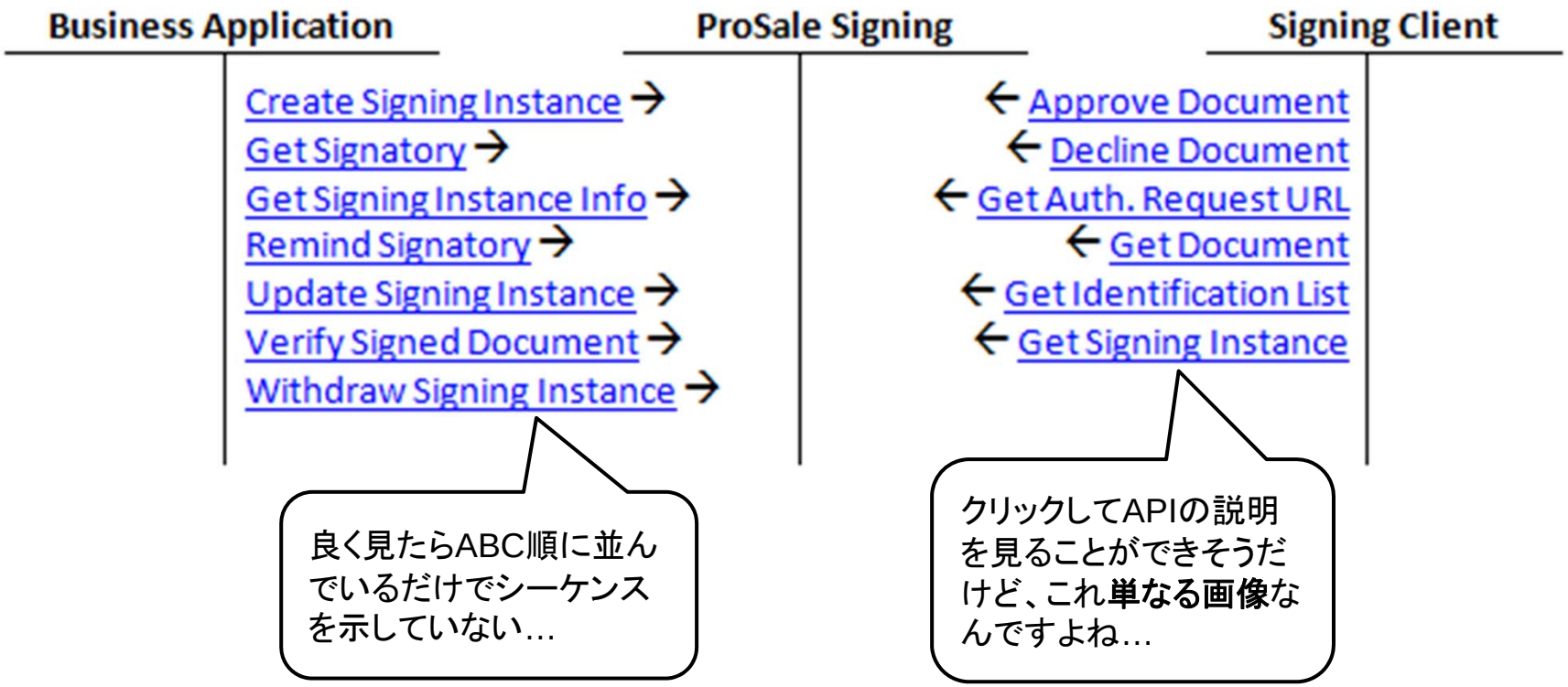
多国語に対応すると言っていましたが既に8言語に対応済み。日本語ニーズがあれば対応するそうです。

署名証明書はWebTrust認証されたオランダの認証局。サブジェクトはSerialNumberのみ個別で少し寂しい。

クラウド署名１: ProSale Sigining のAPI

https://www.comfact.com/Product/API/

※ まだAPIの詳しい情報は無いようだ。要求中。



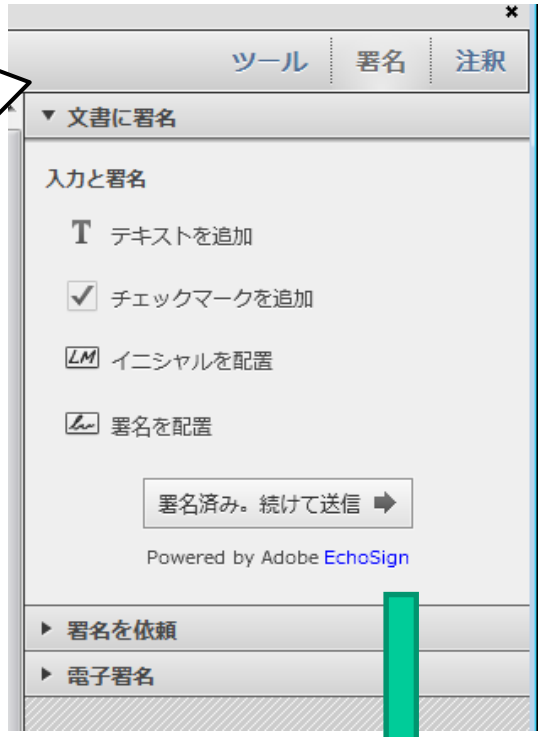
欧州標準化完了がまもなくなのでこれからに期待か…
PKIクラウド署名の実例としては期待できそう。

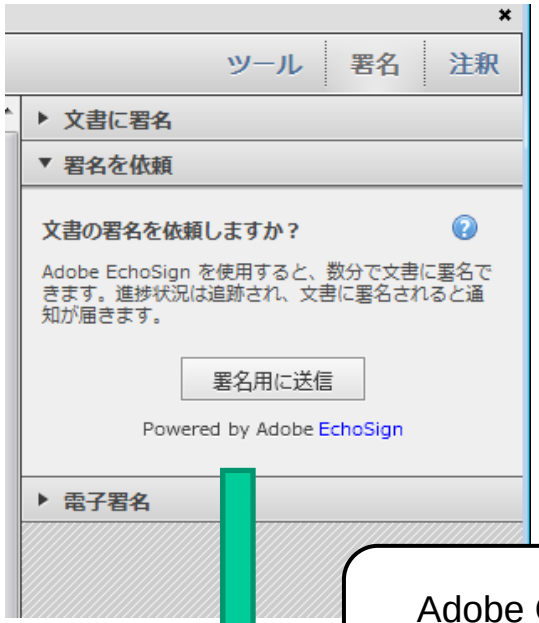
クラウド署名２：EchoSign

https://www.echosign.adobe.com/

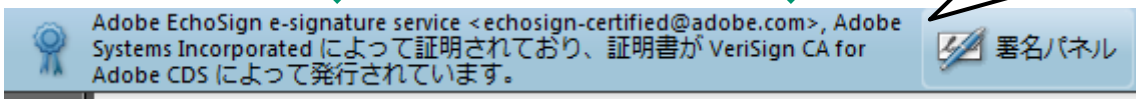
Adobeが買収したクラウド署名サービス。
現在はAdobe Reader/Acrobatに統合されたサービスに。

Adobe Reader からも署名タブで利用可能。





Adobe CDS 証明書で
PKI電子署名される。
<echosign-certified@adobe.com>



クラウド署名２：EchoSign のAPI

https://secure.echosign.com/public/docs/restapi/v1

APIの感想：
シンプルで良く
まとまっている。

EchoSign REST API Version 1

tokens : Access Tokens （認証してアクセストークンを取得）		
	post /auth/tokens	Issues an access token for a user of an application.
transientDocuments : Transient Documents（ドキュメントのアップロードとドキュメントID取得）		
	post /transientDocuments	Uploads a document and obtains the document's ID.
agreements : Agreements（合意処理　**※否認防止・本人確認の為に重要**）		
	post /agreements get /agreements get /agreements/{agreementId} get /agreements/{agreementId}/documents get /agreements/{agreementId}/documents/{documentId} get /agreements/{agreementId}/auditTrail get /agreements/{agreementId}/combinedDocument put /agreements/{agreementId}/status	Creates an agreement. Sends it out for signatures. Retrieves agreements for the user. Retrieves the latest status of an agreement. Retrieves the IDs of all the. Retrieves the file stream of a document of an agreement. Retrieves the audit trail of an agreement identified by agreementid. Gets a single combined PDF document for the documents associated. Cancels an agreement.
reminders : Reminders （催促）		
	post /reminders	Sends a reminder for an agreement.
users : Users （ユーザ操作）		
	post /users get /users	Creates a new user in the Echosign system Gets all the users in an account.
libraryDocuments : Library Documents （保管ドキュメント操作）		
	get /libraryDocuments get /libraryDocuments/{libraryDocumentId} get /libraryDocuments/{libraryDocumentId}/documents get /libraryDocuments/{libraryDocumentId}/documents/{documentId} get /libraryDocuments/{libraryDocumentId}/auditTrail get /libraryDocuments/{libraryDocumentId}/combinedDocument	Retrieves library documents for a user. Retrieves the details of a library document Retrieves the ID of the document associated with library document Retrieves the file stream of a library document. Retrieves the audit trail associated with a library document Retrieves the combined document associated with a library document

クラウド署名３：SignNow

https://signnow.com/

Barracuda Networks, Inc.のクラウド（モバイル）署名サービス。
以前はPKI電子署名をサーバ署名として付与していたはず…
試してみたら現在は非PKI型になっているようだ。

PKI電子署名の署名フィールド作成は可能。

メールアドレスを登録すると1ヶ月のフリートライアルが可能。

PKI電子署名は付与されない。

クラウド署名３：SignNow のAPI

https://signnow.atlassian.net/wiki/display/SAPI/REST+Endpoints

SignNow API

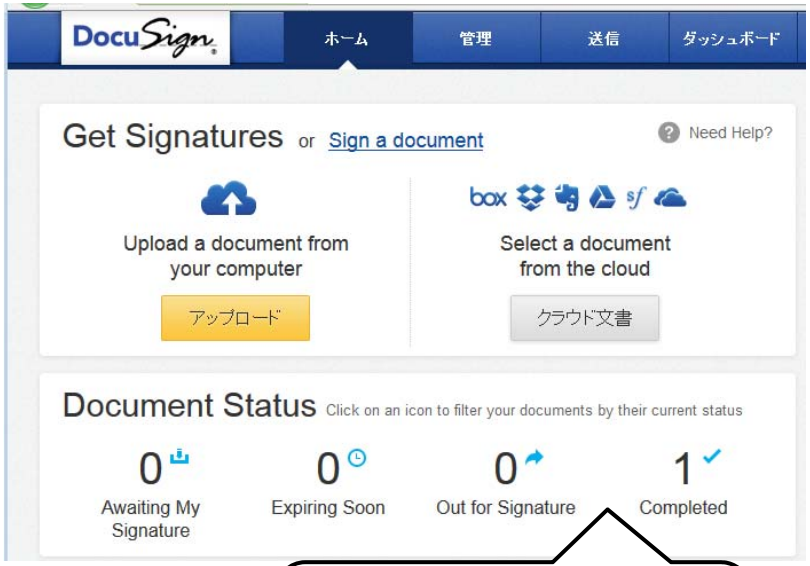
/user （ユーザ操作）	
POST /user	Create a user. Recently changed to not generate a token.
GET /user	Retrieve a user resource.
GET /user/documentsv2	Retrieve a list of the user's documents.
/oauth2 （認証してアクセストークン取得）	
POST /oauth2/token	Request an access token for a user.
GET /oauth2/token	Verify an access token for a user.
/document （ドキュメントと署名の処理）	
POST /document	Uploads a file and creates a document.
PUT /document/<id>	Update an existing document.
GET /document/<id>	Retrieve a document resource.
GET /document/<id>/download	Download a collapsed document.
POST /document/<id>/invite	Create an invite to sign a document.
POST /document/<id>/download/link	Creates a one-time use URL for anyone to download the document as a PDF.
POST /notaryinvite	Create a notary invite to sign a document.

APIの感想：
シンプルだけど
シンプルすぎる
かも？

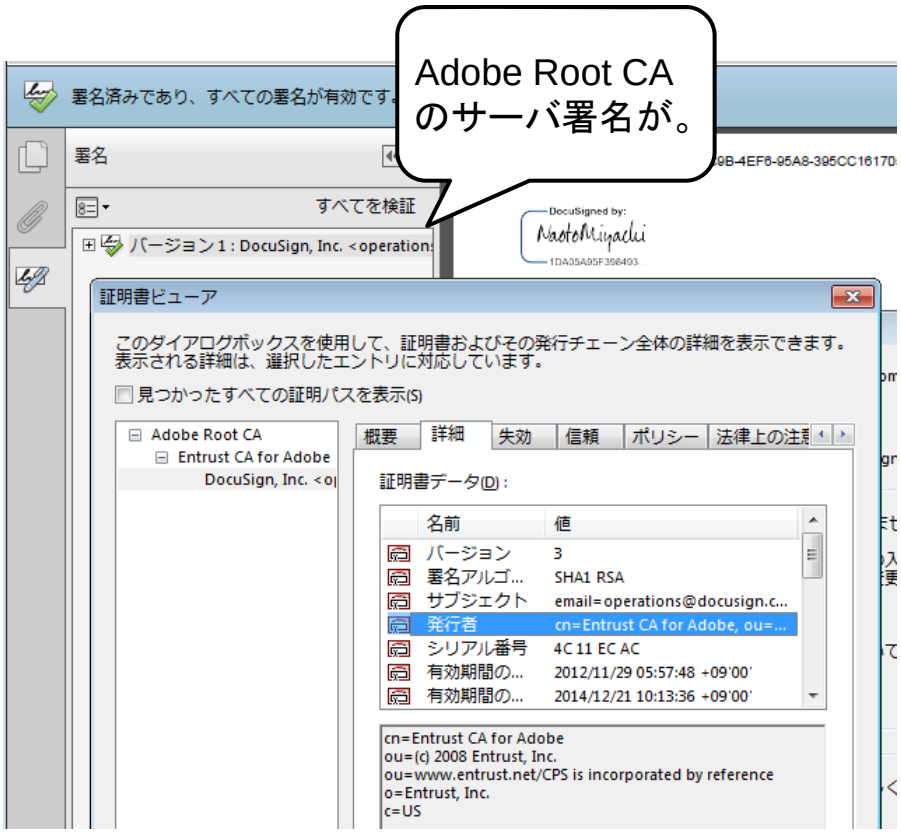
クラウド署名４：DocuSign

https://www.docusign.com/

DocuSign, Inc.のクラウド署名サービス。
以前は非PKI電子署名だったはず…
試してみたら現在はPKI型のサーバ署名になっているようだ。



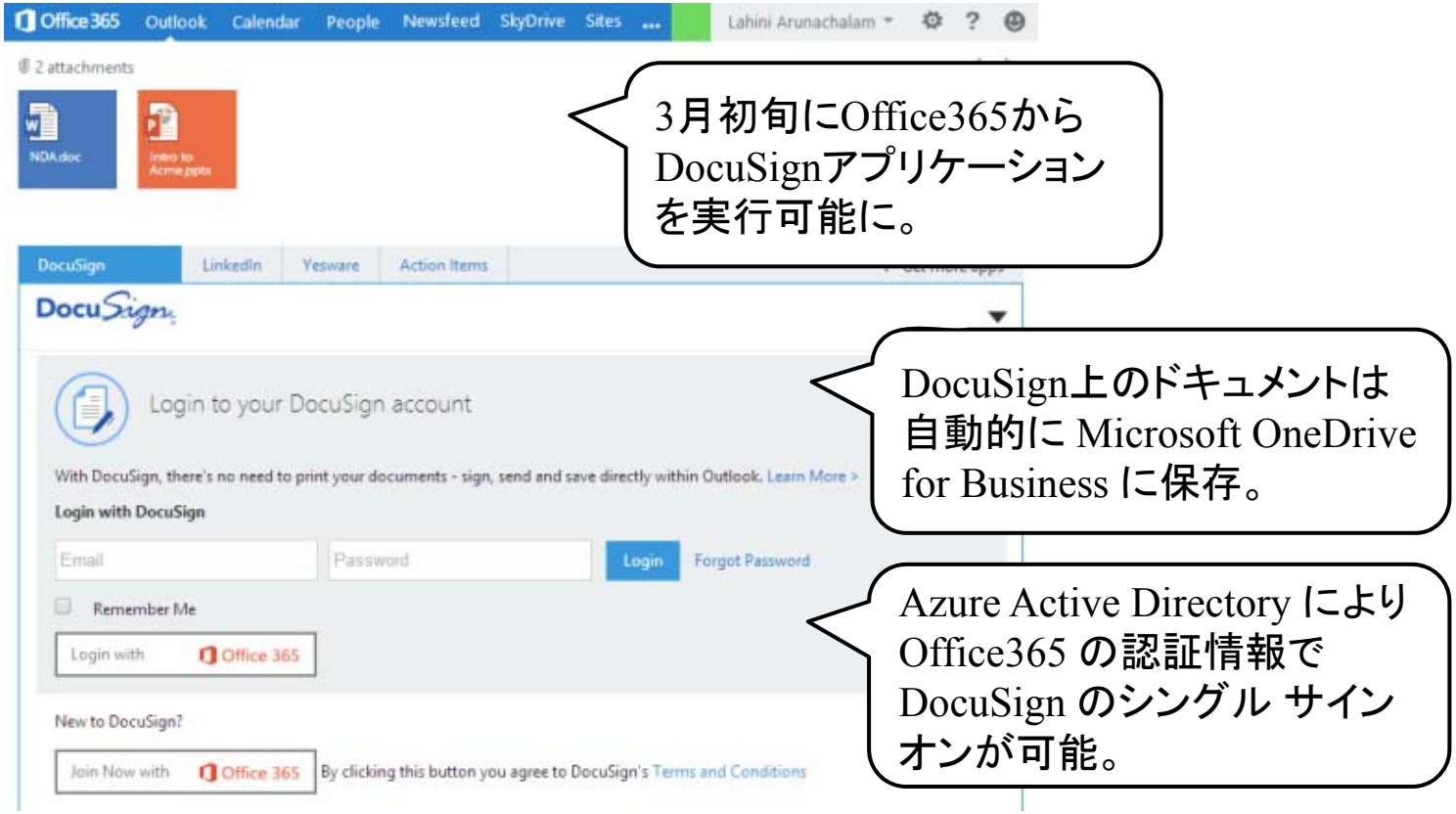
メールアドレスを登録すると2週間のフリートライアルが可能。



クラウド署名４：DocuSign と Office365

http://www.microsoft.com/en-us/news/press/2014/feb14/02-17docusignpr.aspx

2014年2月17日に米MicrosoftがDocuSignと提携を行い、「Office 365」に電子署名機能を統合すると発表。



3月初旬にOffice365から DocuSignアプリケーション を実行可能に。

DocuSign上のドキュメントは 自動的に Microsoft OneDrive for Business に保存。

Azure Active Directory により Office365 の認証情報で DocuSign のシングル サイン オンが可能。

クラウド署名４：DocuSign のAPI

https://www.docusign.com/sites/default/files/REST_API_Guide_v2.pdf

DocuSign REST API version 2（抜粋）

/oauth2 （認証してアクセストークン取得）	
/login_information （ユーザ情報）	
/accounts （DocuSign操作）	
/accounts/{accountId}	Account for information operations.
/accounts/{accountId}/billing_plan	Account billing plan operations.
/accounts/{accountId}/brands	Account bland profile operations.
/accounts/{accountId}/connect	DocuSign Connect operations.
/accounts/{accountId}/custom_fields	Gets a list of all envelope custom fields associated.
/accounts/{accountId}/envelopes	Send envelopes, get envelopes information.
/accounts/{accountId}/folders	Account folder operations.
/accounts/{accountId}/groups	Group operations.
/accounts/{accountId}/permission_profiles	Permission profiles operations.
/accounts/{accountId}/recipient_names	Get Recipient Names.
/accounts/{accountId}/search_folders	Get List of Envelopes in a Folders.
/accounts/{accountId}/settings	Account setting operations.
/accounts/{accountId}/templates	Template of account.
/accounts/{accountId}/unsupported_file_types	Get List of Unsupported File Types.
/accounts/{accountId}/users	Account user operations.
/accounts/{accountId}/views/console	Post Authentication View.
/accounts/provisioning	Get Account provisioning information.
/billing_plans （支払プラン情報）	

APIの感想：
ここに書いたのはほんの一部。
全120APIある。
高機能のようだが難しそう…

既存クラウド署名サービスAPIまとめ

JNSA

- 多くのサービスが OAuth2.0 認証をサポート。
  - 認証は重要。今後 OpenID Connect 等の対応も期待。
- ほぼ全てのサービスが REST API をサポート。
  - クラウドサービスと言うならREST APIは必須！
- API は標準化されておらず各サービスでバラバラ。
  - サービス内容も異なるので仕方が無い面もある。
  - OASIS DSS (XML署名) もあるがさすがに古い…
- 署名よりも合意プロセスを重視した API がメインか。
  - 米国系のサービスが多い為にこれも仕方が無い。
  - 今後は欧州系PKI電子署名サービスに期待できそう。
- cURL による REST API の利用例も多く見かけた。
  - Good! ハンズオンの勉強会ができそう！

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

モバイル署名：はじめに

モバイル署名は欧州では昔から注目されていた。
現在 ETSI にてモバイル長期署名フレームワーク策定中。

SR 019 020 Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment
http://www.e-signatures-standards.eu/mission

※ 現在はドラフトが上記URLから入手可能。
※ CAdES/XAdES/PAdES等と同じくESIで策定している。

フレームワークを策定して、シナリオ毎に利用ケースを想定して普及と標準化を目指している。
本日は主なシナリオを紹介する。

モバイル署名のシナリオ

JNSA

■ ローカル署名：モバイル自身で署名を行うシナリオ
- シナリオ1：モバイルから直接署名サーバ呼び出して署名
- シナリオ2：サービス提供者から署名サーバ経由で署名
- シナリオ3：モバイル自身で署名生成を全て行う

■ リモート署名：署名サーバで署名を行うシナリオ
- シナリオ1：モバイルから直接署名サーバ呼び出して署名
- シナリオ2：サービス提供者から署名サーバ経由で署名

※ モバイルは署名の承認処理を行う

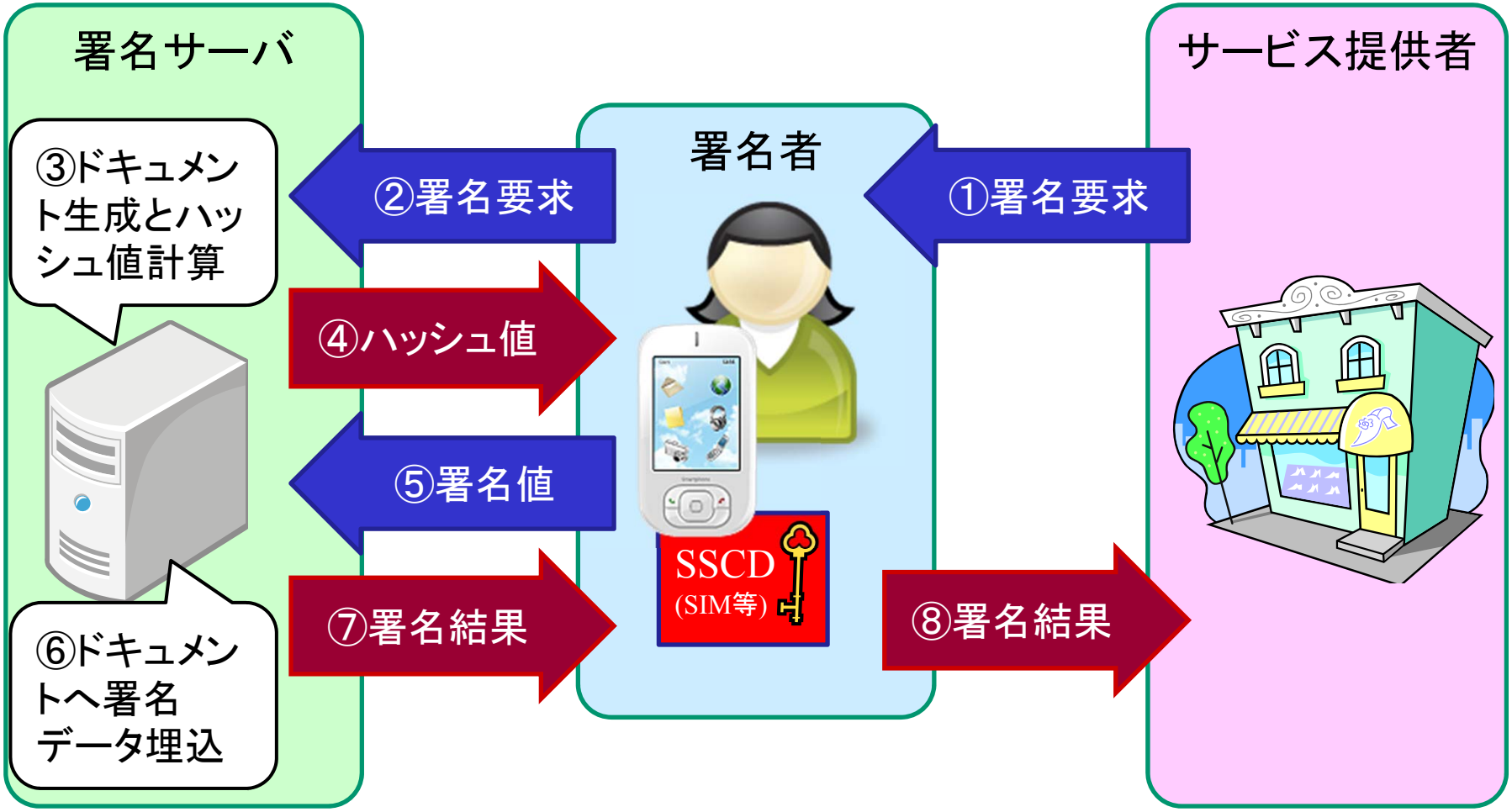
■ 鍵分割署名：モバイルと署名サーバで鍵を分割して保有

■ 署名検証：モバイルからの要求で検証サーバが検証する

※ ETSI仕様とは少し異なる分類。ETSIもまだまとまっていない？

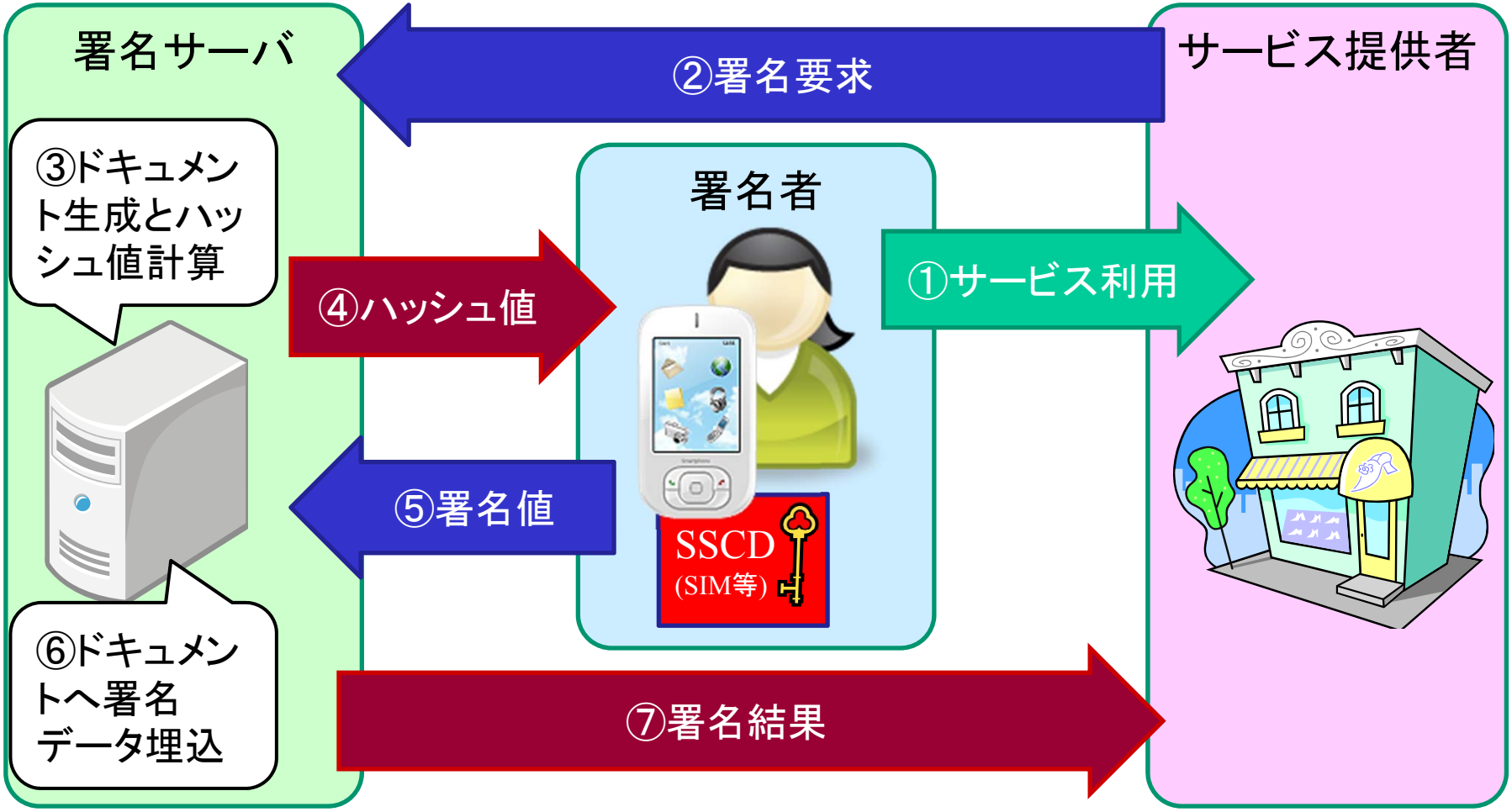
モバイル署名：ローカル署名シナリオ1

モバイルから直接署名サーバを呼び出して署名



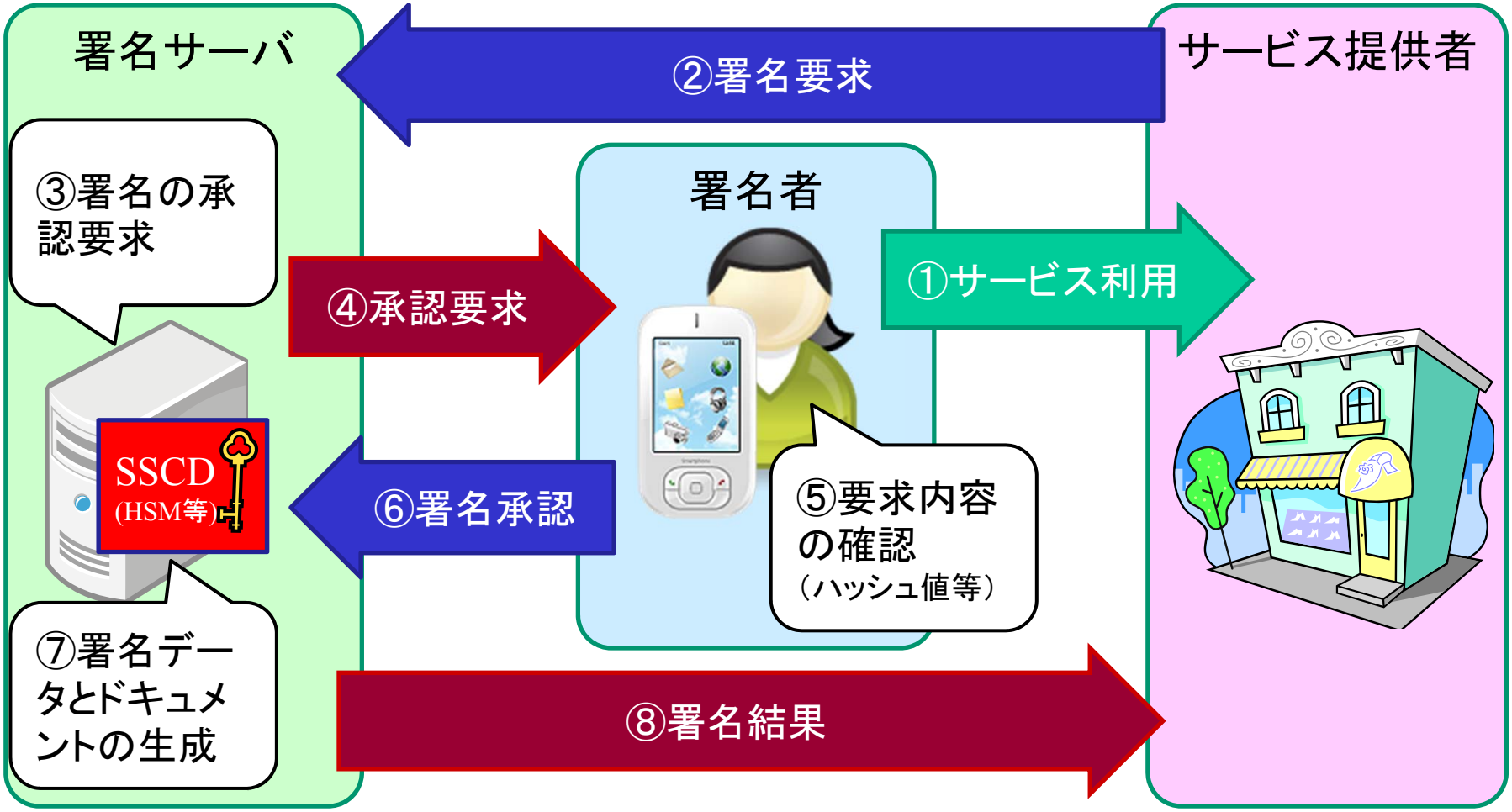
モバイル署名：ローカル署名シナリオ2

サービス提供者から署名サーバ経由で署名



モバイル署名：サーバ署名シナリオ2

サービス提供者から署名サーバ経由で署名



ETSIモバイル長期署名のまとめ

JNSA

- モバイルによる長期署名の標準化ニーズは強い。
  - モバイル長期署名がCAdES/XAdES/PAdESと同レベル。
- モバイルが非力な時代の影響が残っている。
  - 昔から使われているのでその時代の前提が多い。
  - 現在のスマートフォンやタブレットは能力が高い。
- クラウド利用において重要なAPIに全く触れていない。
  - 利用シナリオの分析と利点・問題点の整理がメイン。
- まだドラフトレベルで内容もまとめきれていない。
  - 今後も継続してチェックして行く必要はあるだろう。
- その他注目点。
  - 署名鍵の分割とは具体的にどうやるのか？
  - 検証シナリオはモバイルに限らず重要と考える。

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

クラウド署名・モバイル署名の考察

JNSA

■ REST API公開とモバイル連携が前提
- クラウド署名と言えばモバイル署名を含む
- API標準化やモバイルシナリオ整理が望ましい

■ 認証は重要（署名に必要なLoAを良く考える）
- 署名時にはID/パスワード以外の要素で認証を
- 認証レベルが担保されるならサーバ署名も可能

■ 秘密鍵のサーバ預託時にはSSCDでしっかり管理
- サーバ内のSSCD署名プロセス標準化も必要
- モバイルに秘密鍵を持つケースも考慮が必要

■ 非PKI電子署名も含めて考えて行く必要あり
- 電子エビデンスの調査や標準化

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

電子署名WGの活動計画

JNSA

スキルアップTFで新しいことにチャレンジ！

- 今年スキルアップTFでは勉強会を開いてきた。
- 来年は成果が残る活動をメインにしたい。

テーマ案：

- クラウド署名やサーバ署名の標準化
- 非PKI電子署名の調査（電子エビデンス）
- PKI署名に関しても新しい方式等の調査
- 試験環境（遊び場プロジェクト）の推進
- オープンソースプロジェクトの推進
- 一般（JNSA非会員）向けの勉強会実施

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会

これまでのスキルアップTF勉強会実績

JNSA

第1回：7月：長期署名入門
講師＞電子署名WGオールスター 宮崎氏、佐藤氏、石本氏、西山氏、宮地

第2回：8月：クラウド署名とHSM
講師＞タレス・ジャパン 住田氏、セーフネット/JIPDEC客員研究員 亀田氏、他

第3回：9月： jsrsasign / jsjws 勉強会
講師＞富士ゼロックス 漆嶌氏
補足＞JavaScriptによるRSA/PKIモジュールとJSON署名

そろそろネタ切れなので継続した勉強会は難しい。

第4回：10月： PDF電子署名仕様入門
講師＞ラング・エッジ 宮地

第5回：11月：クラウド時代のデータセキュリティ
講師＞ガードタイム 柳原氏
補足＞ガードタイム社による非PKI署名他

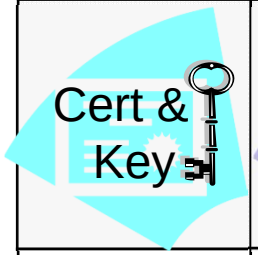
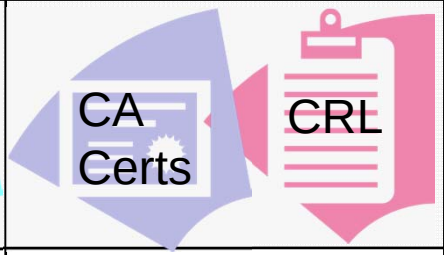
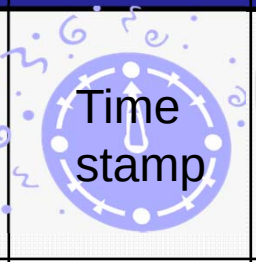
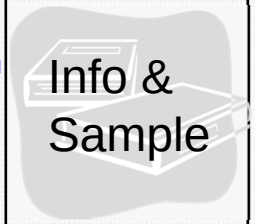
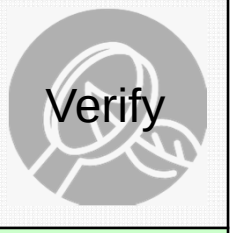
第6回：1月：電子署名WG合宿ダイジェスト

第7回：2月：オープンデータにおける署名・タイムスタンプの活用
講師＞ラング・エッジ 宮地

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

遊び場プロジェクト
～プログラマの為のお試しと教育の環境構築～

JNSA

CA機能				TSA機能	情報公開	署名機能	検証機能
							
証明書・鍵サービス	リポジトリ公開		OCSP発行	タイムスタンプ発行	ソース他公開	サービス提供	サービス提供
	HTTP	LDAP					
対話画面による発行	CA証明書は公開 CRLは定期的に更新 出来ればCSP/CP等も		証明書DBまたはCRL連動し発行	CA機能でTSA証明書を準備	各機能実装情報やサンプルを公開	APIや対話画面を用意してクラウド的にモバイル署名も考慮して検討する	
OpenSSLのCA機能認証連携	OpenSSLの簡易CA機能を利用画面は作成が必要		OpenSSLで可能？ocspオプション利用	準備完了 FreeTSA	Wiki, Blog GitHub 等	Ruby on Rails 等かCA機能と連携？FreeXAdES, jsrsasign等の利用	
証明書・秘密鍵は登録制等にして完全フリーは難しいかも。一応本人確認くらいはする？OCSPは最初は無くても良いかもしれない。				認定TSAからの提供も歓迎	長期署名サンプル等ノウハウも	クラウド署名の実証実験的にできるとベストHSM等使えると面白い	
JNSAではかつて「チャレンジPKI http://www.jnsa.org/mpki/index_j.html 」があった。今は使えない。							

興味を持った技術者がフリーで使えてプラグテストや実証実験にも使える！

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

クラウド署名・モバイル署名の実証実験

JNSA

目的（世界に先がけて標準化）:

認証と連携したクラウドの署名・検証をAPI化

→ 認証に OpenID Connect with OAuth2.0 等を利用しIdP連携
→ 出来ればSSCD（HSM）等も試したい（協力や協賛を募集）
→ 同意プロセス等も実際に実装してみて課題を調査検討
→ 機能を整理して将来は標準化やガイドラインへ

モバイル機器との連携を行う（モバイル署名）

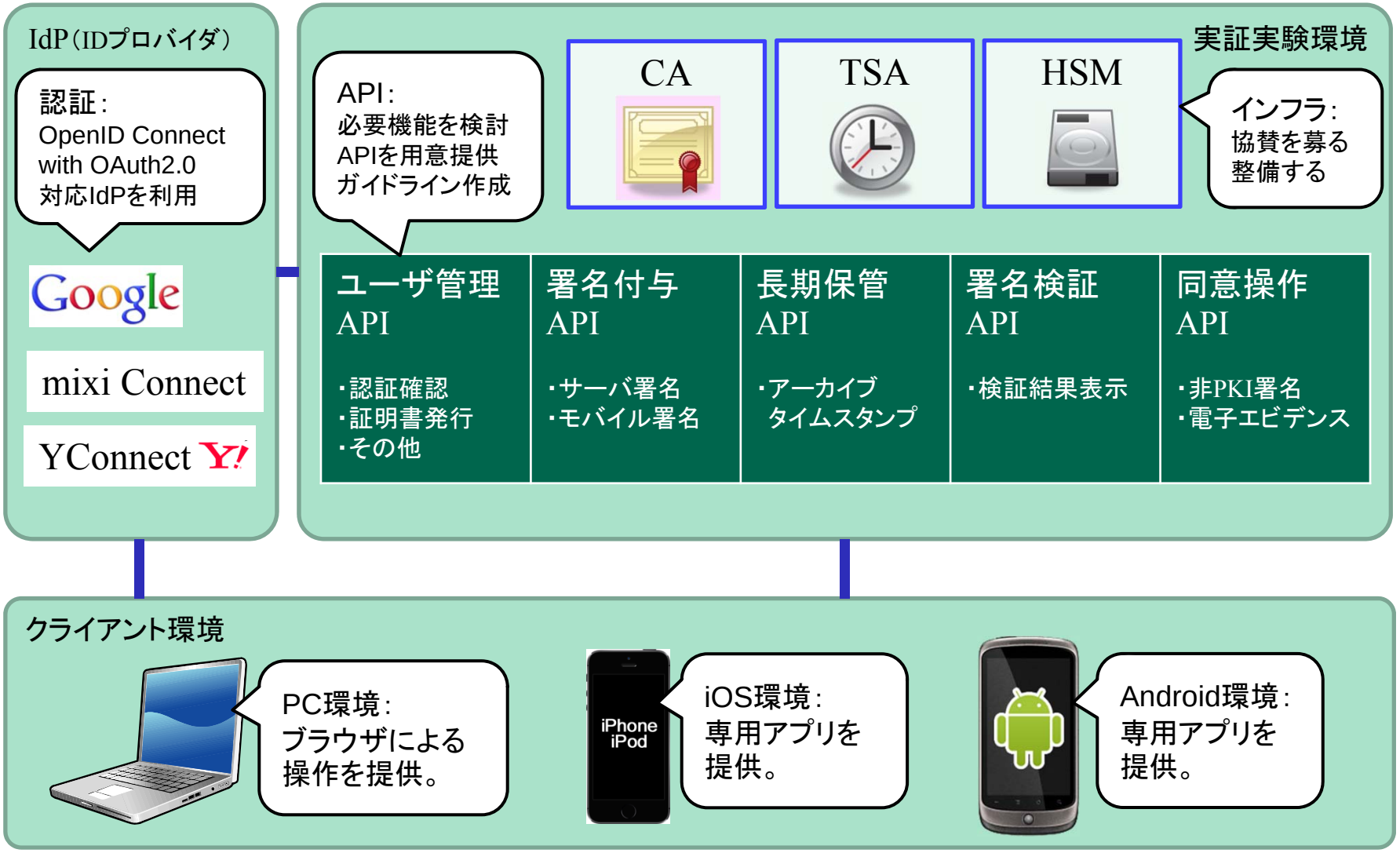
→ 秘密鍵の持ち方や手順を検討して実際に試せる環境を
→ iOS/Androidの署名・検証アプリの試作も行いたい

実証実験に必要となるお試しインフラの整備

→ オープンソースプロジェクトの積極利用と新規開発
→ 協賛頂けるベンダーからリソースの提供を受ける

Copyright (c) 2000-2014 NPO日本ネットワークセキュリティ協会

クラウド署名・モバイル署名の実証実験



FreeTSAプロジェクトお試し

http://www.langedge.jp/tsa

RFC3161タイムスタンプお試しの為のフリープロジェクト
OpenSSL 1.0.X系とApache ＋ Perl でお手軽TSA構築
http://www.langedge.jp/blog/index.php?itemid=665

▽ フリーTSA公開中なので試せます！（※ cURLが必要）

```
// タイムスタンプリクエストの生成
> openssl ts -query -data test.txt -cert -sha512 -out req.tsq
Loading 'screen' into random state - done

// タイムスタンプリクエストの送信とレスポンスの取得
> curl -k --data-binary @req.tsq "http://www.langedge.jp/tsa" > resp.tsr
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2966  100  2864  100   102  20457    728 --:--:-- --:--:-- --:--:-- 20457

// タイムスタンプレスポンスを使った検証
> openssl ts -verify -data test.txt -in resp.tsr -CApath root.pem -CAfile root.pem
Verification: OK
>
```

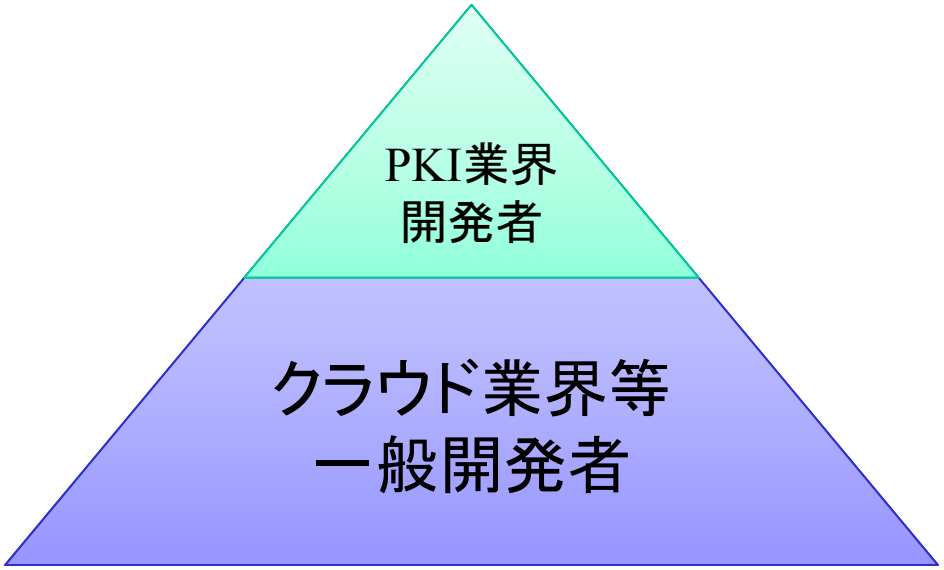
課題:タイムスタンプトークンの抽出ができない。

一般向けの勉強会やハンズオン実施

JNSA

一般開発者向けに勉強会やハンズオンを実施

→ 署名や証明書発行やタイムスタンプの使い方を解説
→ 実際にAPIをたたいて貰ったりプログラミングしたりする
→ PKI基礎知識を説明し利用する可能性をアピールする
→ PKI若手育成と新規参入者の獲得を目指す



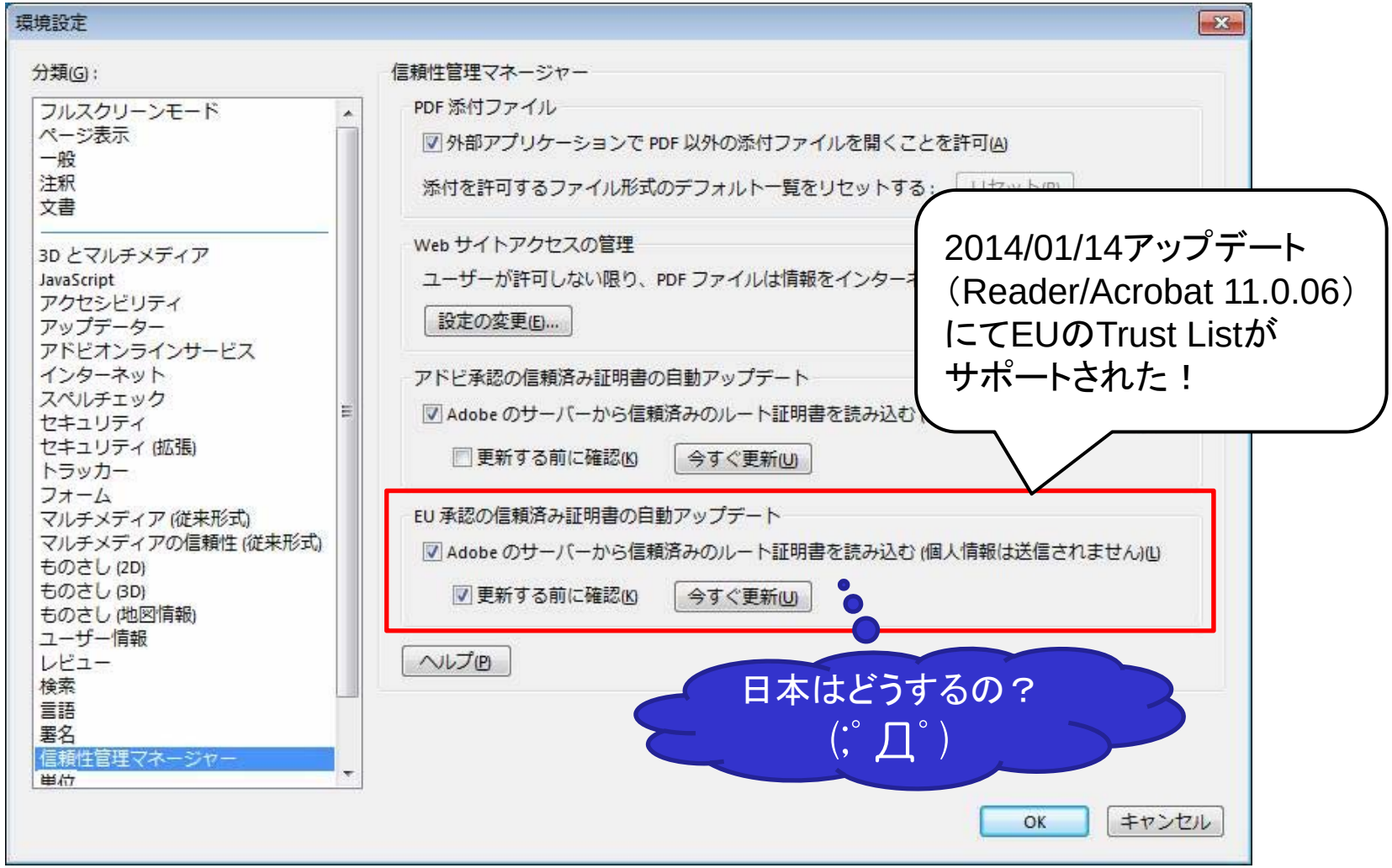
既存PKI技術者の
スキルアップを図る。

裾野を広げて
電子署名技術の
一般化を目す！

おまけ：Adobe信頼性管理マネージャー

http://blogs.adobe.com/publicpolicy/2014/01/22/update-alignment-of-adobe-approved-trust-list-aatl-and-eu-trust-list-eutl/

Update: Alignment of Adobe-Approved Trust List (AATL) and EU Trust List (EUTL)



ご清聴ありがとうございました。

電子署名WGへの参加者募集中です！

https://www.facebook.com/eswg.jnsa.org

Copyright (c) 2000-2014　NPO日本ネットワークセキュリティ協会