TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste"

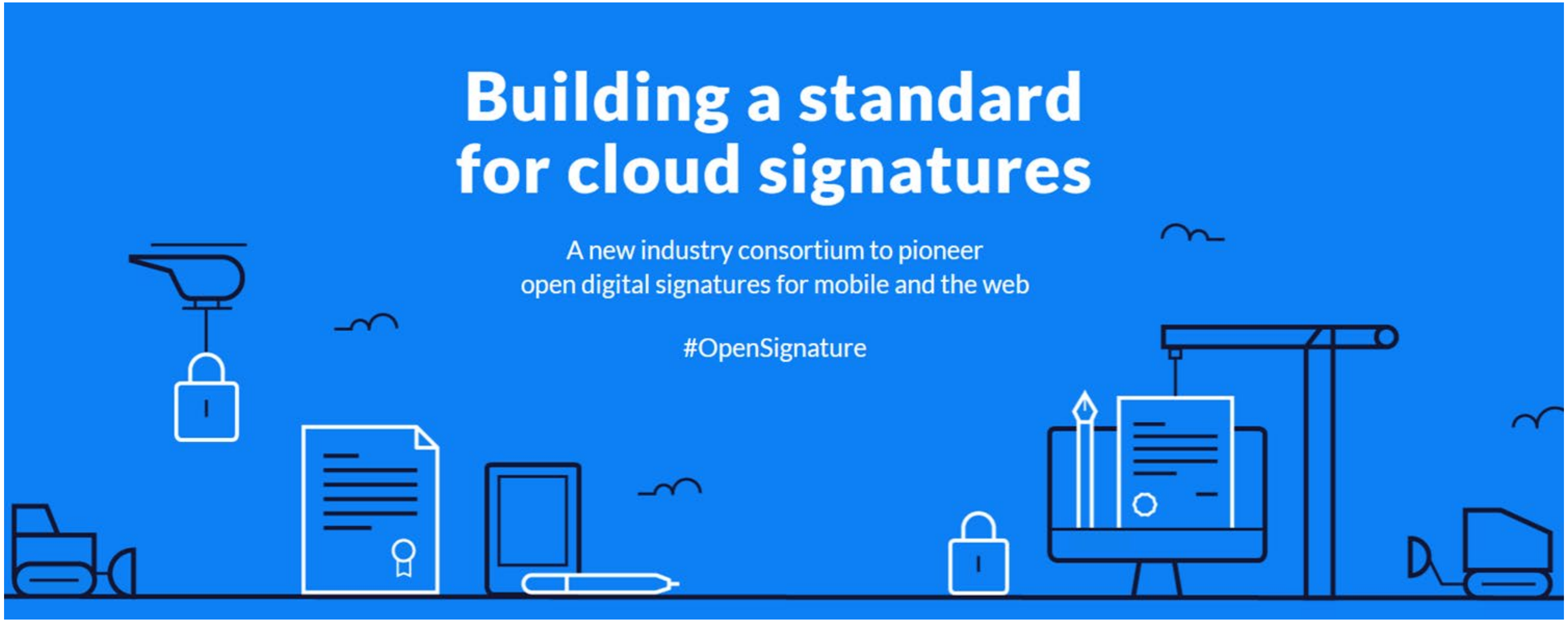
Berlin, 27.09.2023

Cloud Signature Consortium (CSC)

International standard for connecting remote signatures

Viky MANAILA
President CSC

CSC – Vision & Mission

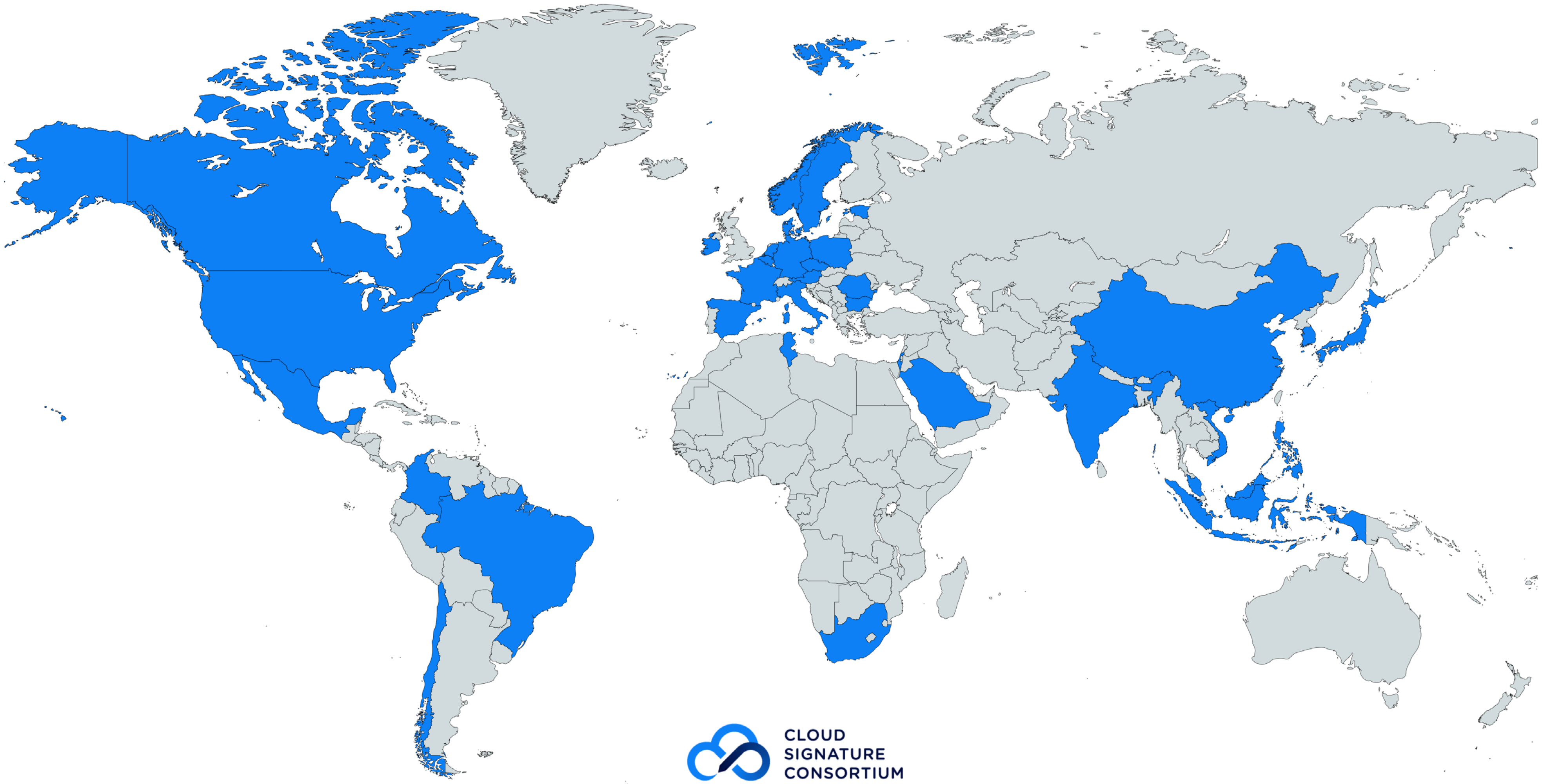


CLOUD
SIGNATURE
CONSORTIUM

www.cloudsignatureconsortium.org

The primary standard for cloud-based digital signatures

- Established in 2016
- 71 members from 41 countries
- Cooperation with ETSI
- ETSI TS 119 432 standard
- V2 standard released



CLOUD
SIGNATURE
CONSORTIUM

Signing documents with EUDIW – High Level Concept

TelеTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

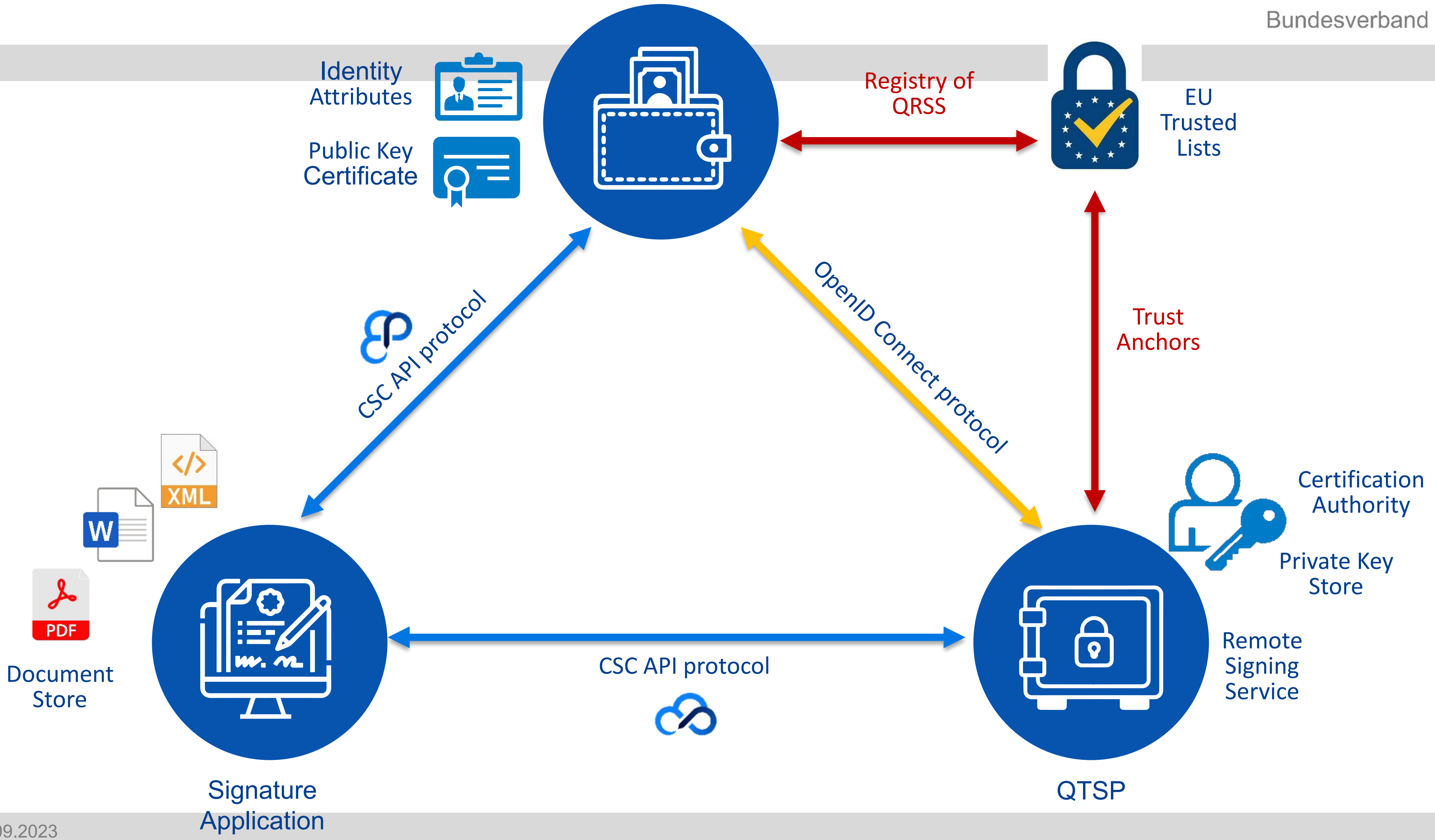
Combination of QTSP/TSP and RP signing service

1. The user views the document(s) and consents to sign
2. The user is authenticated using EUDI Wallet
3. The user can sign with his digital certificate, or can choose a QTSP that can issue a short lifetime digital certificate
4. A qualified certificate (short lifetime) is issued for the authenticated identity of the user
5. API for signing standardised by CSC

CLOUD SIGNATURE CONSORTIUM

Signing documents with EUDIW – High Level Concept

- a signature can be based on different types of attributes; most signatures rely on identifying data contained in the PID
- the role of the participant facilitating the signing/sealing functionality is an electronic signature/seal provider
- **the signing process**, including how to show the document to the user and obtain consent to sign **will be initiated by the Relying Party**
- the RP is also responsible for sharing the signed document with the user
- the approach will be a remote (server- or cloud-based) signing/sealing process


Identity
Attributes
Public Key
Certificate
Registry of
QRSS
EU
Trusted
Lists
CSC API protocol
OpenID Connect protocol
Trust
Anchors
Certification
Authority
Private Key
Store
Remote
Signing
Service
XML
W
PDF
Document
Store
CSC API protocol
Signature
Application
QTSP

CSC contribution to QES with the EUDI Wallet

TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- The Identity Wallet …
  - … stores identity attributes and verified identity credentials
  - … provides authentication and identification, **it's not a QSCD**
  - … can initiate a Qualified Electronic Signature, **it's not a signature application**.
- The QTSP generates short-term or Long-term qualified certificates
  - and stores the signing credentials in the QSCD on behalf of signatories.
- The Qualified Electronic Signature is performed remotely by the signatory
  - with the QSCD managed by the QTSP, by authenticating with the EUDI Wallet.

Multiple Use Cases supported

1. The Identity Wallet enables a QSCD hosted remotely by a QTSP to issue a **short-term** qualified certificate for remote electronic signature
   - A signatory can seamlessly obtain a qualified certificate and create a qualified signature "on-the-go" with no preliminary setup or configuration.
2. The Identity Wallet enables a QSCD hosted remotely by a QTSP to issue a **long-term** qualified certificate for remote electronic signature
   - A signatory can easily obtain a qualified certificate with a one-time digital identification event.
3. The Identity Wallet is used to **authenticate** with a QSCD hosted remotely by a QTSP, storing a qualified certificate for remote electronic signature
   - A frequent signatory can create qualified signatures quickly and in total control of existing signing credentials.

Thank you!

Viky Manaila

vmanaila@intesigroup.com