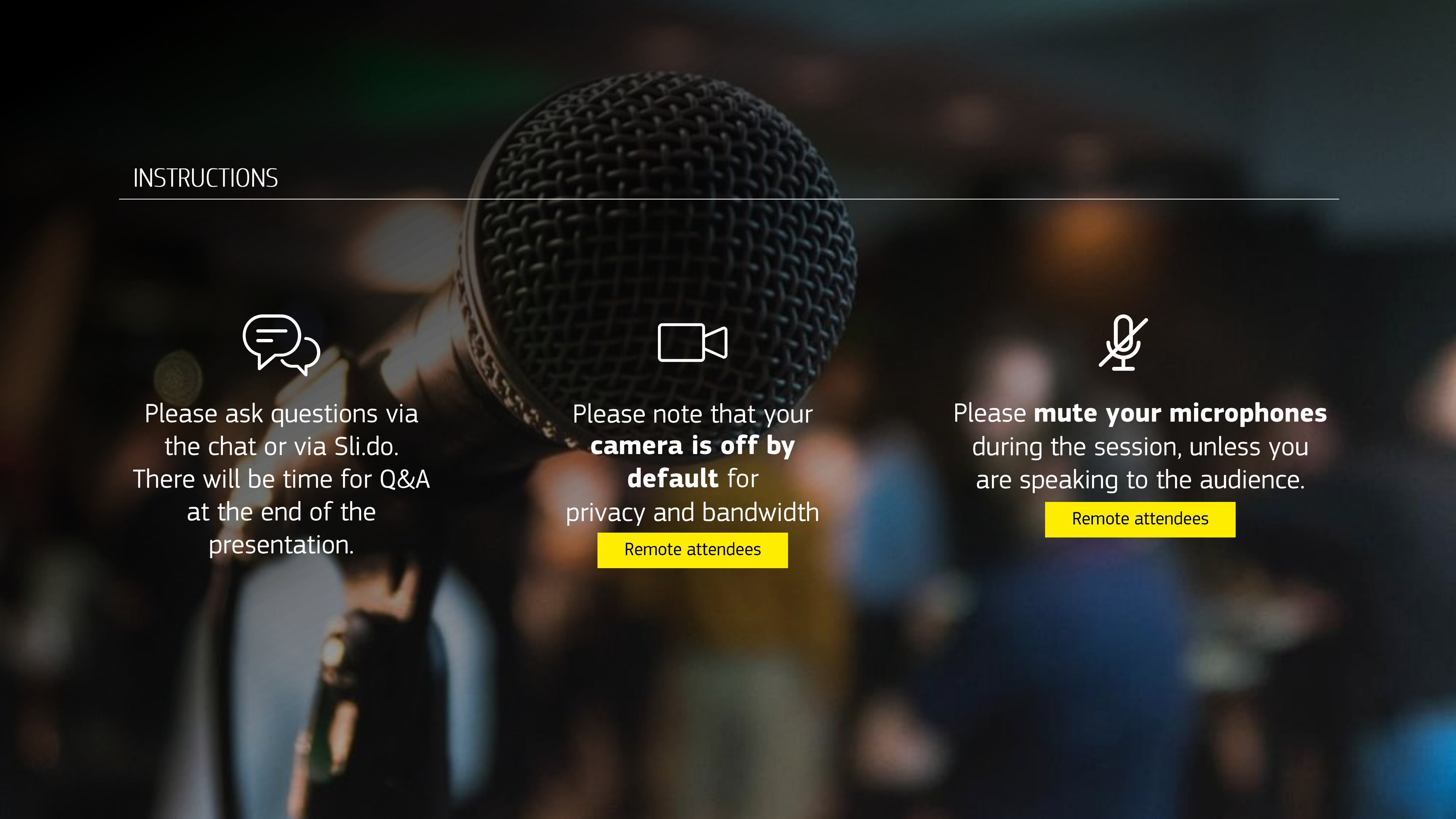
WELCOME

EC-3rd Countries Trust Services Forum

Brussels

12 June 2023 | 09:00– 17:30 CET



INSTRUCTIONS

Please ask questions via the chat or via Sli.do. There will be time for Q&A at the end of the presentation.

Please note that your **camera is off by default** for privacy and bandwidth

Remote attendees

Please **mute your microphones** during the session, unless you are speaking to the audience.

Remote attendees

Agenda of the day

01 02 03 04 05 06 07 08 09 10 11 12

	ID	TIME	TOPIC	SPEAKERS
AM	1.	09:00 - 09:15	Welcome words	Lorena BOIX ALONSO (European Commission)
	2.	09:15 - 09:35	The eIDAS Regulation present and future • eIDAS regulation • eIDAS 2.0	Gudrun STOCK (European Commission)
	3.	09:35 – 09:55	• Current state of international partnerships • Policy around the recognition of third countries trust services	Vicente ANDREU NAVARRO (European Commission)
	4.	09:55 – 10:15	• European Commission’s Third Countries Trusted Lists Programme • Presentation of the pilot in the eIDAS Dashboard	Apostolos Tolis APLADAS (European Commission)
	5.	10:15 - 10:30	Trust services in the Republic of Albania • Regulatory Framework on trusted services • Competences of the supervisory body • Registration/Accreditation of QTSP • Trust list/ Electronic Identification Scheme • International Aspects	Ermela CEKANI (Albania)
		10:30 - 10:50	*Coffee break*	
	6.	10:50 - 11:50	Panel discussion	Sylvie LACROIX (Sealed), Viky MANAILA (IntesiGroup), Evgenia NIKOLOUZOU (ENISA)
	7.	11:50 - 12:05	Presentation of the TC AdES LOTL and the UA collaboration	Olivier BARETTE (Nowina Solutions)
PM		*12:05 - 13:35*	*Lunch break*	
	8.	13:35 - 13:50	Data Free Flow with Trust – Proof of Concept between Japan and the European Union	Prof. TEZUKA (Japan)
	9.	13:50 - 14:05	Trust services infrastructure in Ukraine	Oleksandr KOZLOV (Ukraine)
	10.	14:05 - 15:50	How the specifications of the TC AdES LOTL and the XML MRA elements work	Olivier BARETTE (Nowina Solutions), Olivier DELOS (Sealed)
		15:50-16:20	*Coffee break*	
	11.	16:20-17:05	Q&A	eIDAS Dashboard team
	12.	17:05-17:15	Closing remarks	Natalia ARISTIMUÑO PÉREZ (European Commission)

Meet your hosts for today

Apostolos (Tolis) APLADAS

Program Manager, DG DIGIT, European Commission

Vicente ANDREU NAVARRO

Policy Officer, DG CNECT, European Commission

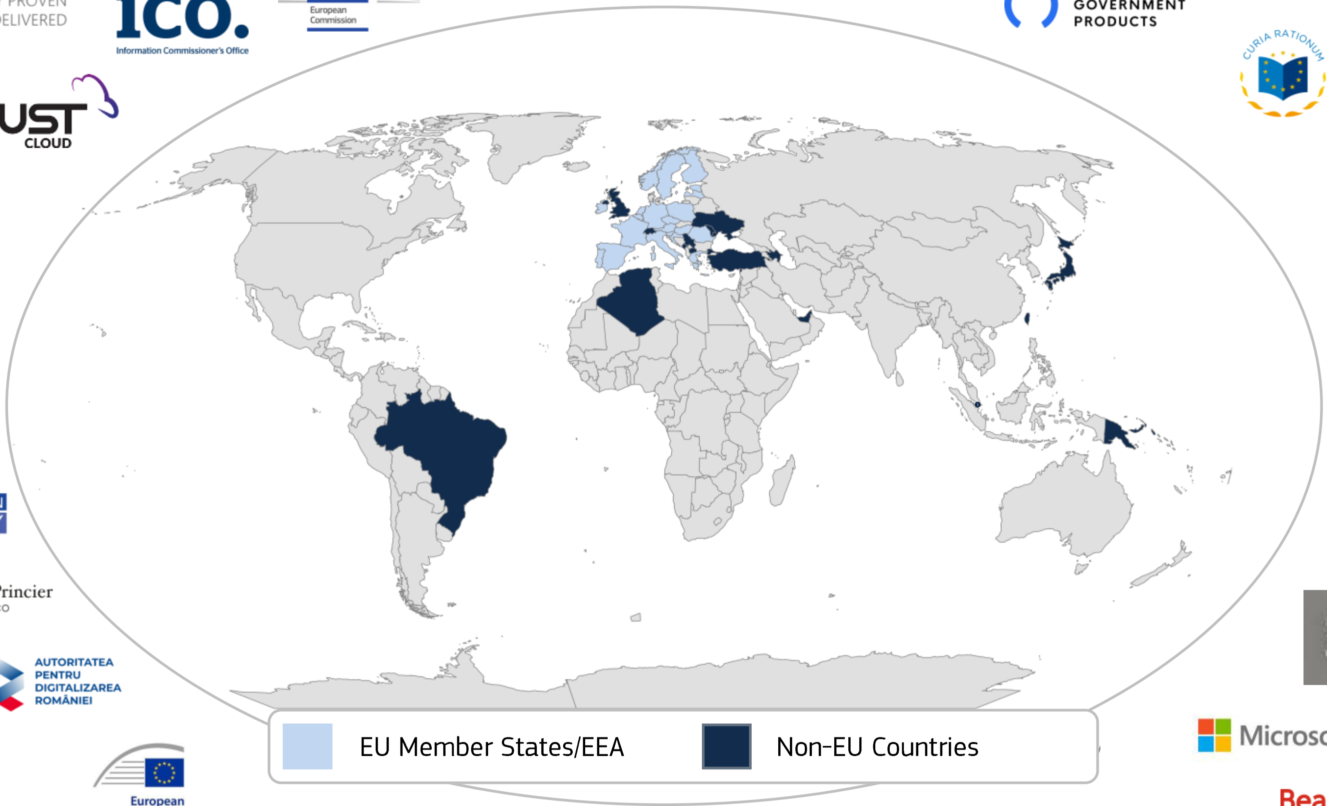
Yi Qi HO

eSignature onboarding manager, representative of DG DIGIT, European Commission

More than 200 attendees from private companies and public Institutions

+27 EU/EEA Member states

+15 Non-EU countries



eGA e-governance academy

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

SEALED Trust Services Architects

亞洲誠信 TRUSTAsia

INTESI GROUP

慶應義塾大学 Keio University

DIGITAL AND POPULATION DATA SERVICES AGENCY

Дія

EU4DigitalUA ПРЯМУЄМО РАЗОМ

ENTRUST

DocuSign

EUROPEAN PUBLIC PROSECUTOR'S OFFICE EPPO

CERTITRUST CONFIDENCE IN THE DIGITAL ERA

assurity

INFOCERT TINEXTA GROUP

Adobe

GOVTECH SINGAPORE

Nowina SOLUTIONS

European Commission

ascertia IDENTITY PROVEN TRUST DELIVERED

ico. Information Commissioner's Office

OPEN GOVERNMENT PRODUCTS

economie

CURIA RATIONUM EUROPEAN COURT OF AUDITORS

CLOUD

Deloitte.

Republic of Serbia MINISTRY OF TRADE, TOURISM AND TELECOMMUNICATIONS

TRUST CLOUD

teknei

HUAWEI

European Parliament

iLabs a trustworthy internet of everything

SMART NATION & DIGITAL GOVERNMENT OFFICE

Intesa a Kyndryl Company

CERTIFICATION AUTHORITY

SK

Gouvernement Princier PRINCIPAUTÉ DE MONACO

PRIME MINISTER'S OFFICE HUNGARY

pwc

EPFL

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

swisscom

grnet

European Investment Bank

Microsoft

BearingPoint.

المركز الوطني للأمن السيبراني National Cyber Security Center

asseco

Namirial

cosmos

TERASIGN GLOBAL

ADACOM CYBER SECURITY

bit4id

zetes

ART

CYBERNETICA

Signicat

And more…

1

Welcome words

Lorena BOIX ALONSO

Director for Digital Society, Trust and Cybersecurity – DG CNECT, European Commission

2

The eIDAS Regulation present and future

Gudrun STOCK

Deputy Head of Unit – DG CNECT, European Commission

eIDAS vs. European Digital Identity Framework

Electronic/Digital Identification

eIDAS

- Voluntary provision of national eID means
- Notification – peer review
- Identification for cross-border access to public services

European Digital Identity Framework

- All Member States to provide Digital Identity Wallets
- Harmonised standards – certification
- Identification + exchange of attributes for cross-border access to public and private services

eIDAS

- Electronic signatures, seals, timestamps
- Website Authentication Certificates (WACs)
- Electronic Registered Delivery Services

European Digital Identity Framework

- Electronic archiving
- Electronic ledgers
- Managing remote electronic signature and seal creation devices
- Electronic attestation of attributes

Trust Services

> “The European Council calls for the development of an **EU-wide framework** for **secure public electronic identification** (e-ID), including interoperable **digital signatures**, to provide **people with control** over their online identity and data as well as to enable access to **public**, **private** and **cross-border** digital services.”

- European Council Conclusions, 2 October 2020

European
Commission

2030
DIGITAL
DECADE

Digital targets in the Union by 2030 (the ‘digital targets’)

The European Parliament, the Council, the Commission and the Member States shall cooperate with a view to achieving (…) the digitalisation of public services, where 100 % of Union citizens have access to secure electronic identification (eID) means that are recognised throughout the Union, enabling them to have full control over identity transactions and shared personal data (…)

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030

New Trust Services

Electronic archiving

Guarantees the integrity of data or documents, the accuracy of their origin and legal features throughout the conservation period

Electronic ledgers

Tamper proof electronic record of data, that provides authenticity and integrity, accuracy of date and time, and of the chronological order

Management of remote electronic signature and seal creation devices

Will provide security, uniformity, legal certainty and consumer choice to remote signatures

Electronic attestation of attributes

Attestation in electronic form that allows the authentication of attributes

Towards a European Digital Identity

Free for use by all citizens

All EU citizens and businesses may use it for free on a voluntary basis

Accepted everywhere

Recognised by private and public service providers for all transactions that require authentication

Secure and privacy oriented

Citizens can control and protect their identity, personal data and digital assets

Use Cases

The wallet will allow users to

- **Prove** who they are when using Digital Public Services or opening an Bank account
- **Controlling personal data** when Logging into Social Networks

- **Prove** they possess a Driving Licence
- **Obtain and present** Medical Prescriptions
- **Demonstrate** their Social Security Status

- **Present**
  - Loyalty cards
  - Membership cards
  - Tickets

- **Sign** contracts and other Declaration of intent or consent
- **Authorise** payments

European Digital Identity Work Strands

Legislative Process

- Negotiation of the proposal for the revision of the **eIDAS regulation** underpinning the EUDI Framework

Wallet Technical Specifications

- Member States and the Commission working on a **common toolbox** consisting of an **architecture and reference framework,** common standards and specifications, guidelines and best practices for the EUDIW

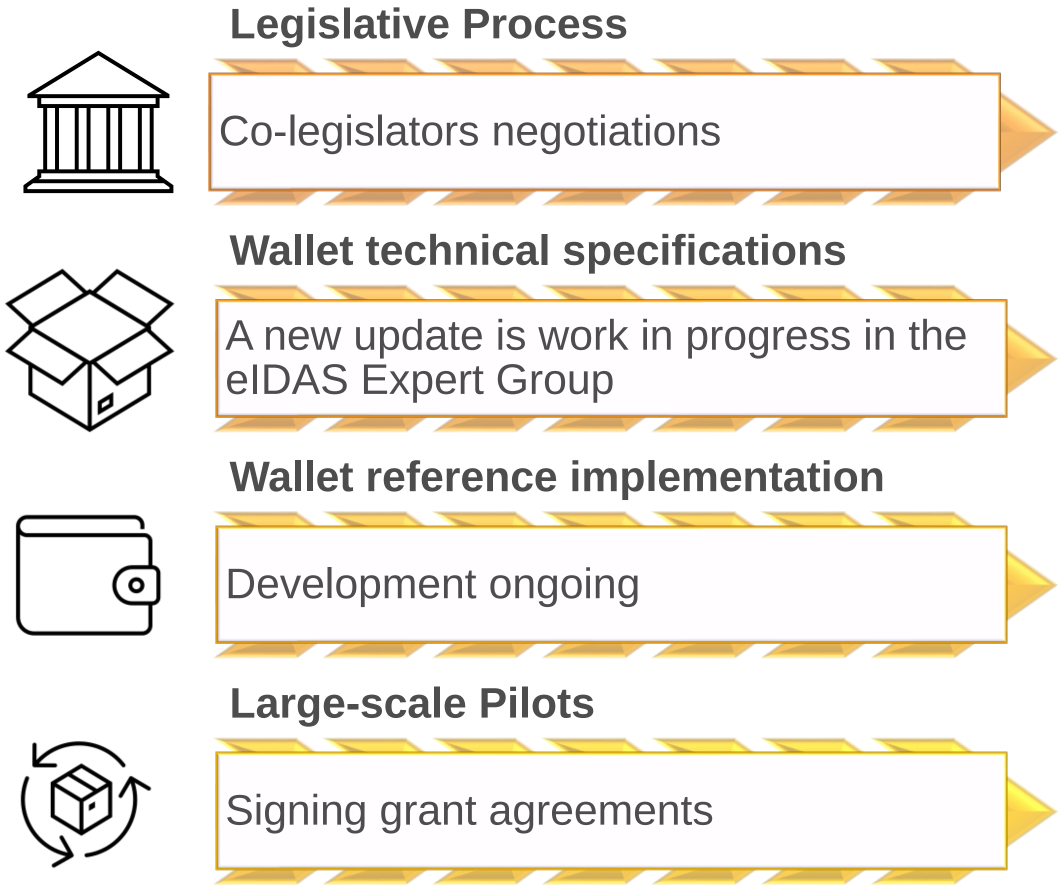
Large-scale Pilots

- **Grants** under the Digital Europe Programme for **large-scale pilots around use-cases** for the EUDIW

Wallet Reference Implementation

- A **reference implementation** of the EUDIW based on the technical specifications agreed by the toolbox

Milestones



Legislative Process

Co-legislators negotiations

Trilogues started 21st March, revised Regulation expected to be adopted within 2023

Wallet technical specifications

A new update is work in progress in the eIDAS Expert Group

9th of February 2023 first release, continuous updates from April 2023

Wallet reference implementation

Development ongoing

First release in June 2023, second release September 2023 and third release December 2023

Large-scale Pilots

Signing grant agreements

Four large-scale pilots testing and enhancing the wallet launched on 1st April 2023

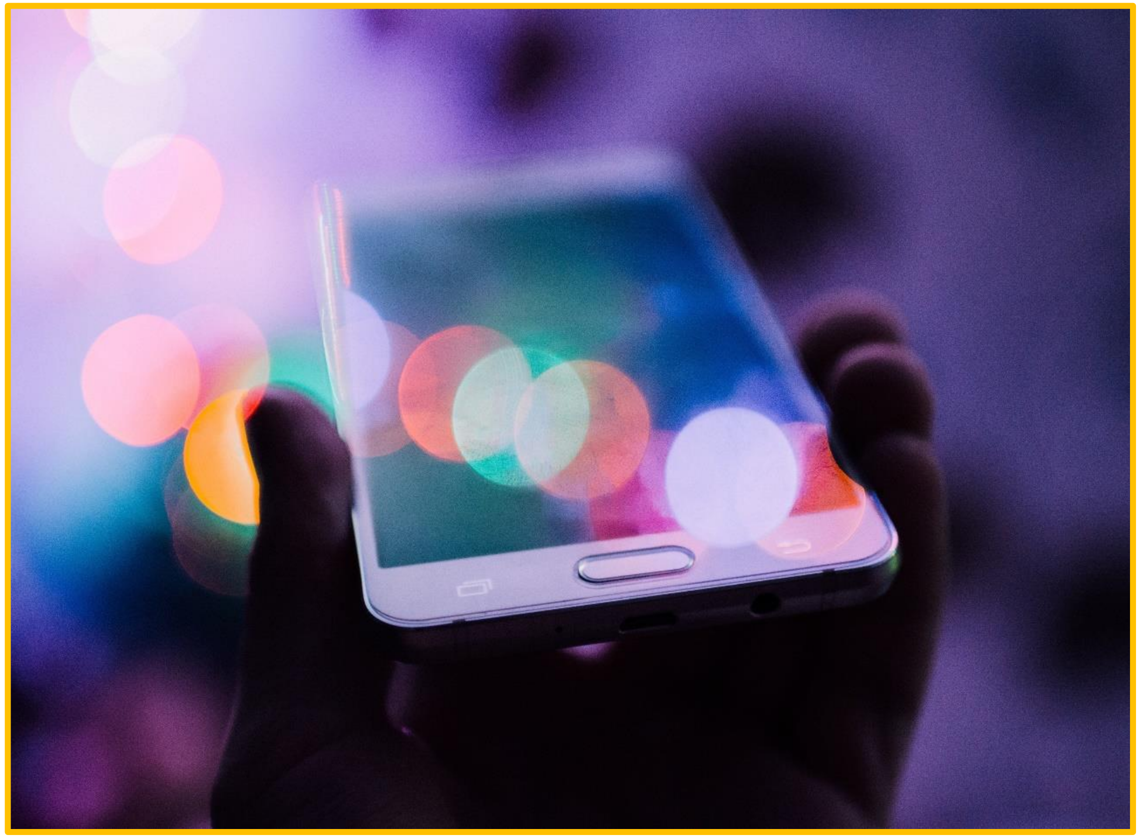
The Architecture and Reference Framework

- The first release of the ARF represents the initial consensus version containing the fundamental elements necessary for developing an EUDI Wallet prototype.

- The architecture needs to aline with the legislative process which is still ongoing

- The document is open and shared on github to collect feedback from stakeholders.

- New releases with additional specifications will come in short cycles based on the feedback received. The next one is expected in June.



European Commission

Wallet Reference Implementation

Objectives

- Build reference technical infrastructure to support interoperability and implementation of the EUDIW and its ecosystem
- Support Member States and other stakeholders in developing, implementing and scaling up the EUDI Framework
- Enable large-scale pilots by providing reference wallet and use-cases in national / stakeholder context

Scope

- Authentication (Q2 2023)
- Identification & mDL (Q3 2023)
- Subsequent releases (e.g. extended functionalities, feedback from large-scale pilots)

Outcome

- Open-Source reference wallet application and libraries tested, certified, ready to be used by Member States to implement the wallet

Four Large-Scale Pilots

POTENTIAL
European Consortium
for Digital Identity

20 countries

56 public and 80+ private entities

Use cases:

Electronic Government services, Bank Account opening, SIM registration, mobile driving licence, Remote Qualified Electronic Signature and ePrescription.

EWC

19 countries

18 public and 40+ private entities

Use cases:

Digital Travel Credentials, Payments, Legal persons

DC4EU

23 countries

36 public and 40+ private entities

Use cases:

Educational credentials and professional qualifications, Portable Document A1 (PDA1), European Health Insurance Card (EHIC).

NOBID
CONSORTIUM

8 countries

6 private and 15 private entities

Use cases:

payments use-cases at both a cross-country and cross-sector level with partners coming from both private and public sector

Total budget: >90 Million (50% EU contribution), >250 Participants,

Use-cases

- **Mobile Driving Licences (mDL) –** for online and physical interactions
- **Opening a Bank Account –** to verify a user's identity when opening a bank.
- **SIM Registration –** Wallet to prove their identity in pre- and post-paid SIM card contract registration
- **eSignatures** - provide a secure digital signature when signing contracts online
- **Accessing government services – to** file taxes or apply for supports
- **ePrescription –** identifying **and** providing details of prescription to a pharmacies
- **Payments -** store credentials and facilitate payments in account-to-account and card-based transactions
- **Travelling –** quick airplane boarding and quick border crossings (e.g. by a storing Digital Travel Credentials)
- **Organisational Digital -** business-to-government or business-to-business interactions
- **Freedom of Movement –**social security documents such as European Health Insurance Card
- **Education/Professional Qualification –** educational qualification or professional

Thank you

European Commission

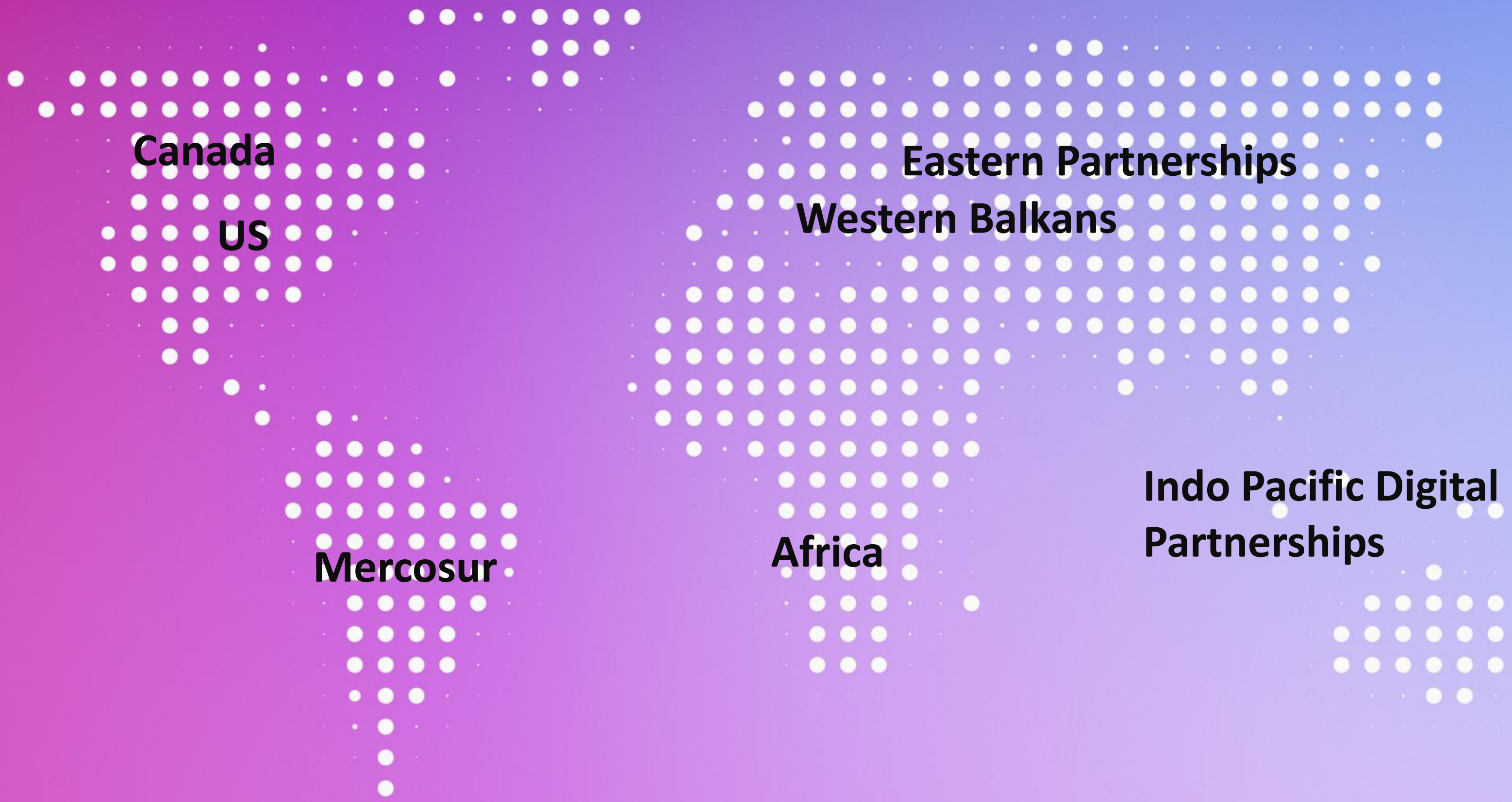
3

Current state of international partnerships

Vicente ANDREU NAVARRO

Policy Officer – DG CNECT, European Commission

International cooperation and eIDAS



OECD

UN

G7 / G20

International cooperation and eIDAS

- Activities in this area are currently established at **three different levels**:
    - Association Agreements between third countries and the EU
    - Dialogues and information exchanges (formal and informal)
    - Pilots and proofs of concept
    - Participation in international initiatives:
        - UN's UNCITRAL model law
        - OECD's Guidelines for the governance of Digital Identities

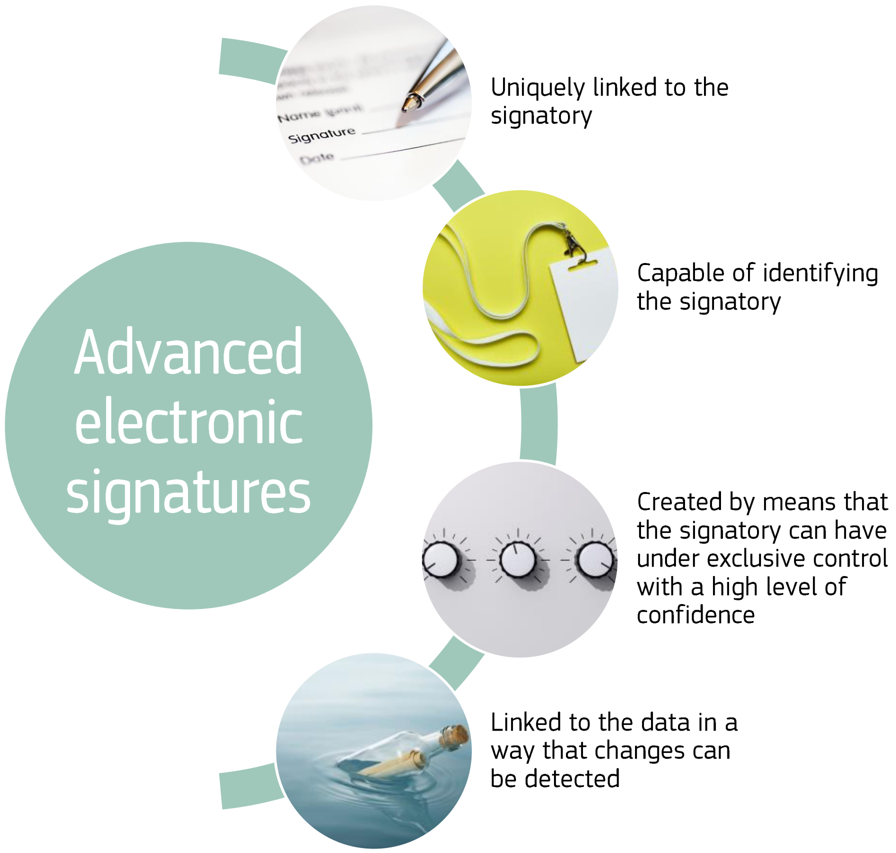
And very recently, validation tools for third countries' electronic signatures by EU member states (**TC AdES LOTL**).

International cooperation and eIDAS

- The possibilities for cooperation are **limited by the regulation** itself:
    - Mutual recognition of Qualified Trust Services is possible under article 14 of eIDAS
    - Mutual recognition of electronic identities is not considered in eIDAS (although, being an exclusive competence of the EU could be the object of international agreements under art. 218 TFEU)
- Mutual recognition of QTS under article 14 of eIDAS has never been implemented so far
- The **proposal for a new eIDAS regulation modifies article 14** in order to make the process more straightforward (adding the possibility of achieving the same goal via implementing acts)

Recognition of TC electronic signatures

Only QES have the equivalent legal effect of handwritten signature in the EU, but…



Advanced electronic signatures

Uniquely linked to the signatory

Capable of identifying the signatory

Created by means that the signatory can have under exclusive control with a high level of confidence

Linked to the data in a way that changes can be detected

…legal effects of electronic signatures cannot be denied solely on the grounds that they are in electronic form or that they are not qualified.

Recognition of TC electronic signatures

- Process triggered by the invasion of Ukraine and the need to validate Ukrainian electronic signatures in EU member states
- The aim was to create a set of tools that could facilitate compliance with eIDAS (undeniability, in principle, of legal effects of electronic signatures)
- Imposes no obligations to member states beyond what was already established in eIDAS

- Formal checks are performed by the COM on TC's electronic signatures that offer a sufficient level of trust based on the approximation to EU regulation and standards

Inclusion in the TC AdES LOTL

- No need for an international agreement as it does not involve mutual recognition of qualified electronic trust services
- Straightforward procedure:
    - Formal request by the TC's authorities to DG CNECT
    - Technical assessment by DG DIGIT of the legal and technical aspects of TC electronic signatures (they must be equivalent/similar to EU QES under the TC's regulations)
    - Technical works addressed to include the pointers to TC LOTL in the EU TC AdES LOTL

Effects

- Validation of TC's electronic signatures equivalent to EU QES becomes an easy task
- Although they cannot be considered as EU QES, the EU TC AdES LOTL offers the added value of the technical assessment by the COM of the electronic signatures generated in the TC
- First step towards future mutual recognition of qualified trust services

4

European Commission’s Third Countries Trusted Lists Programme

Apostolos Tolis APLADAS

Programme Manager – DG DIGIT, European Commission

Components of eSignature

eSignature is composed of **six main components**:

The **Digital Signature Software (DSS)** open-source library is an open-source software library for electronic signature creation and validation. DSS supports the creation and verification of interoperable and secure electronic signatures in line with European legislation, and it can be re-used in an IT solution for electronic signatures to ensure its alignment with European legislation and standards.

The **eIDAS Dashboard** that unifies and centralizes the DIGITAL eSignature and eID building blocks new and already existing tools and information related to the eIDAS trust services backbone e.g., TL Browser, eSignature validation test cases, eIDAS lists, notification tool, eIDAS eID Node management and reporting.

The **Trusted List Browser** is an online tool provided by the European Commission that allows for searching qualified trust service providers in Europe.

The **TL Manager** is a web application for browsing, editing, and monitoring Trusted Lists used by the Trusted List Operators of each Member State.

ETSI signature Conformance Checker is a tool that allows users to test the interoperability and conformity of their e-signature solutions

The **Pilot for the International Compatibility of Trust Services** that illustrates how the mutual recognition between the eIDAS qualified trust services and third country's trust services.

Current status

An overview of the current status of eSignature

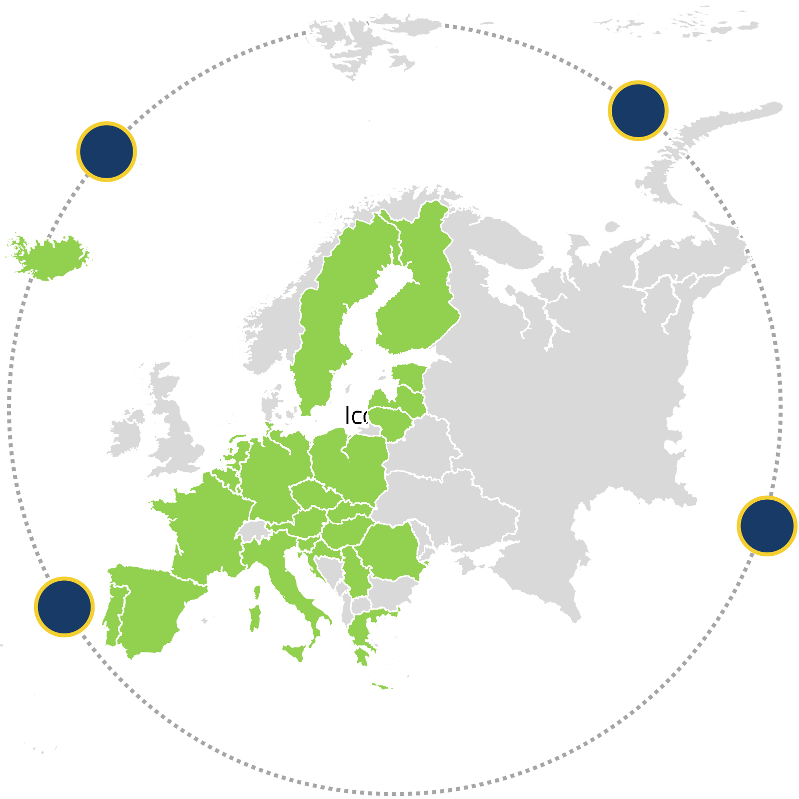
TLSO Community

30 different countries are part of the TLSO Community. The goal of this community is to help set up Trusted Lists and to keep them error-free. The countries in green are the TLSOs known to be very active members of the community

Qualified Trust Service Providers

There are 234 Qualified Trust Service Providers active in the EU

For the latest statistics, please consult the real-time dashboard.



DSS Libraries

The DSS Libraries have been downloaded more than 45.000 times

Conformance Checks

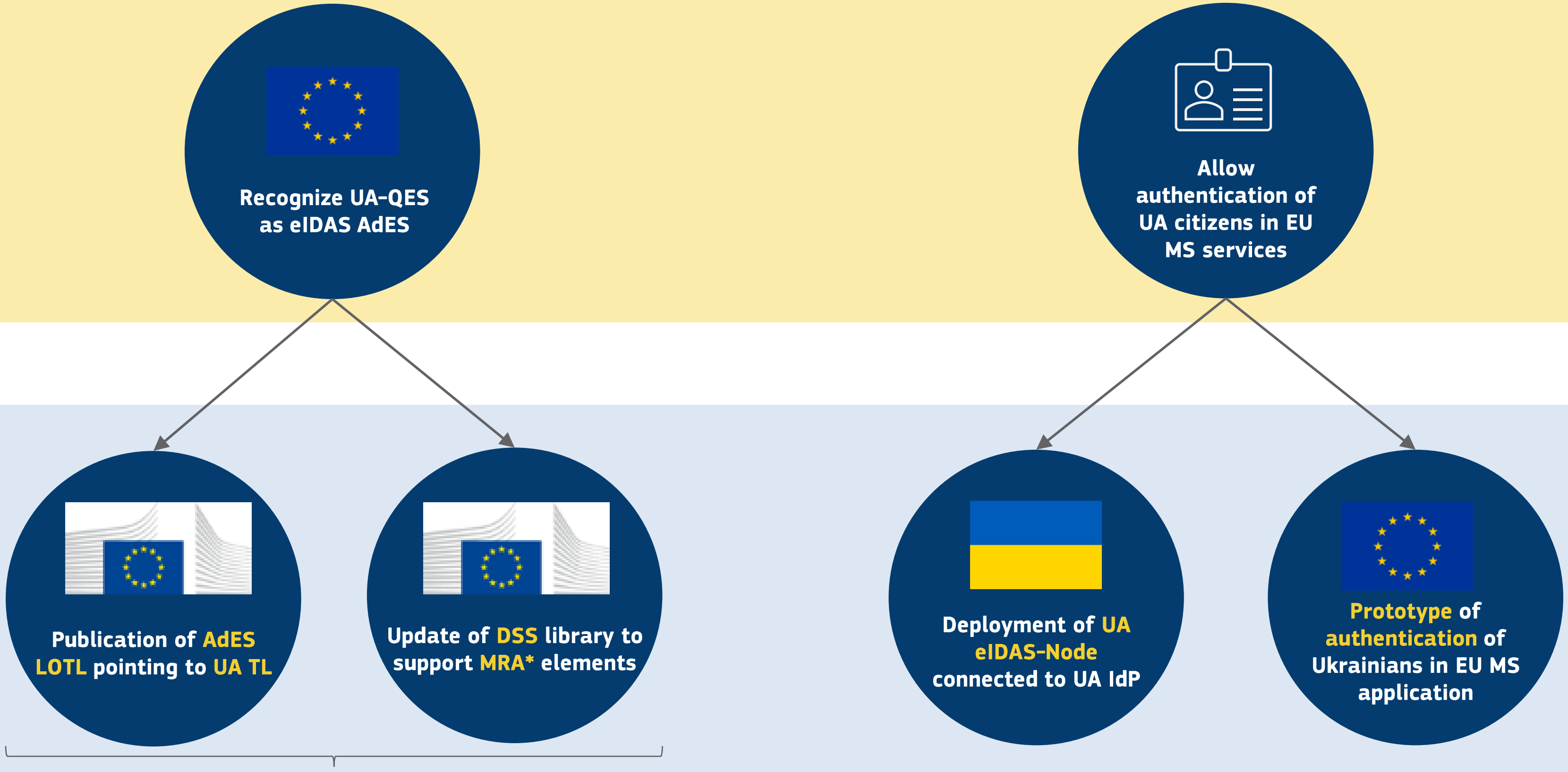
51 282 performed conformance checks using ETSI Conformance Checker

*Numbers collected in March 2023

The Genesis of the Third Countries Trusted Lists (TCTL) Programme

Formal request received from the **Ukrainian Government** to:

Technical implementation by EC and UA:



Recognize UA-QES as eIDAS AdES

Allow authentication of UA citizens in EU MS services

Publication of AdES LOTL pointing to UA TL

Update of DSS library to support MRA* elements

Deployment of UA eIDAS-Node connected to UA IdP

Prototype of authentication of Ukrainians in EU MS application

Supported by **eIDAS Art. 27(1)**
To be adopted by MSs on a **voluntary basis**

** The MRA technical element was introduced in the context of the pilot for international compatibility of Trust Services of the eSignature building block*

Objective, scope and solution

Objective: Provide **technical means** for the Member States to **facilitate** the validation of electronic signatures originating from 3rd countries

Scope: Recognition of a 3rd country's Qualified Electronic Signatures (**TC QES***) as eIDAS Advanced Electronic Signatures (**eIDAS AdES**)

Solution:

1) Host a **TC AdES LOTL**, for **voluntary** Member States to:
   - download and authenticate the TC's trusted list
   - validate TC QES* as eIDAS AdES, using the **machine-processable** MRA element, as specified in the Pilot for the International Compatibility of Trust Services
2) Update the DSS library to support the **processing** of the MRA element

* Recognize electronic signatures that are **not qualified in the EU**, but that **meet similar requirements** in third countries regulatory framework, as being fit for purpose in contexts requiring an **advanced electronic signature**.

Third Countries Trusted Lists (TCTL) Programme

A **streamlined** and **well-defined onboarding journey** for the 3rd countries willing to align their Trust Services with the European ones

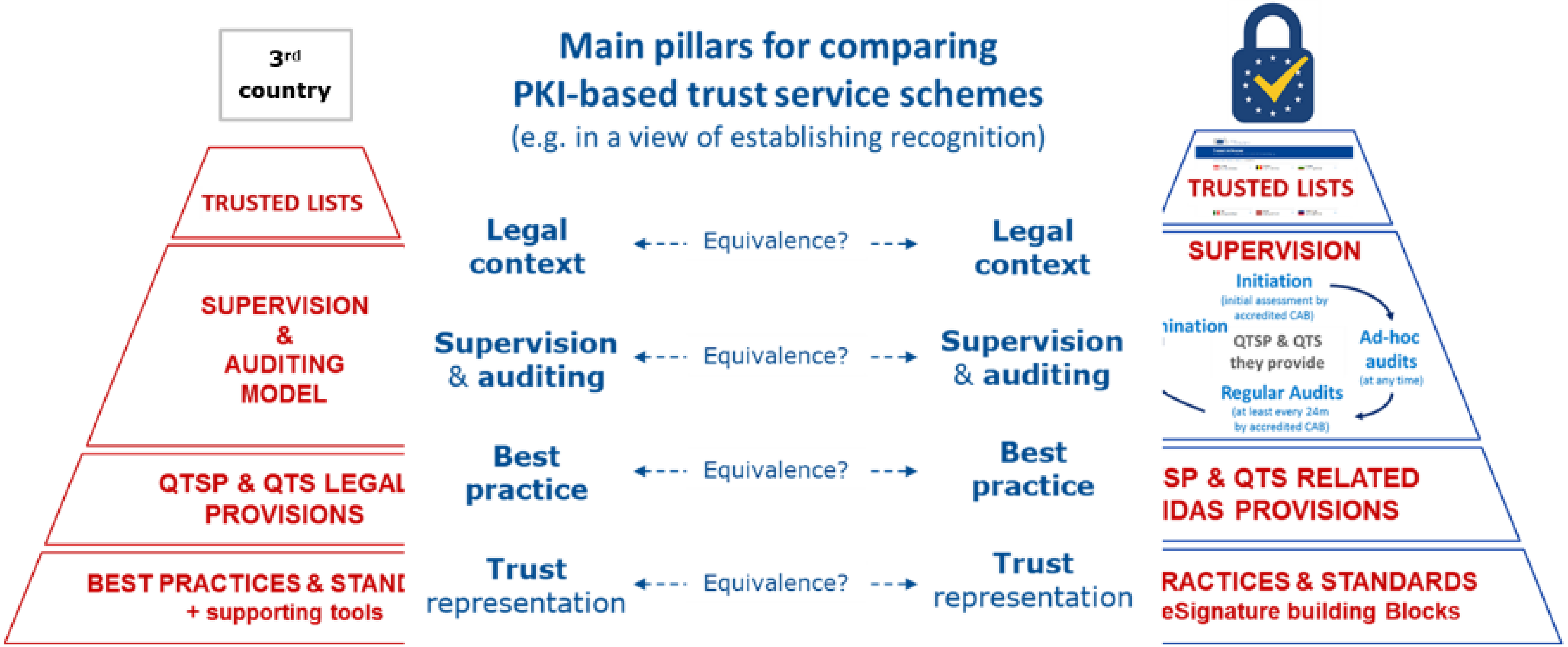
Version 2.2 of MRA element's specification, usage and XSD (ZIP archive), which enables relying parties to understand the syntax and semantic of the TC AdES LOTL. The **Digital Signature Software (DSS)** which supports since version **5.11.1** the interpretation of the content of the TC AdES LOTL

Signature applicability rules which enable relying parties to determine whether an electronic signature or seal fits in the recognition scheme established by the TC AdES LOTL

eIDAS Dashboard TCTL specific sections. The **document repository** with all the necessary documentation and guidance for the 3rd countries is available here

Publication of the TC AdES LOTL with a pointer to 3rd countries' Trust Services to facilitate the validation of electronic signatures and seals supported by certificates issued by trust service providers established in . This comprehensive list includes all relevant information necessary to interpret the content of ' trusted lists in compliance with the EU's requirements and best practices for validating advanced electronic signatures and seals. The EU also acknowledges the demand for voluntary recognition of Third Country trust services, particularly for the recognition of electronic signatures and seals in the context of Articles 27 and 37 of the eIDAS Regulation

Guidance for 3rd Countries in preparatory phase



3rd country

TRUSTED LISTS

SUPERVISION & AUDITING MODEL

QTSP & QTS LEGAL PROVISIONS

BEST PRACTICES & STANI
+ supporting tools

Main pillars for comparing PKI-based trust service schemes
(e.g. in a view of establishing recognition)

Legal context	←--- Equivalence? ---→	Legal context
Supervision & auditing	←--- Equivalence? ---→	Supervision & auditing
Best practice	←--- Equivalence? ---→	Best practice
Trust representation	←--- Equivalence? ---→	Trust representation

TRUSTED LISTS

SUPERVISION

Initiation
(initial assessment by accredited CAB)

ıination

QTSP & QTS they provide

Ad-hoc audits
(at any time)

Regular Audits
(at least every 24m by accredited CAB)

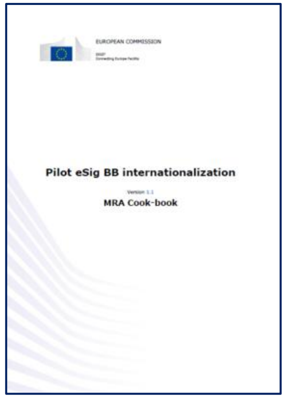
SP & QTS RELATED
IDAS PROVISIONS

RACTICES & STANDARDS
eSignature building Blocks

Path to mutual recognition

- EC provides guidance & technical pilot tools to assist 3rd countries
- Assessment on four pillars (Legal, Supervision & auditing, Technical, Trusted List)
- DEP eSignature’s international compatibility pilot support material

  https://eidas.ec.europa.eu/efda/home/#/screen/international



EUROPEAN COMMISSION

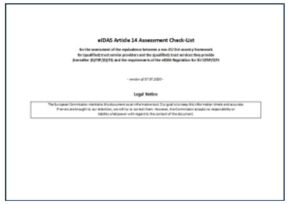
DIGIT
Connecting Europe Facility

Pilot eSig BB internationalization

Version 1.1

MRA Cook-book

MRA CookBook



eIDAS Article 14 Assessment Check-List

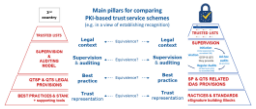
for the assessment of the equivalence between a non-EU 3rd country framework
for (qualified) trust service providers and the (qualified) trust services they provide
(hereafter (Q)TSP/(Q)TS) and the requirements of the eIDAS Regulation for EU QTSP/QTS

- version of 07.07.2020 -

Legal Notice

The European Commission maintains this document as an informative tool. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them. However, the Commission accepts no responsibility or liability whatsoever with regard to the content of the document.

eIDAS Article 14
Assessment
Check-List
(4 pillars)


3rd country
Main pillars for comparing
PKI-based trust service schemes
(e.g. in a view of establishing recognition)
TRUSTED LISTS
SUPERVISION & AUDITING MODEL
QTSP & QTS LEGAL PROVISIONS
BEST PRACTICES & STANDARDS + supporting tools
Legal context
Supervision & auditing
Best practice
Trust representation
Equivalence?
Equivalence?
Equivalence?
Equivalence?
Legal context
Supervision & auditing
Best practice
Trust representation
TRUSTED LISTS
SUPERVISION
SP & QTS RELATED IDAS PROVISIONS
RACTICES & STANDARDS
eSignature building Blocks

EUROPEAN COMMISSION

Pilot eSig BB internationalization

Version 1.1

MRAinfo element specification

EUROPEAN COMMISSION

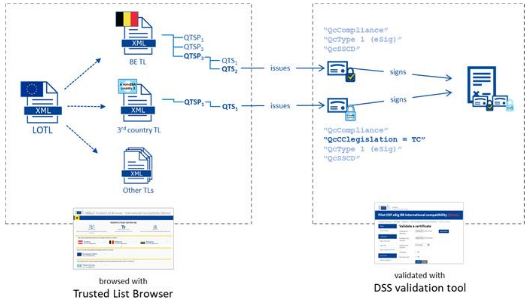
Pilot eSig BB internationalization

Version 1.1

MRAinfo element usage

Trusted List support

- MRA element specification (and XML Schema Definition)
- MRA element usage
- In EU LOTL & Foreign TL



Technical tools

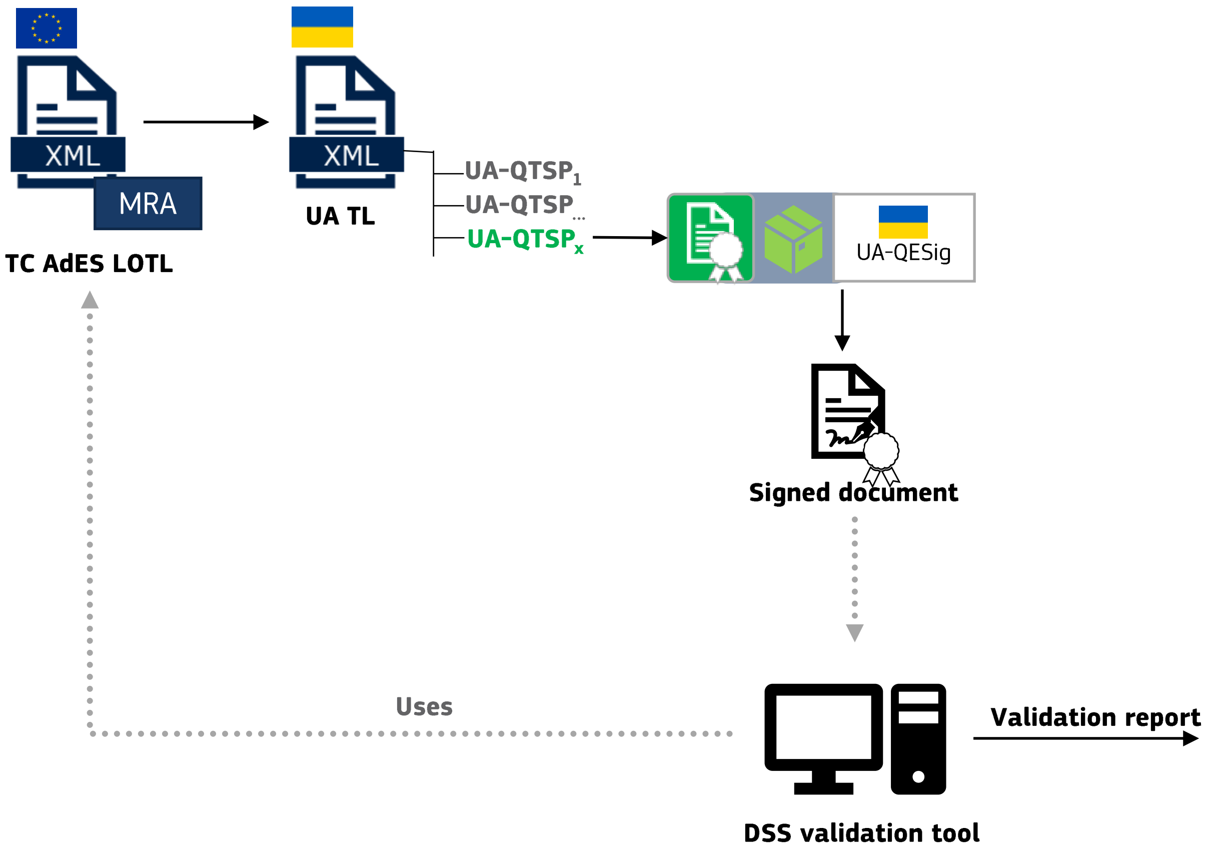
- Test LOTL
- Small test PKI
- Sample signed document
- Demo web application to validate signatures/certificates, based on DSS library
- Updated TL Browser

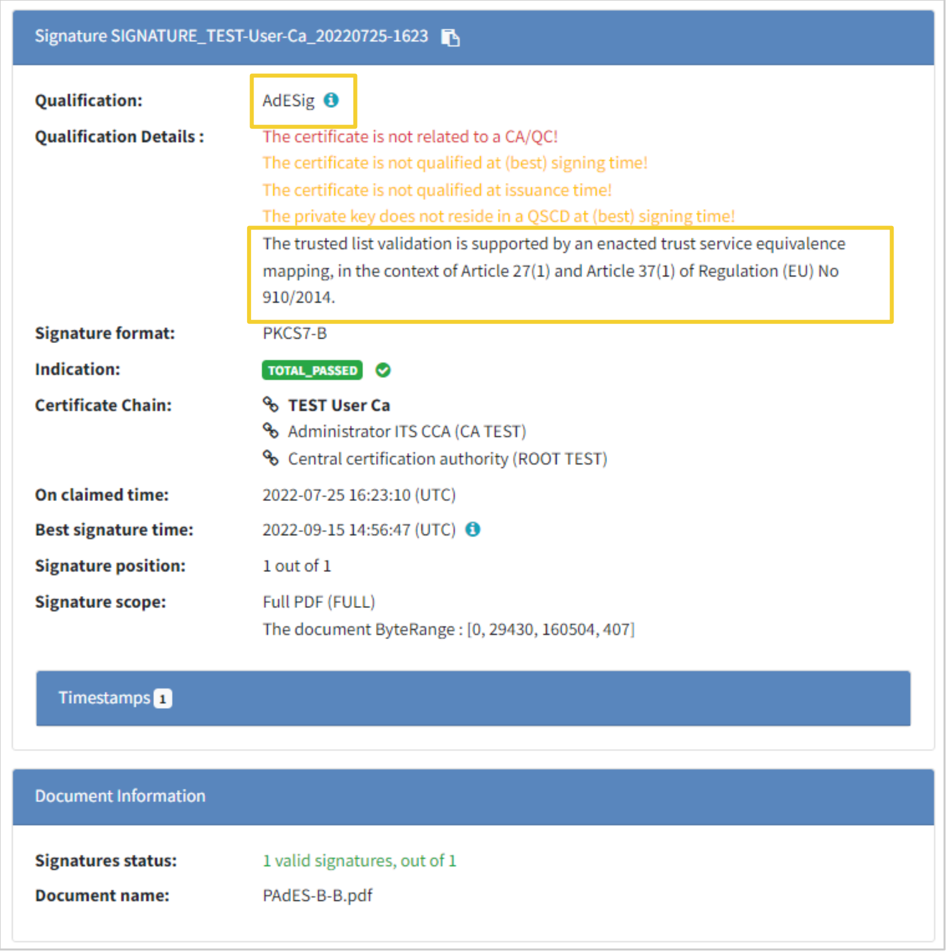
European Commission Third Countries Trusted Lists (TCTL) Programme

Publication of **TC AdES LOTL** & update of **DSS library** to support the **processing of MRA elements**

International Compatibility Pilot for Trust Services

Contains technical documentation and specifications for the technical execution of Art. 14 mutual recognition agreement or facilitating Art. 27(1) application to non-EU electronic signatures.





Signature SIGNATURE_TEST-User-Ca_20220725-1623

Qualification: AdESig

Qualification Details :
The certificate is not related to a CA/QC!
The certificate is not qualified at (best) signing time!
The certificate is not qualified at issuance time!
The private key does not reside in a QSCD at (best) signing time!
The trusted list validation is supported by an enacted trust service equivalence mapping, in the context of Article 27(1) and Article 37(1) of Regulation (EU) No 910/2014.

Signature format: PKCS7-B

Indication: TOTAL_PASSED ✓

Certificate Chain:
TEST User Ca
Administrator ITS CCA (CA TEST)
Central certification authority (ROOT TEST)

On claimed time: 2022-07-25 16:23:10 (UTC)

Best signature time: 2022-09-15 14:56:47 (UTC)

Signature position: 1 out of 1

Signature scope: Full PDF (FULL)
The document ByteRange : [0, 29430, 160504, 407]

Timestamps 1

Document Information

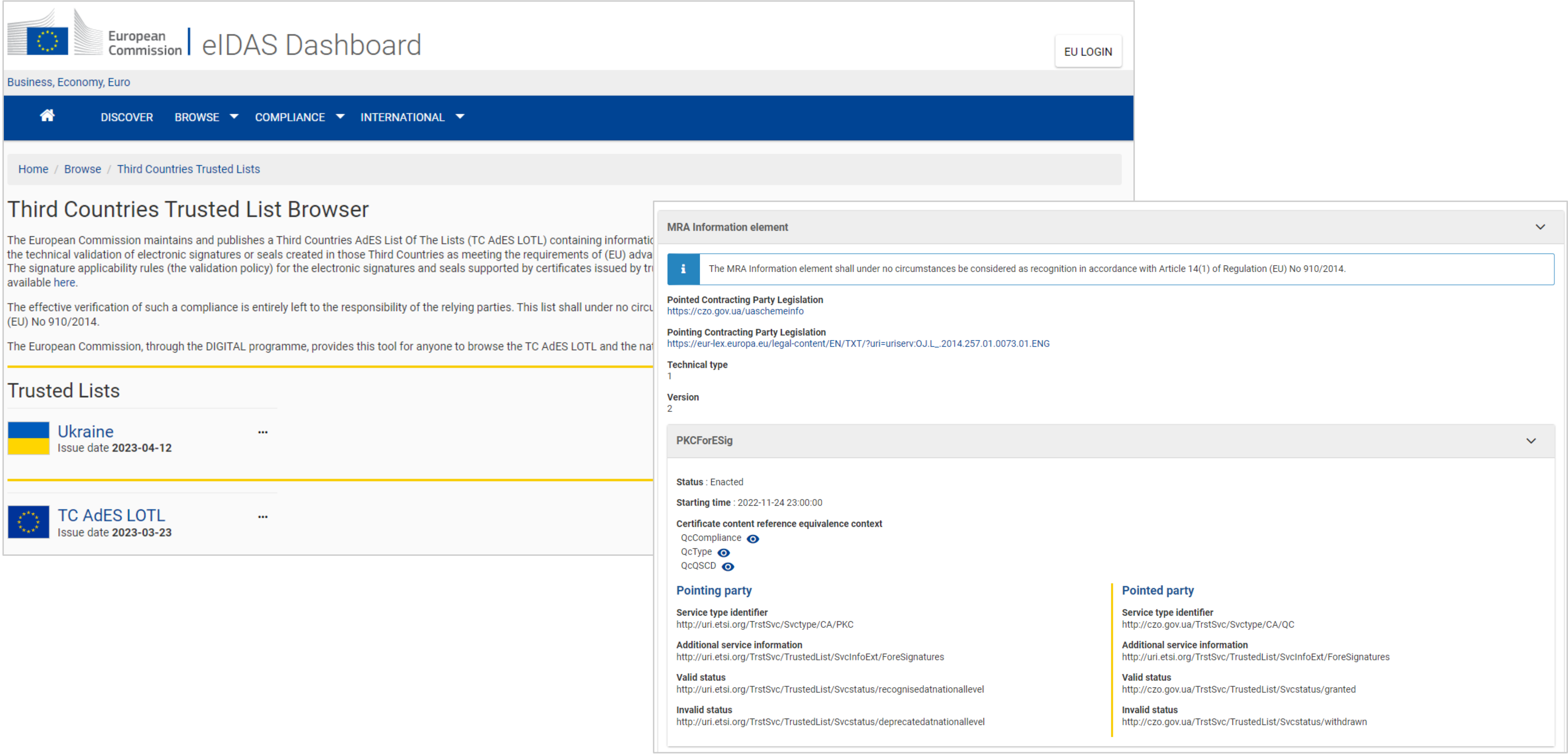
Signatures status: 1 valid signatures, out of 1

Document name: PAdES-B-B.pdf

eSignature

European Commission’s Third Countries Trusted Lists (TCTL) Programme

User-friendly display of **TC AdES LOTL** in the eIDAS Dashboard



Third Countries Trusted List Browser

The European Commission maintains and publishes a Third Countries AdES List Of The Lists (TC AdES LOTL) containing informatio
the technical validation of electronic signatures or seals created in those Third Countries as meeting the requirements of (EU) adva
The signature applicability rules (the validation policy) for the electronic signatures and seals supported by certificates issued by tr
available here.

The effective verification of such a compliance is entirely left to the responsibility of the relying parties. This list shall under no circu
(EU) No 910/2014.

The European Commission, through the DIGITAL programme, provides this tool for anyone to browse the TC AdES LOTL and the na

Trusted Lists

Ukraine
Issue date **2023-04-12**

TC AdES LOTL
Issue date **2023-03-23**

MRA Information element

The MRA Information element shall under no circumstances be considered as recognition in accordance with Article 14(1) of Regulation (EU) No 910/2014.

Pointed Contracting Party Legislation
https://czo.gov.ua/uaschemeinfo

Pointing Contracting Party Legislation
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

Technical type
1

Version
2

PKCForESig

Status : Enacted

Starting time : 2022-11-24 23:00:00

Certificate content reference equivalence context
QcCompliance
QcType
QcQSCD

Pointing party

Service type identifier
http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

Additional service information
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

Valid status
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel

Invalid status
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel

Pointed party

Service type identifier
http://czo.gov.ua/TrstSvc/Svctype/CA/QC

Additional service information
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

Valid status
http://czo.gov.ua/TrstSvc/TrustedList/Svcstatus/granted

Invalid status
http://czo.gov.ua/TrstSvc/TrustedList/Svcstatus/withdrawn

5

Trust services in the Republic of Albania

Ermela CEKANI

Expert – National Authority for Electronic Certification and Cyber Security

TRUST SERVICES IN THE REPUBLIC OF ALBANIA

Ermela Cekani

National Authority for Electronic Certification and Cyber Security

2023

Table of Content

- **Legal regulatory framework in field of Trust Services.**
- **Competences of National Authority on Electronic Certification and Cyber Security**
- **Registration of QTSP to the Supervisory Authority**
- **Requirements for Qualified Trust Service Providers**
- **QTSP/CAB Registration Scheme**
- **Trusted Lists / Electronic Identification Schemes**
- **International Aspects**

Legal regulatory framework

- Law "On Electronic Signature"
- Law “On electronic Identification and Trusted services”

The scope of those laws were to define the necessary legal framework for the recognition of electronic signatures, electronic identification, electronic seals, electronic transmission service and websites authenification in the Republic of Albania.

In compliance with the eIDAS Regulation

Actually the Authority is working on merging the two laws into one single law, including into it:

Missing article

- Remote Identification

Clarifying the article

- qualified electronic signature Creation devices

Competences of National Authority on Electronic Certification and Cyber Security

- National Authority For Electronic Certification and Cyber Security (NAECCS) is the responsible body for the supervision of the Law “On Electronic Signatures”, Law “On Electronic Identification and Trust Services” and their implementing acts.

MISSION

The mission of the National Authority for Electronic Certification and Cyber Security is to enhance the level security in electronic transactions in the domestic market, guaranteeing secure electronic interaction between public authorities and citizens, businesses, enhancing the effectiveness of public and private online services, e-business and e-commerce

Competences of National Authority on Electronic Certification and Cyber Security

1. Registers the Qualified Trust Service Provider that fulfil the requirements set by law.
    - Grant the qualified status to trust service providers and withdraw this status in case of any failure to fulfil requirements
2. Registers the Conformity Assessment Bodies that fulfil the requirements set by law
3. Supervise qualified trust service providers established in Republic of Albania, by performing periodical inspection
4. Determines the rules and standards to be implemented by Qualified Trust Service Provider, issuing qualified electronic certificates, in accordance with EU standards.
5. Analyses the conformity assessment report provided by CAB
6. Inform other supervisory bodies and the public about breaches of security or loss of integrity

Registration of QTSP to NAECCS

Where trust service providers, without qualified status, intend to start providing qualified trust services, they shall submit to the National Authority on Electronic Certification and Cyber Security:

1. A notification of their intention for the services the will provide
2. Relevant documentation according to national legislation, and ETSI/ISO/CEN/ISSS standards, including Legal/ Financial/ Professional/ Technical specifications.
3. The National Authority for Electronic Certification and Cyber Security (NAECCS) has published specific regulations and guidelines for the registration process of trust service providers and CABs
4. NAECCS shall verify whether the trust service provider and the trust services provided by it comply with the requirements set by law

Requirements for Qualified Trust Service Providers

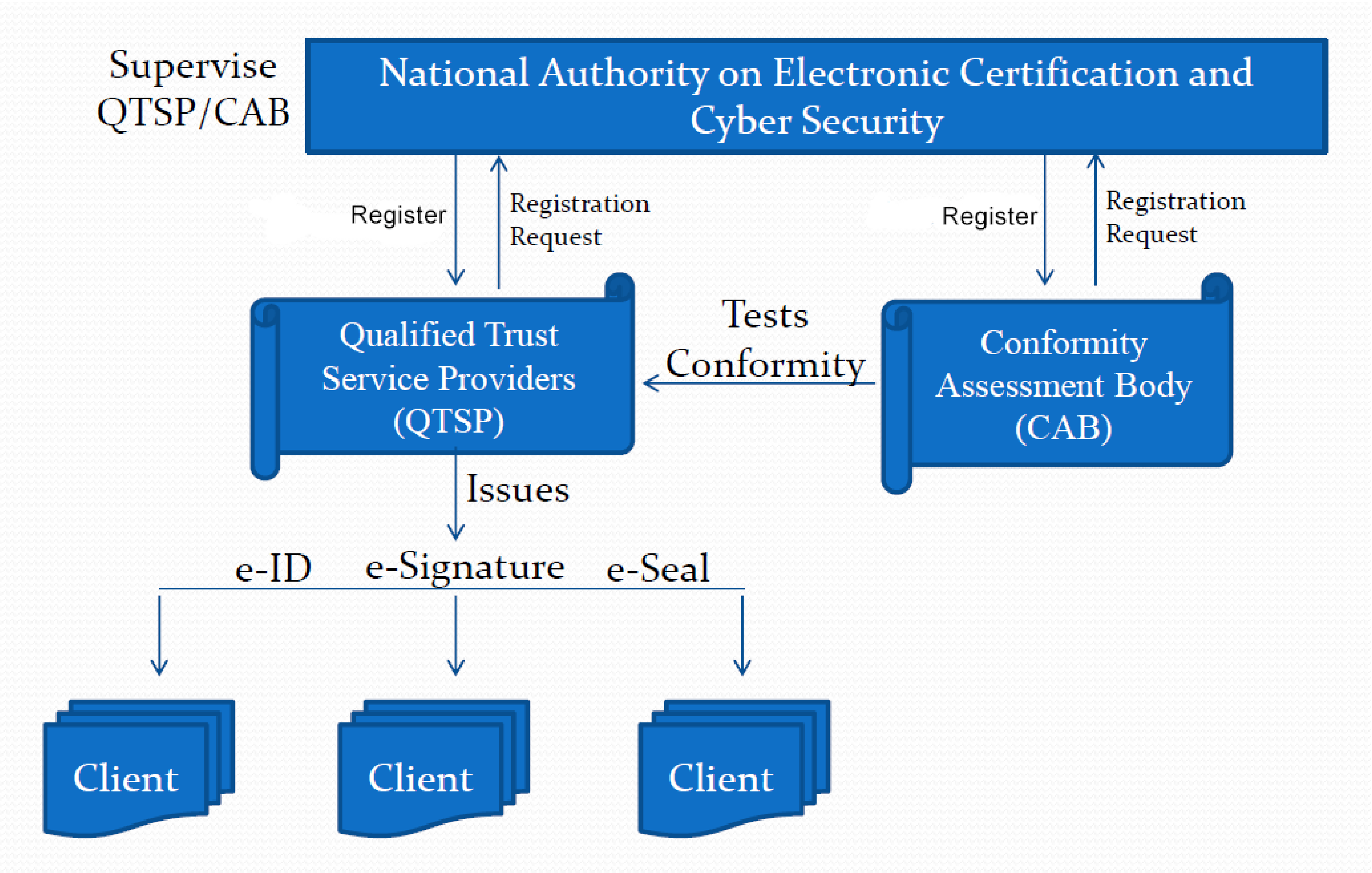
When issuing a qualified electronic certificate, a qualified trust service provider shall verify, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

- by the physical presence of the natural person or of an authorized representative of the legal person;

A qualified trust service provider providing qualified trust services shall:

- inform the NAECCS of any change in the provision of its qualified trust services and an intention to cease those activities
- employ staff and, if applicable, subcontractors who possess the necessary expertise, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules
- use trustworthy systems and products that are protected against modification or unauthorized access
- maintain sufficient financial resources aor obtain appropriate liability insurance for the risk of liability for damages
- record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.
- have an up-to-date termination plan to ensure continuity of service

QTSP/CAB Registration Scheme



Supervise QTSP/CAB

National Authority on Electronic Certification and Cyber Security

Register

Registration Request

Register

Registration Request

Qualified Trust Service Providers (QTSP)

Tests Conformity

Conformity Assessment Body (CAB)

Issues

e-ID e-Signature e-Seal

Client

Client

Client

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Registered Qualified Trust Service Providers

- **The National Agency for Information Society (NAIS)**, a public institution which issues qualified electronic certificates

  - Total number of issued qualified electronic certificates is 339 400

- **ALEAT** a private entity, that issues qualified electronic certificates, in the national ID Card's

  - there have been issued a total of 2 950 000 electronic certificates.

  - there have been revoked a total of 434 000 electronic certificates

Trusted Lists / Electronic Identification Schemes

NAECCS is the responsible body for establishing, maintaining and publishing the trusted lists, including information related to the qualified trust service providers, together with information related to the qualified trust services provided by them.

National Trusted List includes two registered Qualified Trust Service Providers:

- **The National Agency for Information Society (NAIS**) (Public Institution)
- **ALEAT (**private entity)

The Albanian trusted list is published in the official website of NAECCS : **https://cesk.gov.al/trusted-list/**

The electronic identification scheme and the electronic identification means issued thereunder meet the requirements of the **highest level of assurance**

International aspects

- Albania is full member of FESA and ENISA Article 19 Expert group and participates in those meetings at least twice a year

- Since 2014, Albania as a candidate country for membership in the European Union (EU), has had as a main focus the harmonization of the national legislation with the EU *acquis*.

- Within the framework of The National Plan for European Integration 2023-2025, NAECCS is continuously working to approximate the legislation in the field of trusted services with the EU legislation (regulations, standards, guidelines)

THANK YOU FOR YOUR ATTENTION!

Ermela Cekani

NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY

Email: ermela.cekani@cesk.gov.al

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

COFFEE BREAK

10:30 – 10:50

6

Panel discussion

Apostolos Tolis APLADAS

Programme Manager – DG DIGIT, European Commission (MODERATOR)

Panel discussion

Viky MANAILA
Trust Services Director, INTESI GROUP

Sylvie LACROIX
Managing Director, SEALED

Evgenia NIKOLOUZOU
Cybersecurity Officer, ENISA

Ask your questions via Sli.do

Join at
slido.com
#4172 878

7

Presentation of the TC AdES LOTL and the UA collaboration

Olivier BARETTE

Partner – Nowina Solutions

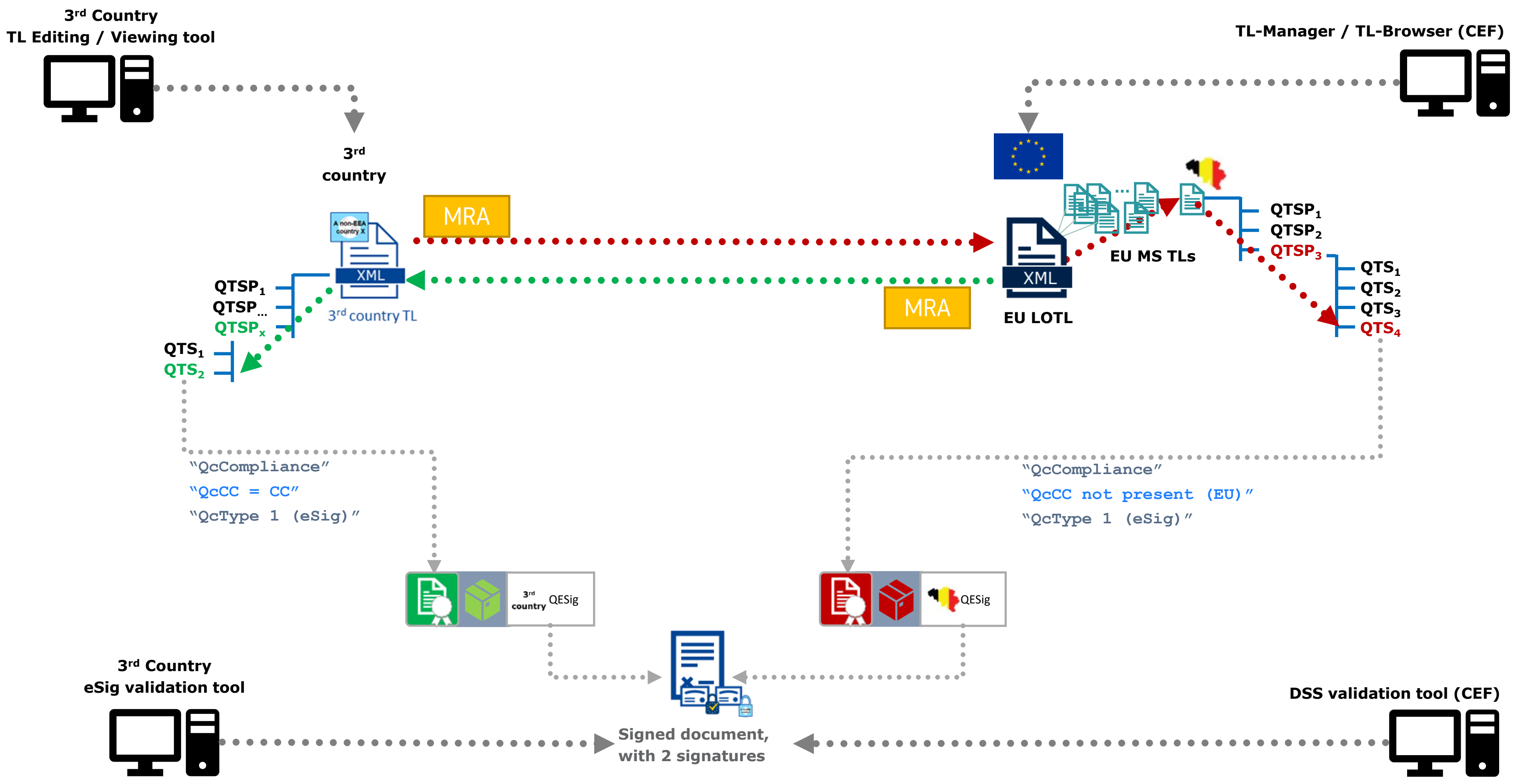
Pilot for the International Compatibility of Trust Services

Objective of the project:

Demonstrate the **technical feasibility** of **mutual recognition** of electronic **signatures**:

- TC qualified signature recognized by **EU**
- **EU** qualified signature recognized by **TC**

Pilot for the International Compatibility of Trust Services



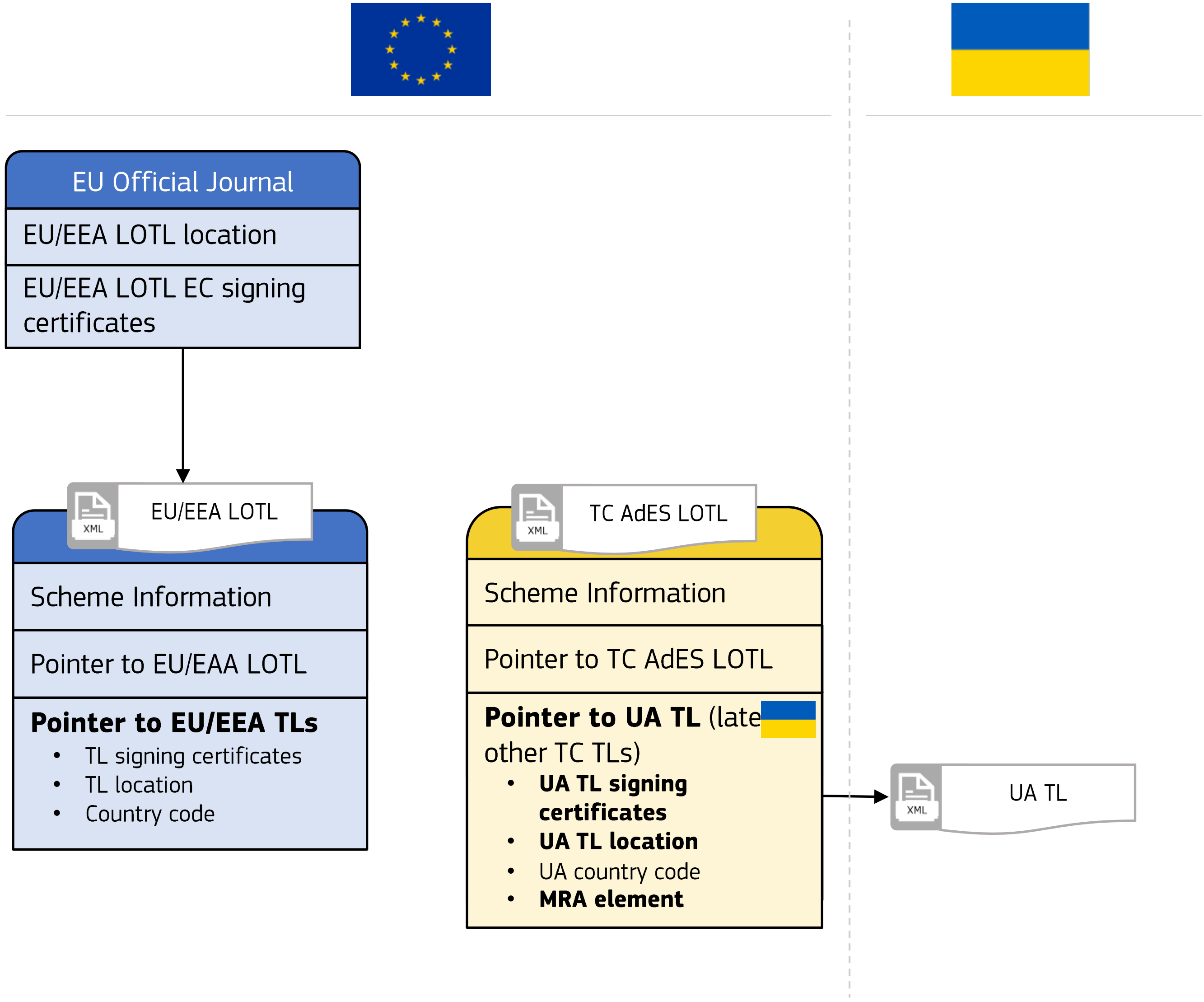
MRA-Info element

Usage n°2: Recognition of electronic signatures from Ukraine as EU advanced electronic signatures

Publication of **TC AdES LOTL** pointing to UA Trusted List (TL)

To allow Member States on a **voluntary** basis to:

- Download and authenticate the TC trusted list;
- Validate **UA-QES as eIDAS AdES**, using the Mutual Recognition Agreement (MRA) element.



EU Official Journal

EU/EEA LOTL location

EU/EEA LOTL EC signing certificates

EU/EEA LOTL

Scheme Information

Pointer to EU/EAA LOTL

Pointer to EU/EEA TLs

- TL signing certificates
- TL location
- Country code

TC AdES LOTL

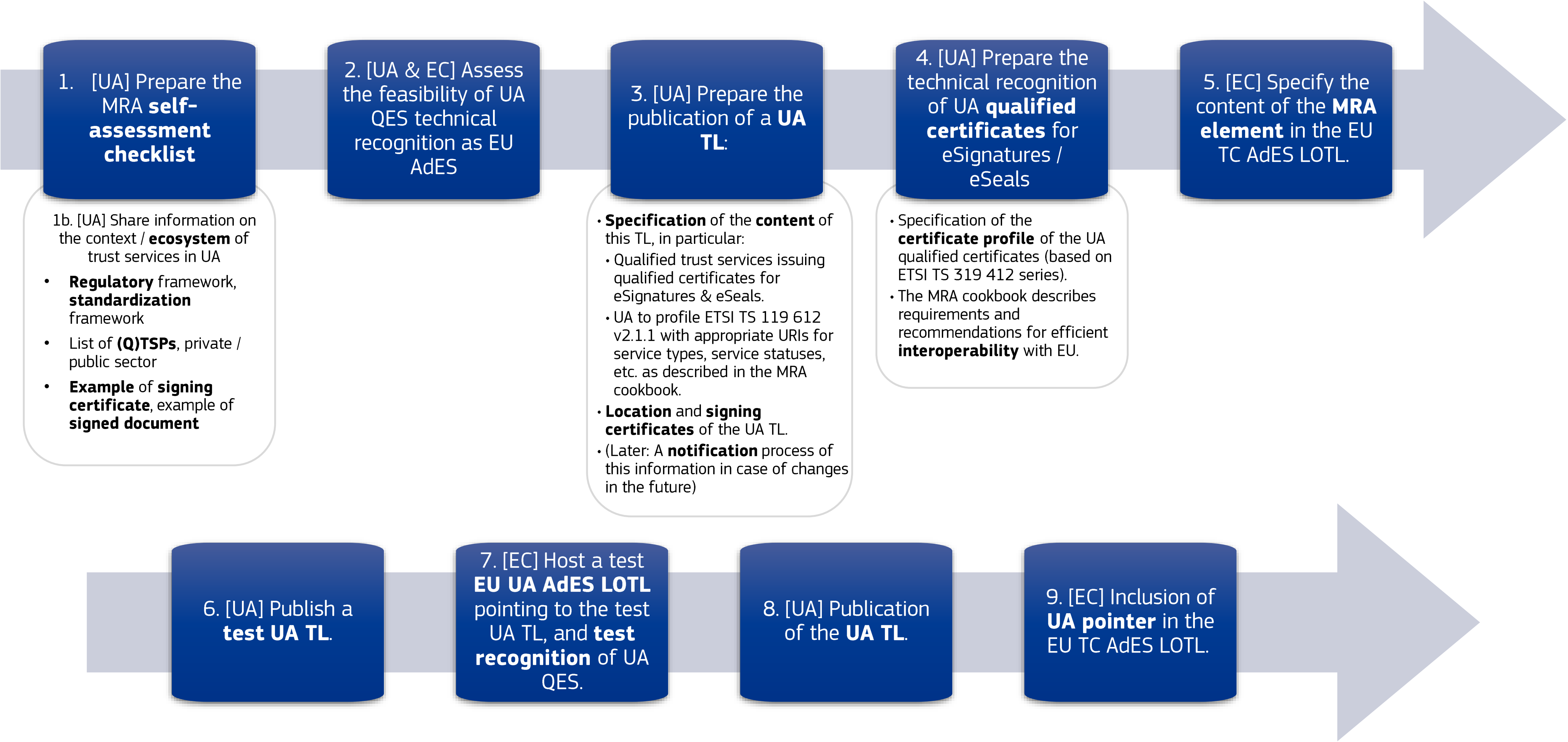
Scheme Information

Pointer to TC AdES LOTL

Pointer to UA TL (late other TC TLs)

- **UA TL signing certificates**
- **UA TL location**
- UA country code
- **MRA element**

Technical process for inclusion in TC AdES LOTL



1. [UA] Prepare the MRA **self-assessment checklist**

1b. [UA] Share information on the context / **ecosystem** of trust services in UA

- **Regulatory** framework, **standardization** framework
- List of **(Q)TSPs**, private / public sector
- **Example** of **signing certificate**, example of **signed document**

2. [UA & EC] Assess the feasibility of UA QES technical recognition as EU AdES

3. [UA] Prepare the publication of a **UA TL**:

- **Specification** of the **content** of this TL, in particular:
  - Qualified trust services issuing qualified certificates for eSignatures & eSeals.
  - UA to profile ETSI TS 119 612 v2.1.1 with appropriate URIs for service types, service statuses, etc. as described in the MRA cookbook.
- **Location** and **signing certificates** of the UA TL.
- (Later: A **notification** process of this information in case of changes in the future)

4. [UA] Prepare the technical recognition of UA **qualified certificates** for eSignatures / eSeals

- Specification of the **certificate profile** of the UA qualified certificates (based on ETSI TS 319 412 series).
- The MRA cookbook describes requirements and recommendations for efficient **interoperability** with EU.

5. [EC] Specify the content of the **MRA element** in the EU TC AdES LOTL.

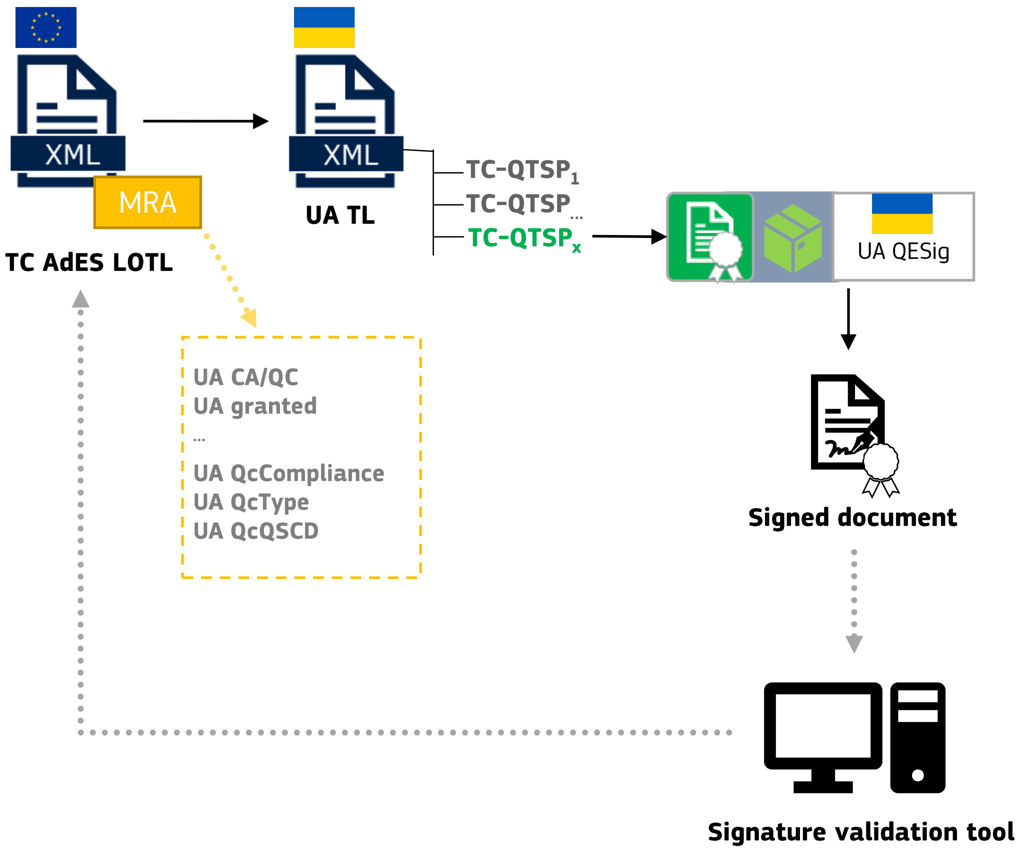
6. [UA] Publish a **test UA TL**.

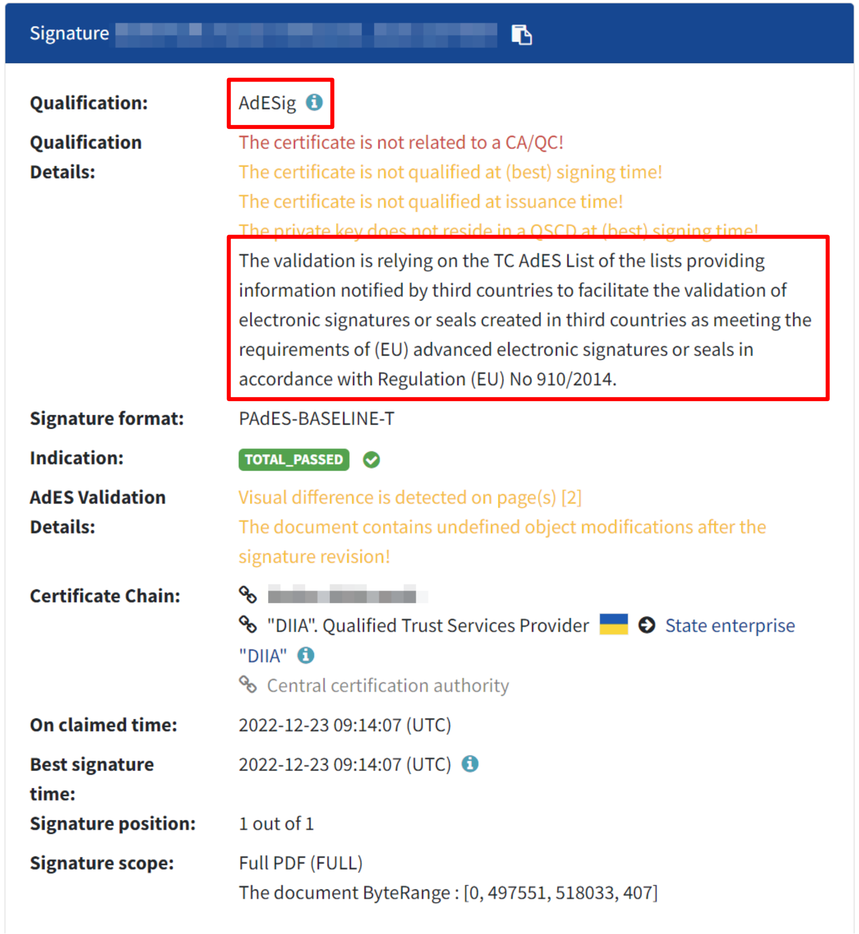
7. [EC] Host a test **EU UA AdES LOTL** pointing to the test UA TL, and **test recognition** of UA QES.

8. [UA] Publication of the **UA TL**.

9. [EC] Inclusion of **UA pointer** in the EU TC AdES LOTL.

Recognition of electronic signatures from Ukraine with DSS





Signature [redacted]

Qualification: AdESig

Qualification Details:
The certificate is not related to a CA/QC!
The certificate is not qualified at (best) signing time!
The certificate is not qualified at issuance time!
The private key does not reside in a QSCD at (best) signing time!
The validation is relying on the TC AdES List of the lists providing information notified by third countries to facilitate the validation of electronic signatures or seals created in third countries as meeting the requirements of (EU) advanced electronic signatures or seals in accordance with Regulation (EU) No 910/2014.

Signature format: PAdES-BASELINE-T

Indication: TOTAL_PASSED ✓

AdES Validation Details:
Visual difference is detected on page(s) [2]
The document contains undefined object modifications after the signature revision!

Certificate Chain:
[redacted]
"DIIA". Qualified Trust Services Provider State enterprise "DIIA"
Central certification authority

On claimed time: 2022-12-23 09:14:07 (UTC)

Best signature time: 2022-12-23 09:14:07 (UTC)

Signature position: 1 out of 1

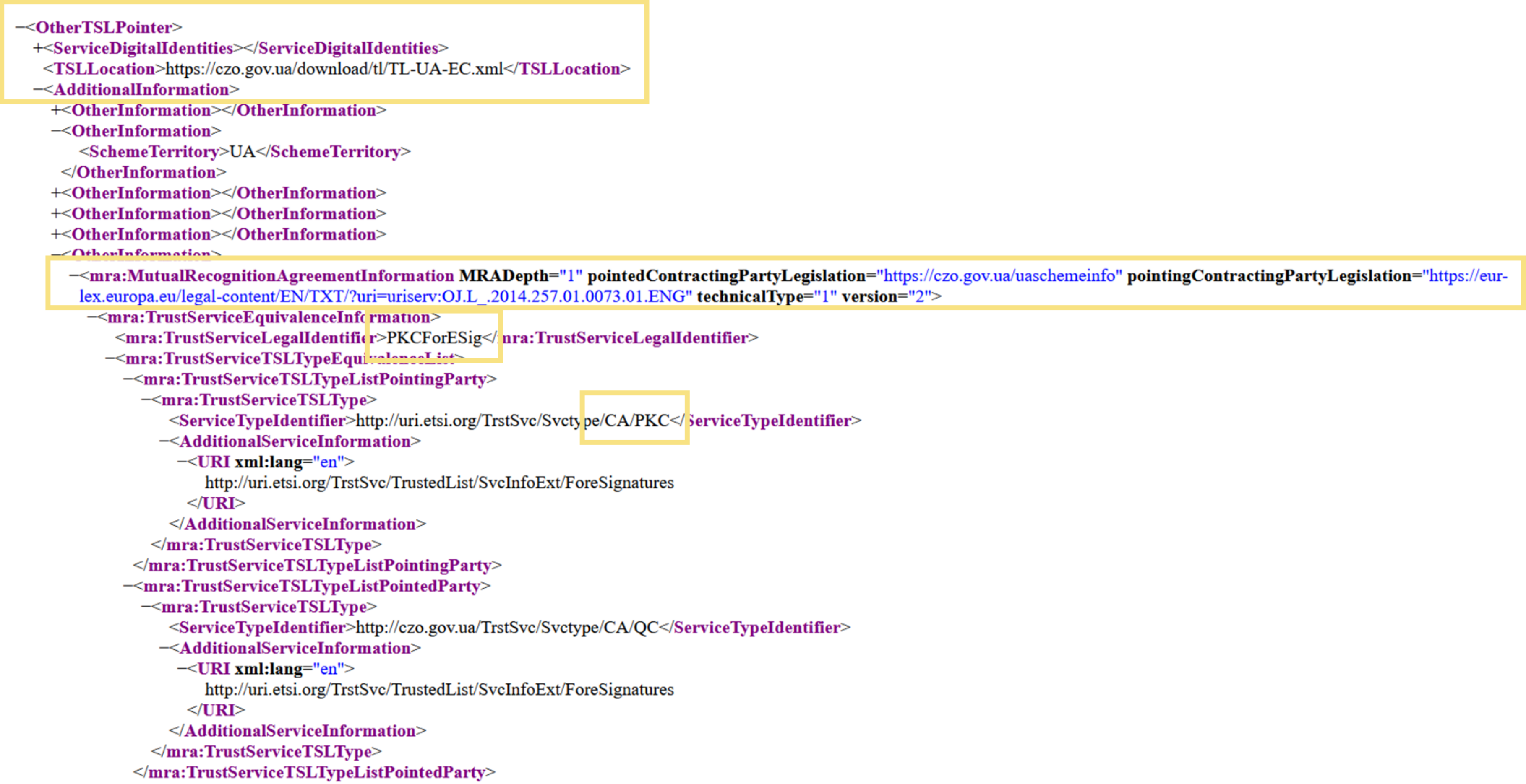
Signature scope: Full PDF (FULL)
The document ByteRange : [0, 497551, 518033, 407]

MRA-Info element specifications

Illustration based on the TC AdES LOTL pointing to the UA TL

MutualRecognitionAgreementInformation element as an additional information included to the OtherTSLPointer element of the “Pointers to other TSLs”.

This MRA Info element contains a sequence of TrustServiceEquivalenceInformation elements.



```
−<OtherTSLPointer>
  +<ServiceDigitalIdentities></ServiceDigitalIdentities>
   <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
  −<AdditionalInformation>
    +<OtherInformation></OtherInformation>
    −<OtherInformation>
        <SchemeTerritory>UA</SchemeTerritory>
     </OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    −<OtherInformation>
      −<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPartyLegislation="https://czo.gov.ua/uaschemeinfo" pointingContractingPartyLegislation="https://eur-
       lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" technicalType="1" version="2">
        −<mra:TrustServiceEquivalenceInformation>
           <mra:TrustServiceLegalIdentifier>PKCForESig</mra:TrustServiceLegalIdentifier>
          −<mra:TrustServiceTSLTypeEquivalenceList>
            −<mra:TrustServiceTSLTypeListPointingParty>
              −<mra:TrustServiceTSLType>
                 <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</ServiceTypeIdentifier>
                −<AdditionalServiceInformation>
                  −<URI xml:lang="en">
                     http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                   </URI>
                 </AdditionalServiceInformation>
               </mra:TrustServiceTSLType>
             </mra:TrustServiceTSLTypeListPointingParty>
            −<mra:TrustServiceTSLTypeListPointedParty>
              −<mra:TrustServiceTSLType>
                 <ServiceTypeIdentifier>http://czo.gov.ua/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
                −<AdditionalServiceInformation>
                  −<URI xml:lang="en">
                     http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                   </URI>
                 </AdditionalServiceInformation>
               </mra:TrustServiceTSLType>
             </mra:TrustServiceTSLTypeListPointedParty>
```

Summary

Objective, scope and solution

Objective: Provide **technical means** for the Member States to **facilitate** the validation of electronic signatures originating from Ukraine (and, later, other countries in need) in the context of eIDAS Article 27(1)

Scope: Recognition of Ukrainian Qualified Electronic Signatures (**UA QES***) as eIDAS Advanced Electronic Signatures (**eIDAS AdES**)

Solution:

1) Host a TC AdES LOTL, for **voluntary** Member States to:
   - ○ download and authenticate the UA trusted list (and, later, other countries in need)
   - ○ validate UA QES* as eIDAS AdES, using the **machine-processable** MRA element, as specified in the Pilot for the International Compatibility of Trust Services:

   https://eidas.ec.europa.eu/efda/intl-pilot/#/screen/home/demo

   https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tc-tl

2) Update the DSS library to support the **processing** of the MRA element:

   https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Signature+Service+-++DSS

* Recognize electronic signatures that are **not qualified in the EU**, but that **meet similar requirements** in third countries regulatory framework, as being fit for purpose in contexts requiring an **advanced electronic signature**.

LUNCH BREAK

12:05 – 13:35

ANNEX (Panel discussion slides)

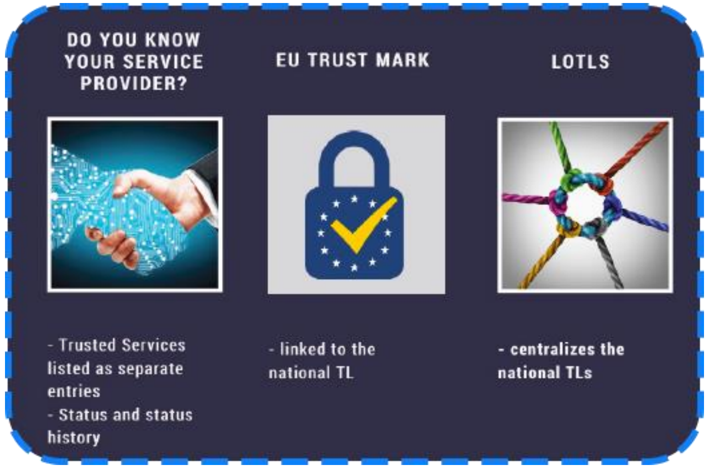
Trust in Time

Trust List Human Readable format

2010 - 2012

Trust List Machine Readable format

2016



DO YOU KNOW YOUR SERVICE PROVIDER?

- Trusted Services listed as separate entries
- Status and status history

EU TRUST MARK

- linked to the national TL

LOTLS

- centralizes the national TLs

BREAKING NEWS

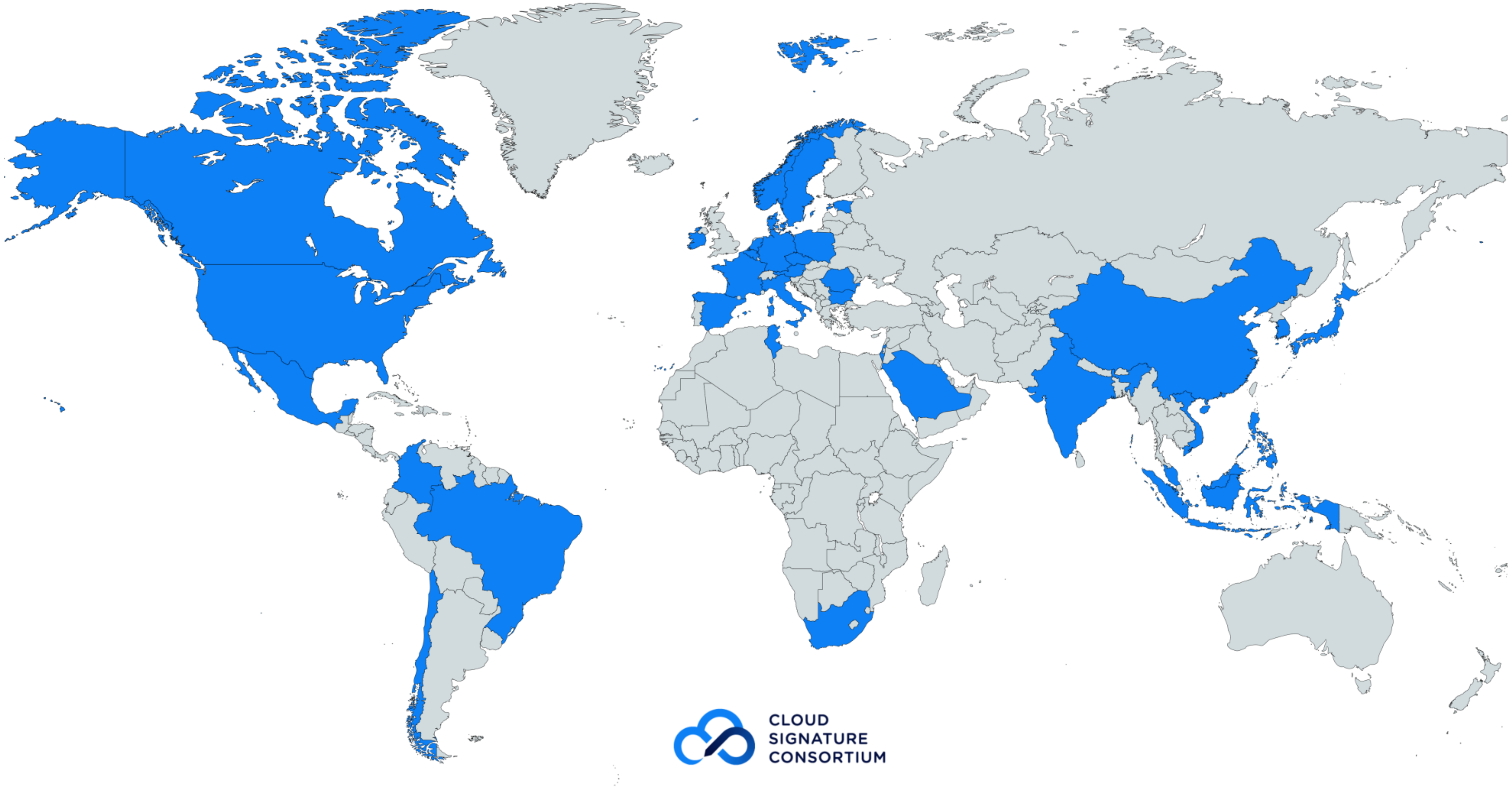
US commercial and gov. Relying Parties identify and validate digital signatures issued by EU TL CAs

PROOF OF CONCEPT

- technical implementation of the policy trust
- TL with SBCA cross-certified CAs

EU Relying Party applications identify and validate digital signatures issued by CAs of SBCA/FPKI

Trust Service Providers – QES & AdES



CLOUD SIGNATURE CONSORTIUM

Viky MANAILA

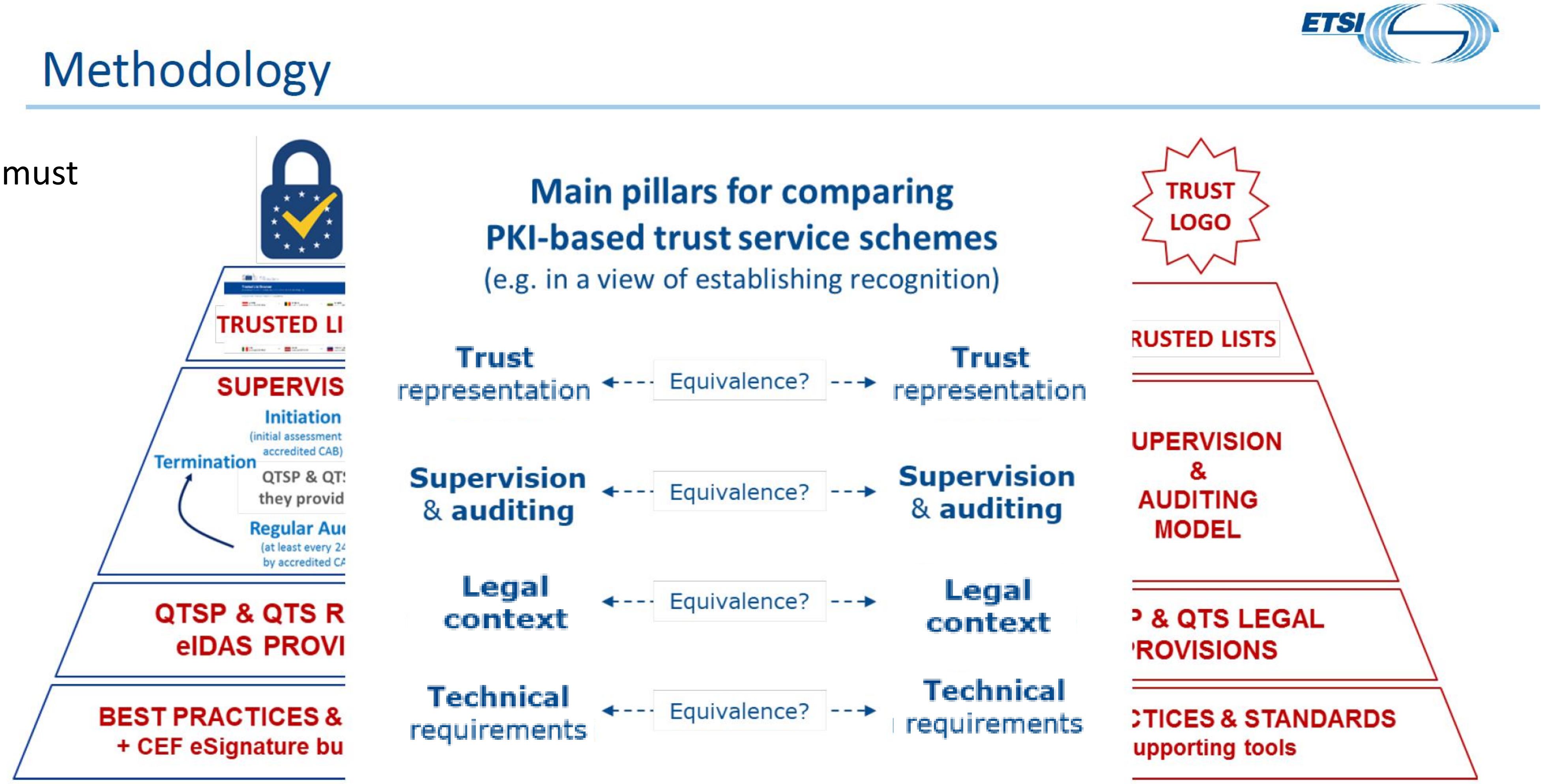
Thank you!

Viky Manaila 💯

eIDAS, Digital Identity, Digital Signatures & PKI expert

Mutual recognition QTS as per eIDAS Art.14:

- Trade agreement
- QTS equivalence only
- Foreign “Q”TS (& “Q”TSP) must meet eIDAS requirements
- Reciprocity



Methodology

Main pillars for comparing PKI-based trust service schemes

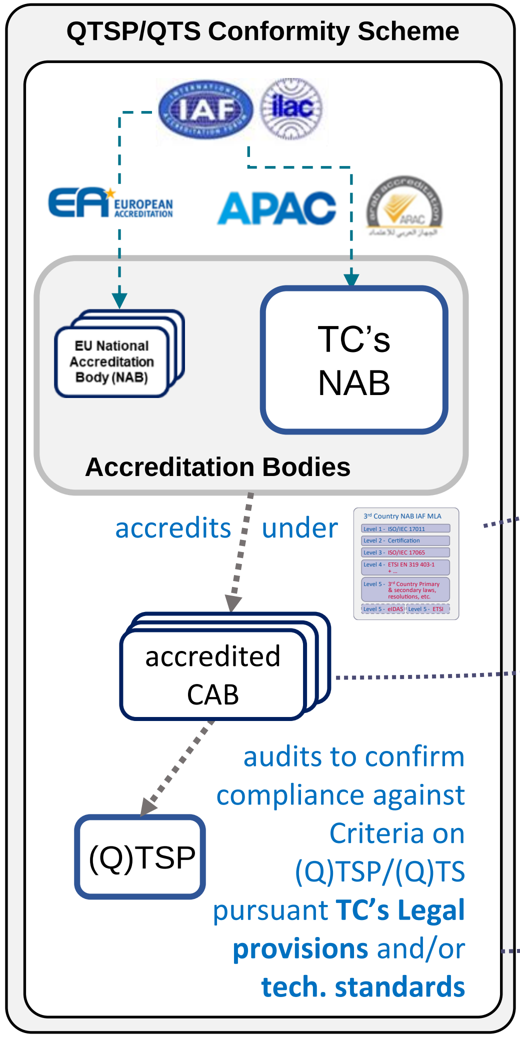
(e.g. in a view of establishing recognition)

Trust representation	Equivalence?	Trust representation
Supervision & auditing	Equivalence?	Supervision & auditing
Legal context	Equivalence?	Legal context
Technical requirements	Equivalence?	Technical requirements

source: ETSI Study on Globalisation of Trust and ETSI TR 103 684

Sylvie LACROIX

Challenges



QTSP/QTS Conformity Scheme
IAF
ilac
EA EUROPEAN ACCREDITATION
APAC
ARAC
EU National Accreditation Body (NAB)
TC's NAB
Accreditation Bodies
accredits
under
accredited CAB
audits to confirm compliance against Criteria on (Q)TSP/(Q)TS pursuant TC's Legal provisions and/or tech. standards
(Q)TSP

3rd Country NAB IAF MLA

- Level 1 - ISO/IEC 17011
- Level 2 - Certification
- Level 3 - ISO/IEC 17065
- Level 4 - ETSI EN 319 403-1 + …
- Level 5 - 3rd Country Primary & secondary laws, resolutions, etc.
- Level 5 - eIDAS | Level 5 - ETSI

Options:

→ TC CABs accredited by TC's NAB (IAF MLA ?)

→ TC CABs accredited by other NAB (IAF MLA signatory)

→ **Foreign CABs accredited under conformant scheme**

(Q)TSP

E.g. certification against:

- TC's Laws, byLaws, & SB's decisions,

- ETSI standards, and/or

- eIDAS

Audits schedule

- Initial audit
- Regular 2-yearly audit from initial audit
- Surveillance audits
- Ad hoc audit at discretion of Supervisory Body
- Termination audit

(Q)TSP/(Q)TS conformity scheme in TC

IAF MLA signatories

Membership of the IAF MLA is facilitated by membership in the AFRAC, ARAC, EA, IAAC, or APAC MLAs for recognised programs. IAF (N)AB Members who are signatories of these regional MLAs can be accepted into the IAF MLA for recognised programs on application to the IAF MLA.

Peer review

(N)ABs are admitted to the IAF MLA only after a most stringent evaluation of their operations by a peer evaluation team that is charged to ensure that the applicant complies fully with both the international standards and IAF requirements. IAF, and its (N)AB members, invest significant cost and resources to ensure and maintain the integrity of the MLA through robust peer evaluation. The MLA and its signatories are under constant review. The peer evaluation process is ongoing and extensive, covering all economies on a regular programme.

- EN 319 403-1 on requirements for bodies auditing TSPs
  - Primary reference: ISO/IEC 17065 specifying general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services
  - Supplements ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of TSPs
  - Incorporates additional requirements on CABs relating to the audit of a TSP's management system, as defined in ISO/IEC 17021 and in ISO/IEC 27006
- TS 119 403-2/-3 on additional requirements for CABs auditing
  - Part 2 : TSPs issuing PTC (e.g. as in CA/Browser)
  - Part 3 : QTSPs against eIDAS Regulation
    - Conformity assessment scheme
    - Conformity assessment report

Sylvie LACROIX

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SUPPORT THE TRUST SERVICES ECOSYSTEM

CSA: Support the development and implementation of Union policy in the field of electronic identity and trust services

Evgenia Nikoulouzou
ENISA, Policy Implementation and Develoment unit

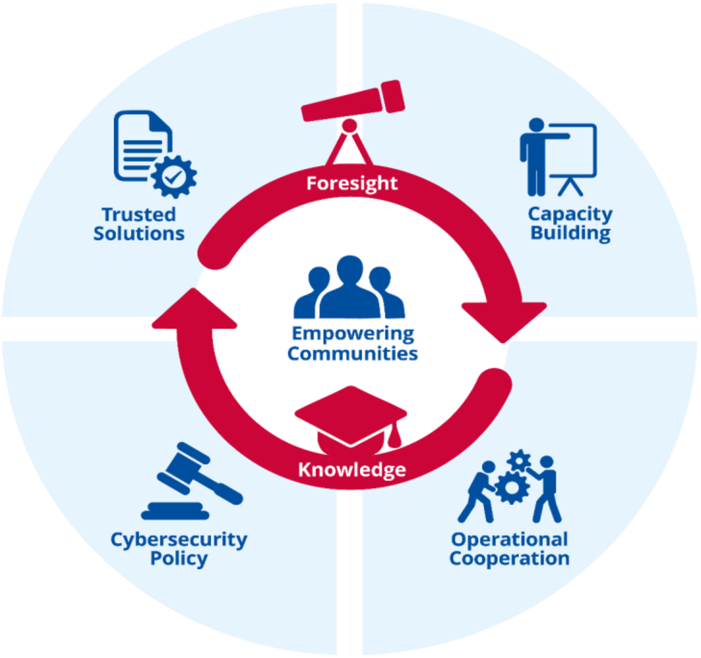
12 | 06 | 2023

Evgenia NIKOLOUZOU

ENISA – THE EU CYBERSECURITY AGENCY

Established in 2004, ENISA currently operates under Regulation 2019/881, often referred to as the ‘Cybersecurity Act’

- Development and implementation of EU policy and law, including by supporting the EU Member States
- Assistance with capacity-building, for example in developing national CSIRTs
- Supporting operational cooperation at EU level, for example by providing advice and issuing guidelines
- Development of EU cybersecurity certification framework and fostering its adoption
- Increasing the level of cybersecurity knowledge and information, for example through topic-specific assessments
- Raising cybersecurity awareness
- Contributing to research and innovation
- Fostering international cooperation



A TRUSTED AND
CYBER SECURE EUROPE

eIDAS: POLICY CONTEXT FOR ENISA

ENISA mandate - CSA Article 5

Support the development and implementation of Union policy in the field of electronic identity and trust services, in particular by providing advice and issuing technical guidelines, as well as by facilitating the exchange of best practices between competent authorities

eIDAS Regulation 910/2014, Trust Services, Article 19

- Support MS with supervision and security measures
- Support MS with incident reporting, and cross-border notifications
- Annual reports Trust services incidents
- CIRAS Incident reporting and Analysis system
- ENISA mandated by the eID Cooperation Network to support Incident reporting

NIS2 proposal - brings trust services under NISD

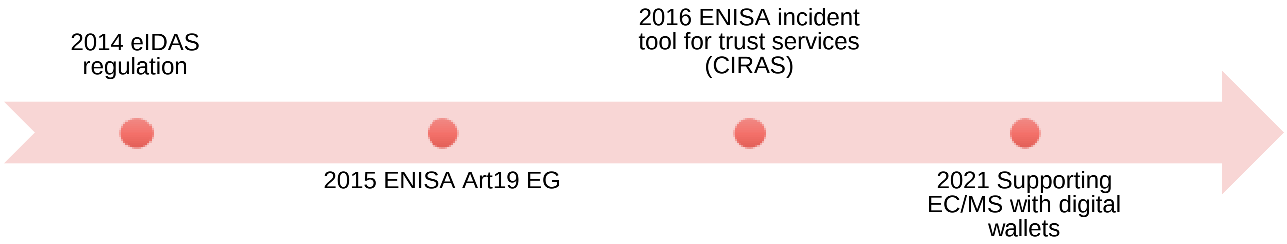
ENISA supports the NIS Cooperation group

eIDAS2 package

- **Proposal for eIDAS2 - COM (2021) 281 final**
- **Commission Recommendation on Toolbox for Digital Identity wallets**

ENISA supports the EC toolbox work – technical security measures

OVERVIEW OF ENISAACTIVITIES


2014 eIDAS regulation
2015 ENISA Art19 EG
2016 ENISA incident tool for trust services (CIRAS)
2021 Supporting EC/MS with digital wallets

Provide Guidance

- 17 reports to support TSPs and SBs
- 5 reports to support Relying Parties

Foster collaboration and information exchange

- ENISA Trust Services Forum (annual conference since 2015)
- Workshops in remote ID proofing

Incident Reporting

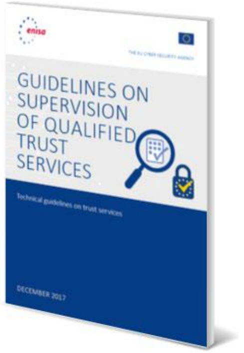
- Cyber incident reporting tool, CIRAS
- Annual incident report

ciras

ENISA ECATS EG

- Facilitate information exchange between the SBs
- Secretariat of ENISA ECATS EG
- Hosting of 21 meetings of ENISA ECATS EG since 2015

ECATS
European Competent Authorities for Trust Services
powered by ENISA


GUIDELINES ON SUPERVISION OF QUALIFIED TRUST SERVICES

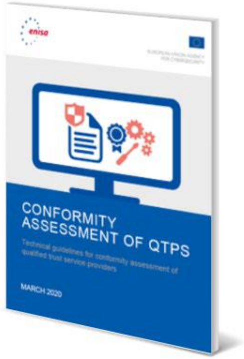
Technical guidelines on trust services

DECEMBER 2017

RECOMMENDATIONS FOR QTSPS BASED ON STANDARDS

Technical guidelines on trust services

MARCH 2021


CONFORMITY ASSESSMENT OF QTPS

Technical guidelines for conformity assessment of qualified trust service providers

MARCH 2020

WORKSHOP

Remote Video Identification: Attacks and Foresight

10 MAY 2023, Amsterdam

REMOTE VIDEO IDENTIFICATION
ATTACKS AND FORESIGHT
10 May 2023
9.30–16.30 CET
Amsterdam

[Material and presentations](https://www.enisa.europa.eu/events/remote-video-identification-attacks-and-foresight)
https://www.enisa.europa.eu/events/remote-video-identification-attacks-and-foresight

SAVE THE DATE

9th Trust Services and eID Forum
15th CA-DAY

11 – 12 OCTOBER 2023, Vienna

9th
Trust Services and eID Forum
Powered by ENISA

Find more under: Trust Services — ENISA (europa.eu), Building Trust in the Digital Era: ENISA boosts the uptake of the eIDAS regulation — ENISA (europa.eu)

THANK YOU!

QUESTIONS?

☎ +30 698 505 1405

✉ eID@enisa.europa.eu

🌐 www.enisa.europe.eu