CLOUD
SIGNATURE
CONSORTIUM

Cloud Signature Consortium and Validation Services

Andrea Valle | Chairman of the Board

25–27 сентября 2018 года, г. Санкт-Петербург

CLOUD
SIGNATURE
CONSORTIUM

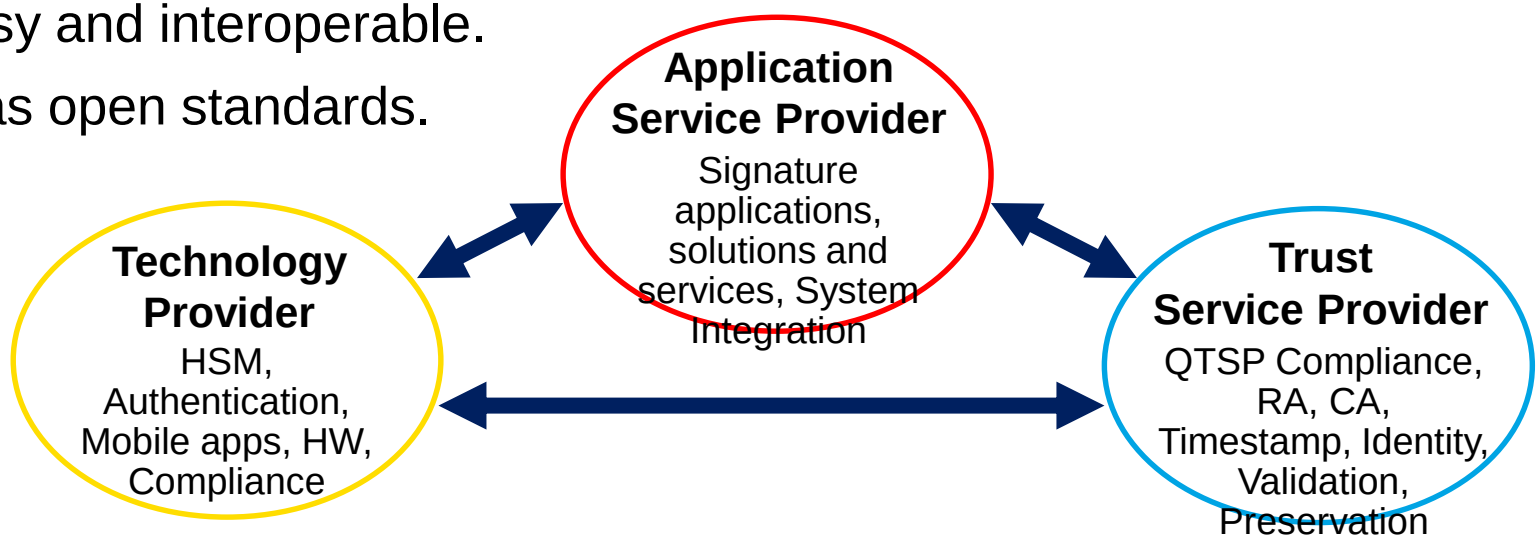
Building a standard for cloud signatures

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

#OpenSignature

The Cloud Signature Consortium

- The **Cloud Signature Consortium** was been 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 the interaction between Solution, Technology and Trust Service Providers.
  - Develop technical specifications for protocols and APIs to make these interactions easy and interoperable.
  - Publishing the specifications as open standards.



CLOUD SIGNATURE CONSORTIUM

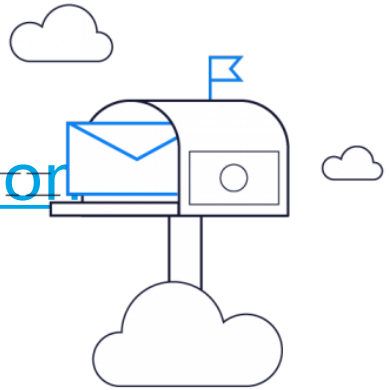
Founding Members

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

Current status

- **The Consortium has been incorporated as a Not For Profit Association**
  - It has acquired legal personality to support its membership expansion worldwide.
  - Working with ETSI to establish a Cooperation Agreement to allow mutual exchange of contributions for the development of standards for trust services.
- **The first release of the CSC Specifications is publicly available**
  - http://www.clousignatureconsortium.org/specifications
- **The Consortium is developing a Conformity Checker**
  - Test service implementations for interoperability and performance analysis.

Interested to join? www.cloudsignatureconsortium.org/co



A quick look into the Standard

CLOUD
SIGNATURE
CONSORTIUM

The Cloud Signature Consortium Technical Specifications

- **The first release of the CSC Specifications aimed at covering architectures, protocols and APIs for Remote Signature creation.**
  - Defines Web Service APIs based on REST protocol and JSON data-interchange. Modern and easy to implement.
- **Able to dynamically grow, with self discovery capacity**
  - Designed to support of growing and modular services, in line with the mission/capabilities of providers.
  - Services may implement only a particular subset of the API. 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.
  - Multi-Factor-Authorization can be obtained by combining multiple mechanisms.
- **Designed to support eIDAS requirements and CEN / ETSI standards**
  - Also supports a broader set of requirements, including those outside of the EU standardization domain.

Validation Services Technical Specification

- **The Consortium has developed API specification for Validation Services**
  - Contribution from various CSC members, in particular from Asseco.
  - Based on the experience with existing services (e.g. WebNotarius) and with the implementation of PEPPOL projects.
- **Will be submitted to ETSI as part of the Cooperation Agreement**
  - Contribution as a protocol profile for signature validation (e.g. TS 119 442).
- **Current draft under review to evaluate the alignment with the STF work**
  - Will be available for public comments.

Main characteristics supported by CSC Signature Validation Services

- Synchronous and asynchronous operations
- Multi-policy support
- Support of EUTL and other Trusted Lists (non-EU, custom)
- Certificate chain Validation
- Signature Validation and Augmentation
- Hook for Preservation services
- Lightweight JSON protocol
- Privacy by design

Next steps of the Consortium

CLOUD
SIGNATURE
CONSORTIUM

Standardization roadmap

- **The Cloud Signature Consortium's roadmap includes protocols and API supporting multiple trust services**
  - Cloud Signature (Remote Signature)
  - Signature validation and augmentation
  - Electronic Identity
  - Long-term Preservation
- **Services benefit from a common API framework and unified approach**
  - Client and user authentication
  - Resource authorization
  - REST+JSON API
  - Standard and interoperable by design
  - Privacy by design

Thank you

Andrea Valle |
avalle@adobe.com

CLOUD
SIGNATURE
CONSORTIUM