資料2－2

2019年2月15日

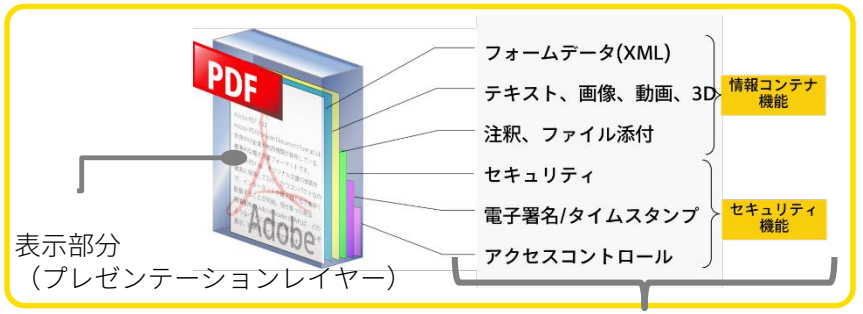
PDF文書を対象にした電子署名／タイムスタンプ技術の実装例
～Acrobat Reader/Adobe Acrobat/Adobe Sign～

アドビシステムズ株式会社｜今西祐之

本日の内容

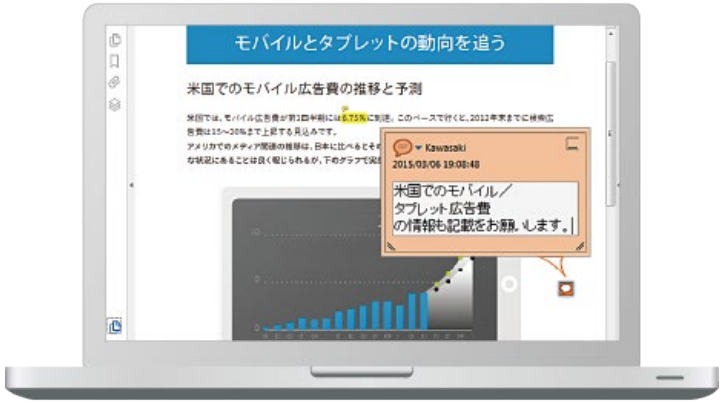
- PDF文書における電子署名／タイムスタンプの使用
  - PDFにおける電子署名の仕組み
  - PDF文書の変更と改ざん
  - タイムスタンプ
- 電子サインサービスAdobe Signにおけるリモート署名の統合
  - 電子サインサービス「Adobe Sign」の概要
  - 電子サインの特長と課題（電子署名と比較）
  - Cloud Signature Consortiumについて
  - 電子サインとリモート署名の統合（デモ）
  - 今後の課題
- 添付資料
  - Cloud Signature Consortium Update (JT2A Meeting –7th November 2018)
    - Andrea Valle (Cloud Signature Consortium 会長) の講演資料

PDF（Portable Document Format）



- Portable Document Format – PDF1.7/2.0
  - 電子文書の国際標準規格（ISO 32000-1/2）
    - アドビが開発・維持してきた仕様を国際標準化機構に譲渡
    - 将来に渡り安心して運用できるファイルフォーマット
    - 長期保存（PDF/A）や技術文書交換（PDF/E）など用途別サブセットのISO規格あり
  - どんな環境でも同じ体裁で表示される
    - 内容（テキスト）や文書属性の抽出・検索が可能
    - 文書単位のセキュリティ（文書の保護）が確保できる
    - 写真、イラスト、音声、ビデオ、アニメなども含められる自己完結のフォーマット

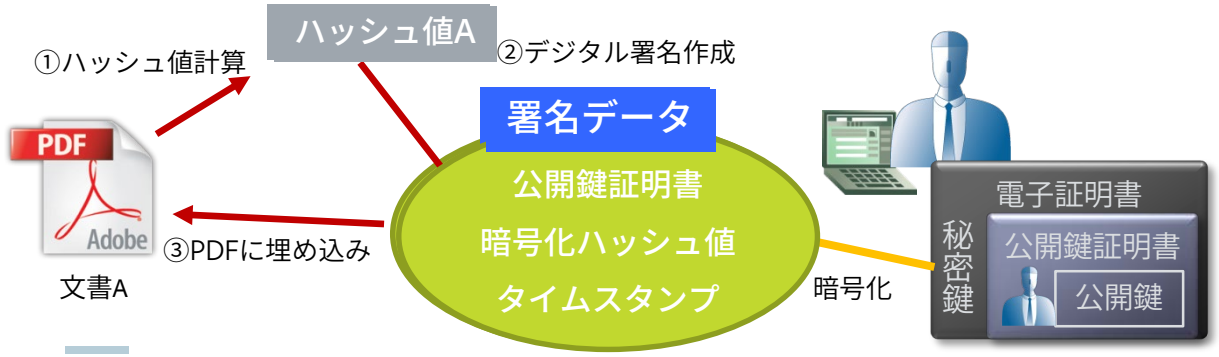
Acrobat DC

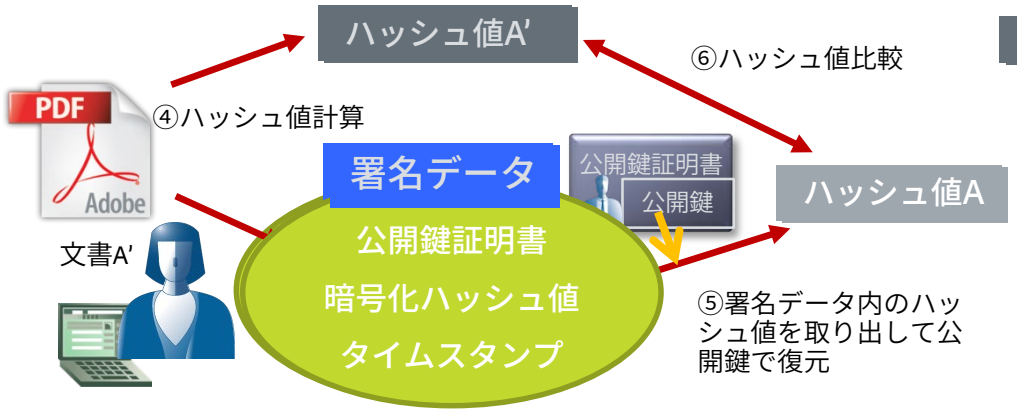


デバイスを問わず同じ表示

Acrobat DC
Mobile

PDFにおける電子署名の仕組み（１）





④～⑥改めて文書内容のハッシュ値を計算し、デジタル署名に埋め込まれたハッシュ値と比較する。違っていれば改竄あり

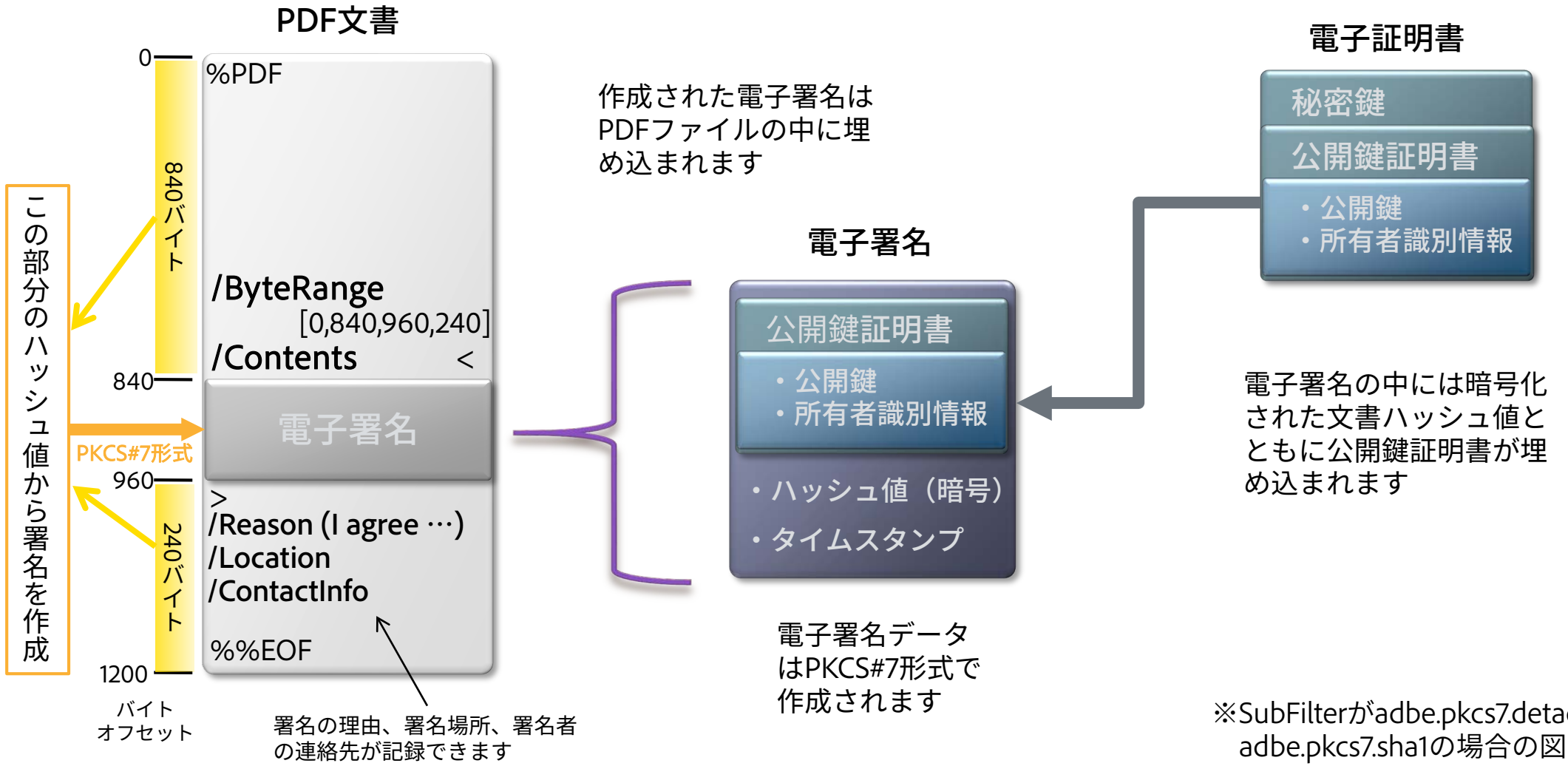
Enveloped型

署名データを署名対象データの中に含む包含形式で作成されます

電子署名によって保証できること

- 本人が署名したこと
- 改ざんされていないこと

PDFにおける電子署名の仕組み（２）



※SubFilterがadbe.pkcs7.detachedまたはadbe.pkcs7.sha1の場合の図です

署名に使用できるデジタルID（電子証明書）

Adobe Acrobat/Acrobat Reader

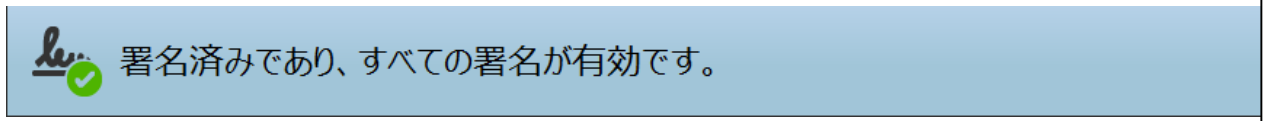
- X.509電子証明書
  - Windows証明書ストア
  - 証明書ファイル（PKCS#12形式、.pfx形式）
  - セキュリティトークン（API：MSCAPI／PKCS#11）
- 署名に使用できる条件
  - 証明書の有効期限内
  - Key Usage／Extended Key Usageに従う
    - http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/changes.html#id2

条件を満たさないと一覧に表示されません

署名後の改ざんと変更

- 署名（証明／承認）後に内容／表示が変更される文書がある **変更？改ざん？**
  - 複数の関係者が署名を追加するケース
  - 関係者に回覧して承認を得る。その際に署名とともに日付やコメントが入れられるケース
  - 発行者の署名入り申請書に記入＆署名を行って申請するケース

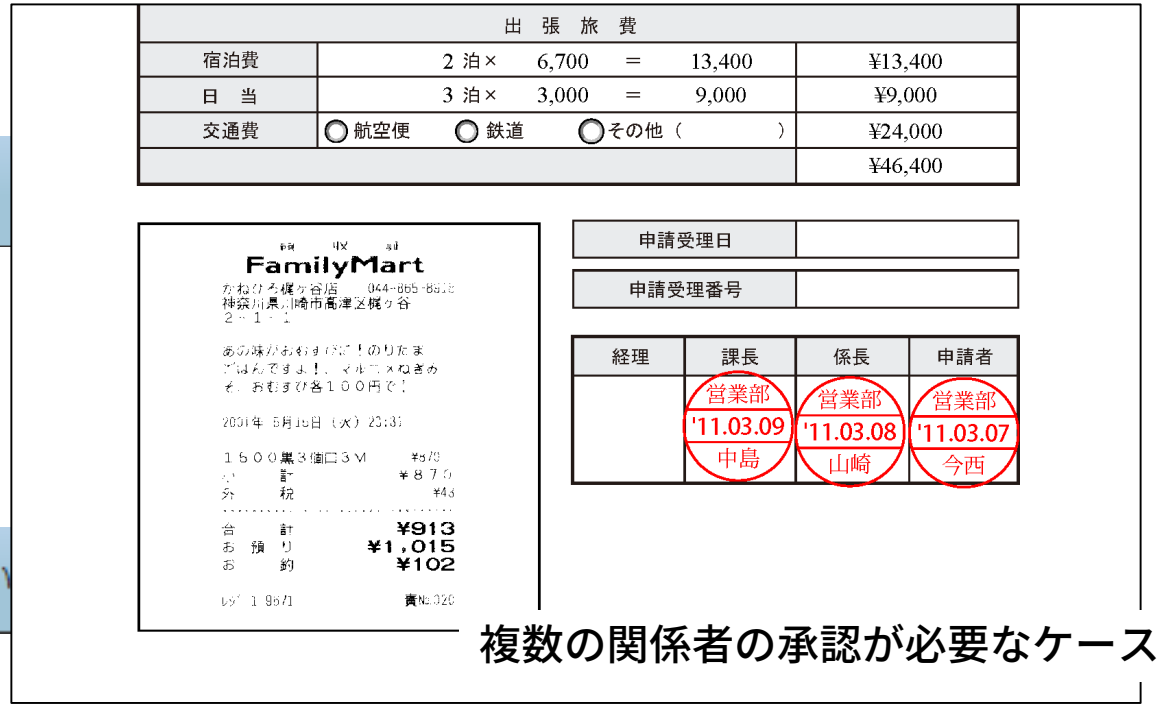
改ざんされていない



フォームへの入力やコメントの追加など想定された操作による変更は、改竄と見做されません

改ざんされた可能性がある

後述のPDFの仕様に則ってオリジナルデータを保持しているのではない変更は、改竄と見做されます



出張旅費		
宿泊費	2 泊× 6,700 = 13,400	¥13,400
日当	3 泊× 3,000 = 9,000	¥9,000
交通費	◯航空便 ◯鉄道 ◯その他（ ）	¥24,000
		¥46,400

FamilyMart

申請受理日	
申請受理番号	

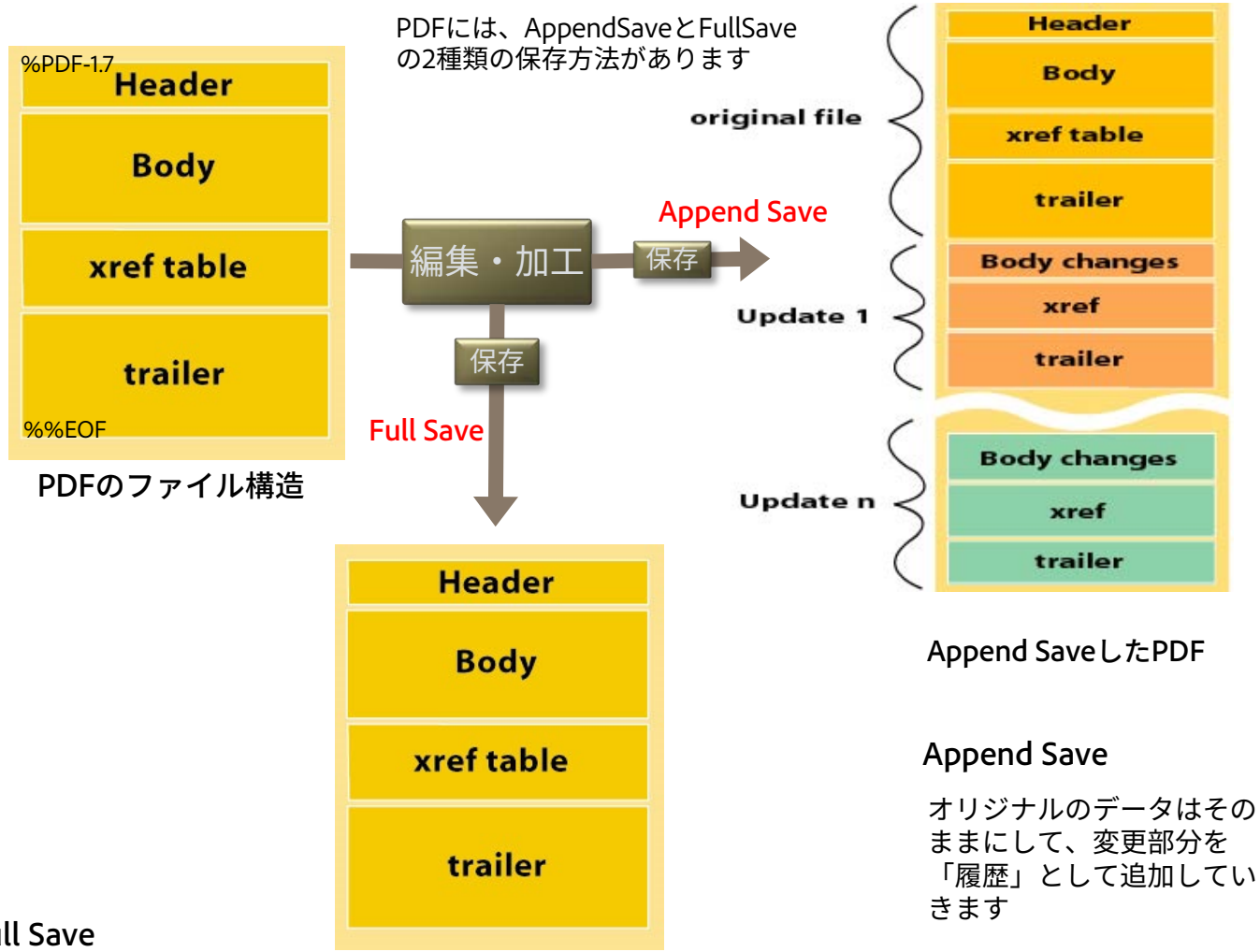
経理	課長	係長	申請者
	営業部 '11.09 中島	営業部 '11.08 山崎	営業部 '11.07 今西

複数の関係者の承認が必要なケース

署名後の改竄と変更：PDFの保存方法

- PDF編集後のFull SaveとAppend Save
  - Full Save
    - PDF全体の構造を再構成して保存
  - Append Save
    - 変更差分をファイルの末尾に追加

※Full Save/Append Saveは、AcrobatやAcrobat Readerの機能の呼び方です。PDFの仕様上では、変更差分をファイル末尾に追加するやり方は、**Incremental Update（増分更新）**と呼びます



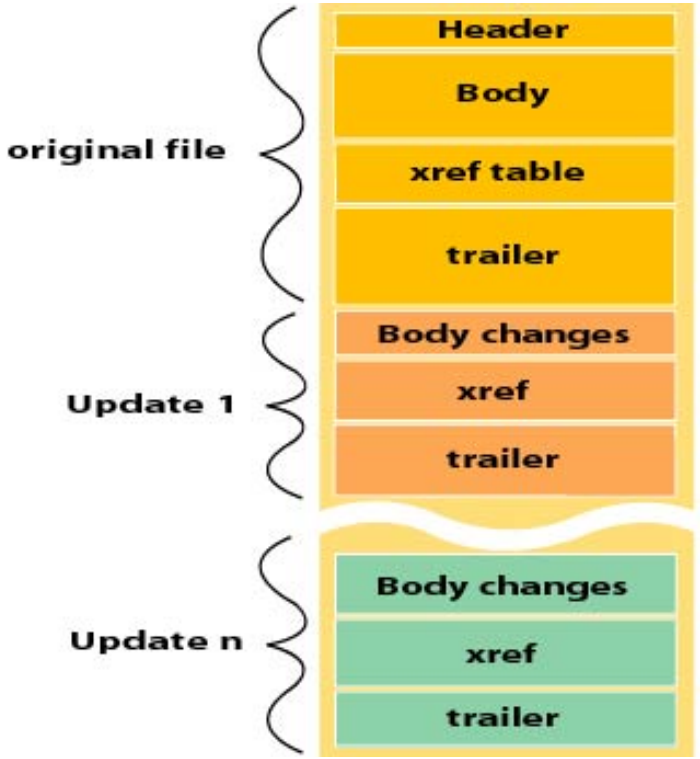
Full Save

変更履歴を消し、コンパクトなPDFとして保存します

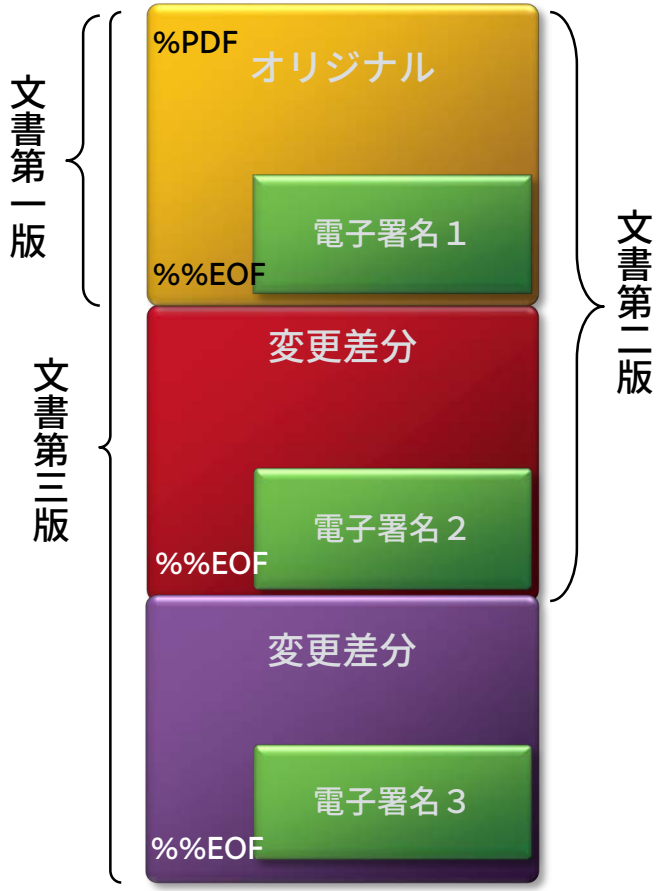
Append Save

オリジナルのデータはそのままにして、変更部分を「履歴」として追加していきます

署名後の改竄と変更：Append Saveを利用した複数署名



Append SaveしたPDF



電子署名入りPDF

デジタル署名１の有効範囲＝文書第1版
デジタル署名２の有効範囲＝文書第2版
デジタル署名３の有効範囲＝文書第3版

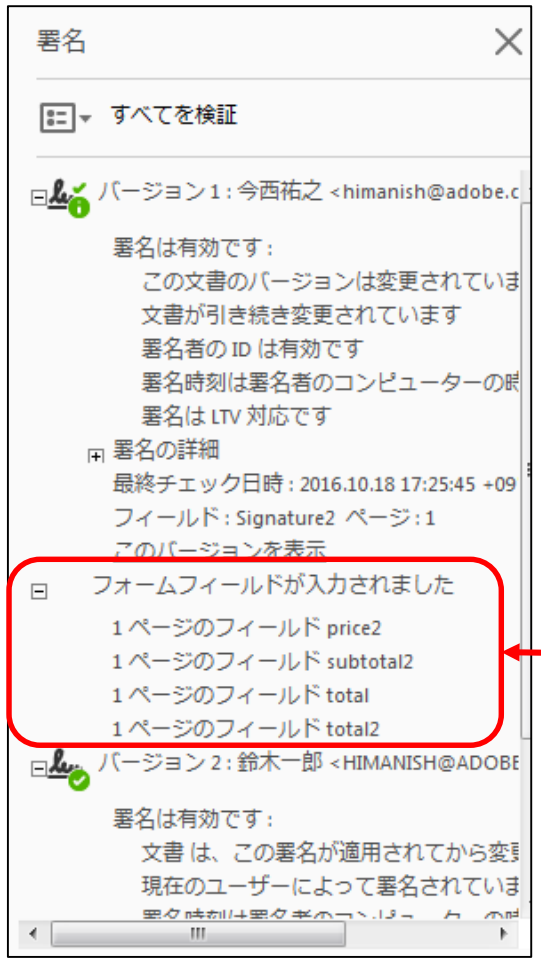
PDFに電子署名を追加するときには、Append Saveが行われます

PDFには複数の署名を順次追加することができます。Append Saveにより、前の版の内容および署名をそのまま残すので、その内容が復元できます

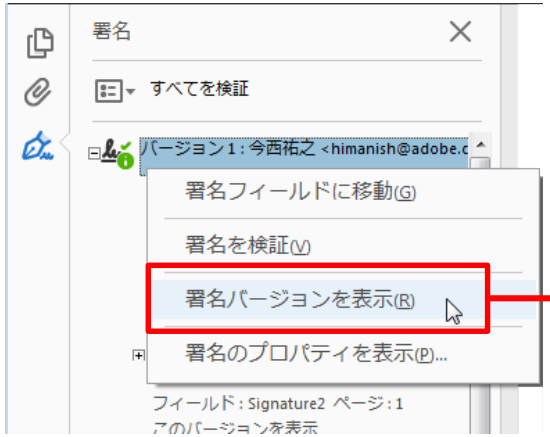
署名後の改竄と変更：署名バージョンの表示

Adobe Acrobat/Acrobat Reader

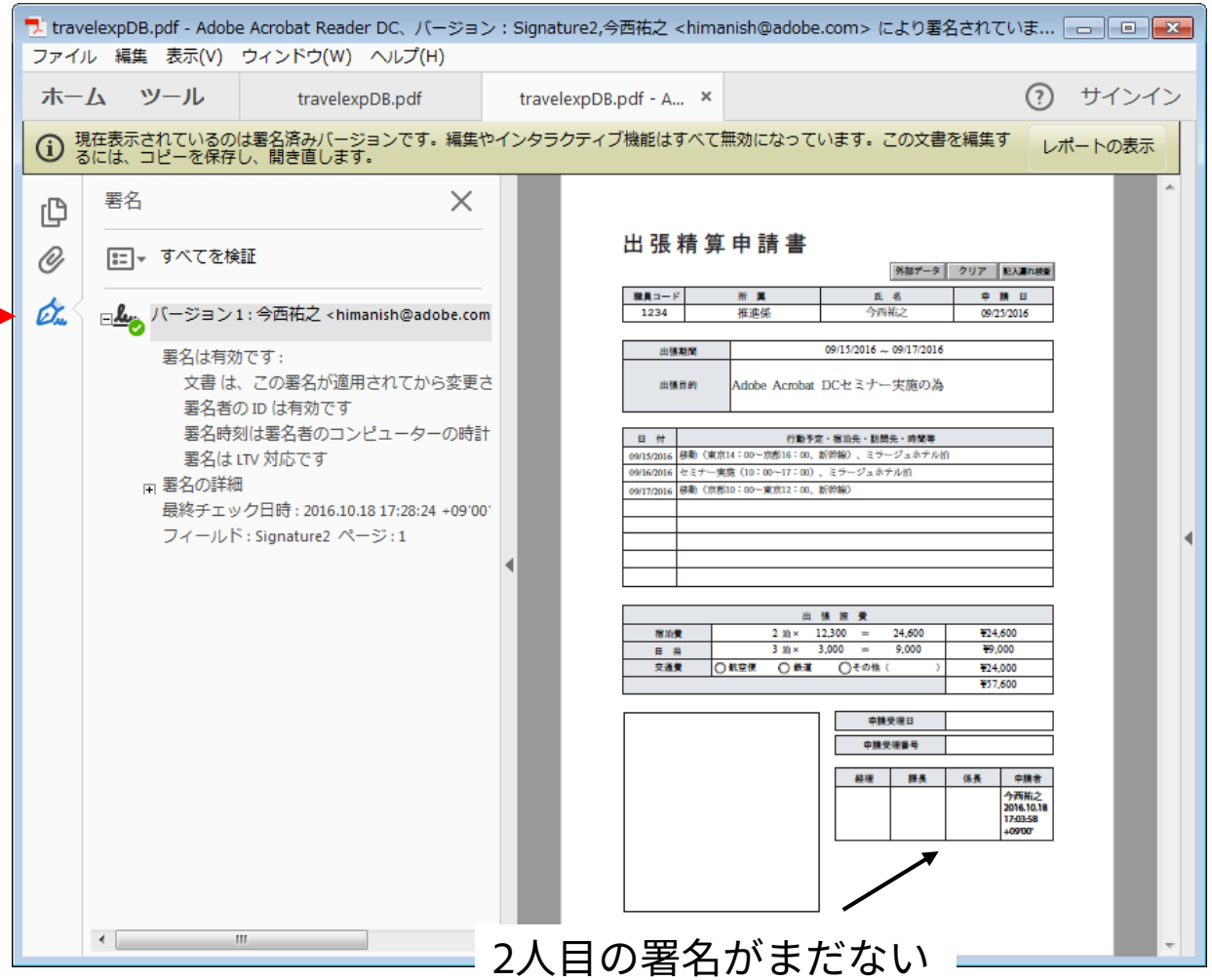
- 署名時の内容を復元して表示



変更箇所



バージョン１の表示



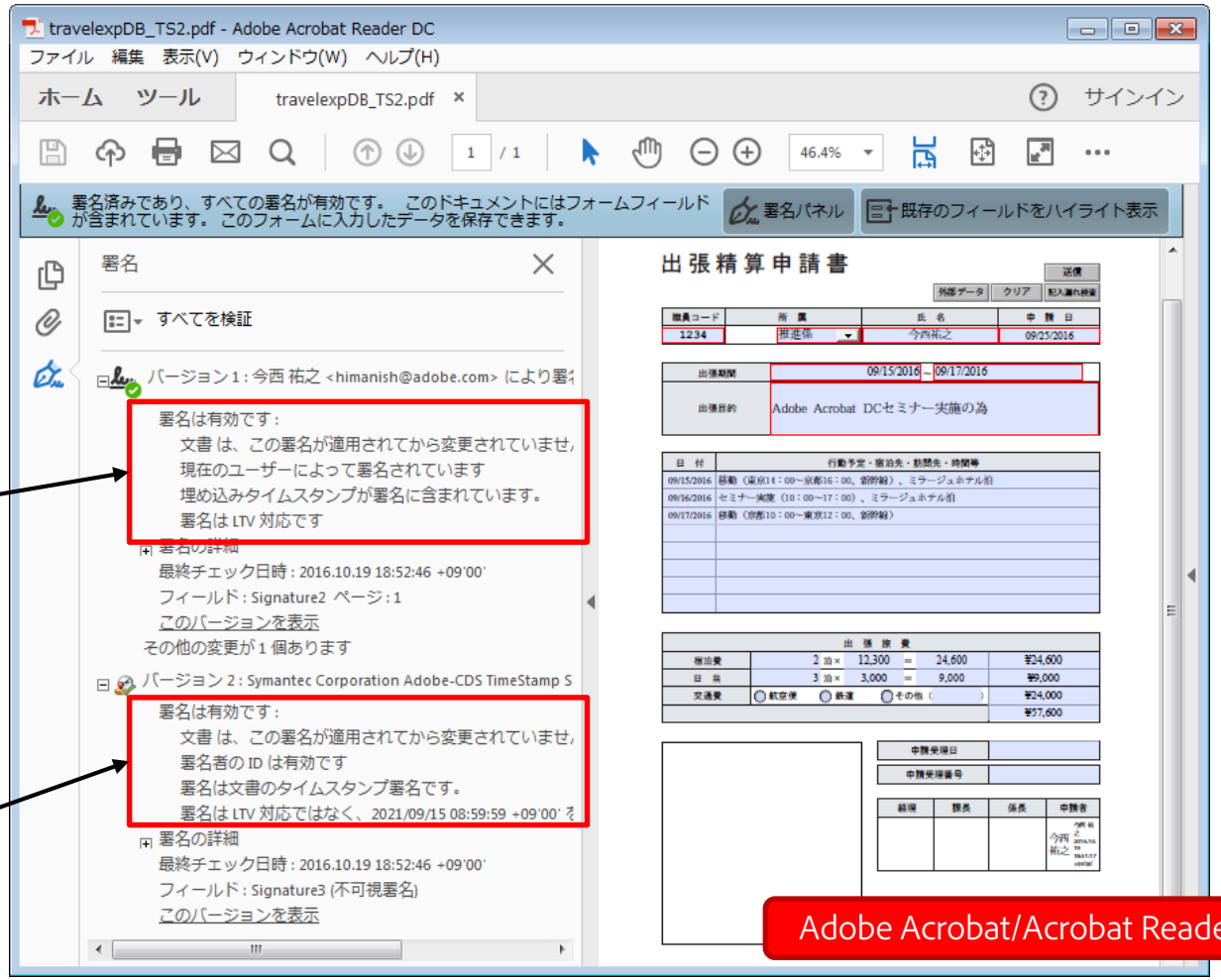
2人目の署名がまだない

タイムスタンプ（RFC3161形式）

- タイムスタンプ
  - 文書の完全性を証明
  - 文書の存在を証明
- 2種類のタイムスタンプ
  - 署名に含まれる埋め込みタイムスタンプ
  - 文書のタイムスタンプ署名

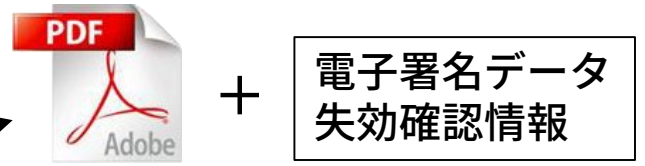
タイムスタンプは署名データに含まれる

タイムスタンプは独立した署名のひとつとして表現される



アーカイブタイムスタンプによる長期署名の実現

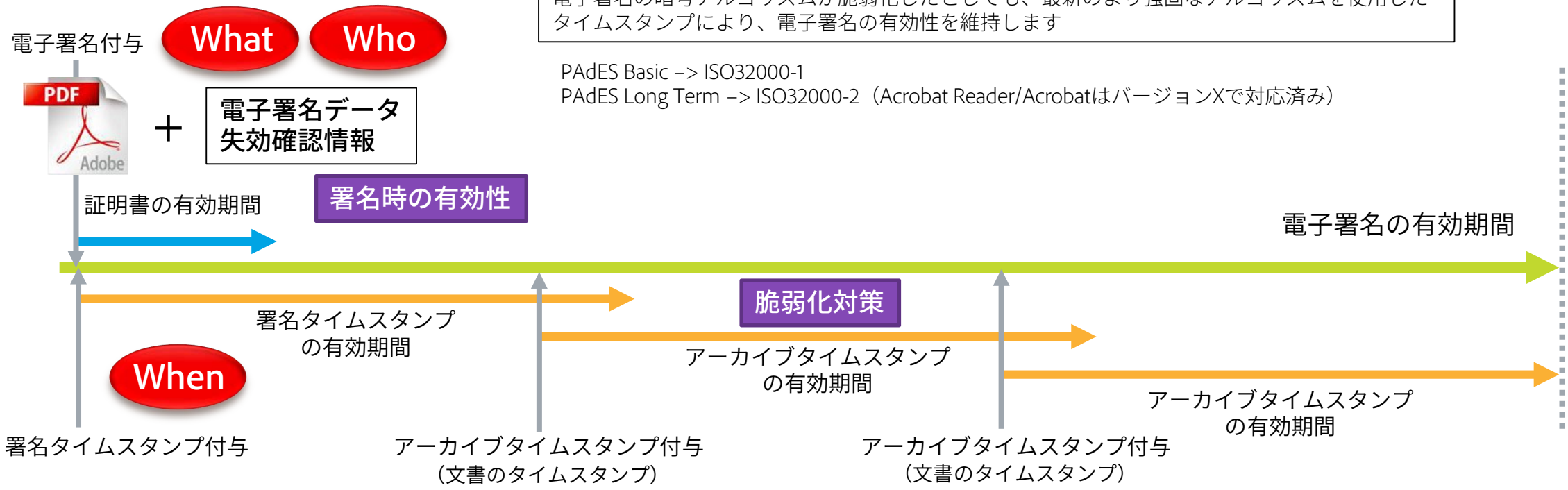
- 長期署名の要件を満たす仕組み
  - 署名当時に電子証明書が有効であったことの確認
    - 署名データとともに署名時の失効確認情報を保存する
  - 電子署名に用いた暗号技術が脆弱化していても検証可能
    - 証明書／タイムスタンプの有効期限内に新たなタイムスタンプを付与して電子署名の有効性を維持する



LTV enabled（長期検証対応）署名

電子署名の暗号アルゴリズムが脆弱化したとしても、最新のより強固なアルゴリズムを使用したタイムスタンプにより、電子署名の有効性を維持します

PAdES Basic –> ISO32000-1
PAdES Long Term –> ISO32000-2（Acrobat Reader/Acrobatはバージョンxで対応済み）



電子署名に使用された証明書による作成者の証明とその信頼性

- 作成者（＝署名者）が本人であることを証明する
  - Self-Sign証明書
    - 作成者が自分自身で身元を保証する
  - 認証局発行の公的な電子証明書
    - 第三者である認証局が身元を保証する
- 認証局の信頼性の根拠
  - 認証局の自己署名証明書を信頼する
    - 自己署名証明書を手作業で取り込む
  - Adobe Acrobat／Acrobat Readerにビルトイン
    - Adobe CDS（Certified Document Service）
  - 信頼できる認証局の証明書リストの自動取込み
    - AATL（Adobe Approved Trust List）
    - EUTL（EU Trust List）

他の認証局発行の証明書で署名された場合は、認証局の自己署名証明書を手作業で取り込まなければなりません

ルート認証局が信頼できるものであり、かつ、署名者に対して信頼チェーンがつながることが確認できて、はじめて署名が信頼できることになる

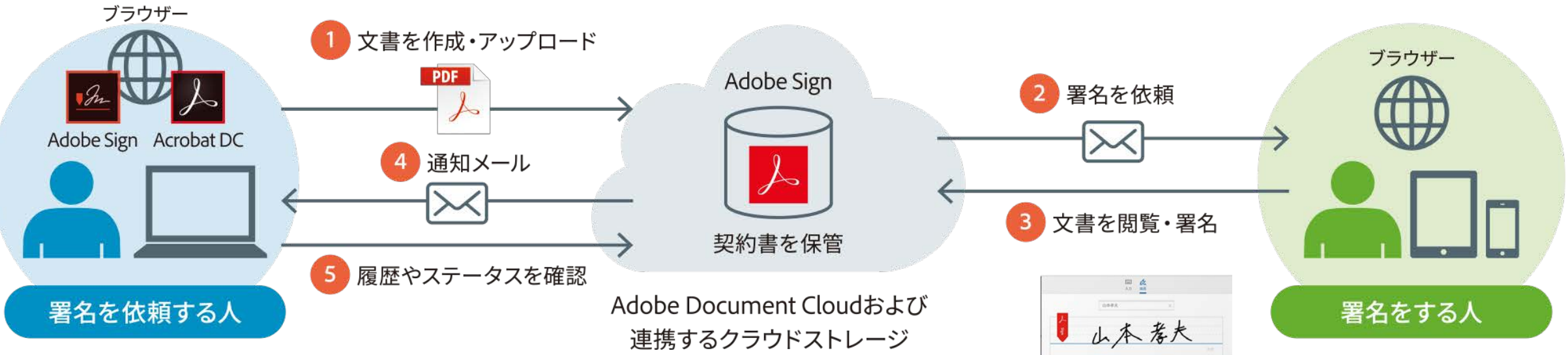
署名検証環境に、ルート認証局の自己署名証明書が取り込まれていなければなりません

ユーザーは、
・知識不要
・手間いらず

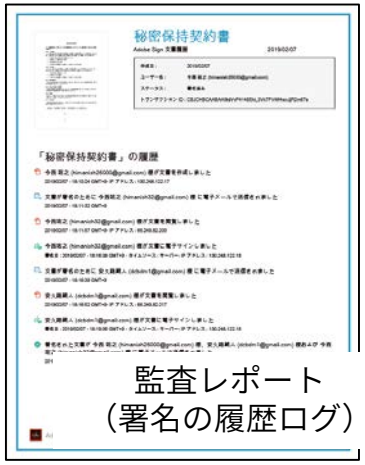
Adobe Acrobat/Acrobat Reader

信頼チェーン

電子サイン（ Adobe Sign ）サービスとそのワークフロー



契約書



監査レポート
（署名の履歴ログ）

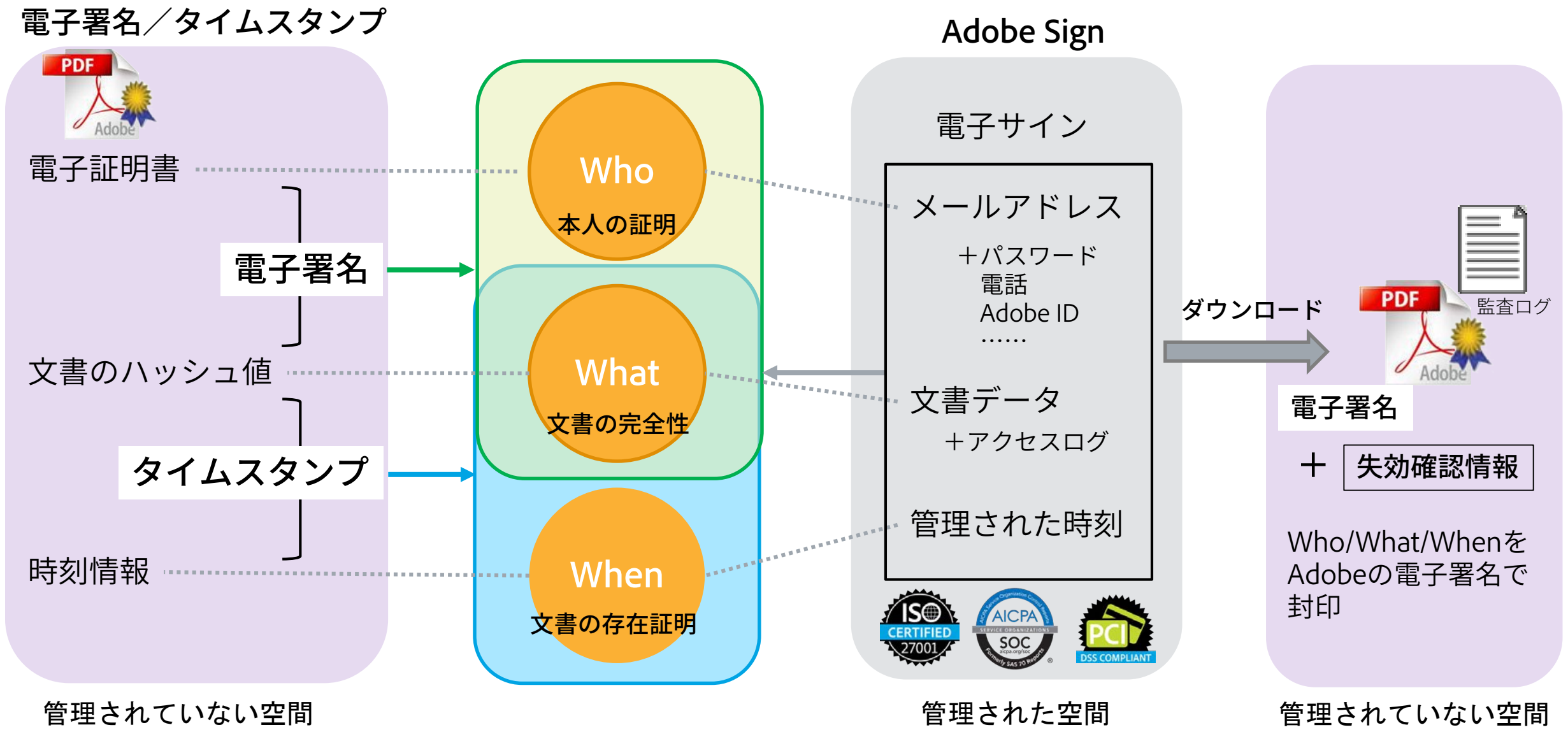
電子サイン

本人性確認
- メールアドレス
- 2要素認証 （PWなど）
＋
署名の履歴ログ

改ざん防止
証明書による文書の封印

「署名を依頼する人」から提供された身元情報（電子メールアドレス等）に基づき「署名をする人」を認証

電子サイン（Adobe Sign）によるWho／What／Whenの証明



電子署名／電子サインの特長と課題

	電子署名	電子サイン
保証レベル	対面またはそれに準ずる方法で身元確認を行う	身元確認は自己申告に基づく
	本人が直接、物理トークンを使用する	物理トークンなどは必須ではない
	業界の規制要件を満たせる	業界の規制要件を満たせない場合がある
使いやすさ	モバイルデバイスやWebアプリケーションでは動作しない	モバイルやWebアプリケーションで動作する
	証明書を管理および維持するのにかなりのITコストがかかる	システムの管理・維持はサービス事業者が行うため、利用者のITコストは低く抑えられる

電子署名／電子サインの特長と課題

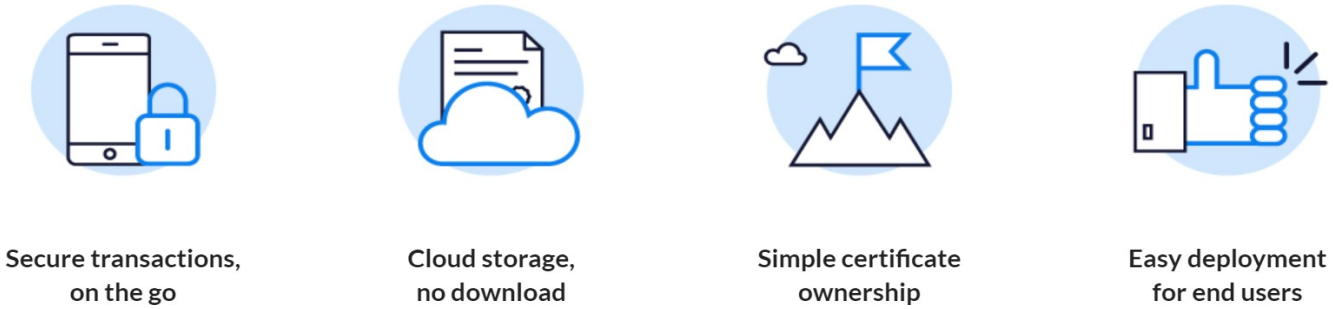
	電子署名	電子サイン
保証レベル	対面またはそれに準ずる方法で身元確認を行う	身元確認は自己申告に基づく
	本人が直接HSM/物理トークンを使用する	物理トークンなどは必須ではない
	業界の規制要件を満たせる	業界の規制要件を満たせない場合がある
使いやすさ	モバイルデバイスやWebアプリケーションでは動作しない	モバイルやWebアプリケーションで動作する
	証明書を管理および維持するのにかなりのITコストがかかる	システムの管理・維持はサービス事業者が行うため、利用者のITコストは低く抑えられる

電子サインの**使いやすさ**と電子署名の高い**保証レベル**の両立

← **Cloud Signature Consortium**の規格に基づき、電子署名のワークフローに**リモート署名**を統合

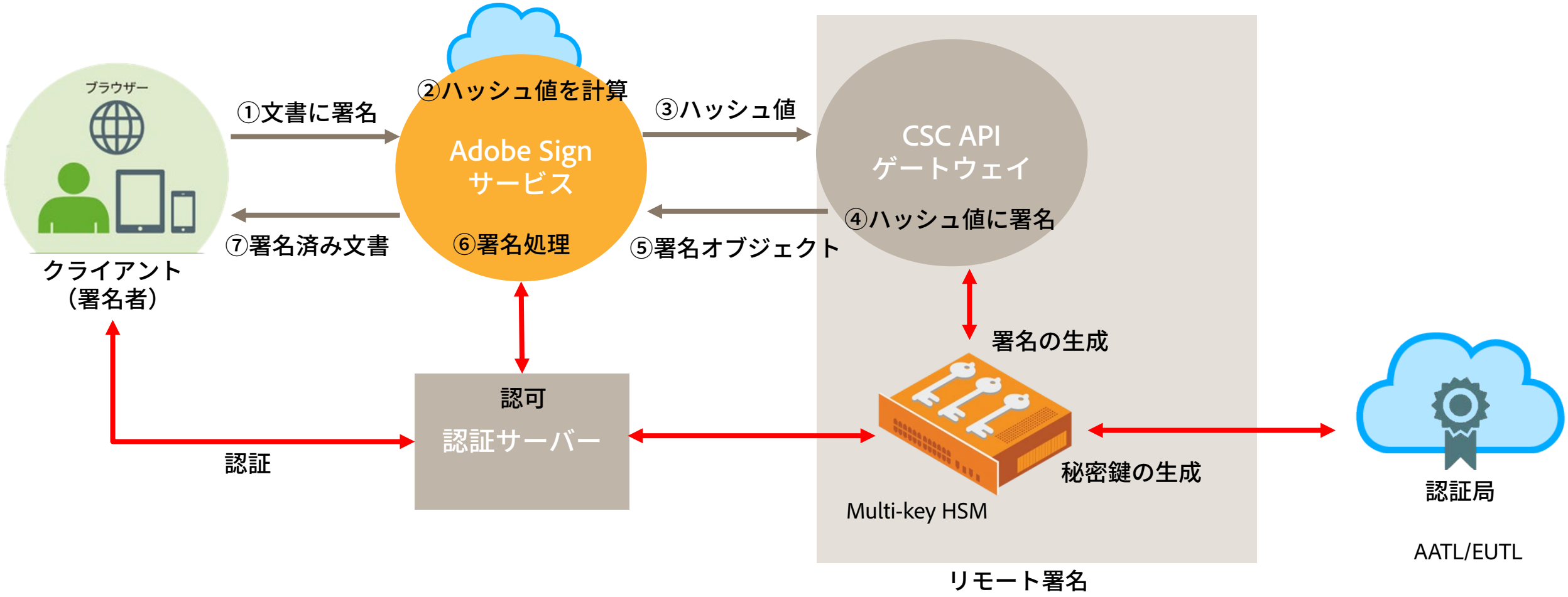
Cloud Signature Consortium

- 2016年に、ソリューション、テクノロジ、およびトラストサービスプロバイダを含む、業界および学術の専門家による国際協力グループによって設立
  - クラウドベースの電子トラストサービスの推進
  - トラストサービス間の相互運用を円滑にするための共通のアーキテクチャーと構成要素の設計
  - 円滑な相互運用のためのプロトコルおよびAPIの技術仕様の開発
  - 技術仕様はオープンスタンダードとして公開



電子サインサービスとリモート署名の統合（Adobe Signの場合）

- Cloud Signature Consortium規格のAPIに基づき、リモート署名をAdobe Signに統合



Adobe Sign：今後の課題

証明書発行の自動化

※サービスプロバイダーとの連携

電子署名の検証

※モバイルデバイスでの署名検証

長期保存

※ダウンロードした書類や署名の有効性


Adobe

Cloud Signature Consortium Update

Andrea Valle

JT2A Meeting – 7th November 2018

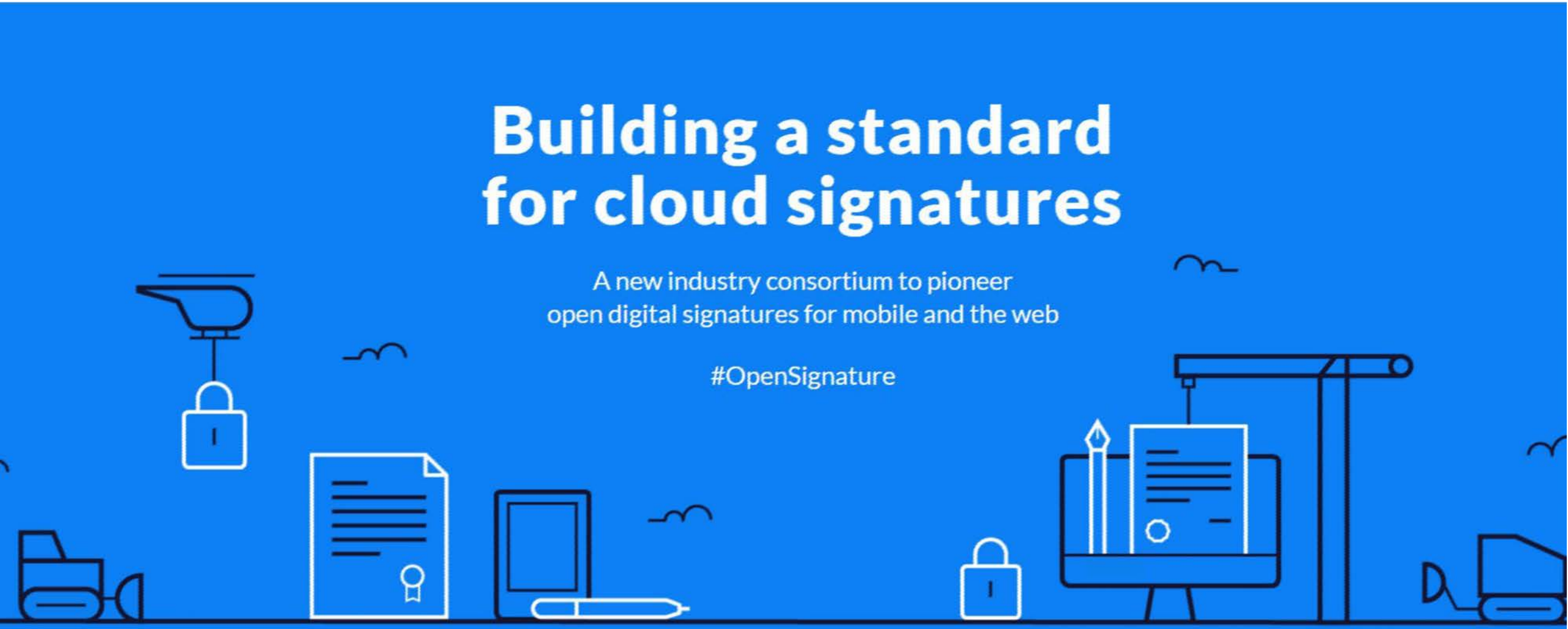
CLOUD SIGNATURE CONSORTIUM

電子署名の利便性を高めるために

- Provide highest **Integrity** and **Authenticity** to an electronic document.
- Meet compliance with the main regulatory and industry requirements.
- Allow users to complete digital signing anytime, anywhere and on any platform: web, mobile, desktop.

CLOUD SIGNATURE CONSORTIUM

クラウド署名コンソーシアム



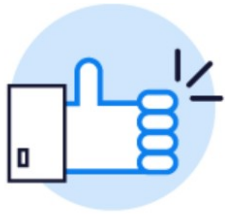
クラウド署名コンソーシアム

- The **Cloud Signature Consortium** was originally founded in 2016 by an international cooperation group of industry and academic experts, including solutions, technology and trust service providers
  - Promoting cloud-based Electronic Trust Services.
  - Design a common architecture and building blocks to facilitate their interaction
  - Develop technical specifications for protocols and APIs to make these interactions easy and interoperable.
  - Publish technical specifications as open standards.

Secure transactions, on the go

Cloud storage, no download

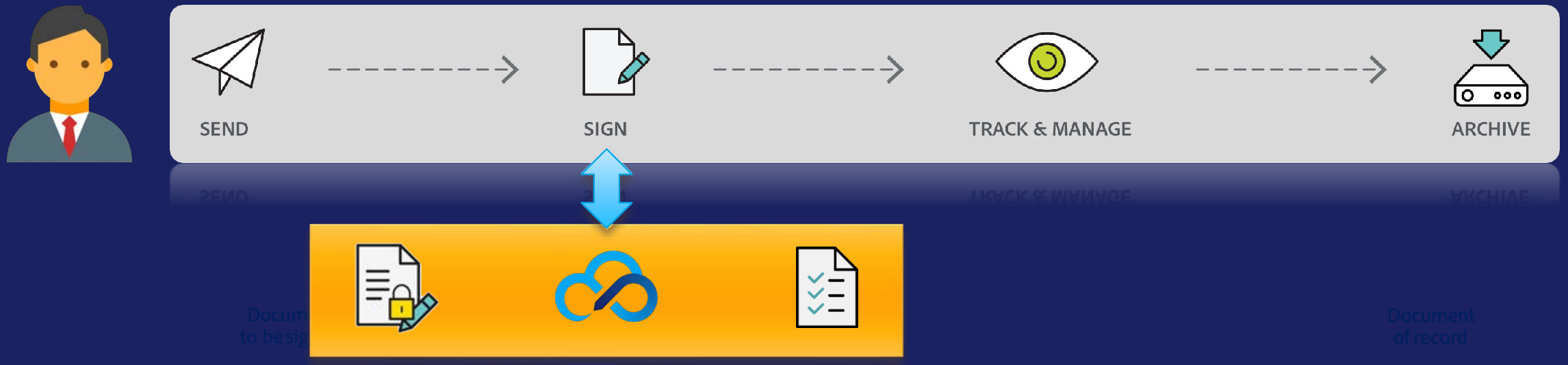
Simple certificate ownership



Easy deployment for end users

電子署名の課題を解決するために

- Define a unified and open standard for cloud-based digital signatures.
- Solve the issue with smart cards and USB tokens that only work on desktop computers.
- Create a network of specialized Trust Service Providers focusing on solutions.
- Combine highest security with powerful document intelligence for business agility.



現在の活動

- **In January 2018 the Consortium became a Not For Profit Association**
  - Acquired legal personality to support membership expansion and advocacy worldwide
- **Cooperation**
  - Establishing a Cooperation Agreement with ETSI to allow mutual exchange of contributions for the development of standards for trust services.
  - The CSC API specification is referenced in ETSI TS 119 432 “Protocols for remote digital signature creation”
  - Active cooperation with Government agencies involved in public policies about remote signatures.
- **Making the CSC API V1 Specification publicly available**
  - Draft available at: https://cloudsignatureconsortium.org/specifications
  - JSON schema
  - OpenAPI schema
  - CSC API V2 is under evaluation and will be released by the end of the year.

クラウド署名コンソーシアム　メンバー

Adobe	USA/Ireland
Asseco Data Systems	Poland
BuyPass	Norway
Certinomis Docapost	France
CertSign	Romania
DigiCert	USA
D-Trust/Bundesdruckerei	Germany
eMudhra	India
GMO GlobalSign	USA/Japan
KPMG	Norway
InfoCert	Italy
Intarsys	Germany
Intesi Group	Italy
Notarius	Canada
QuoVadis WiseKey	Switzerland/Benelux
SafeLayer	Spain
Seiko	Japan
Technische Univ. Graz	Austria
Trans Sped	Romania
Universign	France
Validated ID	Spain
Worldline ATOS	France

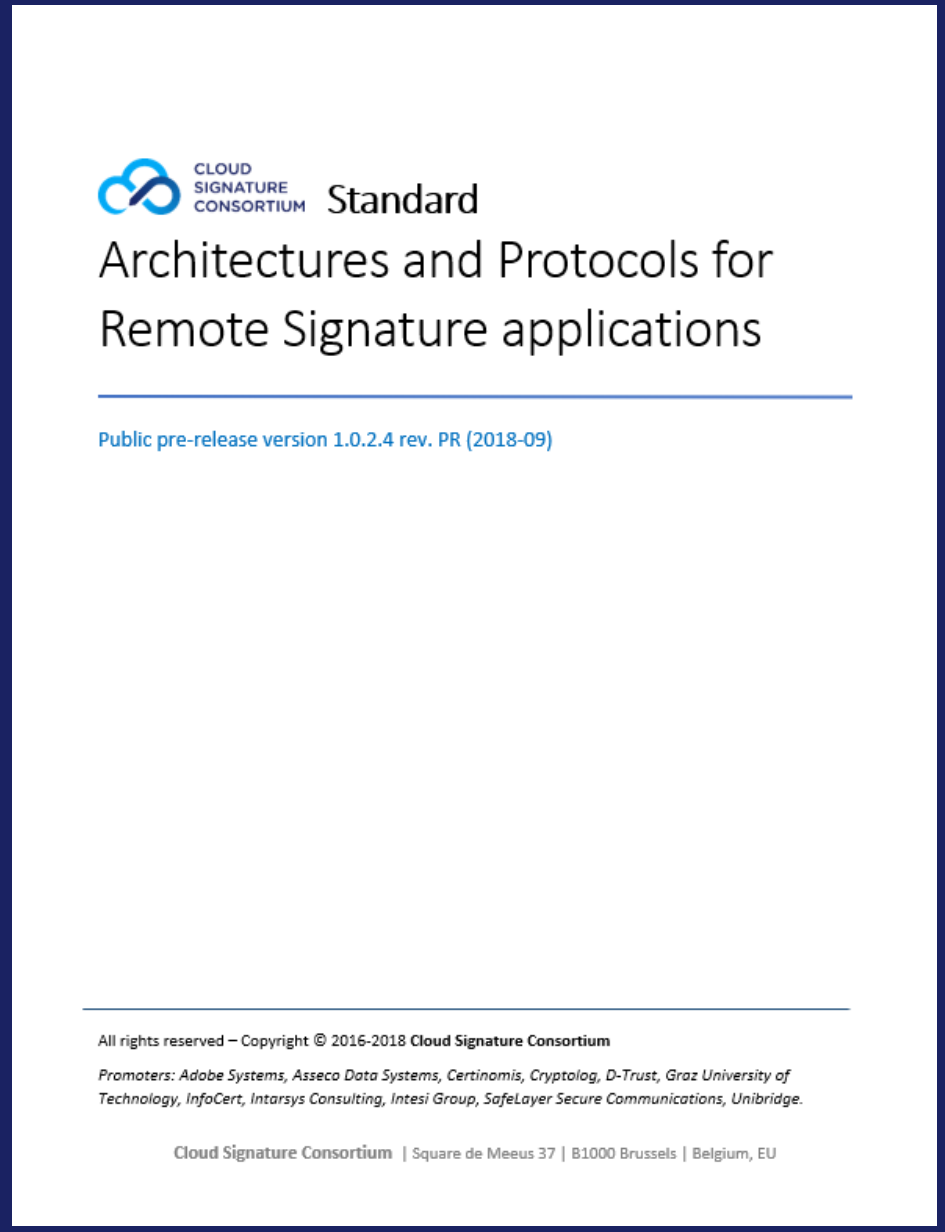
CLOUD SIGNATURE CONSORTIUM

クラウド署名コンソーシアムへの参加について

- **The Cloud Signature Consortium is a technical community**
  - Joining the CSC means becoming part of an active community of adopters and endorsers:
    - Service Providers, Solution Providers, Technology Providers, System Integrators, Consultants, Auditors.
  - Contribute to the development of the standard:
    - Influence and drive strategic directions
    - Benefit from early access to API specifications.
  - Marketing initiatives, Public policies
- **Conformity Checker**
  - The Consortium has developed a Conformity Checker software to help testing service implementations for interoperability and performance analysis.

https://cloudsignatureconsortium.org/contacts

CSCスタンダードのご紹介


CLOUD SIGNATURE CONSORTIUM

Standard

Architectures and Protocols for Remote Signature applications

Public pre-release version 1.0.2.4 rev. PR (2018-09)

Promoters: Adobe Systems, Asseco Data Systems, Certinomis, Cryptolog, D-Trust, Graz University of Technology, InfoCert, Intarsys Consulting, Intesi Group, SafeLayer Secure Communications, Unibridge.

Cloud Signature Consortium | Square de Meeus 37 | B1000 Brussels | Belgium, EU

CLOUD SIGNATURE CONSORTIUM

CSC技術仕様の簡単なご紹介

- **The CSC Specification V1 covers architectures, protocols and APIs for Remote Signature Creation**
  - Web Service API based on REST protocol and JSON data-interchange. Modern and easy to implement.
- **Designed for growth. Self-discovery capacity**
  - Supports modular services, in line with the mission/capacity of providers and consumers.
  - Services may implement only a particular subset of the API. Clients can easily discover the supported APIs.
- **Native support of client and user authentication**
  - Covers multiple implementation contexts: desktop and mobile apps, cloud-based and on-premise services.
  - Supports Basic/Digest auth, TLS, OAuth, SAML, OpenID Connect.
- **Flexible support of credential authorization mechanisms**
  - Supports static secrets, synchronous and asynchronous OTP, OAuth, SAML, OIDC.
  - Multi-Factor-Authorization can be obtained by combining multiple mechanisms.
- **Designed to support eIDAS requirements and CEN / ETSI standards**
  - But flexible to support a broader set of requirements for Global adoption.

Standardization Roadmap

CLOUD
SIGNATURE
CONSORTIUM

標準化へのロードマップ

- **Expand the API to support additional TrustServices**
  - Core API for Cloud Signatures (Remote Digital Signatures)
  - Identity Verification and Authentication
  - Certificate enrollment automation
  - Signature validation and augmentation
  - Long-term Preservation
- **All future services will benefit from a common API framework and unified design**
  - Client and user authentication
  - Flexible resource authorization
  - REST+JSON API
  - Open Standard and interoperable
  - Privacy by design

Adobe Sign

Fast deployment.

Our web and mobile apps are ready when you are. Your users will get a quick-start email. They can learn through our awesome tutorials. Or dive right in with our easy interface.

Mobile power.

Send, track, and manage signing processes on the go. Collect in-person signatures. Or scan paper docs with your mobile camera and send them for signature in a flash.

Error-proof workflows.

Design business processes that everyone can follow, every time. Just drag and drop to create workflow templates that reduce mistakes and improve compliance.

Branded experiences.

Your organization's brand is important — to you, your team, and your customers. Adobe Sign reflects your brand, not ours, so you can position your company as the leader it is.

Self-serve forms.

Put forms on your website, so customers can fill, sign, and return in seconds. Or create an internal portal for employees to find the right form quickly.

Document templates.

Upload any popular document type or get it from online storage. Easily add signature or form fields, and then send for signature or save it as a reusable template.

Online payments.

Connect to your Braintree account (a PayPal service) to securely collect payments — right when customers fill and sign forms.

Adobe Sign

Trusted and legal.

With Adobe Sign, your electronic signatures are legally valid and enforceable. They meet the most demanding requirements and comply with e-sign laws around the world.

Cloud signatures.

We delivered the first open, standards-based digital signatures for web and mobile. So you can offer easy-to-use, high-assurance digital IDs that are internationally compliant.

Automatic audit trails.

Reduce legal risk. Automatically store a complete audit trail of every transaction in a secure online repository. Quickly find what you need, when you need it.

Reliable and secure.

Get uptime you can count on, while ensuring security and privacy. Adobe Sign delivers high performance around the world and complies with the most stringent security standards.

ISO 27001

PCI DSS

SOC

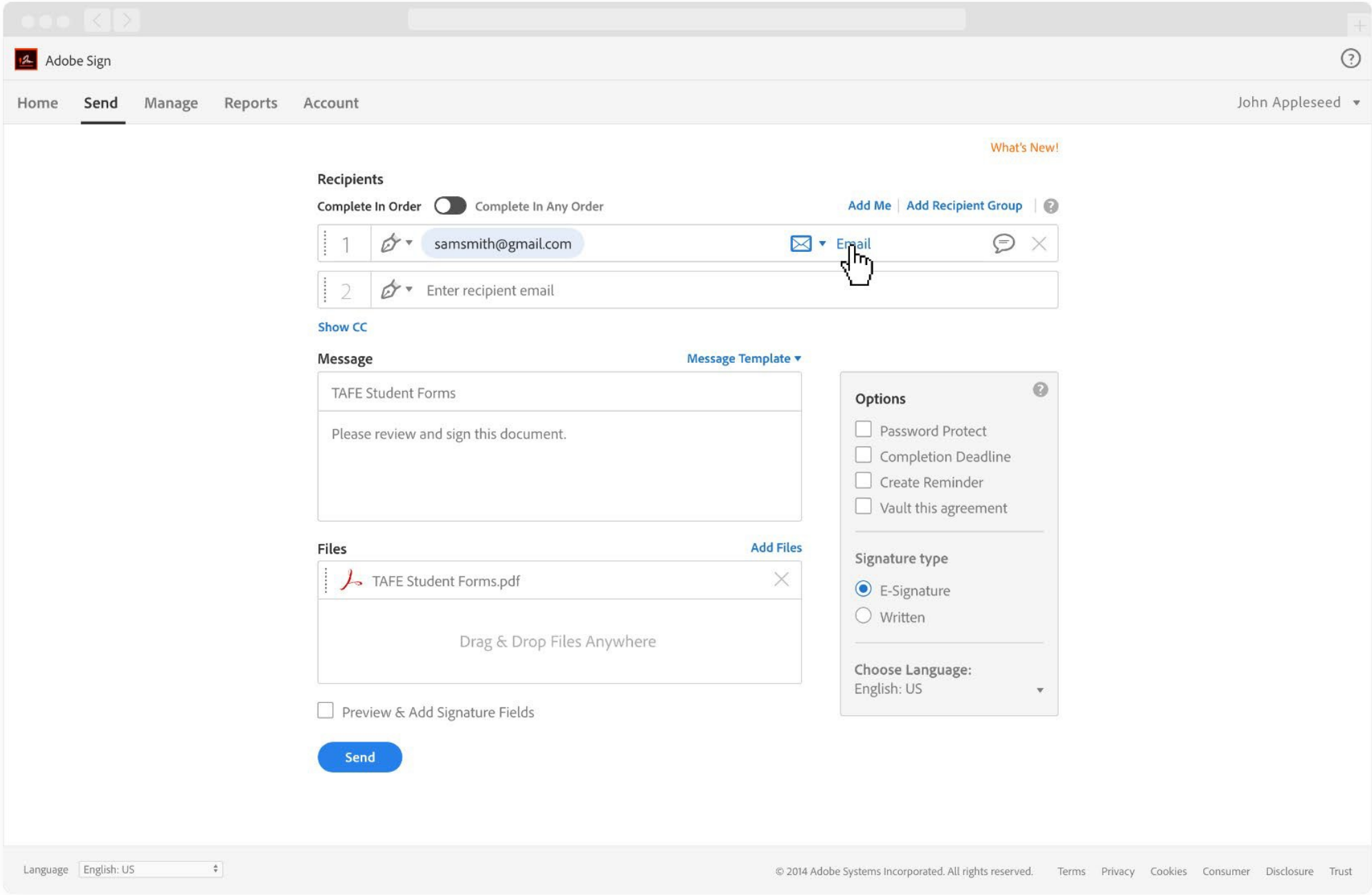
21 CFR

CSC仕様に適応したAdobe Sign

- **Adobe Sign implements the preliminary V0 of the CSC specifications**
  - Works from any laptop or mobile device, using a web browser or dedicated app
  - Supports OAuth for user-centric authentication
  - Supports ETSI standards for Advanced and Qualified Signature
  - Supports ETSI PAdES-B-LT for long term validity. Expanding to support PAdES-B-LTA

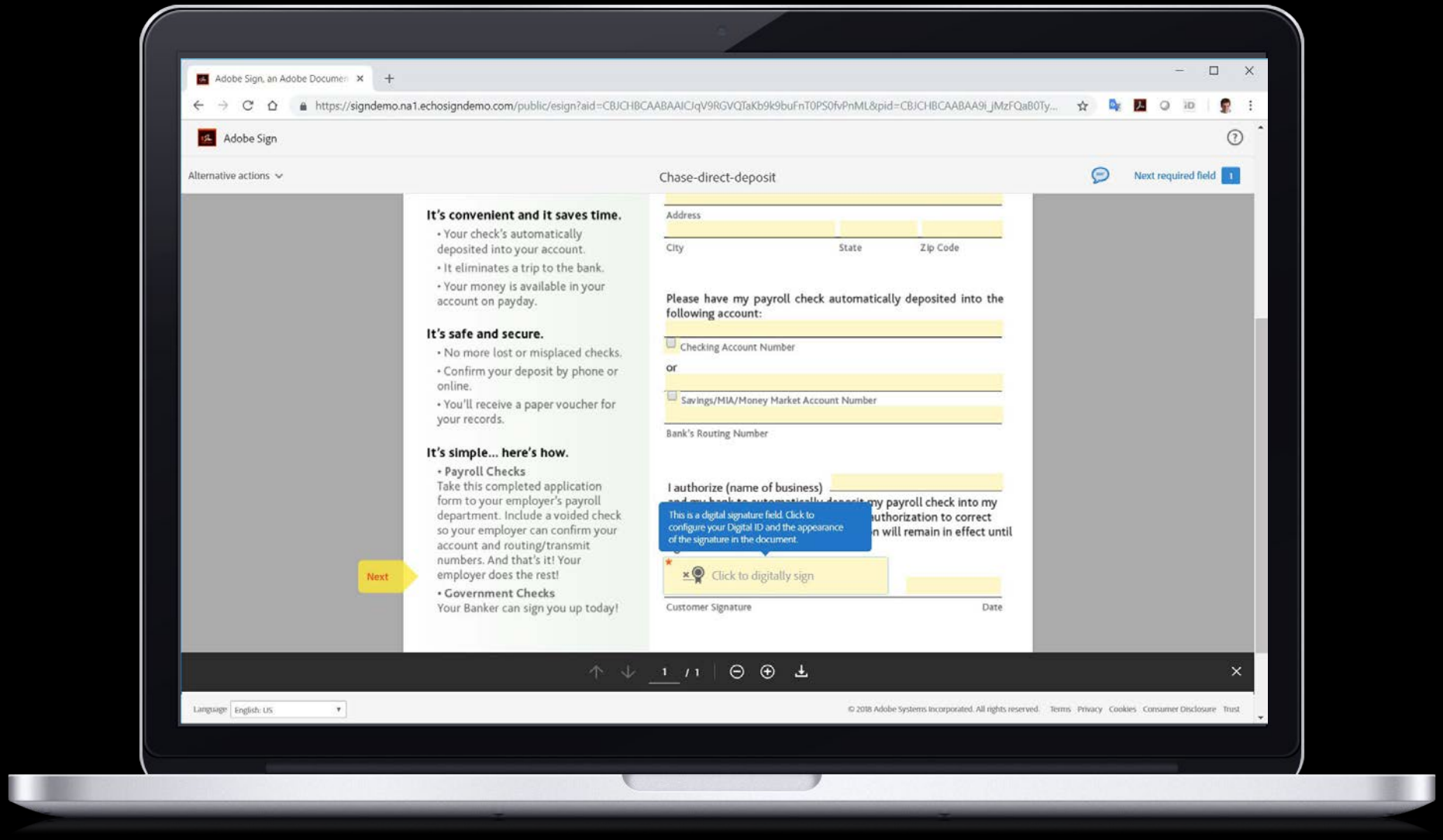
- **The CSC advantage**
  - A new CSC provider can be onboarded in 2 working days (Configure and Test)
  - Authentication and authorization mechanisms are under the control of the Provider
  - Unique market coverage for the Enterprise market
    - Work with multiple providers supporting multiple Regions and languages
    - Wide support of operational models
    - Wide industry and regulatory compliance (e.g. Pharma / Finance)

Adobe Sign Cloud Signature Demo


Adobe Sign
Home
Send
Manage
Reports
Account
John Appleseed
What's New!
Recipients
Complete In Order
Complete In Any Order
Add Me
Add Recipient Group
1
samsmith@gmail.com
Email
2
Enter recipient email
Show CC
Message
Message Template
TAFE Student Forms
Please review and sign this document.
Files
Add Files
TAFE Student Forms.pdf
Drag & Drop Files Anywhere
Preview & Add Signature Fields
Send
Options
Password Protect
Completion Deadline
Create Reminder
Vault this agreement
Signature type
E-Signature
Written
Choose Language:
English: US
Language
English: US
© 2014 Adobe Systems Incorporated. All rights reserved.
Terms
Privacy
Cookies
Consumer
Disclosure
Trust

Click the signature field to start signing

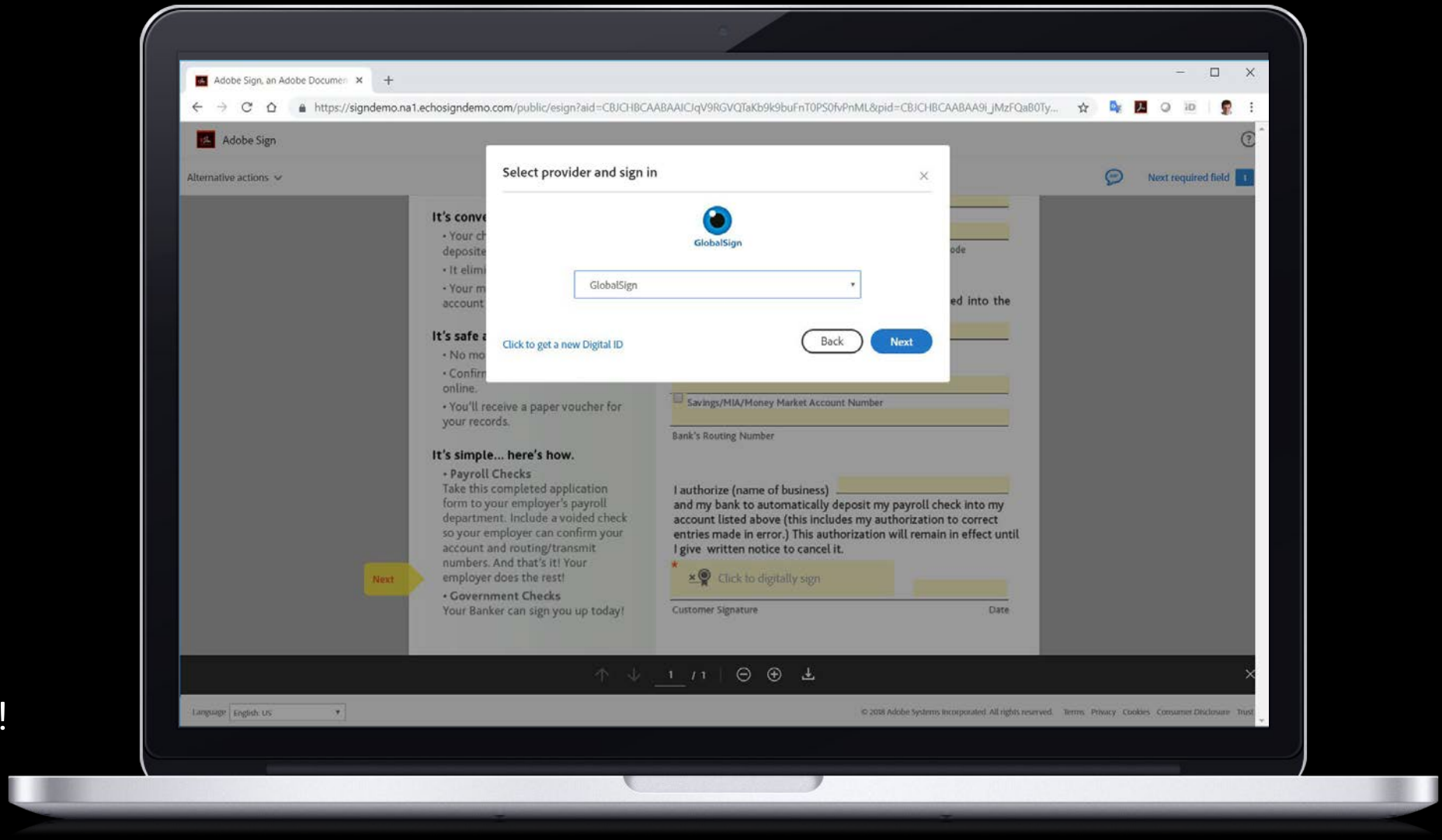
- **Fill in data fields** as needed.
- Click on the **signature field** to apply the digital signature.



Select your Provider

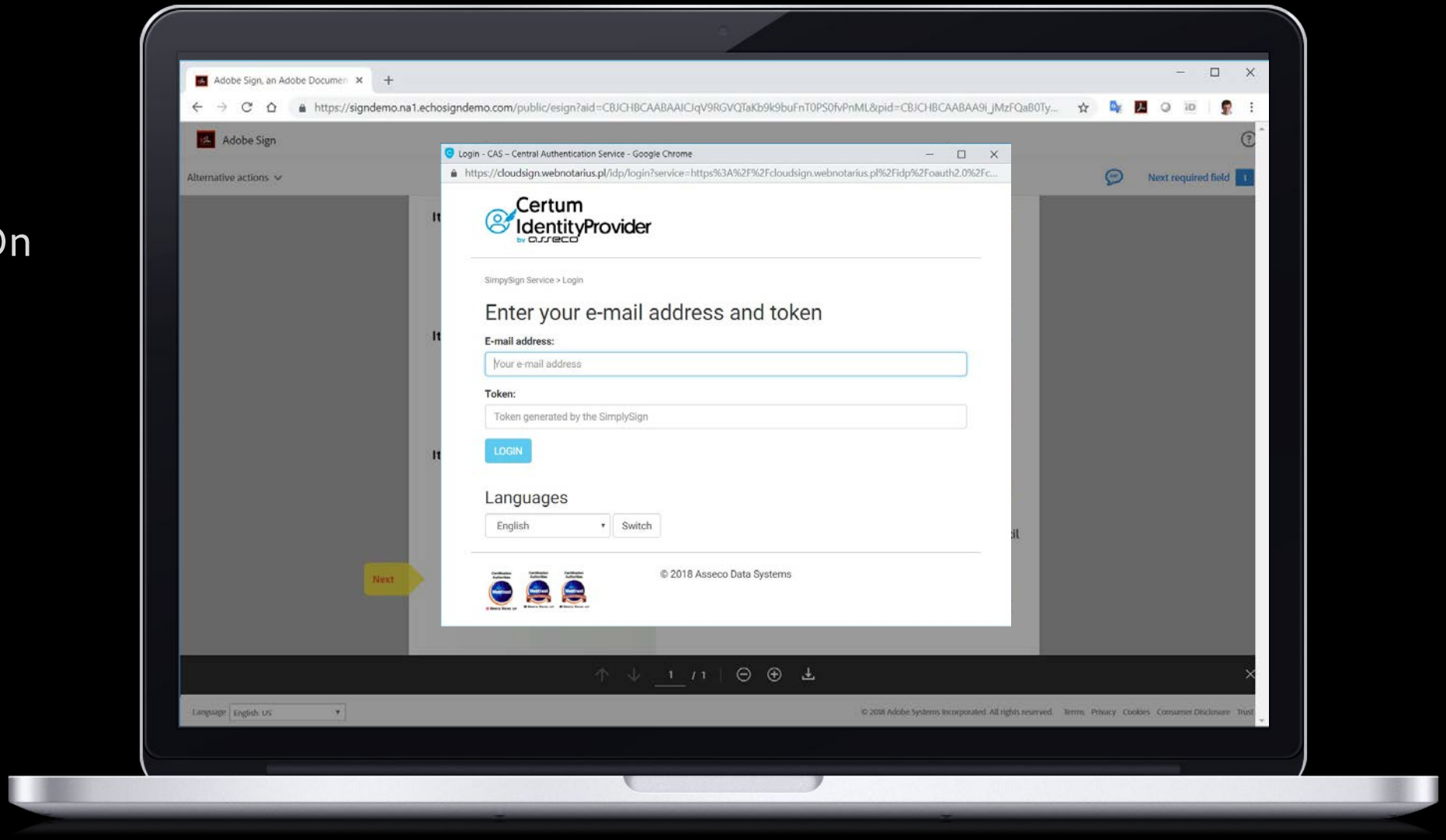
- **Select the CSC Provider** as needed.

- Currently available providers:
  - Asseco
  - BankID Sweden
  - BankID Norway
  - GlobalSign
  - InfoCert
  - Intesi Group
  - Seiko
  - Trans Sped
  - …more coming soon!



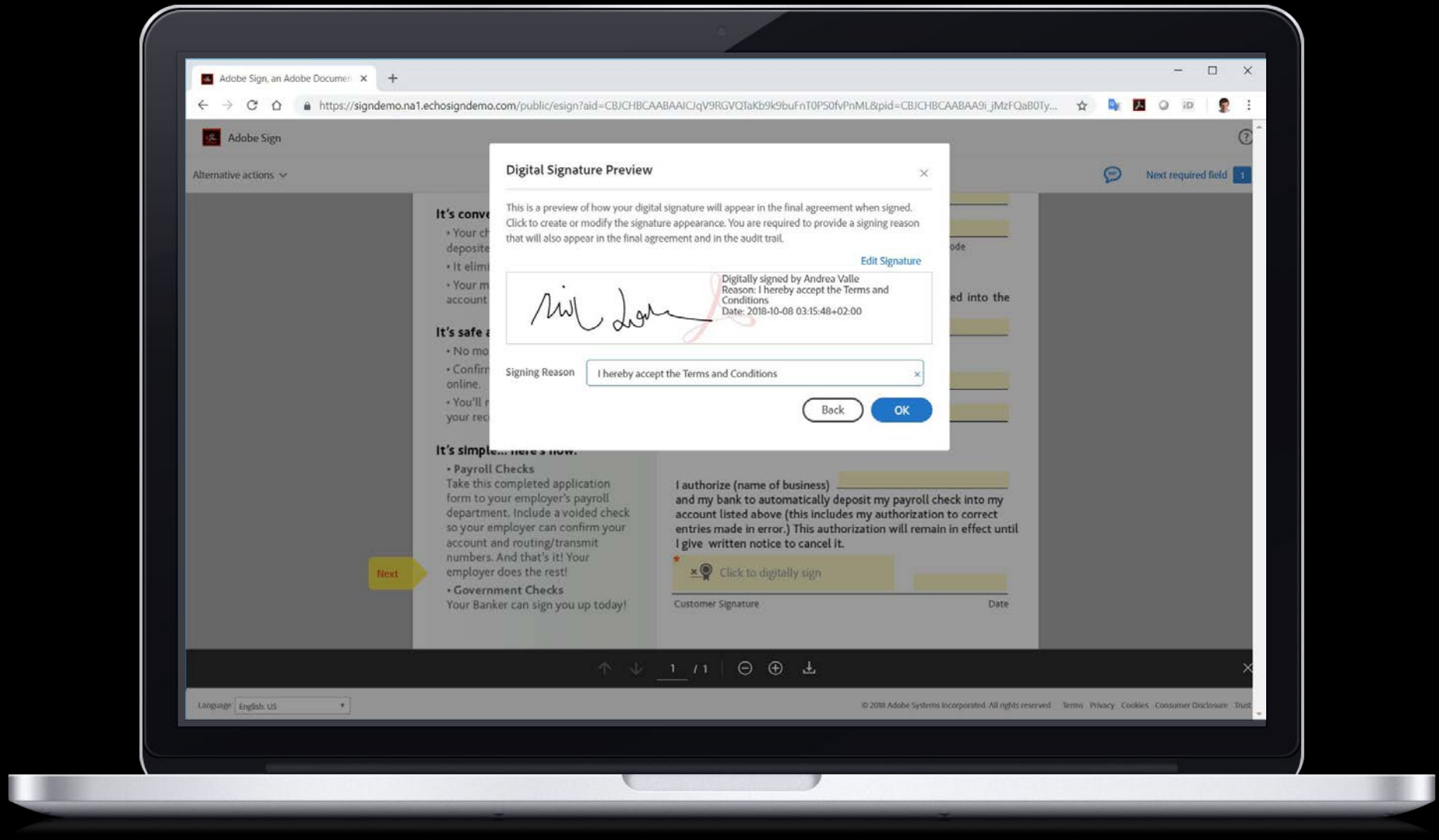
Authenticate with your Provider

- **Authenticate** with the chosen Provider using OAuth.
- Supports Single Sign On for Enterprise environments



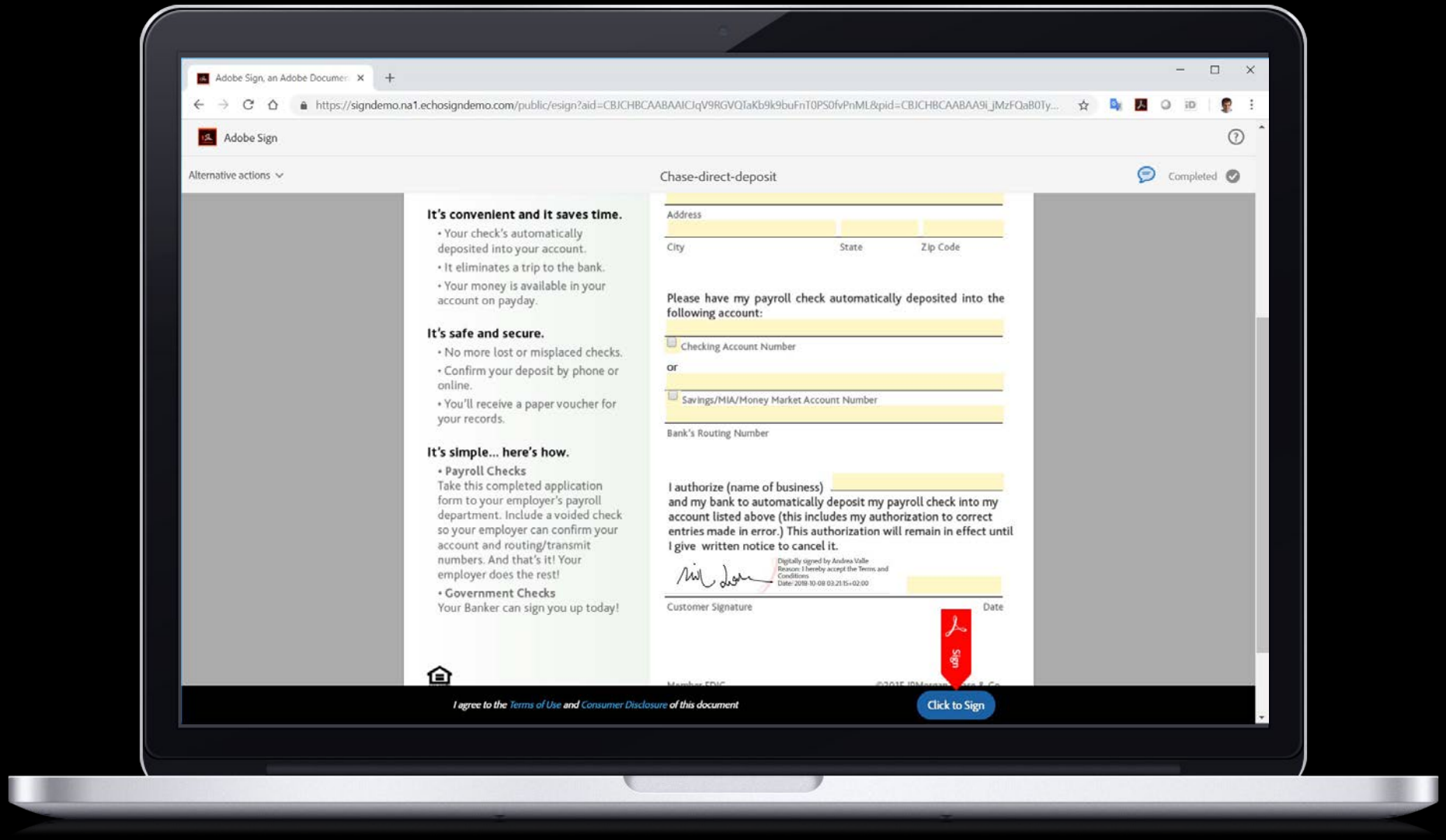
Configure and Preview your signature

- **Preview** the visual presentation of your digital signature. Shows how it will appear in the final signed agreement.
- Add a **Signing Reason** if needed.



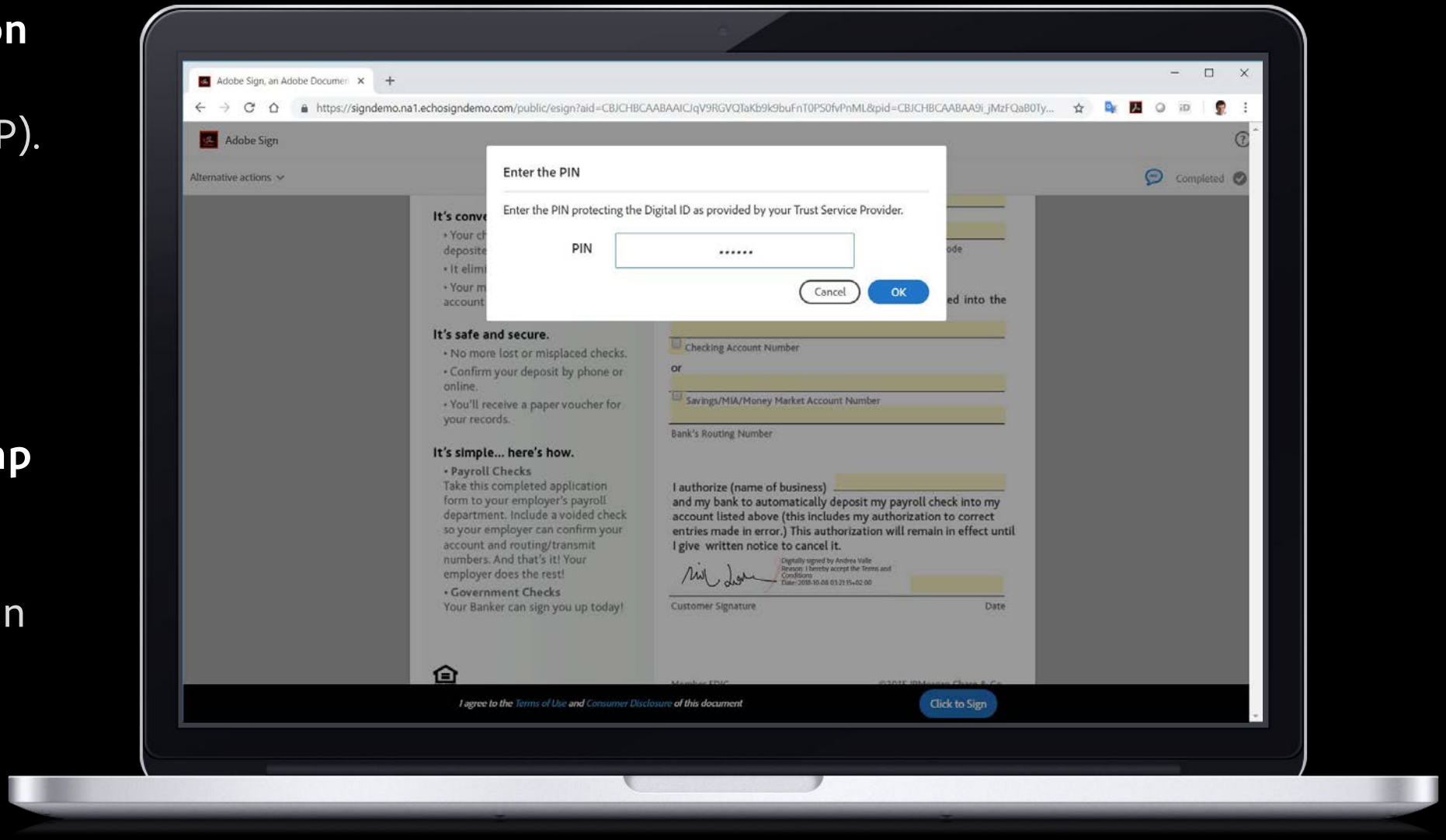
Apply the digital signature to the document

- Complete any other required form fields.
- Accept the terms and conditions as required and press the **Click to Sign** button.



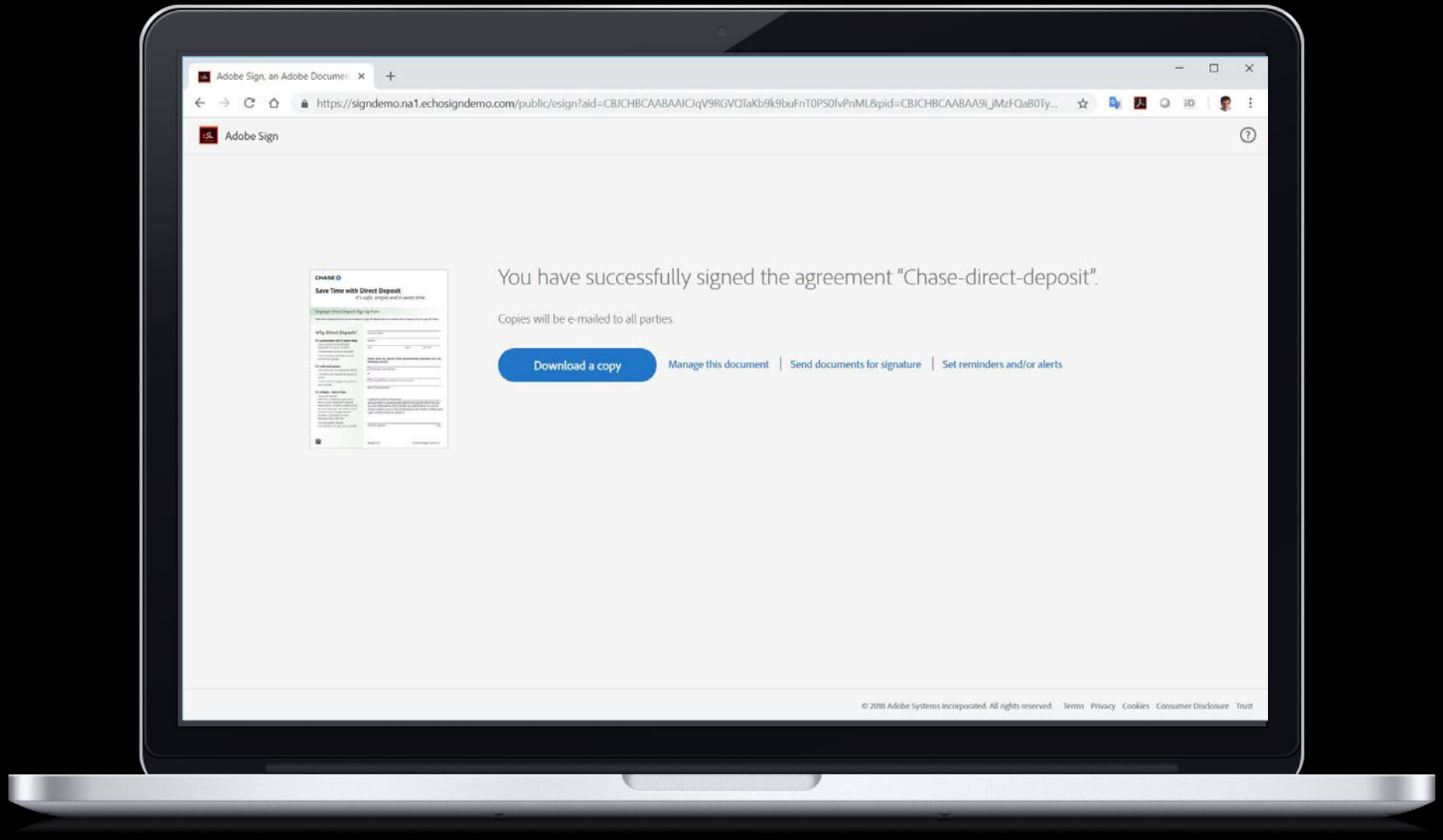
Authorize the signature

- Enter the **authorization data** that protects the Digital ID (e.g. PIN/OTP).
- Also supports other authorization factors via OAuth.
- A **Qualified Timestamp** is also automatically applied as a proof of existence and to obtain a Long Term Validity signature.



You have successfully signed the agreement!

- Your **Cloud Signature** has been applied successfully.
- The signed document is **archived** for unlimited time.
- You can **download a copy** of your signed document when needed at any time.



A look into Adobe's 2019 Roadmap

Adobe's Cloud Signature Roadmap

- **Adobe Cloud Signature Partner program**
  - Co-sell and co-marketing opportunity for TSPs
  - Develop custom solutions with Adobe Sign APIs
- **Support of OAuth for signature authorization**
  - Gives the Provider full control of the authorization process
- **Add Cloud Signature support to Adobe Acrobat and Reader**
  - Create remote signatures from the ubiquitous desktop applications with *Zero Footprint Setup*
- **Expand Cloud Signature services with Dynamic Identity Verification**
  - Currently supporting multiple eID schemes in Europe, extending to other eID schemes (e.g. My Number in Japan)
  - Simplified integration with Corporate Identity Services with dynamic certificate generation.
- **User Experience enhancements**
- **Onboard additional Trust Service Providers**

CLOUD
SIGNATURE
CONSORTIUM

Thank you!

Andrea Valle
avalle@adobe.com