

E-GOVERNMENT AND DIGITAL TRUST, EXPERIENCE FROM ABROAD

DIGITAL TRUST & PAPERLESS CONFERENCE - APRIL 2018



ABOUT SAFELAYER

- Independent Software vendor ISV
- Cyber security technologies for critical infrastructures
- Since 1999
- VARs in EMEA+LATAM
- Madrid + Barcelona

PKI for secure eIDs

WAC and devices (IoT)

eID validation and federation

Electronic signature and mobility

STANDARDIZATION AND QUALITY

STANDARDS

CERTIFICATIONS / HOMOLOGATIONS





























ETSI CAdES/XAdES Interoperability Tests













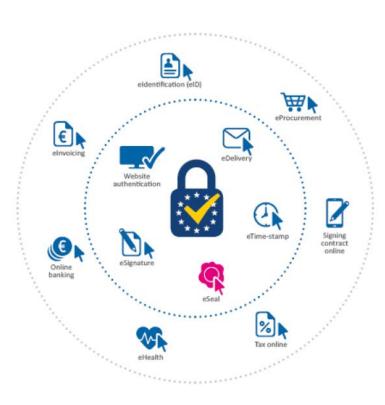




MAJOR SHIFT IN TRUST SERVICES

Directive 1999/93/EC

- Advanced electronic signatures (AES)
- Qualified electronic signatures (QES)



eIDAS Regulation 2014

- More trust services are now regulated
- Boost trust and convenience
- Normalizes remote signature for AES/QES
- Cross-border transactions (EU Trusted Lists)

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) consilium.europa.eu/uedocs/cms data/docs/pressdata/en/trans/144112.pdf. Source: ec.europa.eu/digital-agenda/en/trust-services-and-eid



STANDARDIZATION FORUMS



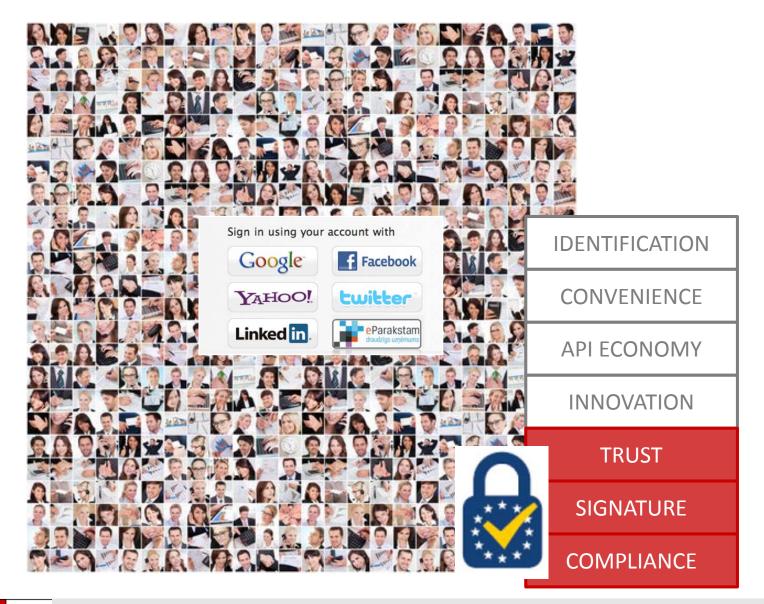
 The CEN/TC 224/WG17 workgroup, in which Safelayer is actively participating, is heading work on technical specification for server signing requirements (CEN/EN 419 241 series)



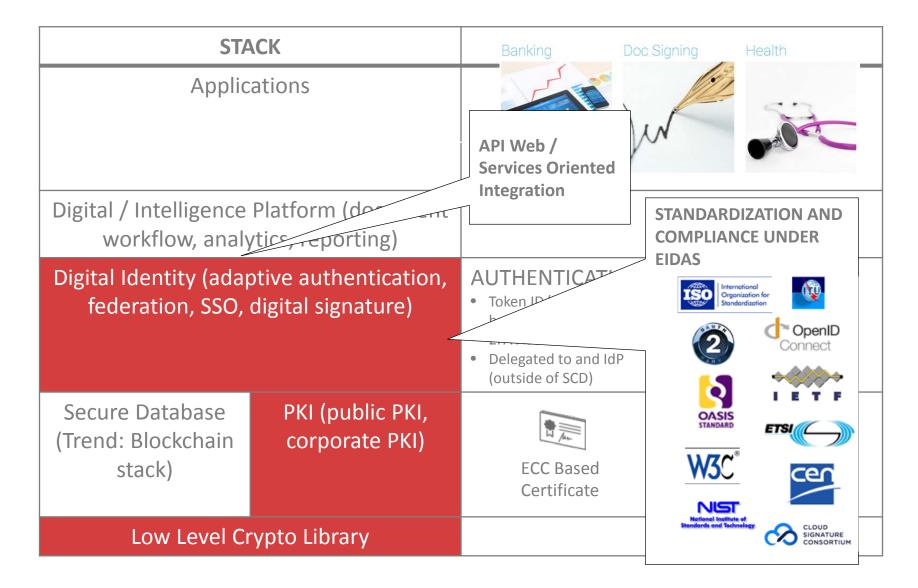
Remote Signing Protocol

• Group of industry and academic organizations committed to standardize the protocols for cloud-based digital signatures that will support web and mobile applications. **Safelayer** participates as a cofounder.

DIGITAL TRUST IMPLEMENTATION



DIGITAL TRUST STACK



STANDARDIZATION AND COMPLIANCE UNDER EIDAS (I/II)

ETSI EN 319 401: General Policy Requirements for Trust Service Providers

ETSI EN 319 411: Policy and Security Requirements for Trust Service Providers issuing Certificates

CEN TS 419 261: Security Requirements for Trustworthy Systems Managing Certificates and time-stamps

ETSI EN 319 412 Profiles for Trust Service Providers issuing certificates

ETSI EN 319 412-1: Overvlew and common data structures

ETSI EN 319 412-2: Certificates Issued to natural persons

ETSI EN 319 412-3: Certificates Issued to legal persons

ETSI EN 319 412-4: Web sites certificates Issued to organizations

CEN EN 419 221: Protection Profiles for TSP cryptographic modules ETSI EN 319 421:
Policy and
Requirements for Trust
Service Providers
issuing Time-Stamps

CEN TS 419 261:
Security Requirements
for Trustworthy
Systems Managing
Certificates timestamps

ETSI EN 319 422: Time-stamping protocol and timestamp profiles

CEN EN 419 231:
Protection Profile for
Trustworthy Systems
supporting time
stamping

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

TW4S

CEN TS 419
241: Security
Requirements
for
Trustworthy
Systems
Supporting
Server Signing

QSCD: OCSI <u>Attestato</u> di <u>Comformità</u> n.1/16 – <u>Thales</u> e-Security

œŋ

ETSI TS 119 612: Trusted Lists

ETSI EN 319 102: Procedures for Creation and Validation of AdES Digital Signatures

ETSI EN 319 122 /TS 103 173- CAGES digital signatures ETSI EN 319 132/TS 103 171- XAGES digital signatures

ETSI EN 319 142 /TS 103 172 - PAdES

digital signatures

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

TrustedX



ETSI EN 319 412-5: QC Statements



STANDARDIZATION AND COMPLIANCE UNDER EIDAS (II/II)

ETSI EN 319 401: General Policy Requirements for Trust Service Providers

ETSI EN 319 411: Policy and Security Requirements for Trust Service **Providers issuing Certificates**

CEN TS 419 261: Security Requirements for Trustworthy Systems Managing Certificates and time-stamps

ETSI EN 319 412 Profiles for Trust Service Providers issuing certificates

ETSI EN 319 412-1: Overviewand ETSI EN 319 412-3: Certificates issued to legal persons ETSI EN 319 412-2: Certificates ssued to natural persons common data structures

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

ETSI EN 319 421: Policy and Requirements for Trust Service Providers issuing Time-Stamps

CEN TS 419 261: Security Requirements for **Trustworthy Systems** Managing Certificates timestamps

ETSI EN 319 422: Timestamping protocol and time-stamp profiles

CEN EN 419 231: Protection Profile for Trustworthy Systems supporting time stamping

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

ETSITS 119 431: Policy and security requirements for trust service providers

ETSI TS 119 432: Protocols for remote digital signature creation

CEN EN 419 241-1: General System Security Requirements

QSCD

CEN EN 419 241-2: Protection Profile for QSCD for Server Signing EN 419 221-5: Cryptographic

ETSI TS 119 441: Policy requirements for TSP providing signature validation services

> ETSI TS 119 612: Trusted Lists

ETSI EN 319 102: Procedures for Creation and Validation of AdES **Digital Signatures**

PAdES 319 122 /TS 103 173- CAdES 319 132/TS 103 171- XAdES EN 319 142/TS 103 172 digital signatures digital signatures ETSI EN EN ETSI ETSI

digital signatures

CEN EN 419 221: Protection Profiles for TSP cryptographic modules

TrustedX



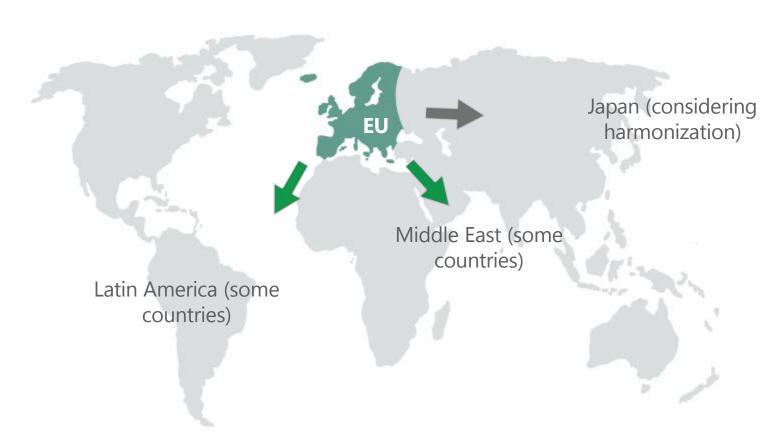
ETSI EN 319 412-4: Web sites certificates issued to organizations

EN 319 412-5: QC Statements

ETSI



STANDARDIZATION AND GEOGRAPHIES



Countries outside EU interested in Mobile ID and ETSI standards for remote signing

(*) Source: Safelayer



SAFELAYER EXPERIENCE

- Mobile and cloud trends require new forms of identity that provide Trust and Convenience
- Global acceptance of standards is the result of years of work by international working groups (*)
- Increase of AES and QES signatures types using Mobile and/or Remote Signature
- Increase of QTSP providing eSig/eSeals QCerts

(*) CEN/TS 419241 – Security Requirements for TW4S where published in April 2014



https://webgate.ec.europa.eu/tl-browser/#/ More than 150 QTSPs issuing QCs over 29 countries TL (19-06-17)



SAFELAYER DEMO PORTAL

Demo Online: http://demo.safelayer.com

Safelayer ID Services demo portal

Identity Services, aka "eIDAS", is the new concept for electronic IDentification (eID), Authentication (A) and Signature (S) proposed by Safelayer

Banking



Doc Signing



Health



Thanks

www.safelayer.com +34 917 080 480

©1999-2018 Safelayer Secure Communications, S.A. All Rights Reserved. This material is intellectual property of Safelayer Secure Communications S.A. This material may be used or copied only in accordance with Safelayer.