



Adobe

# Cloud Signatures and the Adobe Approved Trust List Program

North America Workshop on Trust Services Globalization | September 3, 2019

Andrea Valle | President

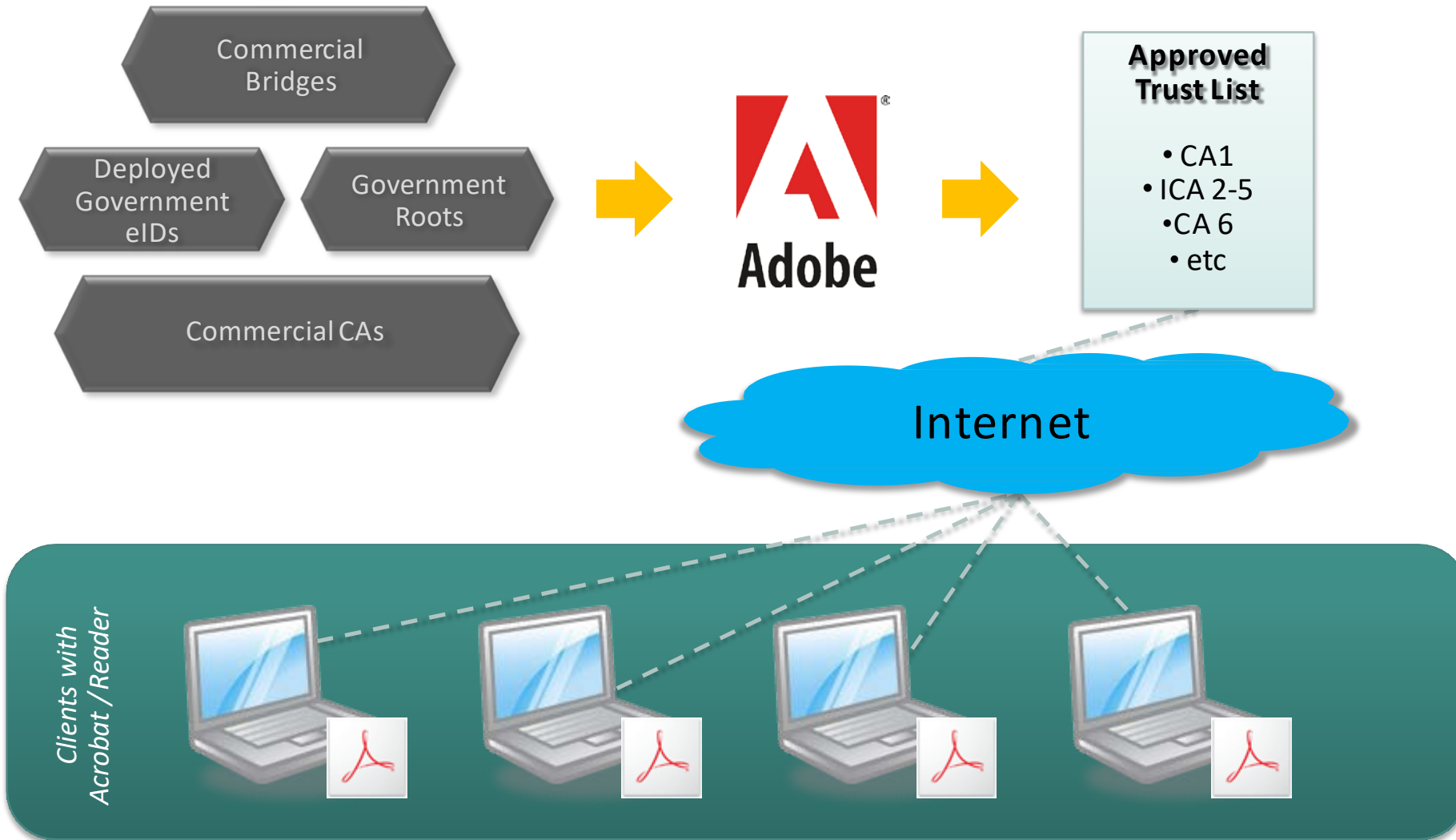


CLOUD  
SIGNATURE  
CONSORTIUM

# All about PDF signatures

- ETSI standard EN 319 142 referenced in ISO 32000
- PDF is the most widely used format for digitally signing documents
- Estimated volume of 10+ Billion PDF digitally signed every year
- Sign and Validate in Adobe Acrobat Reader for free
- More than 500 million monthly active users in Adobe products

# Adobe Approved Trust List | Concept



# A look into the AATL program



- Established in 2008
- Works with Adobe Acrobat and Acrobat Reader since version 9.0
- 70 active members, covering about 100 TSP
- Membership fee for Commercial providers
- Free membership for non-commercial Government providers
- <https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>



# AATL Program Requirements


- Audited CA operations: WebTrust, ETSI EN 319 411, etc.
- Good end user key gen and key storage mechanisms: FIPS 140-2 L2, QSCD, Common Criteria, Medium HW Assurance
- Strong Identity Proofing: face to face or equivalent (e.g. real-time Video ID)
- SHA256 and stronger. SHA1 deprecated
- Revocation services mandatory
- Security Breach notification
- Policy restrictions for non-compliant sub-CA

# AATL characteristics and benefits



Certified by Adobe Sign, a Document Cloud solution, Adobe Systems Software Ireland Ltd., certificate issued by Intesi Group EU Qualified Electronic Seal CA G2.

- Visual Trust and assurance
  - Is this signature valid?
  - Has the document been changed?
  - Can I trust the signatory?
- Consistent requirements
- Full interoperability
- Great User Experience

 Digitally signed by Andrea Valle  
Reason: This is a test signature  
Date: 2017-12-05  
15:17:10+01:00

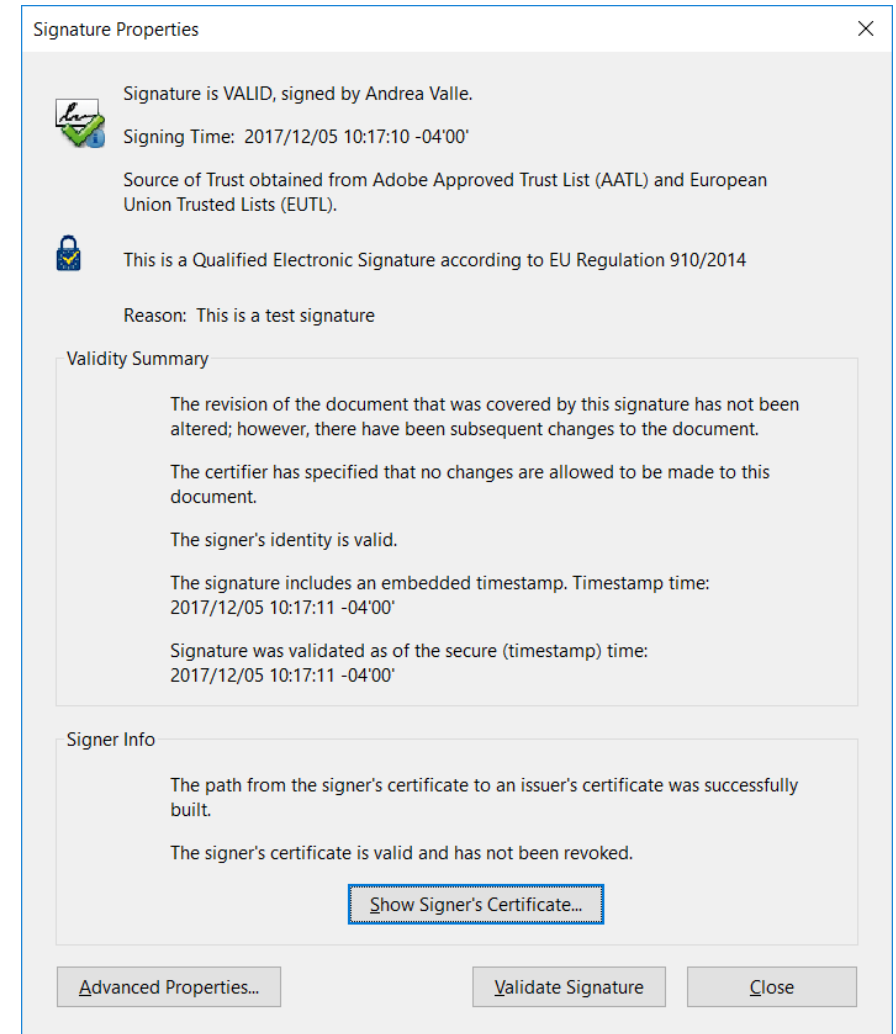
Higher assurance standards + convenient trust configuration

=

High value, automatically trusted digital signatures

# EU Trusted List support

- Adobe Acrobat and Acrobat Reader natively support EU Trusted Lists (EUTL)



- <https://helpx.adobe.com/document-cloud/kb/european-union-trust-lists.html>

# Digital Signatures in the era of Cloud

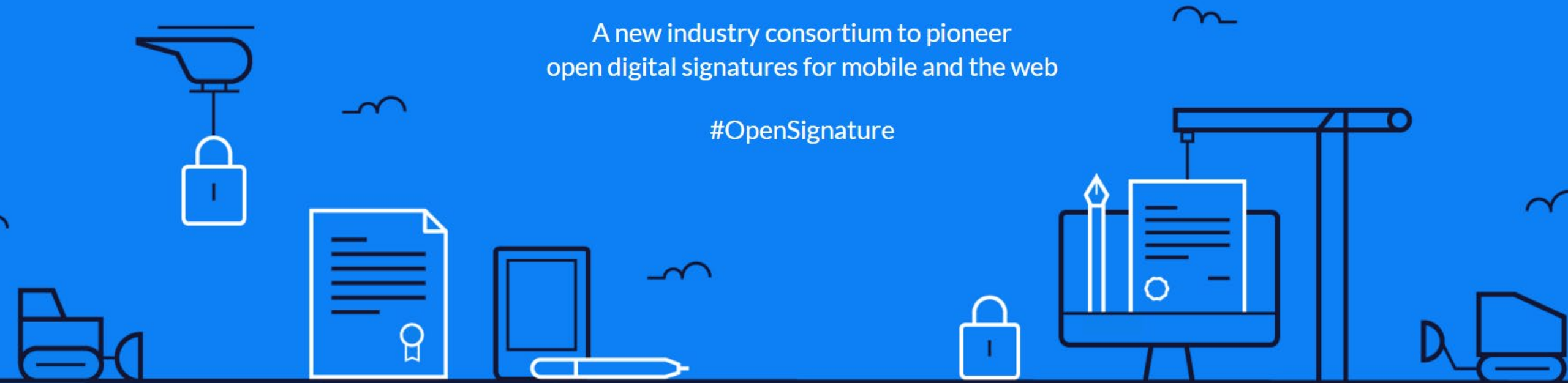




# Building a standard for cloud signatures

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

# The CSC Members



# A quick look into the CSC Standard



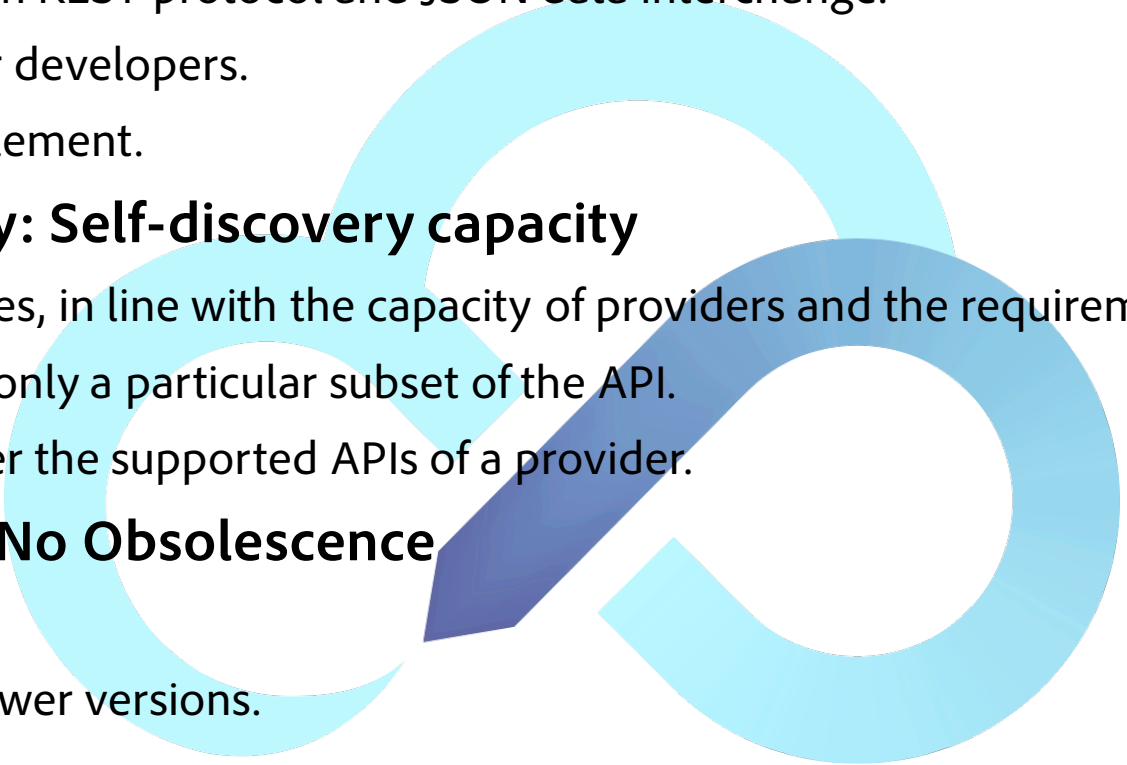
## Architectures and protocols for remote signature applications

Published version 1.0.4.0 (2019-06)

All rights reserved – Copyright © 2016-2019 Cloud Signature Consortium VZW

WVZ multiozonno aruengit? duod eL02-2102 © rthgnrpoD – bevrertr zrngh III A

# The CSC Technical Specifications V1 in a nutshell

- **The CSC Specification: architectures, protocols and API for Remote Signature Creation**
    - Web Service API based on REST protocol and JSON data interchange.
    - Simple learning curve for developers.
    - Modern and easy to implement.
  - **Designed for flexibility: Self-discovery capacity**
    - Supports modular services, in line with the capacity of providers and the requirements of consumers.
    - Services can implement only a particular subset of the API.
    - Clients can easily discover the supported APIs of a provider.
  - **Designed for growth: No Obsolescence**
    - API Versioning
    - Retro compatibility of newer versions.
- 

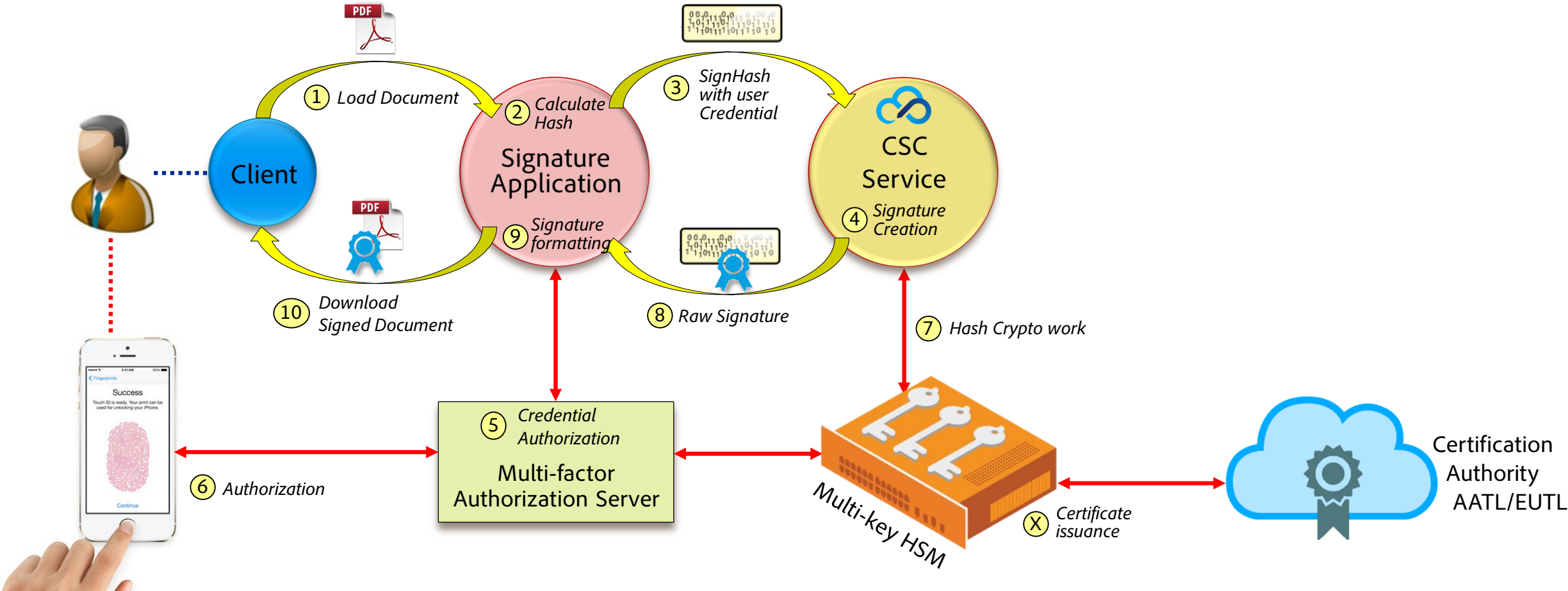


# The CSC Technical Specifications V1 in a nutshell (cont.)

- **Native support of client and user authentication**
  - Supports HTTP Basic/Digest auth and OAuth.
  - Can be implemented in multiple contexts:
    - Desktop and Mobile apps, Cloud-based and on-premise services.
- **Flexible support of credential authorization mechanisms**
  - Credentials can be controlled with static secrets, online and offline OTP, OAuth.
  - Multi-Factor-Authorization can be obtained by combining multiple mechanisms.
- **Support technical requirements of ETSI and CEN standards for remote signatures**
  - But flexible to support a broader set of requirements for Global adoption.

# 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 multi-factor authorization.



# Conclusions

1. Global Trust Service interoperability.
2. Quality of Identity Proofing.
3. Move digital signatures to the Cloud.



**Adobe**