



CLOUD
SIGNATURE
CONSORTIUM

Andrea Valle | Chairman of the Steering Committee

July 2017

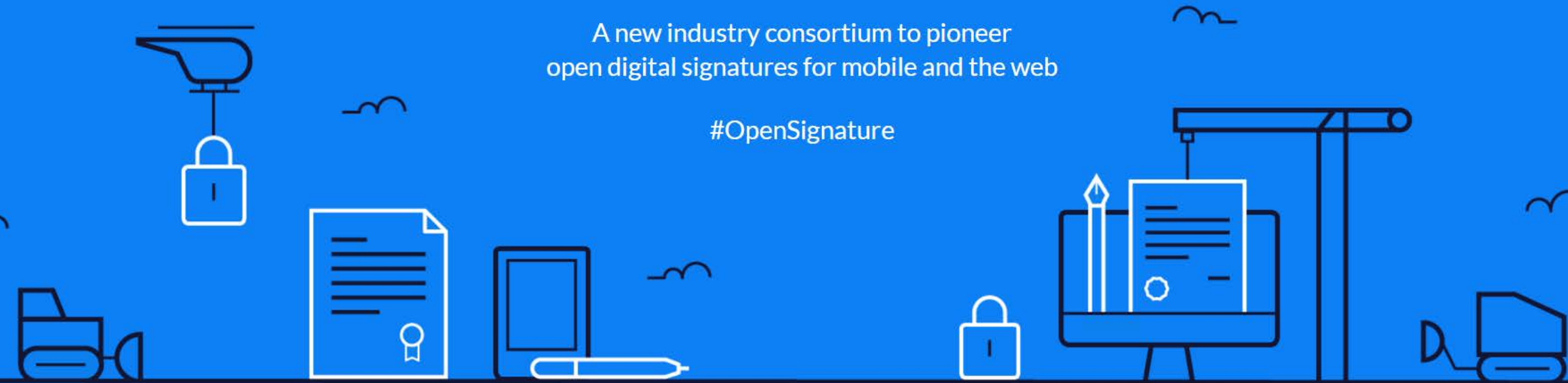
Goals of the Consortium



Building a standard for cloud signatures

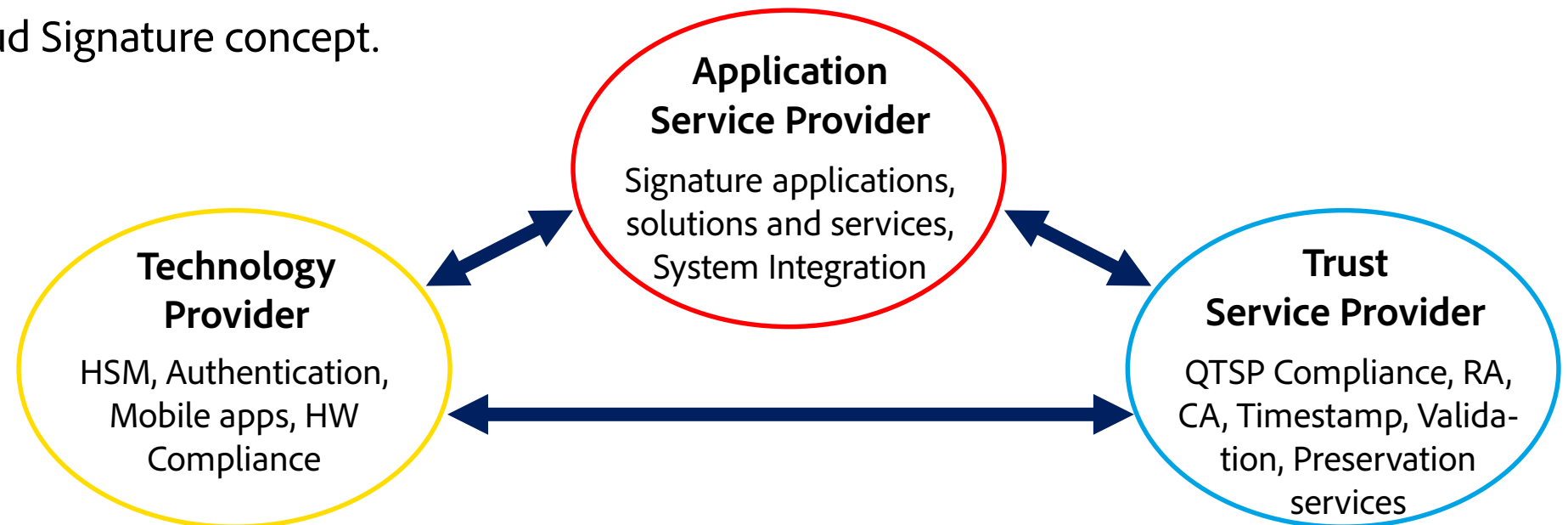
A new industry consortium to pioneer
open digital signatures for mobile and the web

#OpenSignature



The Cloud Signature Consortium

- The **Cloud Signature Consortium** was funded at the beginning of 2016 by an international cooperation group of industry and academic experts, including solutions, technology and trust service providers, aiming at:
 - Designing a common architecture and building blocks to facilitate the interaction between Solution, Technology and Trust Service Providers.
 - Developing technical specifications for protocols and APIs to make these interactions interoperable.
 - Publishing the specifications as an open standard.
 - Promoting the Cloud Signature concept.



Funding Members

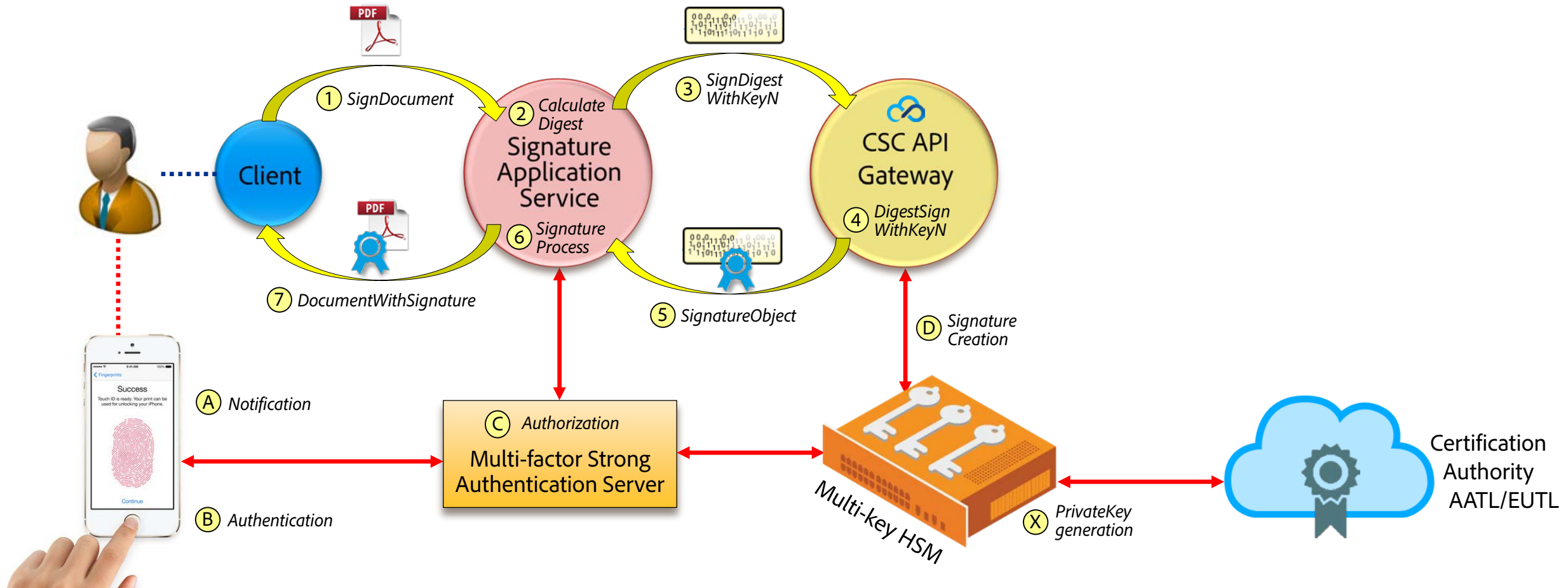
Adobe	Ireland/USA
Cryptolog / Universign	France
Docapost / Certinomis	France
Intesi Group	Italy
InfoCert	Italy
Asseco Data Systems	Poland
D-Trust/Bundesdruckerei	Germany
Intarsys	Germany
Izenpe	Spain
SafeLayer	Spain
SwissSign	Switzerland
Technische Universität Graz	Austria
Unibridge	Norway



Multiple scenarios for Cloud Signing

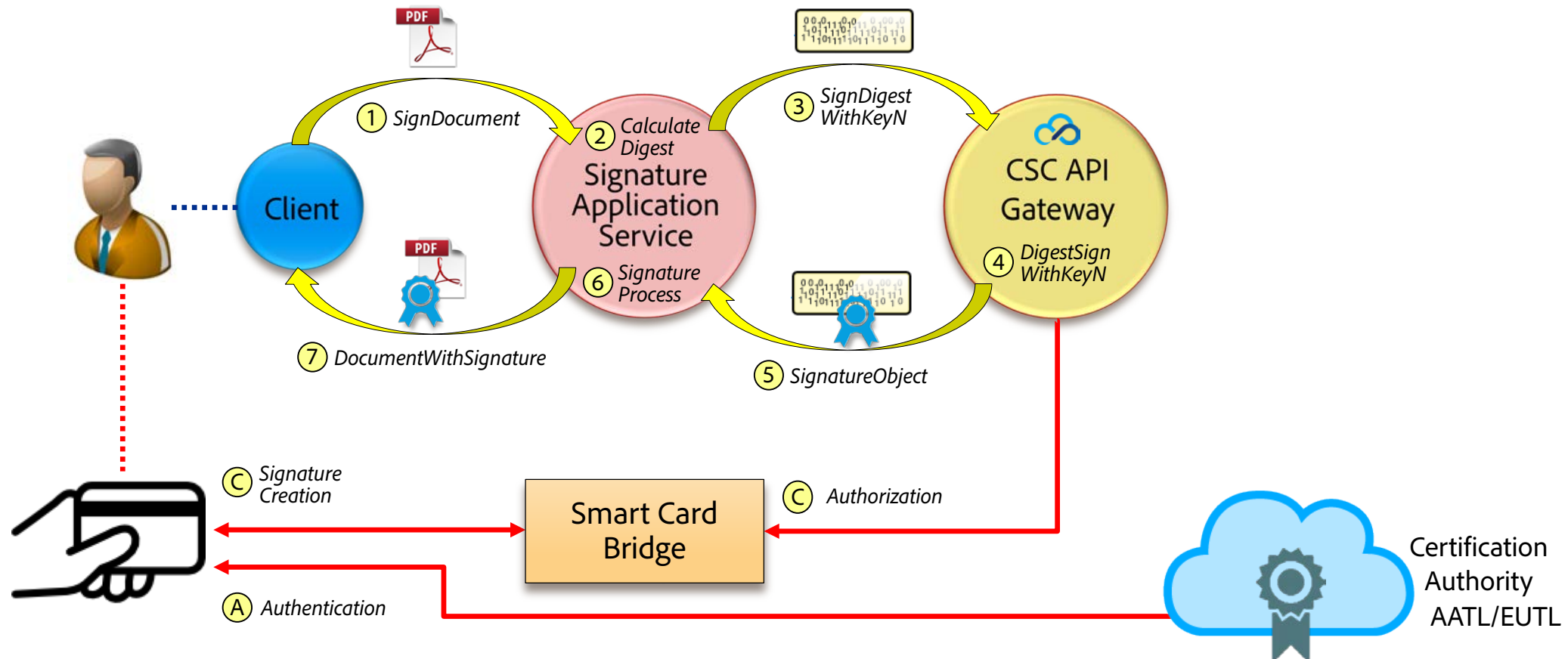
[1] Multiple credentials hosted in centralized HSM

- The personal signature device is replaced by multi-user HSM hosted by a Trust Service Provider offering secure access through multi-factor strong authentication.



[2] Cloud-enabled Smart Card

- A personal signature creation device is connected to a Cloud-based Signature Application Service instead of using a desktop tool for signing. The Cloud service provides a preview of the document and drives the signature through Web or Mobile user interactions.



A quick look into the Standard

The Cloud Signature Consortium Technical Specifications

- **The initial scope of the CSC Specifications is to cover architectures, protocols and APIs for Remote Signature creation.**
- **Designed to support the most demanding CEN and ETSI standards**
 - Goal is to support the broadest set of requirements, including those outside the EU standardization domain.
 - The specifications define Web services APIs based on REST protocols and JSON data-interchange. Modern and easy.
- **A CSC compliant service provides self discovery of its dynamic capabilities**
 - Designed to support modular services in line with the mission/capacity of the provider.
 - Services may implement only a particular subset of the API methods. Clients can easily discover the supported APIs.
- **Complete support of client and user authentication**
 - Covers all possible implementation contexts: desktop and mobile apps, cloud and on-premise services.
 - Supports password-based, OAuth-based, SAML, federated authentication.
- **Flexible support of credential authorization mechanisms**
 - Static secret, synchronous and asynchronous OTP, OAuth-based, SAML, OpenID Connect, FIDO.
 - Multi-Factor-Authorization can be obtained by combining multiple mechanisms.

- **The first release of the CSC Specification (V0) has been published for public comments**
 - Publicly available from <http://www.clousignatureconsortium.org/specifications>
- **The CSC Specifications have been submitted to ETSI for consideration as a contribution to ongoing standardization process**
- **The Consortium is working with ETSI to establish a Cooperation Agreement to allow mutual exchange of contributions for the development of standards for trust services.**

Next steps

Standardization roadmap

- **The Standardization roadmap of the Cloud Signature Consortium includes protocols and API supporting the following services:**
 - Cloud Signature (Remote Signature)
 - Signature validation
 - Signature augmentation
 - Certificate enrollment

- **All these services will benefit from a common service framework**
 - Client and user authentication
 - Resource authorization
 - REST+JSON API
 - Interoperability by design

Membership expansion

- The Cloud Signature Consortium has been officially launched at the end of June 2016, in sight of the adoption of the European eIDAS Regulation.
- About 60 leading businesses in the PKI and Trust Service industry from all over the world are joining the Consortium.
- New memberships will be open soon.

Interested to join? www.cloudsignatureconsortium.org/contacts





Thank you

Andrea Valle | avalle@adobe.com