Building interoperable eIDAS Trust Services

The experience of the Cloud Signature Consortium

CA Day – Berlin – September 26th, 2019

Andrea Valle | President

CLOUD SIGNATURE CONSORTIUM

CLOUD
SIGNATURE
CONSORTIUM

Building a standard for cloud signatures

A new industry consortium to pioneer
open digital signatures for mobile and the web

#OpenSignature

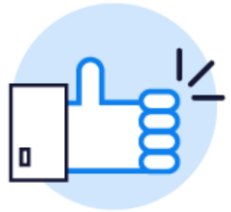
Meet the Cloud Signature Consortium

- The **Cloud Signature Consortium** is an international non-profit association among solution, technology and trust service providers
  - Promote cloud-based Digital Trust Services.
  - Design a common architecture and building blocks to facilitate trust service interoperability
  - Develop technical specifications about protocols and API
  - Publish technical specifications as open standards.

Secure transactions, on the go

Cloud storage, no download

Simple certificate ownership



Easy deployment for end users

CLOUD SIGNATURE CONSORTIUM

The latest events

- **January 2018: The Consortium becomes a Not For Profit Association**
  - Acquired legal personality to support membership expansion and advocacy worldwide
- **September 2018: Membership is open. New members joining the Consortium**
- **December 2018: The CSC API V1 Specification is published**
  - Final version publicly available at: https://cloudsignatureconsortium.org/resources/
  - JSON and OpenAPI schemas
- **April 2019: Cooperation Agreement with ETSI**
  - Allow mutual exchange of contributions for the development of trust service standards
  - The CSC API specification is included in ETSI TS 119 432: “Protocols for remote digital signature creation”
- **June 2019: First Annual General Meeting**
- **Ongoing outreach activities**
  - Active cooperation with various Government agencies developing public policies on remote digital signatures.

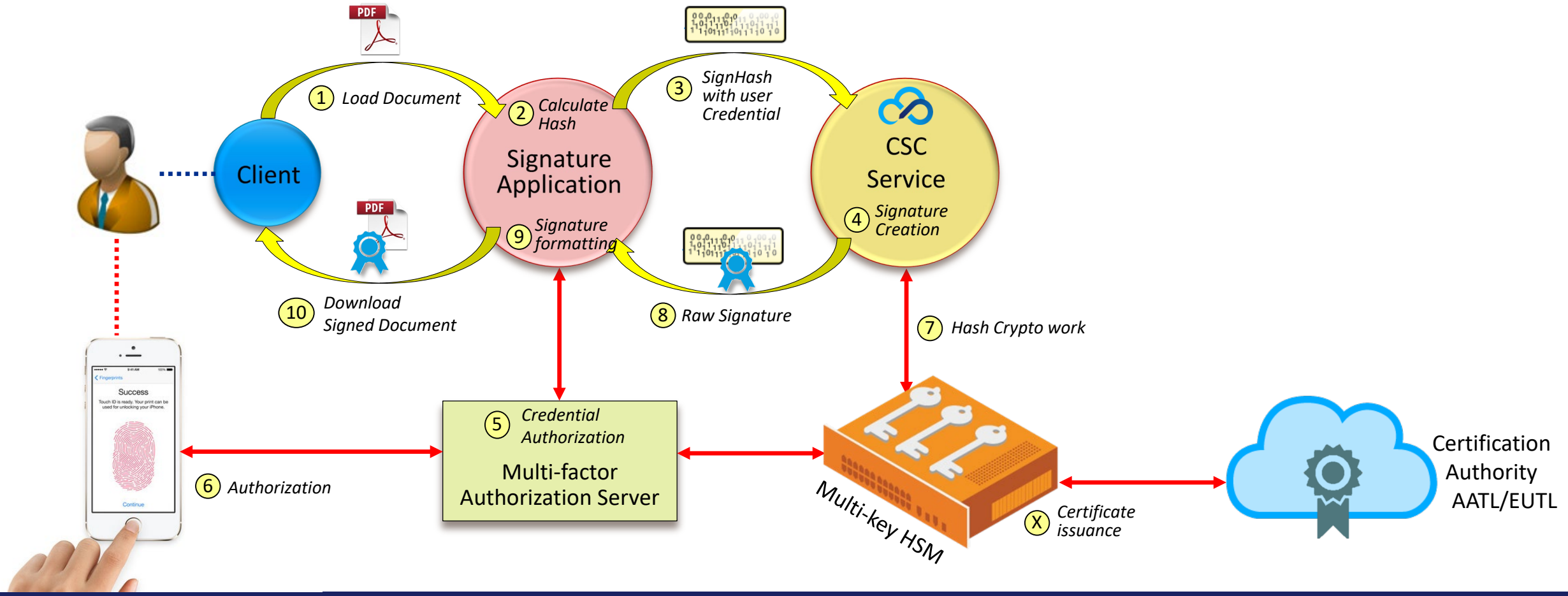
The CSC Members

CSC Solution Architecture

CLOUD
SIGNATURE
CONSORTIUM

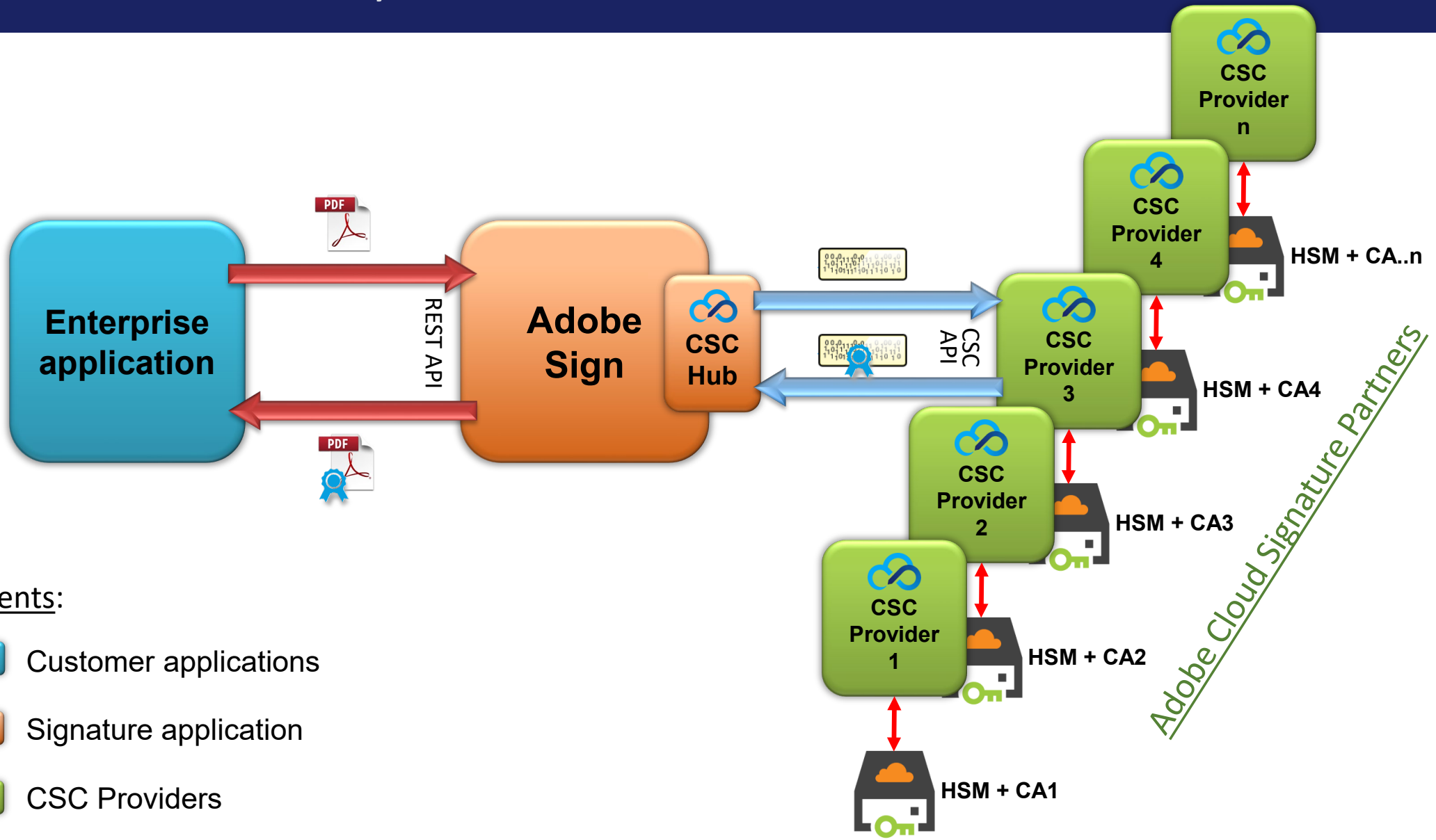
Architecture of a CSC-compliant Cloud Signature Service

- A centralized HSM hosted by the Trust Service Provider offers multi-user credential storage and access with secure control through a multi-factor authorization server.



CLOUD SIGNATURE CONSORTIUM

Adobe and the CSC ecosystem



Environments:

- Customer applications
- Signature application
- CSC Providers

CLOUD SIGNATURE CONSORTIUM

The CSC Standard: aimed at Interoperability

CLOUD SIGNATURE CONSORTIUM

Key interoperability factors in CSC API specification

1. **The API format**
   - Web Service API based on REST protocol and JSON data interchange.
   - Simple learning curve for developers.
   - Modern and fast to implement.
2. **Design for flexibility**
   - Supports modular services, in line with the capacity of providers and the requirements of consumers.
   - Service Providers can implement only a particular subset of the API.
   - Self-discovery capacity: client applications can easily discover the supported APIs of a provider.
3. **Designed for growth**
   - API Versioning
   - Retro compatibility of newer versions: prevent obsolescence of older implementations

Key interoperability factors in CSC API specification (cont.)

4. **Natively support authentication protocols**
   - Support a wide and flexible list of authentication schemes:
     - OAuth 2.0, SAML, OpenID Connect, HTTP Basic/Digest auth.
   - Support multiple use cases: Desktop and Mobile apps, Cloud-based and on-premise services.
5. **Support secure authorization mechanisms**
   - Signing credentials can be controlled with PIN, online and offline OTP, OAuth.
   - Multi-Factor-Authorization can be obtained by combining multiple mechanisms.
6. **Support a broad set of technical requirements**
   - Signature algorithms, formats, key type, key size, padding algorithms, …
   - ETSI and CEN standards for eIDAS-compliant remote signatures
   - Support a broader range of requirements for global adoption.

CSC API next | Anything missing?

- One-shot certificate generation during the “signHash” operation
- Online real-time certificate enrollment
- Native support of Identity Verification components
- Asynchronous operations
- Document signing
- Signature validation

CSC Roadmap 2019-2020

CLOUD SIGNATURE CONSORTIUM

CSC Technical Working Group roadmap 2019-2020

- Expansion of authentication and authorization options
- Alignment with ETSI TS 119 432 standard
- API Error handling update
- Handling of one-shot / short-term certificates
- Conformity checker update
- Signature validation and augmentation protocols

Joining the Cloud Signature Consortium

- **Take part to Technical Community of the Cloud Signature Consortium**
  - Joining the CSC means becoming a member of an active community of adopters and endorsers:
    - Trust 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 updated API specifications.
  - Conformity Checker software to test implementations for interoperability and performance analysis.
- **We're a Partner in Public Policy development**
  - A group of experts in trust service standards development and regulatory compliance.
  - Technical awareness and dissemination initiatives.

https://cloudsignatureconsortium.org/join-us/

CLOUD
SIGNATURE
CONSORTIUM

Thank you!

Andrea Valle
avalle@adobe.com