DIGITAL eSignature

ASIA PKI International Symposium

November 28th, 2023

Apostolos (Tolis) APLADAS

European Commission

01

eSignature Programme

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 **Third Countries Trust List Programme (TCTL)** to achieve mutual recognition between the eIDAS qualified trust services and third country's trust services.

Current status

An overview of the current status of eSignature

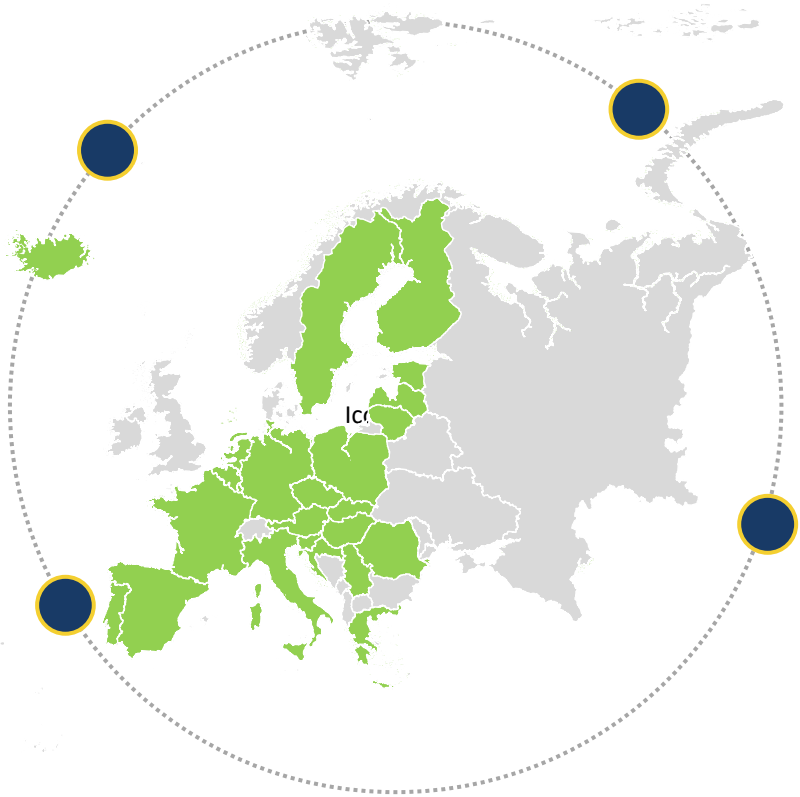
TLSO Community

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

02

European Commission’s Third Countries Trust List Programme – TCTL

TCTL Programme at a glance

TCTL programme by the European Commission offers:

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

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.

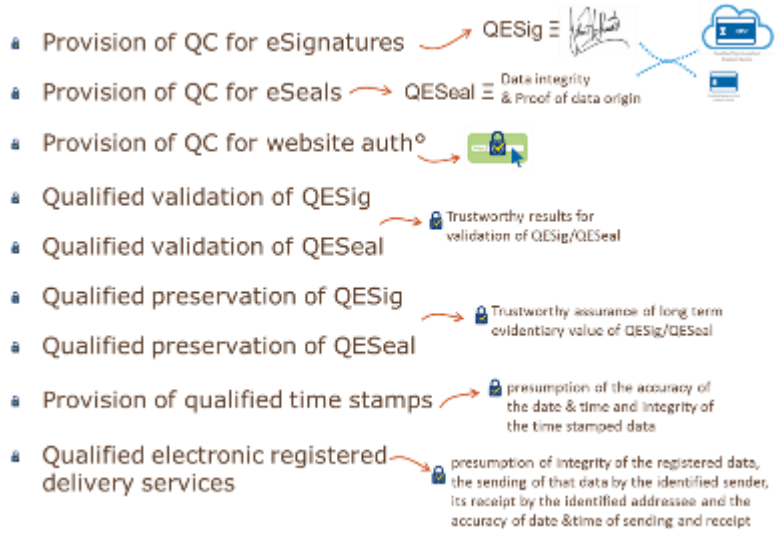
Technical facilities: A test LOTL, a test PKI, sample electronic signatures, DSS library

A **document repository** with all the necessary documentation and guidance for the 3rd countries. This material is available here

EU-3rd Country Mutual Recognition of eIDAS QTSP/QTS

Article 14 of eIDAS Regulation

- Recognition of 3rd country TSP/TS as legally equivalent to EU QTSP/QTS
  - Closed list of 9 types of EU QTSP/QTS

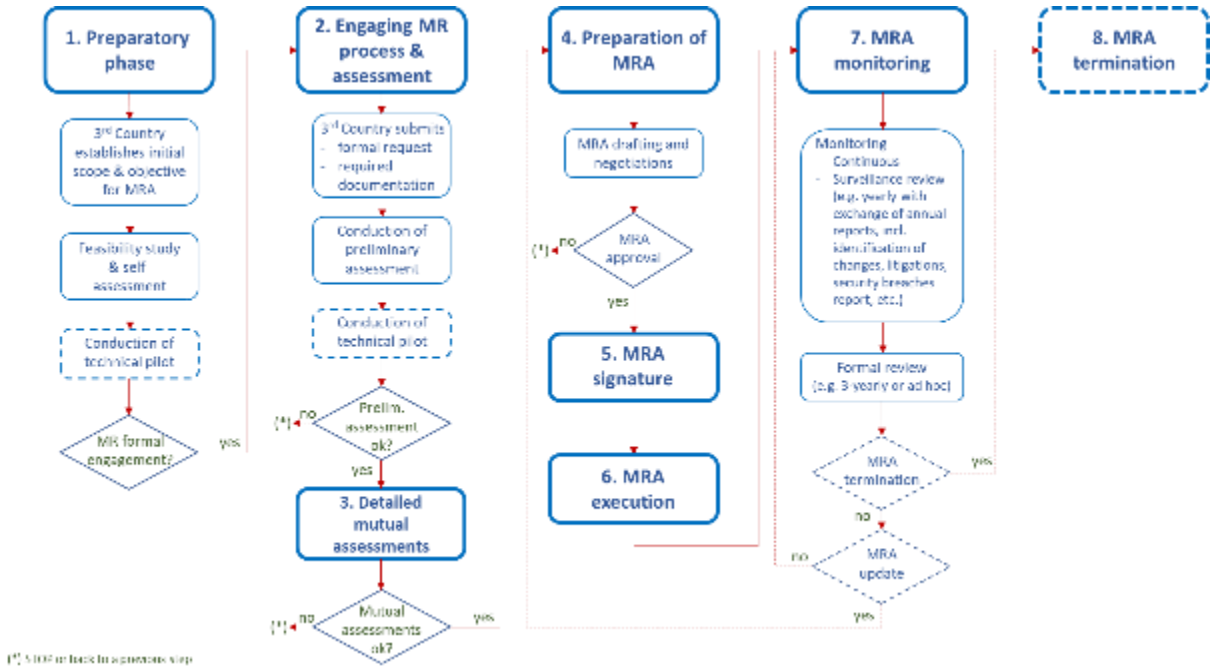


- Under an agreement concluded between the Union and the 3rd country or an international organisation in accordance with Article 218 TFEU
- 3rd country TSP/TS must meet the eIDAS requirements applicable to EU QTSP/QTS
- Reciprocity of the legal equivalence of EU QTSP/QTS in 3rd country or international org.

EU-3rd Country Mutual Recognition of eIDAS QTSP/QTS

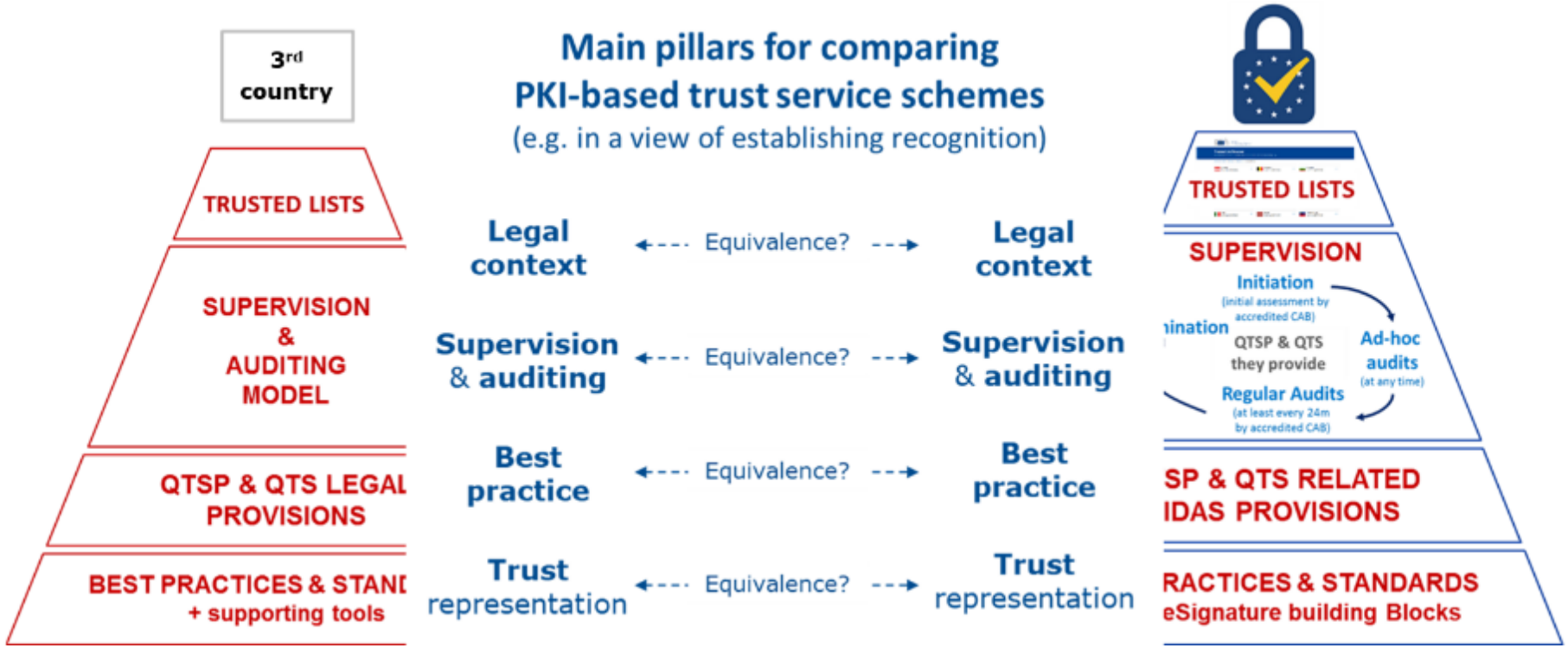
Conclusion of a mutual recognition agreement (MRA) under Art.14 of eIDAS can be a long journey

- A typical eIDAS Art.14 MRA life-cycle process flow



- EC provides guidance and technical pilot tools to assist 3rd countries in the preparatory phase (1)

Guidance for 3rd Countries in preparatory phase



03

Collaboration with UA and the first publication of TC AdES LOTL

Collaboration with Ukraine (UA)

Context

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

- Recognize UA-QES as eIDAS AdES
- Allow authentication of UA citizens in EU MS services

Technical implementation by EC and UA:

- 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*

Recognition of UA-QES as eIDAS AdES

Legal context – eIDAS Regulation **Chapter III on Trust Services**

Article 27(1) on "Electronic signatures in public services" states:

> *"If a Member State requires an **advanced electronic signature** to use an online service offered by […] a public sector body, that Member State shall*
>
> ***recognize advanced electronic signatures**, […]*
>
> *in at least **the formats or using methods defined in the implementing acts** […]."*

✗ **Must not** be confused with Article 14(1) on "International aspects":

> *"Trust services provided by trust service providers established in a third country shall be recognised **as legally equivalent to qualified trust services** […] where the trust services originating from the third country are recognised under **an agreement concluded** between the Union and the third country […] in accordance **with Article 218 TFEU**."*

Background

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:** Equivalence between Ukrainian Qualified Electronic Signatures (**UA QES**) and eIDAS Advanced Electronic Signatures (**eIDAS AdES**)

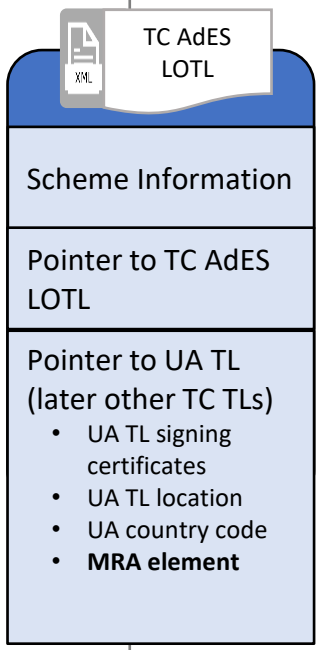
- **Solution:**

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

TC AdES LOTL

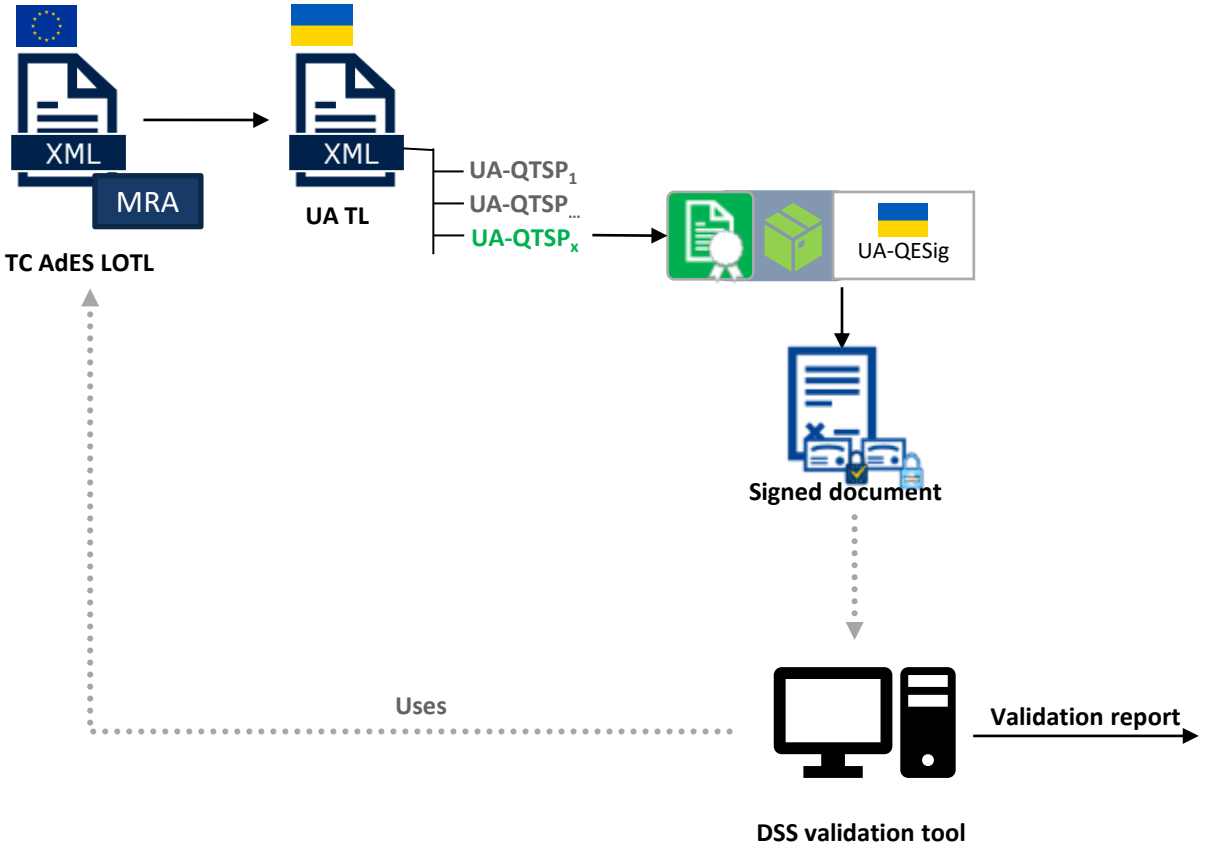
Content

Similar to the EU/EEA LOTL but with an **MRA element** when pointing to a third country TL




```
−<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>
  −<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: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">
```

Recognition of UA-QES as eIDAS AdES



Signature SIGNATURE_Kozlov-Oleksandr_20221223-0914

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:	CAdES-C
Indication:	TOTAL PASSED
Certificate Chain:	Kozlov Oleksandr "DIIA", Qualified Trust Services Provider — State enterprise "DIIA" Central certification authority
On claimed time:	2022-12-23 09:14:56 (UTC)
Best signature time:	2022-12-23 09:14:56 (UTC)
Signature position:	1 out of 1
Signature scope:	Full document (FULL) Full document

Timestamps 2

Document Information

Signatures status:	1 valid signatures, out of 1
Document name:	Signature-C-UA.p7s

EC-UA collaboration deliverables

Publication of the TC AdES LOTL with a pointer to Ukrainian 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

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

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

Under the TCTL Programme, the European Commission has conducted a **technical assessment** of the legal and technical aspects of the Ukrainian electronic signatures. It has verified, checked, and vouched for all elements of conformity, ensuring that Ukraine meets all requirements for being part of the trusted list.

The **Digital Signature Software (DSS)** which supports since version **5.11.1** the interpretation of the content of the TC AdES LOTL

04

The EU Digital Identity Wallet

Characteristics of the EU Digital Identity Wallet

Free use for all citizens

Provided by Member States, all EU citizens may use it for free on a voluntary basis

Accepted throughout the Union

Recognised by private and public service providers (relying parties) for all transactions that require authentication

Secure and privacy oriented

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

Functions of the EU Digital Identity Wallet

Identification

Disclose identity data required for accessing public and private services

Store & present attestations of attributes

E.g. present educational diplomas/reports for enrolling at university; present your driving license for renting a car

Sign & seal electronically

E.g. sign an employment contract to start a new job; authorise a payment

Documents go digital as “electronic attestations”








Identity Card

Medical Prescripto n

Bank Account Informatio n

University Diploma

Driving Licence

Professional certificates

Travel Credentials

Business Registration

How does the wallet work?

Implementation

Set up

Use

Member States

0 mandate

IT Providers

1 build

2 serve

2 download

Wallet User

issue 3

present 6

request 5

Attestation Issuer

Relying Parties

Trust System

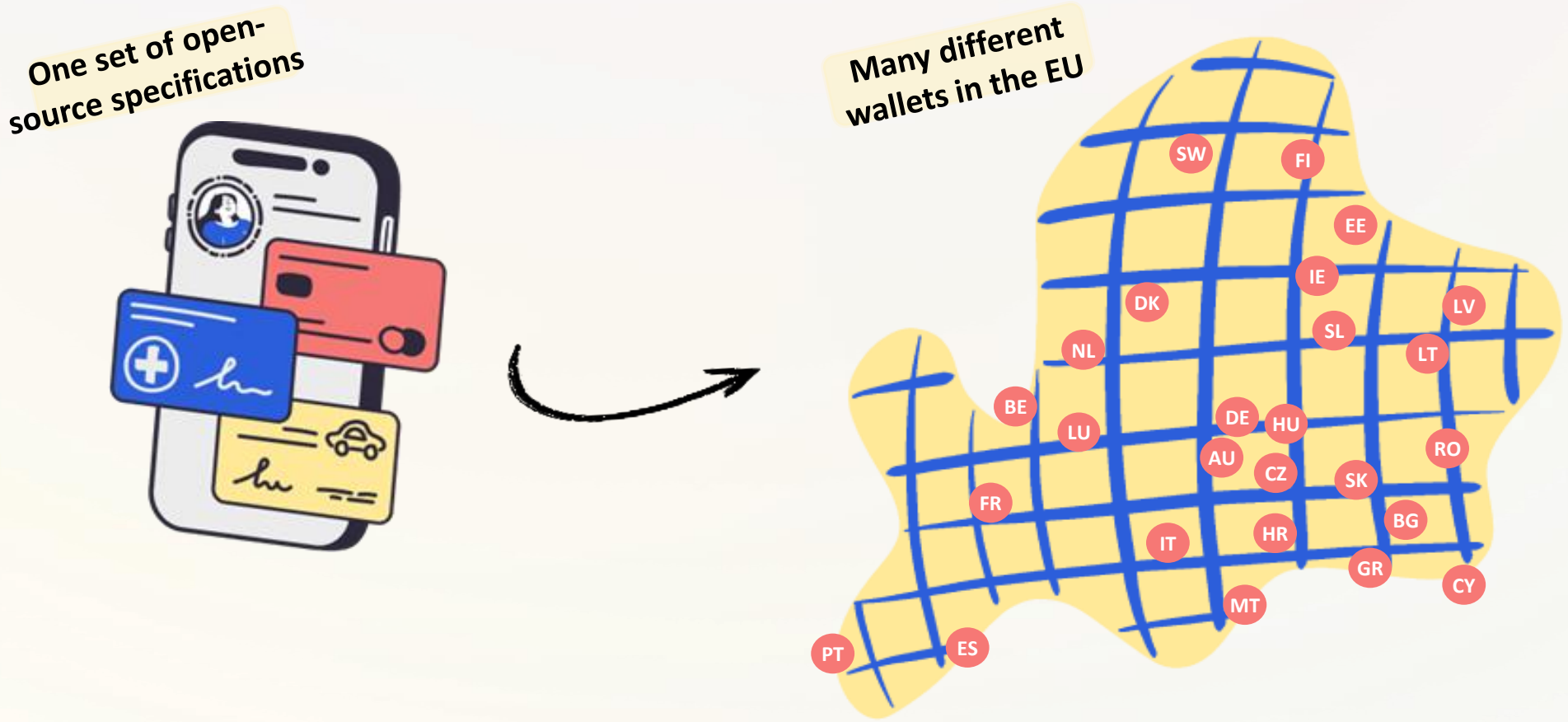
4 record

7 verify issuer authenticity and accreditation status

One set of standards, many different wallets

There will not be one EU Digital Identity Wallet, but many, built to one set of specifications, developed and agreed by Member States in close cooperation with the European Commission.

All Wallets will be interoperable and work seamlessly across borders and services.



The wallet ecosystem

European Institutions

European Commission
European Parliament
European Council

Relying Parties

Public & private organizations which Users will interact with for access to services

Governmental Bodies

National administrations
Data protection authorities
Conformity assessment bodies

Wallet Users
(General Public)

European citizens, residents & businesses

IT Providers

Wallet developers
Device manufacturers
Trust service providers

Large Scale Pilots

4 consortia (Potential, Nobid, DC4EU and EWC)

Issuers

Trusted organisations that issue PID and attestations

The benefits

How will citizens, governments, relying parties and society benefit from the wallet? Discover the many benefits of the EU Digital Identity Wallet

Citizens

- Easily access public and private services
- Easily sign digital documents
- Protect personal data
- Simplify paperwork and admin

Governments

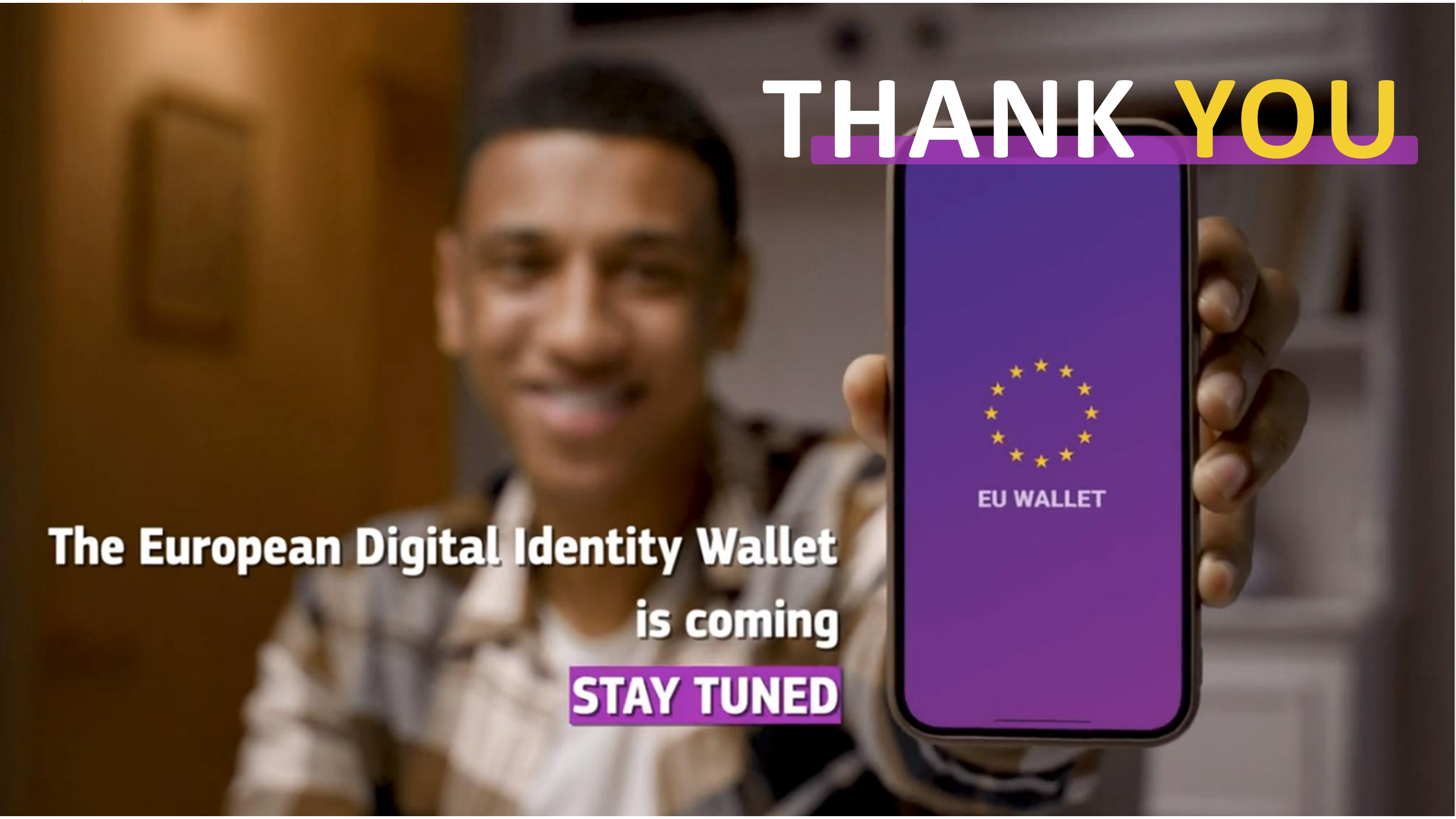
- Improve access to digital services
- Enhance fraud prevention
- Boost security

Relying Parties

- Improve security and privacy
- Cost and efficiency gains through a single set of specifications

Society

- More transactions conducted fully online
- Resources can be allocated elsewhere
- New business opportunities
- Economic Growth


THANK YOU
EU WALLET
The European Digital Identity Wallet
is coming
STAY TUNED