



SAFELAYER

Securing identities across the world!

November 8, 2018

SK ANNUAL CONFERENCE

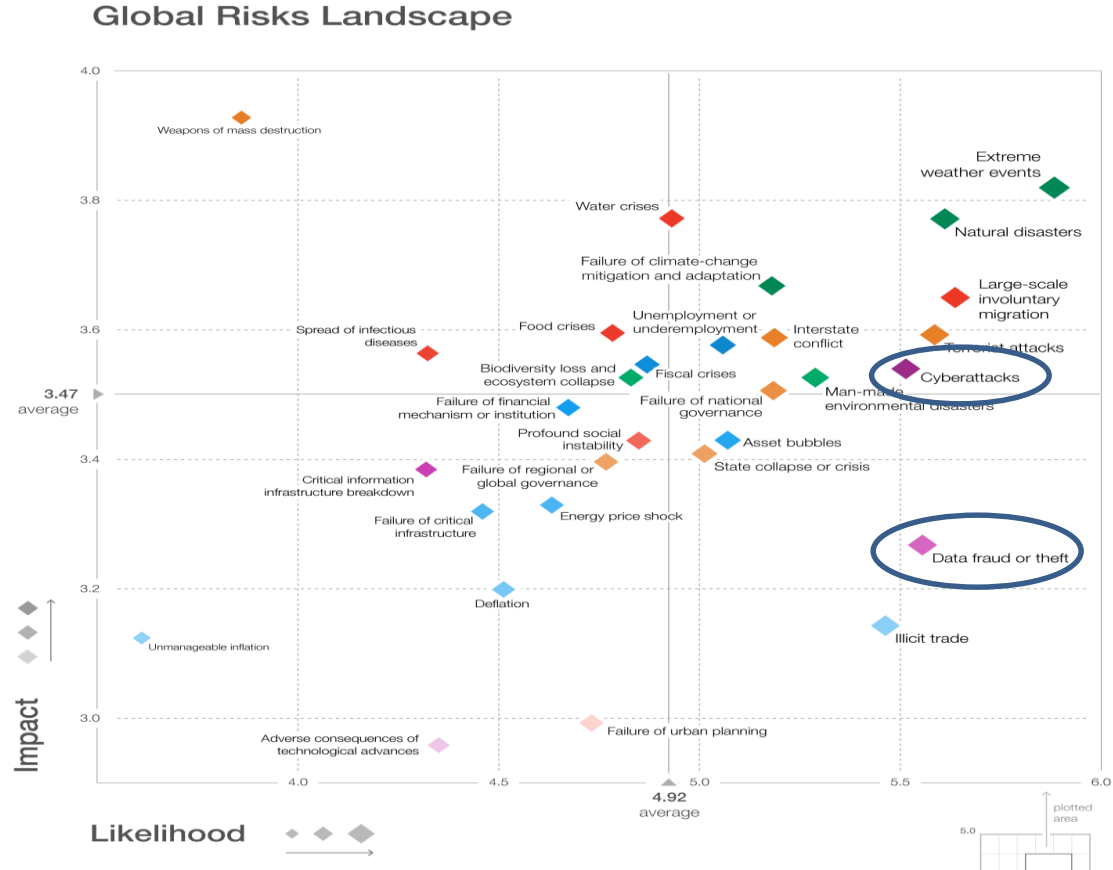
Jordi Buch – VP Sales & Marketing
jbt@safelayer.com

AGENDA

- Trust service trends
- Standardization initiatives
- Safelayer experience
- Registration models
- Lessons learned



GLOBAL RISKS LANDSCAPE



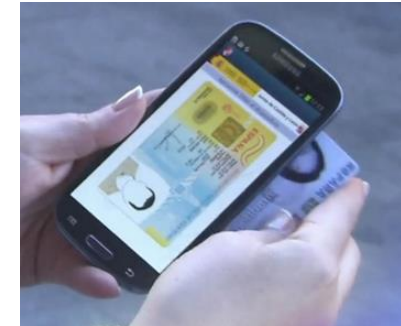
IDENTITY CARDS

- Secure identities based on Public Key Infrastructure (PKI)
 - National eIDs and ePassports
 - eIDs provided by Trust Services Providers
 - Corporate eID cards for employers/providers
- Strong authentication, electronic signature and document encryption



USE CASE - CITIZEN IDENTIFICATION IN SPAIN

- Home Office - Citizen Identification Card (DNI-e)
 - Year started: 2005
 - eID card with contact chip for PKI authentication and electronic signature
 - The new DNI 3.0 incorporates NFC (2015)
 - Issued: More than 60M cards
- Ministry of Finance and Public Administration – Spanish National Mint (FNMT) - CERES (Spanish Certification)
 - Year started: 1996
 - Certification services for public administrations, private companies and citizens
 - About 7,5M active certificates
 - New service CERES Cloud ID for public employees announced (2018)
- Ministry of Industry - Other officially recognized public and private TSPs (currently 22 recognized QTSP)



USE CASE - CITIZEN IDENTIFICATION IN SPAIN

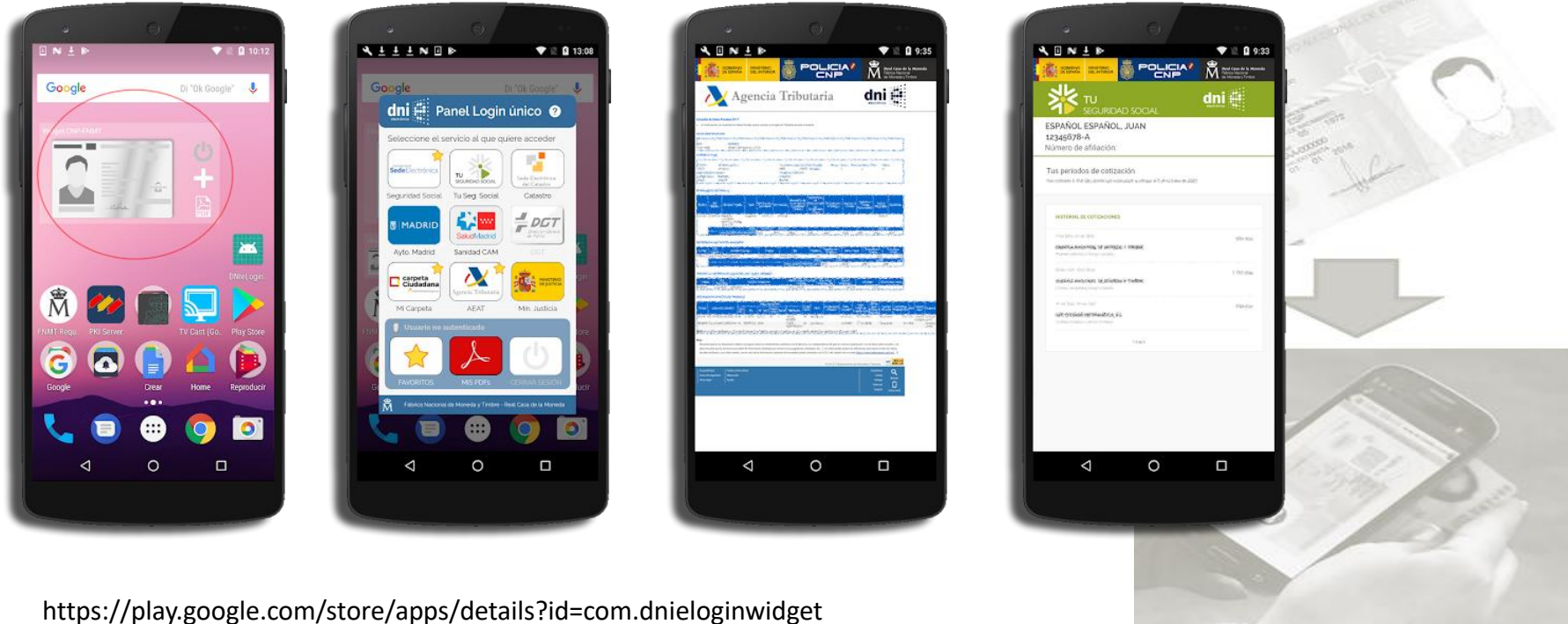
Example (i/ii)



<https://play.google.com/store/apps/details?id=com.maeat2016>

USE CASE - CITIZEN IDENTIFICATION IN SPAIN

Example (ii/ii)

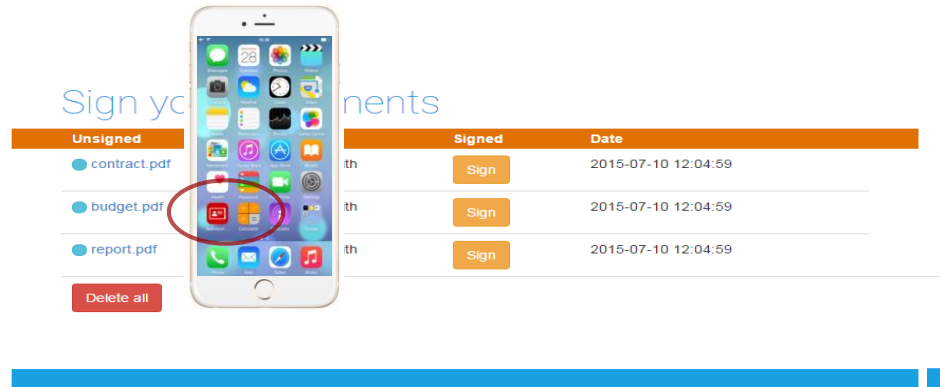


<https://play.google.com/store/apps/details?id=com.dnieloginwidet>

MOBILE AND CLOUD IDENTITY

Mobile and/or Cloud

- Cryptographic key/s in the smartphone
- Strong authentication, electronic signature
- Secure and convenient
- Cryptographic key/s protected by one HSM
- Electronic Signature when combined with strong auth
- Secure and convenient





Example (i/ii)

GTS Mobile ID



Example (ii/ii)



CERES Cloud ID

QUÉ ES CÓMO FUNCIONA POR QUÉ VENTAJAS CONTACTO

The cloud signature service of the Spanish National Mint (FNMT-RCM) is CERES Cloud ID

servicio de firma
centralizada en la nube
de la Fábrica Nacional
de Moneda y Timbre
(FNMT-RCM) se llama:



CERES Cloud ID

SABER MÁS

Ref. <http://www.realcasadelamoneda.es/ceres-cloud-id>,
https://youtu.be/Xm_9C9j9IG8



Facilitate seamless digital transactions among individuals and businesses across the EU

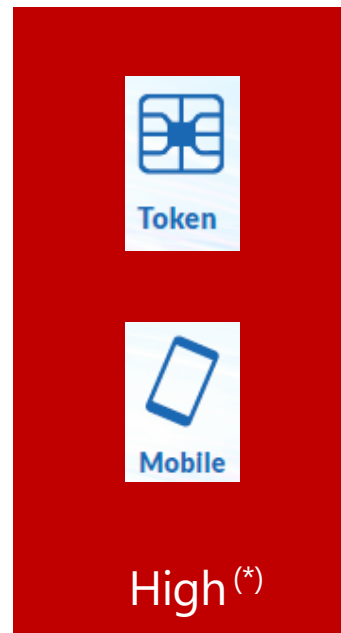
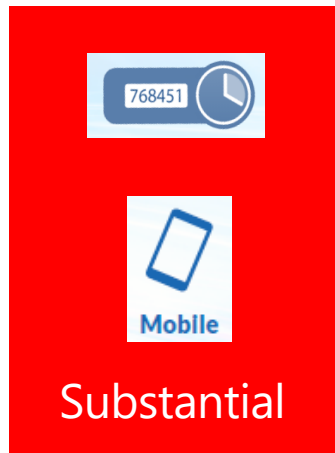
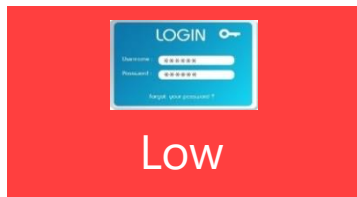
<https://webgate.ec.europa.eu/tl-browser/#/>

Source: European Commission
2018

EIDAS ASSURANCE LEVELS

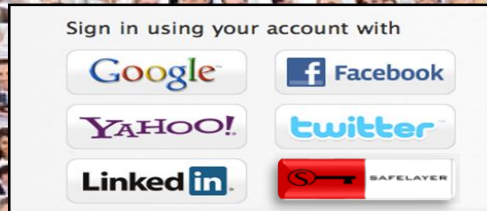
- eIDAS Regulation: Level of Assurance (LoA)
- NIST: Authenticator Assurance Level (AAL), Identification Assurance Level (IAL) and Federation Assurance Level (FAL)
- ITU-T X.1254 / ISO-IEC 29115 classifications

Trust Elevation
when higher
LoA is required



(*) Mobiles requires certain conditions to reach level High

NEW TSP ECOSYSTEMS (I/II)



IDENTIFICATION

CONVENIENCE

API ECONOMY

INNOVATION

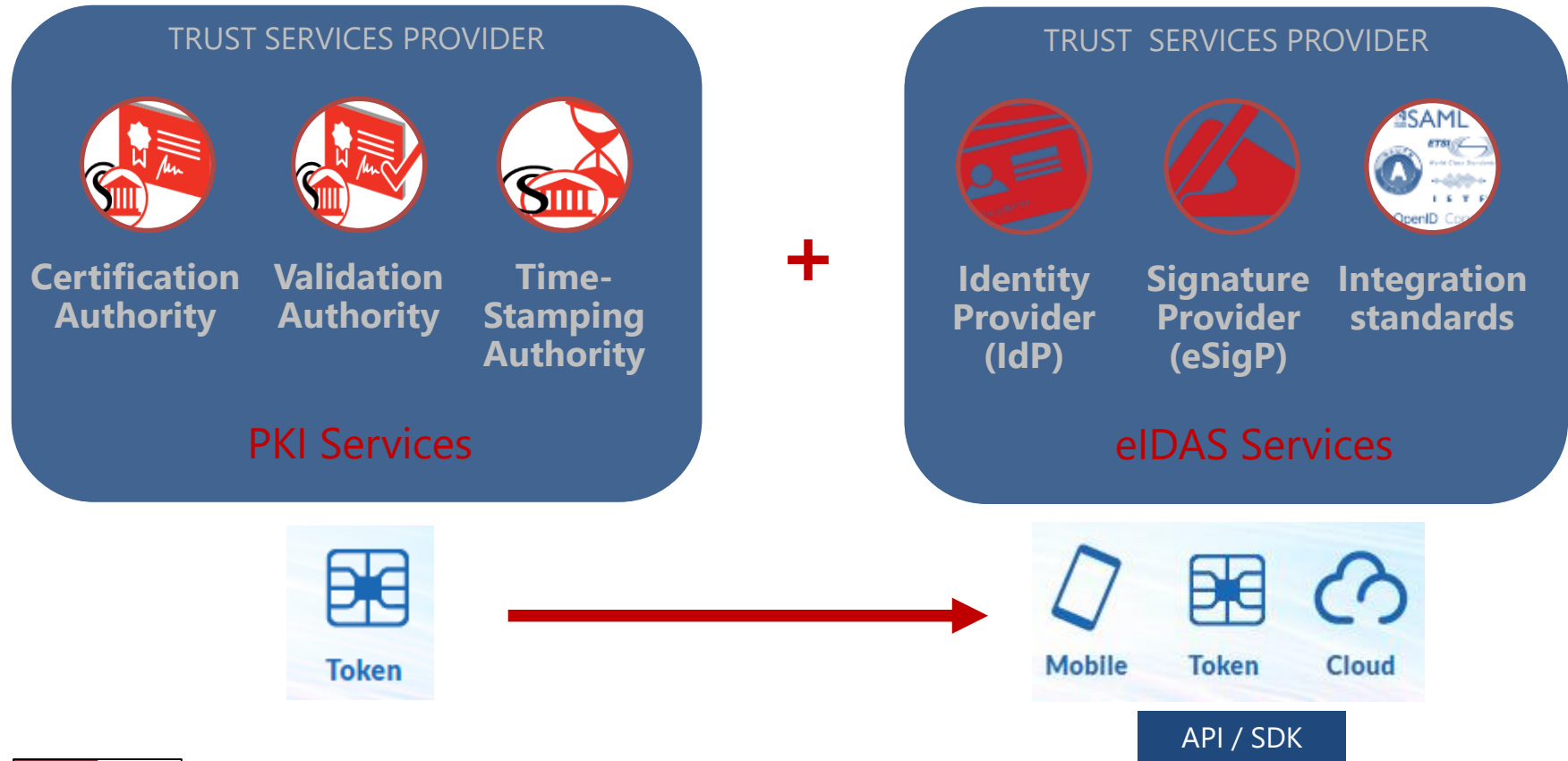
TRUST

SIGNATURE

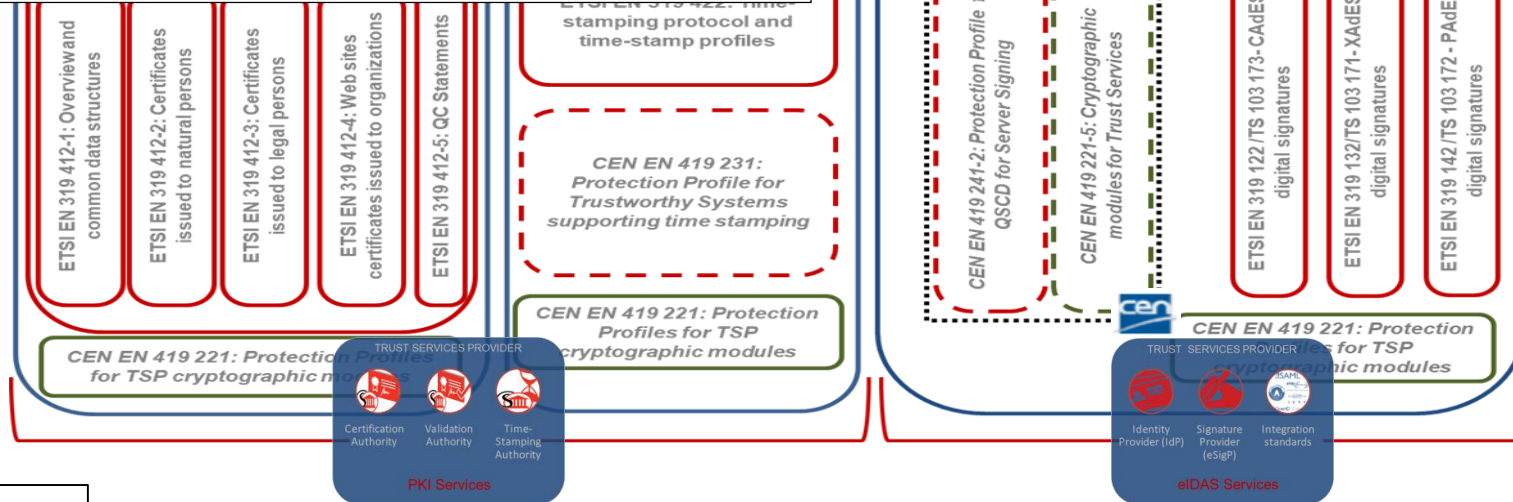
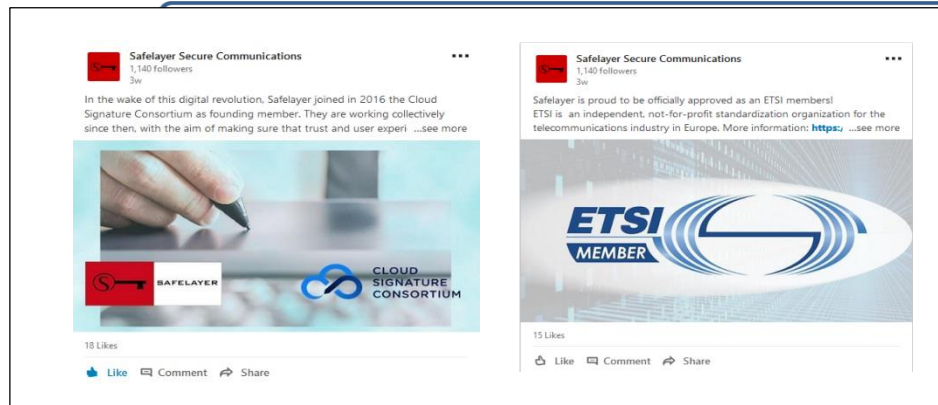
COMPLIANCE



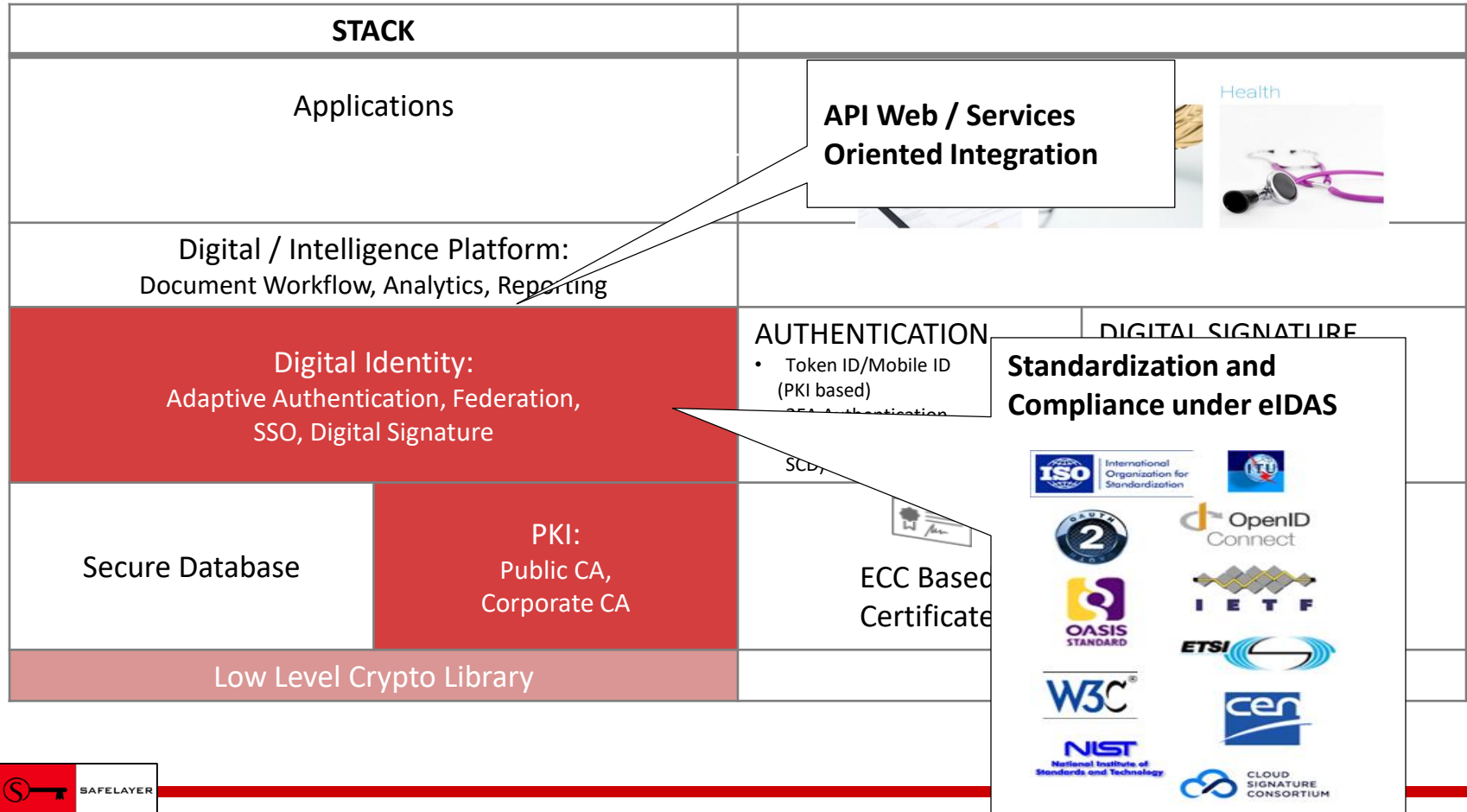
NEW TSP ECOSYSTEMS (II/II)



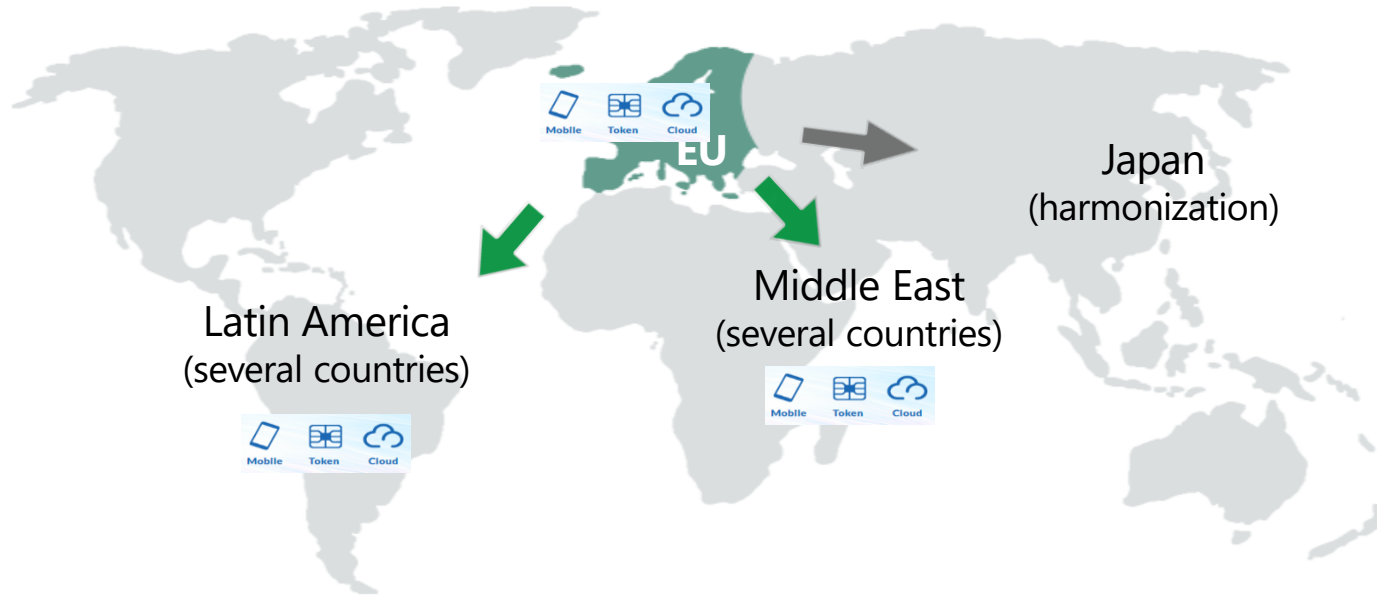
STANDARDIZATION AND COMPLIANCE UNDER EIDAS



DIGITAL TRUST IMPLEMENTATION



SAFELAYER EXPERIENCE



Countries outside EU interested in CEN/ETSI standardization under eIDAS

Source: Safelayer

SAFELAYER EXPERIENCE

EU

- Mobile and cloud trends require new forms of identity that provide Trust and Convenience
- Common acceptance of standards is the result of years of work by different working groups
- Electronic signatures adoption (AES/QES) based on Mobile and/or Server Components growing



eIDAS
Common
Framework



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

LATAM

- Laws that establish the legal presumption of reliability for the electronic signature in most of the countries
- Common acceptance of ETSI/CEN technical standards but not consensus how PKI credentials can be managed by a TSP on behalf of the entities
- Existing and/or ongoing projects that provides new forms of identity leaded by TSPs in Uruguay, Chile, Brazil, Ecuador, Argentina and Colombia

Middle East

- Laws that establish the legal presumption of reliability for the electronic signature in most of the countries
- Common acceptance of ETSI/CEN technical standards. Debates on SIM Card (aka Mobile PKI). No consensus how PKI credentials can be managed by a TSP on behalf of the entities
- Existing and/or ongoing projects that provides new forms of identity leaded by UAE government and Oman

REGISTRATION MODELS



Online with
recognized
credential



Face-to-face



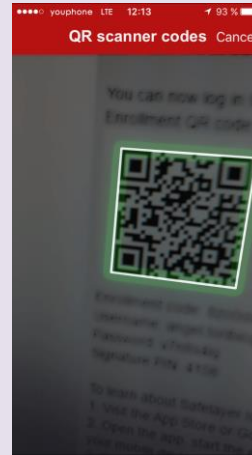
Kiosk + biometry
[optional]



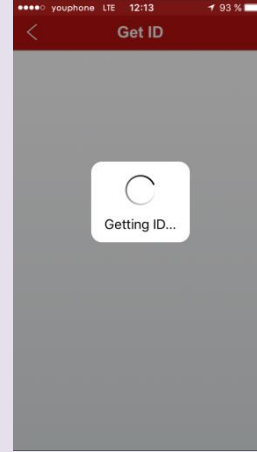
Online document
verification



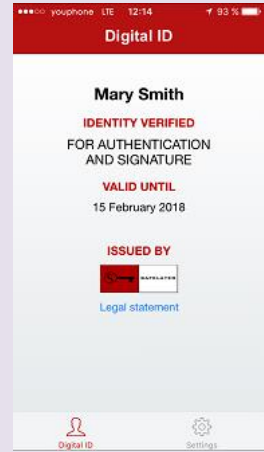
Enrollment QR
code



Scan QR code +
Additional factor
[optional]



Keys are
generated



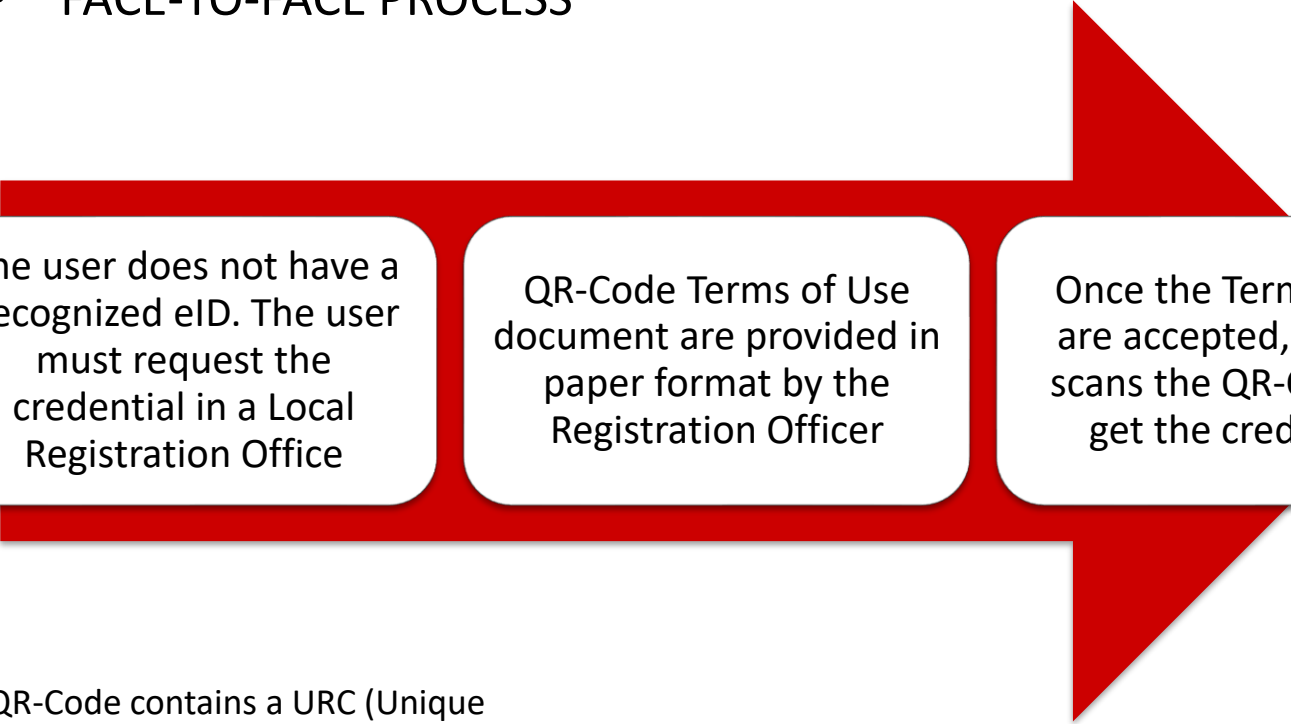
CA issues
PKI certificate/s

NEW CREDENTIALS

EXISTING CREDENTIALS

REGISTRATION – SUMMARY (I/II)

- FACE-TO-FACE PROCESS



The user does not have a Recognized eID. The user must request the credential in a Local Registration Office

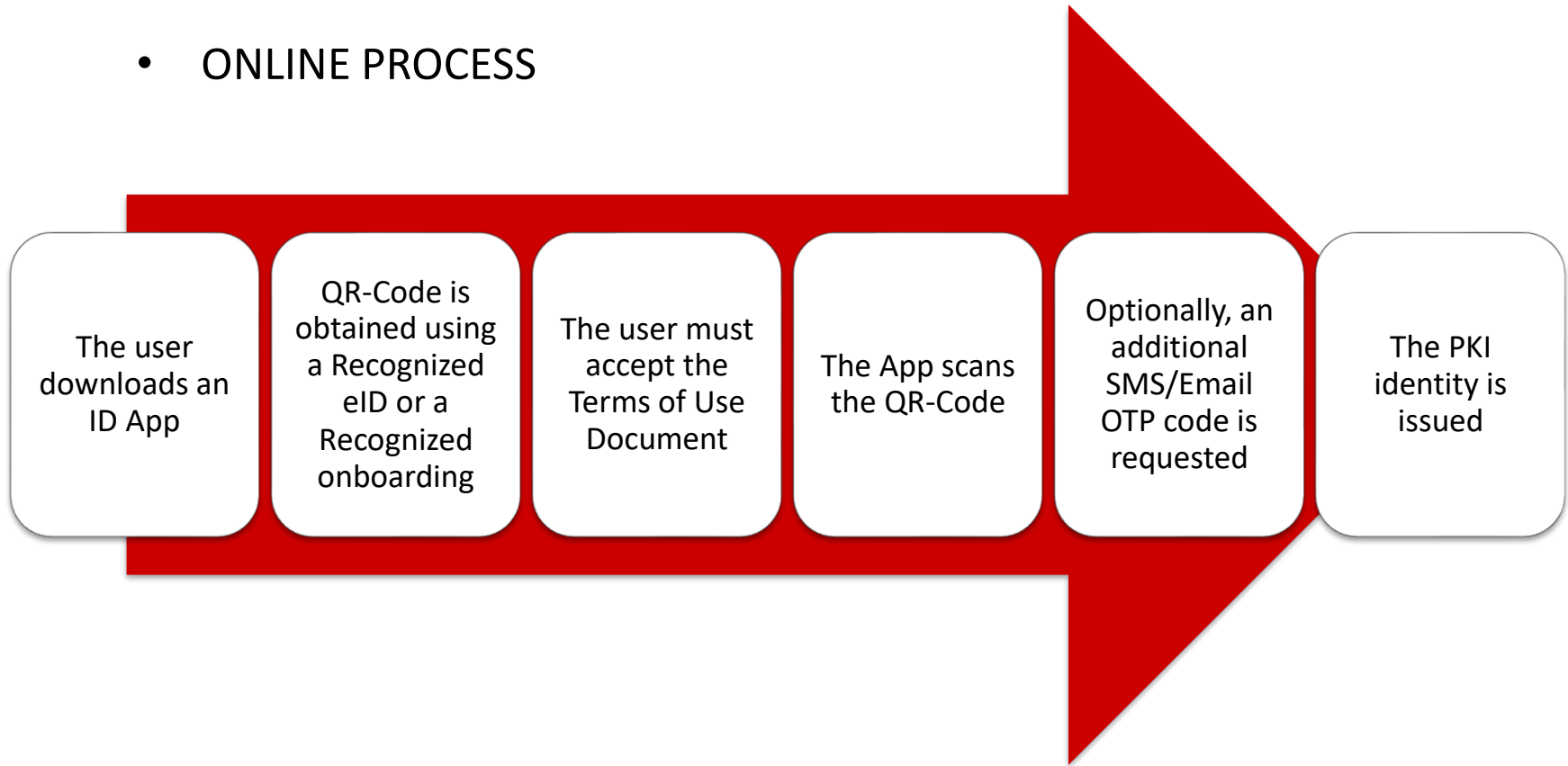
QR-Code Terms of Use document are provided in paper format by the Registration Officer

Once the Terms of Use are accepted, the user scans the QR-Code and get the credentials

(*) The QR-Code contains a URC (Unique Registration Code)

REGISTRATION – SUMMARY (II/II)

- ONLINE PROCESS





- Provides authentication and cloud signing using the following credentials
 - Citizen ID number
 - One time password based on a grid card (B@kQ card) / Mobile identification using citizen smartphone
 - A key/certificate issued by Izenpe in a centralized repository
- It has exceeded the figure of 100,000 certificates, with 500,000 transactions per month. More than 50 integrated service providers
- Extension/plugin is required for Public Employers that use Desktop applications (i.e to use with Adobe Acrobat)



IZENPE SOLICITA SU AUTENTICACIÓN
Inserte su DNI y contraseña para acceder

DNI / NIE

CONTRASEÑA

[¿Olvidó su contraseña?](#)

[MÁS INFORMACIÓN SOBRE B@K](#)

CANCELAR

ACCEDER



Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia solicita su autenticación.

Seleccione cuál de los siguientes medios identificación desea utilizar:

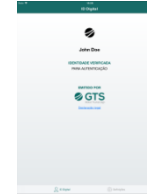
Usuario y contraseña B@k

Usuario, contraseña y juego de barcos (coordenadas)

Certificados Digitales (si tiene tarjeta/ token insértelo antes de acceder)

Cancelar

- Identification and signature services for Public Employees (Health and Public Contract)
- Expected to be recognized in EU TLS as QS Provider ending 2018
- Enrollment processes based on credentials of previous processes. Mainly Portuguese Electronic National ID
- Mobile ID registration:
https://www.globaltrustedsign.com/public_c/mobile



GTS
MOBILE ID

A assinatura digital qualifica:

APP que lhe vai trazer vantagens na hora de se autenticar e confirmar a assinatura dos seus documentos.

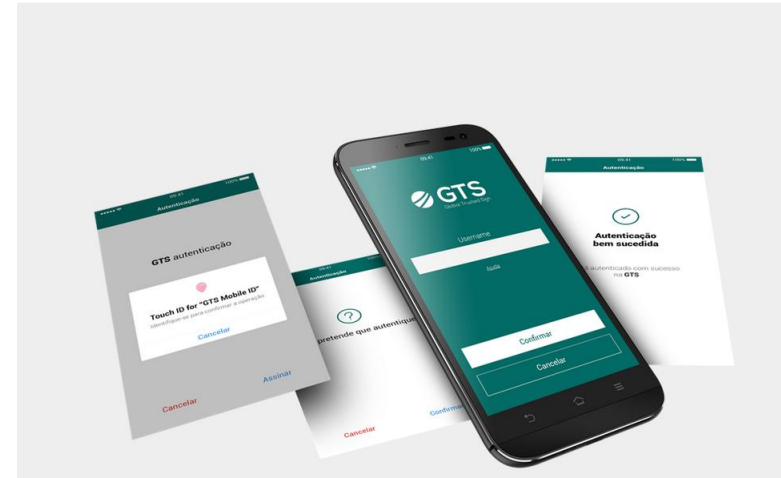
GTS
Global Trusted Sign

Efetue a sua autenticação

Introduzir credenciais:

Utilizador

Palavra-passe





- Enrollment options:
 - Online using a recognized eID + additional factor (sms)
 - Online using a other eIDs + additional factor (courier)
 - Face-to-face enrollment if not have recognized eID
- Agreements with Government / Banking to recognize external eIDs

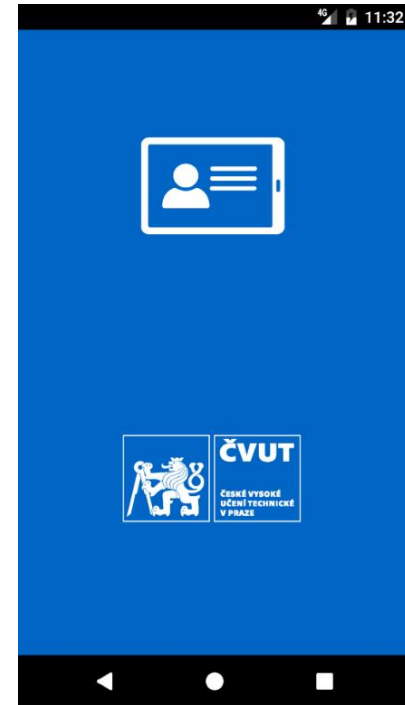
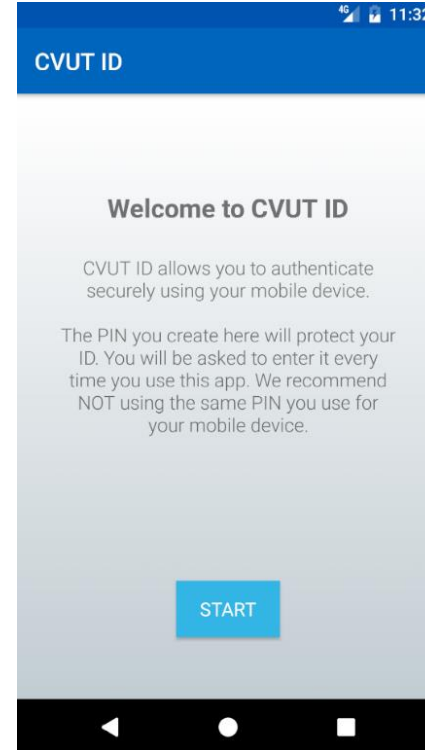
The screenshot shows the 'eParaksts' web interface. At the top, it says 'Please provide the user number:'. Below this is a text input field labeled 'USER NUMBER'. A note states: 'The user number consists of 7 digits and you will find it in your contract.' At the bottom, there are two buttons: 'Cancel' and 'Confirm'. A red link for 'Need help?' is visible at the very bottom.

<https://www.eparaksts.lv/en/>





- Mobile Identification and RSS Services for Students and Staff in CTU
- Enrollment processes based on recognized Czech and Internal CTU Credentials
- Integration with External TSP in Czech



LESSONS LEARNED

- eIDAS trust services require continuous enhancement as requirements evolve
- Continue adding certifications to the products for efficient Conformity Assessment processes
- A continuous partnership with industry is required to develop applications
- Registration based on Kiosk with biometrics seems to gain traction
 - Onboarding processes are being considered

ABOUT SAFELAYER

Independent Software Provider Based in Madrid and Barcelona

Software
provider since

1999



Cyber security
technologies
for critical
infrastructures

Secure eID based
in PKI Technology.
Authentication
and electronic
signature

eIDENTITY

Over **100** organizations in
more than **15** countries put
their trust in the company's
solutions.



Common Criteria
certified



Value Added
Resellers in
EMEA and
LATAM



European Committee for Standardization



CLOUD
SIGNATURE
CONSORTIUM

Participation
on public and
private
initiatives to
create
standards.

Thanks for you attention



www.safelayer.com
sflyr@safelayer.com