

Agenda of the day



01

02

03

04

05

06

07

08

09

10

11

12

ID	TIME	TOPIC	SPEAKERS
1.	09:00 - 09:15	Welcome words	Lorena BOIX ALONSO (European Commission)
2.	09:15 - 09:35	The eIDAS Regulation present and future <ul style="list-style-type: none">eIDAS regulationeIDAS 2.0	Gudrun STOCK (European Commission)
3.	09:35 - 09:55	<ul style="list-style-type: none">Current state of international partnershipsPolicy around the recognition of third countries trust services	Vicente ANDREU NAVARRO (European Commission)
4.	09:55 - 10:15	<ul style="list-style-type: none">European Commission's Third Countries Trusted Lists ProgrammePresentation of the pilot in the eIDAS Dashboard	Apostolos Tolis APLADAS (European Commission)
5.	10:15 - 10:30	Trust services in the Republic of Albania <ul style="list-style-type: none">Regulatory Framework on trusted servicesCompetences of the supervisory bodyRegistration/Accreditation of QTSPTrust list/ Electronic Identification SchemeInternational Aspects	Ermela CEKANI (Albania)
	10:30 - 10:50	<i>Coffee break</i>	
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)
	12:05 - 13:35	<i>Lunch break</i>	
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	<i>Coffee break</i>	
11.	16:20-17:05	Q&A	eIDAS Dashboard team
12.	17:05-17:15	Closing remarks	Natalia ARISTIMUÑO PÉREZ (European Commission)

AM

PM



8

Data Free Flow with Trust – Proof of Concept between Japan and the European Union

Prof. TEZUKA

(Japan)



Satoru Tezuka

Satoru Tezuka

9

Trust services infrastructure in Ukraine



Oleksandr KOZLOV

Senior Expert on eID – EU4Digital UA, e-Governance Academy



Trust services infrastructure in Ukraine

Overall Trust services profile

The file of the Trust List, which contains information about qualified providers of electronic trust services and their electronic trust services, was created in accordance with the provisions of the "Procedure for conducting an experimental project on mutual recognition of electronic trust services between Ukraine and the European Union", approved by the Resolution of the CMU dated 22.10.2022 No. 1311:

[Expand all](#) [Collapse all](#)

› TL information UA (sn7) 2023-05-25 14:21:00 2023-08-25 14:21:00

› Trust Service Providers

<https://czo.gov.ua/download/tl/TL-UA-EC.xml>



the value of the hash function of the TL-UA-EC.xml Trust List file:

<https://czo.gov.ua/download/tl/TL-UA-EC.sha2>



The central certifying body
is the Ministry of Digital Transformation of Ukraine
2023. All rights reserved.



2023. All rights reserved.
is the Ministry of Digital Transformation of Ukraine
The central certifying body

Important resources:
Integrated system of electronic identification
Portal Action
Platform Action.Centers
Guide to public services
Guide to public services
Platform Action.Centers
Portal Action
Integrated system of electronic identification
Important resources:

Since 2018

Trusted list is used for trust representation in Ukraine

ETSI Standards are applicable to UA TSP through national legislation

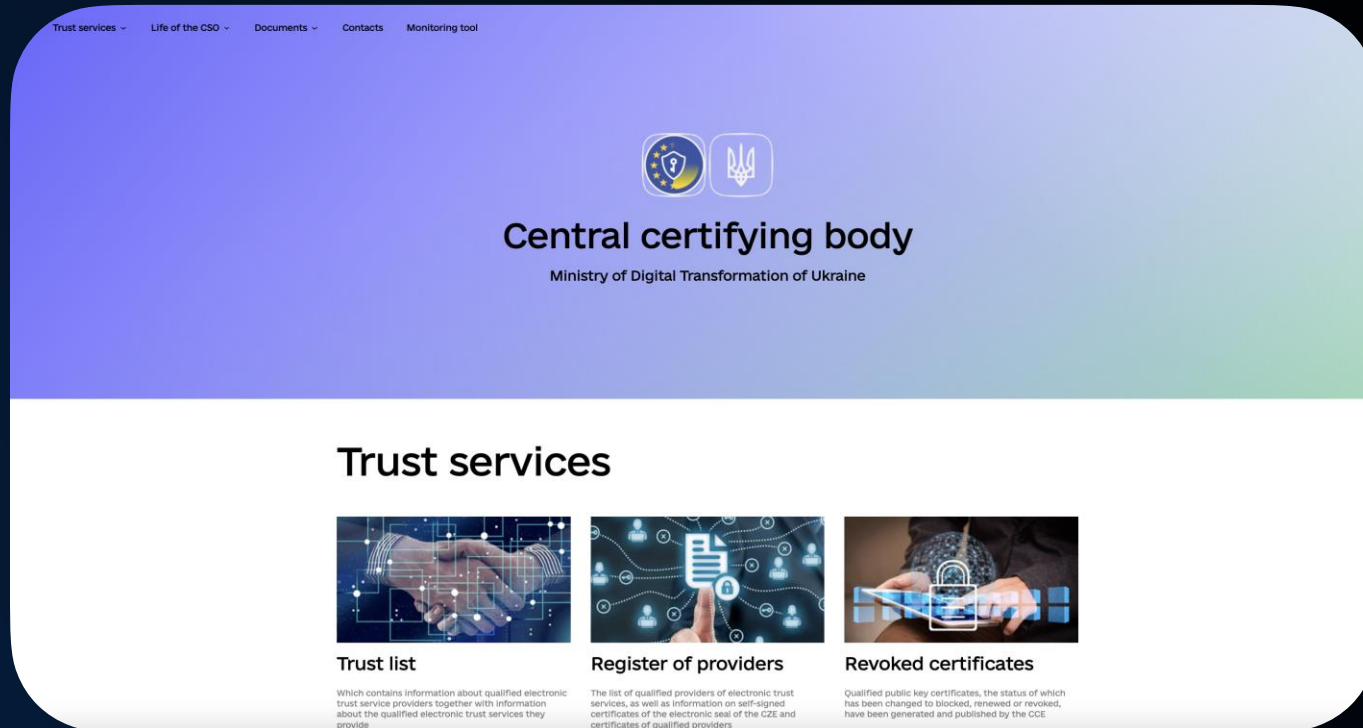
Since 2022

New trusted list for international compatibility was established and maintained

26+

TSPs under supervision of the State Service of Special Communication and Connection

Overall Trust services profile



14M+

qualified certificates for
eSignature generated in 2022

418k+

qualified certificates
for eSeals generated in 2022

702M+

OCSP requests
for root certificates of QTSPs

9M+

Unique users of qualified certificates
for eSignature by the end of 2022

10.3B+

qualified time stamps in 2022

Diia app

14

Digital documents

25

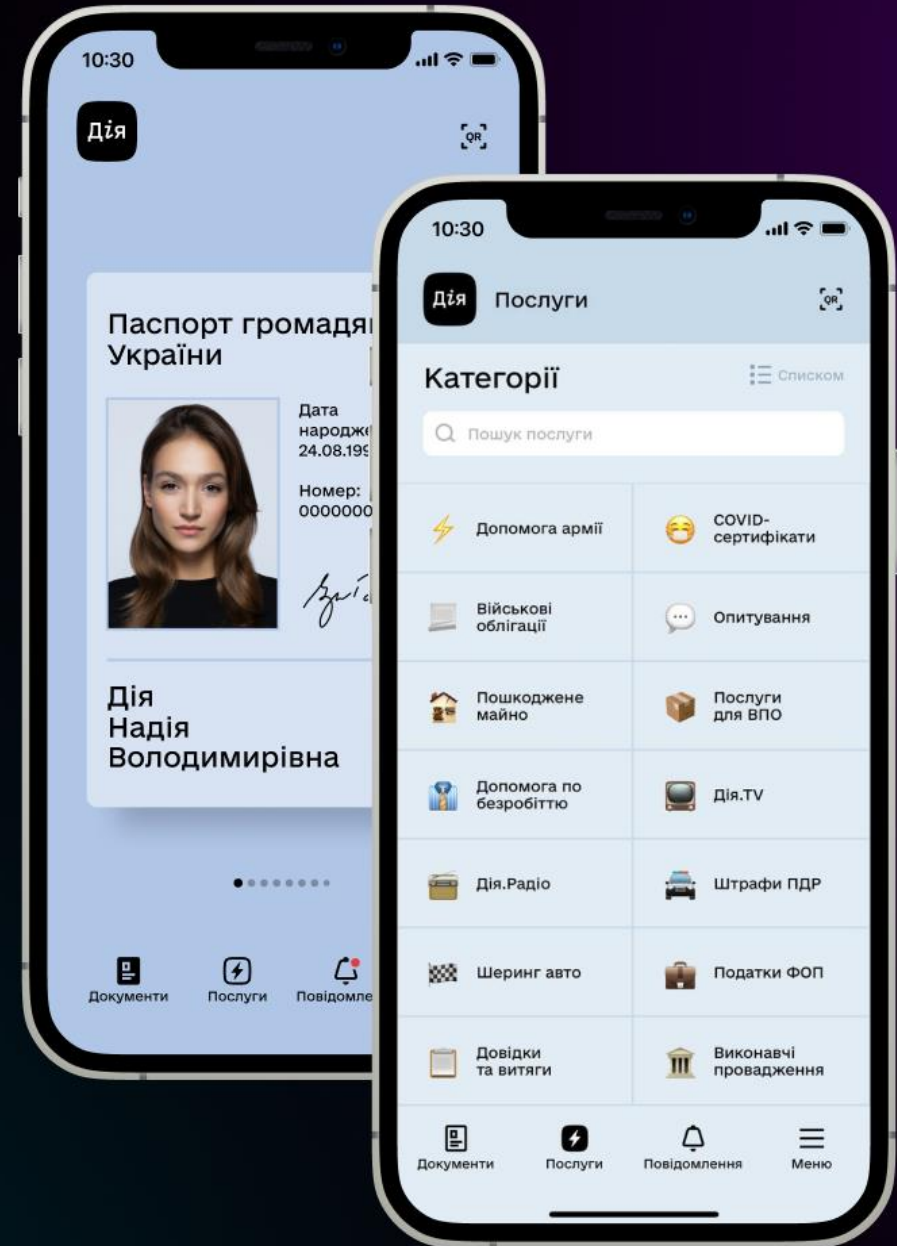
Mobile Services

18,7M+

Active Diia users

6M+

Active Diia.Signature users
(remote QES)



DAILY NUMBER OF USERS

1 - 2,5M

OPERATING SYSTEMS

8.1M+

iOS

31.3M+

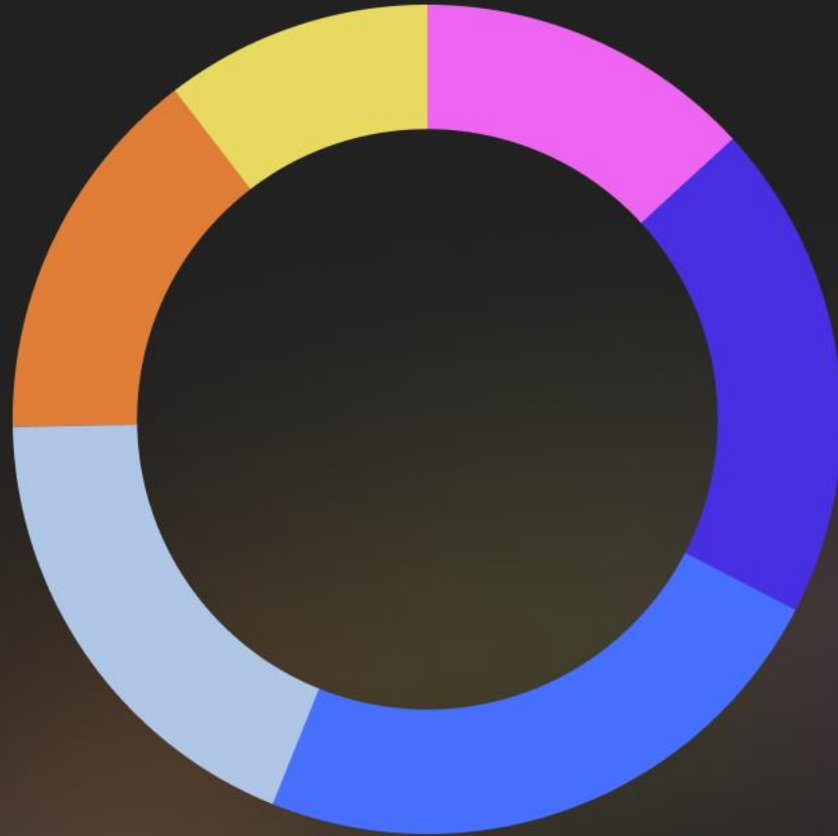
Android

448K+

Huawei

Proof that state superapp is for everyone

USERS' AGE



● up to 24 – 13,23%

● from 25 to 34 – 19,54%

● from 35 to 44 – 23,50%

● from 45 to 54 – 18,62%

● from 55 to 64 – 14,87%

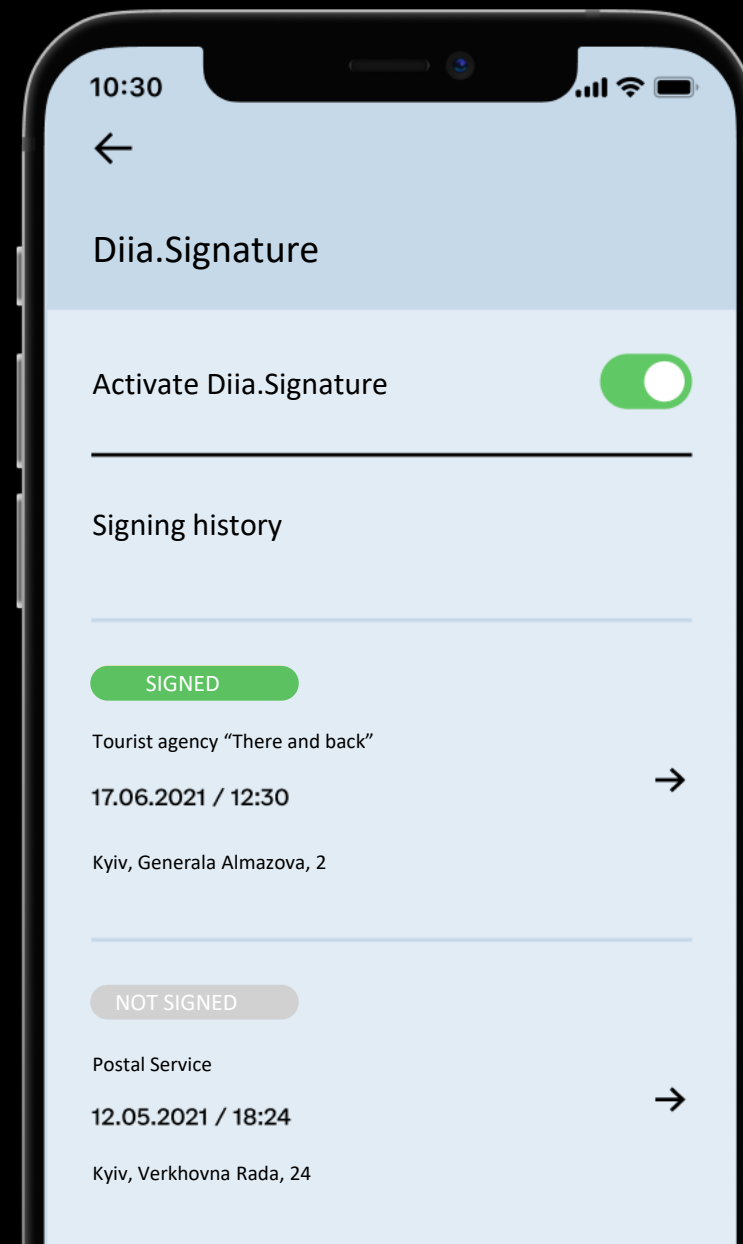
● 65 years+ – 10,24%

Diia.Signature

Qualified electronic signature in your smartphone

Sign a document

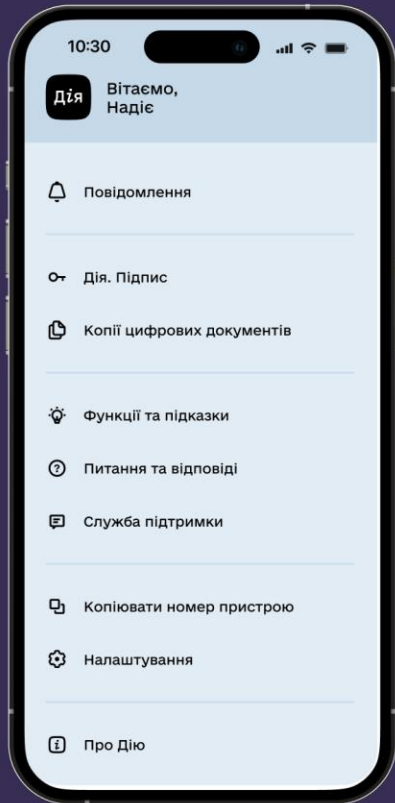
Authenticate



1 minute to generate Diia.Signature

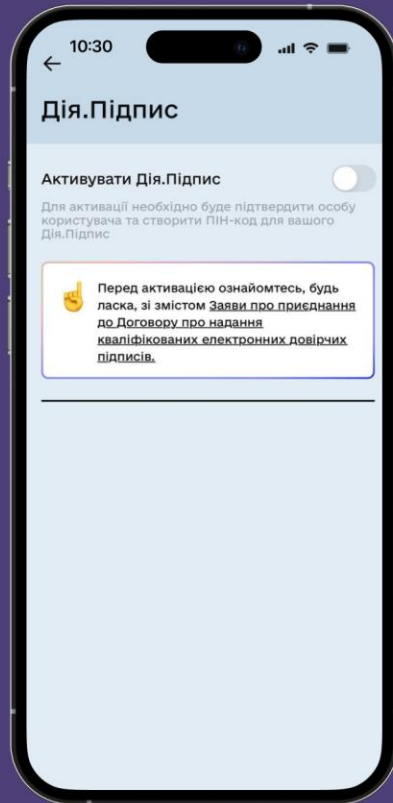
1

Open the menu



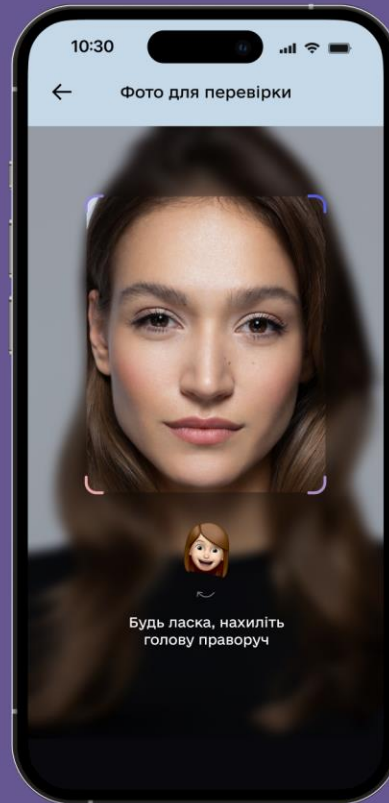
2

Press activate



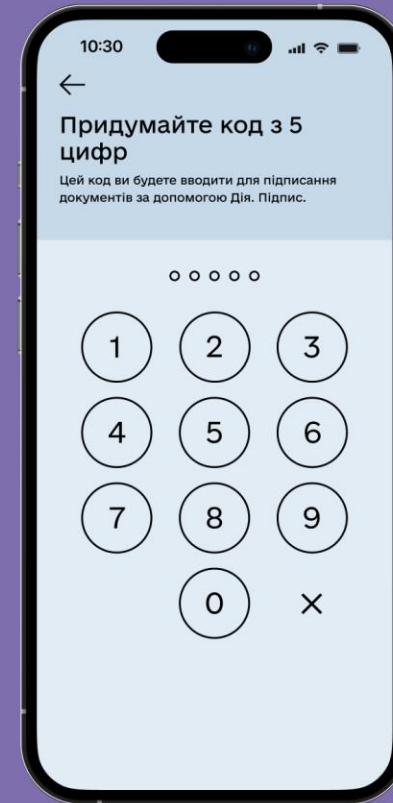
3

Pass facial recognition



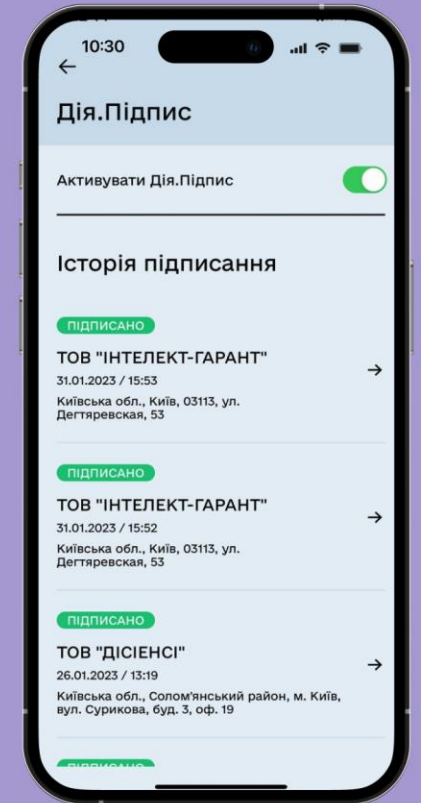
4

Set 5-digit pin code



5

Diia.Signature is generated



MRA with the EU

Road towards mutual recognition of trust services with the EU

- 2017 | Law of Ukraine on Trust Services
Incorporated basic eIDAS principles in UA
- 2019 | Bilateral Pilot with Estonia and Lithuania
Cross-border signature validation tested
- 2020 | Joint Working Plan with the EU
Cross-border eSignature validation tested
- 2021 | Self-assessment eIDAS MRA CookBook
Extensive legal and technological assessment based on eIDAS
Art.14 CheckList
- 2022 | Fine-tuning regulations and infrastructure
Law amendments, signature portal update and new Trust List
for international cooperation
- 2023 | eSignature pilot with EU completed
UA included in the TC AdES LOTL as a first ever third country
interoperable with the EU

Legal context: UA regulations

Ukraine has adopted the law on electronic trust services in 2017 which implemented basic rules and principles of eIDAS into Ukrainian legislation.

The extensive amount of secondary legal acts have been adopted during 2018-2019.

In 2020 self assessment was conducted based on eIDAS Article 14 Checklist

The Draft Law by MinDigit was developed to fully implement eIDAS and adopted in the end of 2022.

Table 1: eIDAS requirements applicable to QTSP/QTS

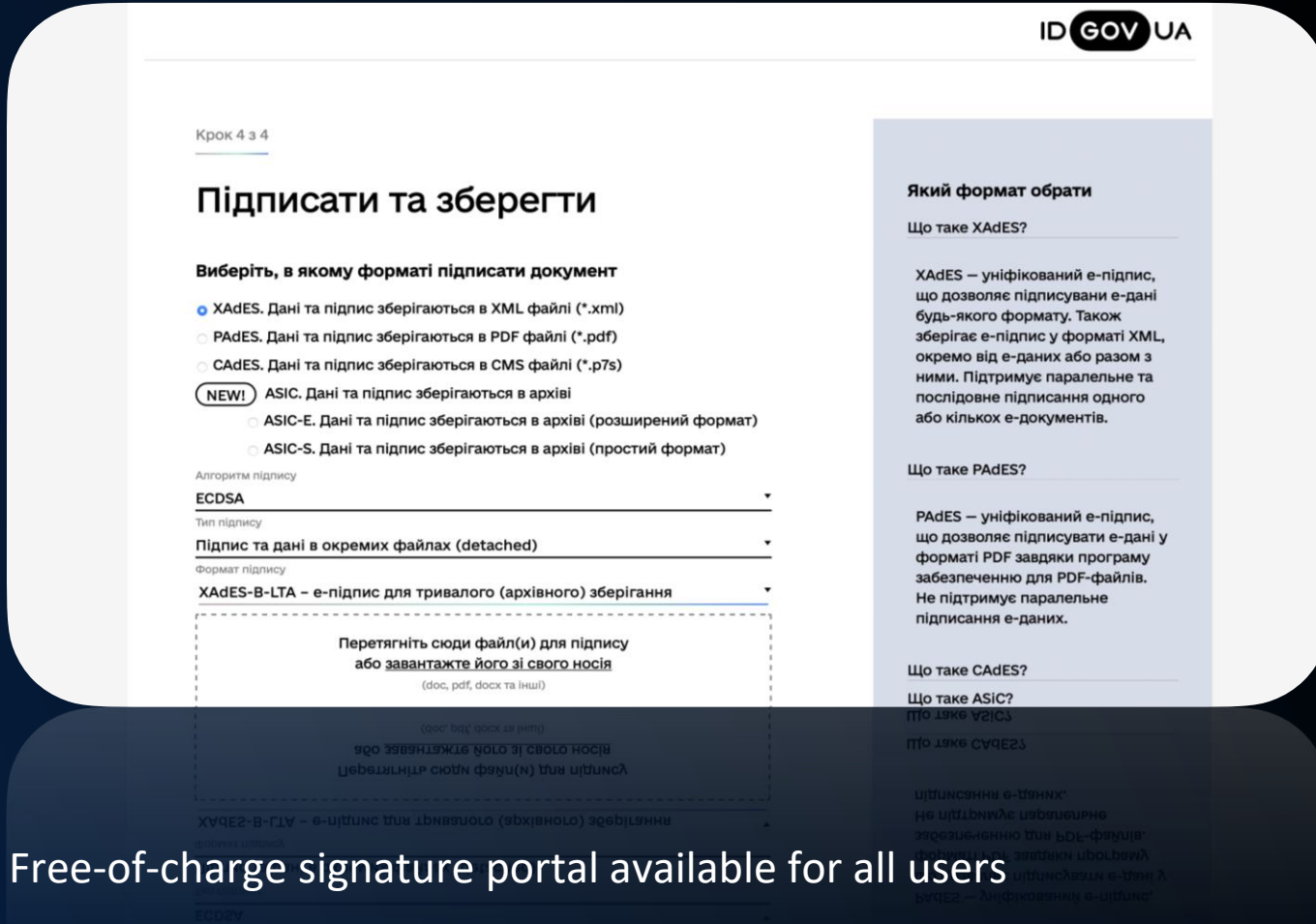
Common eIDAS requirements applicable to all types of QTS	Specific eIDAS requirements applicable to a specific type of QTS
<ul style="list-style-type: none"> - Art.5 - Data processing and protection - Art.13 - Liability and burden of proof - Art.15 - Accessibility for persons with disabilities - Art.19.1 – Security risk assessment and due diligence - Art.19.2 - Security and personal data breach notification - Art.20 – Supervision of QTSPs <ul style="list-style-type: none"> o Audited at least every 24 months by an eIDAS accredited CAB to confirm eIDAS compliance o TSP allows Supervisory Body (SB) and CAB to audit its eIDAS compliance o Remedy any failure to meet eIDAS requirements as instructed by SB - Art.21 - Initiation of a QTS (pre-authorisation) <ul style="list-style-type: none"> o Notification of intention to provide a QTS and initial conformity assessment report o QTSP may begin to provide the QTS after the qualified status has been indicated in the trusted list - Art.23 - Correct use of EU trust mark - Art.24.2 - Requirements for QTSPs <ul style="list-style-type: none"> (a) Inform SB of any change in QTS provisioning and of intention to cease; (b) Requirements on staff; (c) Financial resources and/or liability insurance; (d) Consumer information; (e) Use of trustworthy systems and products; (f) Use of trustworthy systems to store data (including personal data); (g) Appropriate measures against forgery and theft of data; (h) Recording and accessibility of activities related data; (i) Up-to-date termination plan; (j) Lawful processing of personal data. 	<p>Provision of qualified certificates for electronic signatures: Art. 24.1(a) to (d) Art.24.2(k) Art.24.3 Art.24.4 Art.28.1 & Annex I, Art.28.(2), Art.28.(3), Art.28.(4), Art.28.(5)</p> <p>Provision of qualified certificates for electronic seals: Art. 24.1(a) to (d) Art.24.2(k) Art.24.3 Art.24.4 Art.38.1 & Annex III, Art.38.(2), Art.38.(3), Art.38.(4), Art.38.(5)</p> <p>Provision of qualified certificates for website authentication: Art. 24.1(a) to (d) Art.24.2(k) Art.24.3 Art.24.4 Art.45.1 & Annex IV</p> <p>Qualified validation service for qualified electronic signatures: Art.33.1</p> <p>Qualified validation service for qualified electronic seals: Art.40</p> <p>Qualified preservation service for qualified electronic signatures: Art.34.1</p> <p>Qualified preservation service for qualified electronic seals: Art.40</p> <p>Provision of qualified time stamps: Art.42.1</p> <p>Qualified electronic delivery services: Art.44.1</p>

The two sheets “P1. Legal - eIDAS benchmarking” and “P1. Legal-UN-EU laws benchmark.” of the [MRA checklist] companion document respectively allows applicant 3rd countries to perform a self-assessment of:

assessment of:

[MRA checklist] companion document respectively allows applicant 3rd countries to perform a self-

Signature formats



Free-of-charge signature portal available for all users

XADES

XADES B-B; B-T; B-LT; B-LTA

CADES

CADES -BES; -T; -C; -X Long

PADES

PADES B-B; B-T; B-LT; B-LTA

ASiC-e

Qualified certificates

Requirements in Ukraine (1/2)

Qualified certificate statement

ETSI defined qualification for third countries with id-etsi-qcs-QcCClegislation statement



QTSP information

Legal persons: Name and entity code

Natural persons: Full name, ID code, tax ID (there are no TSP as natural persons yet)



Signatory data

Full name (Name, Surname)

ID code (TaxID and/or Demographic register code)

+email

+place of residence

For creator of eSeals

Registered name

Entity code from the Company register

+email

+location of legal person



Validation data

The value of the public key, which corresponds to the personal key

Qualified certificates

Requirements in Ukraine (2/2)



Certificate identity code

serial number of the qualified certificate for a public key, being unique for the entity that issued the certificate



QTSP information

Legal persons: Name and entity code

Natural persons: Full name, ID code, tax ID (there are no TSP as natural persons yet)



eSignature/eSeal of issuing QTSP

Qualified electronic seal of the issuing QTSP with information on certificate validity status validation



Certificate validity

The starting and expiration date of the validity period of the qualified certificate



QSCD or UA certified “SSCD”

id-etsi-qcs-QcSSCD or specifically defined OID to display that the certificate is under signer’s sole control

2023 - UA recognises EU QESs


ID GOV UA

**👍 Файл успішно перевірено.
Усі дані цілі**

Ви можете зберегти підписаний файл.

⌵ Завантажити все архівом

- 📎 **Файл з підписом** ⌵
test-signature-over-picture.asice
303.9 КБ
- 📎 **Файл без підпису** ⌵
test-signature-over-picture.asice
303.9 КБ
- 📎 **Протокол створення та перевірки
кваліфікованого електронного підпису від
18.05.2023** ⌵
test-signature-over-picture_Validation_Report.pdf
303.9 КБ

Дія  Міністерство цифрової трансформації України

Як це працює

Електронний підпис є аналогом власноручного підпису та забезпечує достовірність і цілісність інформації, викладеної у документі, а також дає змогу підтвердити цілісність електронного документа та ідентифікувати особу, яка підписала документ.

Що таке файловий носій?

Що таке токен?


Як працює хмарний підпис?

Як працює підпис з ID-карткою?

Як працює Bank ID?

Як працює Дія.Підпис?

ID GOV UA

Дія  Міністерство цифрової трансформації України

Як це працює

Електронний підпис є аналогом власноручного підпису та забезпечує достовірність і цілісність інформації, викладеної у документі, а також дає змогу підтвердити цілісність електронного документа та ідентифікувати особу, яка підписала документ.

Що таке файловий носій?

Що таке токен?

Як працює хмарний підпис?

Як працює підпис з ID-карткою?

Як працює Bank ID?

Як працює Дія.Підпис?

Підписувачі

Підписувач
ERLICH,MARK
П.І.Б.
ERLICH MARK
Країна
Естонія
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача)
21:46:56 11.11.2022
Сертифікат виданий
EID-SK 2016
Серійний номер
1C91C0C95D60CCA463046F171A449E51
Тип носія особистого ключа
Захищений
Серійний номер носія особистого ключа
Не визначено
Алгоритм підпису
RSA
Тип підпису
Кваліфікований
Тип контейнера
Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису
З повними даними для перевірки (XAdES-B-LT)
Сертифікат
Кваліфікований

303.9 КБ

18.05.2023
кваліфікованого електронного підпису від
Протокол створення та перевірки

як працює Дія.Підпис?

як працює банк ID?

як працює підпис з ID-карткою?

кваліфікований

з повними даними для перевірки (XAdES-B-LT)

підпис та дані в архіві (розширений) (ASiC-E)

кваліфікований

RSA

як працює Дія.Підпис?

як працює банк ID?

як працює підпис з ID-карткою?

International recognition pilot with the EC

ID GOV UA

Підписати файл за допомогою
Електронного підпису →
Дія.Підпис - UA →
Дія.Підпис - EU (бета-тест) →

+ Як це працює?
+ Що нового?
+ Формати підписів?



European Commission

DSS Demonstration WebApp

European Commission > DIGITAL > eSignature > Digital Signature Services > Validate a signature

e-Signature

- Sign a document
- Sign a digest
- Sign a PDF
- Sign with JAdES
- Sign multiple documents
- Counter sign a signature
- Standalone application
- REST/SOAP WebServices

Server side

Validate a signature

Privacy notice: Please note that by using the below functionality of the DSS demonstration, your files are going to be transmitted to the infrastructure of the European Commission. With your action to do so, you consent to this transmission of data and **we strongly advise you to use documents that do not contain sensitive material.** Files that have been transmitted are not retained.

Signed file: Файл не вибрано

Original file(s): Файл не вибрано

Send original file(s) as:

- Complete documents
- SHA1
- SHA256
- SHA384
- SHA512

More options

Implementation on the EU Qualified validation service for qualified electronic signature



The screenshot displays the Dokobit web application interface. The header includes the Dokobit logo, navigation tabs for 'Documents', 'Validations', and 'Company data', and a user profile for Oleksandr Kozlov. The main section is titled 'Documents' and shows a list of signed documents. A sidebar on the left provides filters for document status, and a search bar is located at the top of the document list.

Date	Document Name	Format	Status
2023-05-30	AE TS Oleksandr Kozlov 04.2023 (3)	ASIC	Signed
2023-05-13	sample	PDF	Signed
2023-05-11	Performance record_Kozlov.pdf	ASIC	Signed
2023-03-17	test signature eresidency+ua	ASIC	Signed

Thank you for attention!



Oleksandr Kozlov

Senior expert on eID

eGovernance Academy, EU4DigitalUA

Kyiv office

oleksandr.kozlov@ega.ee

10

How the specifications of the TC AdES LOTL and the XML MRA elements work



Olivier BARETTE
Partner – Nowina Solutions



Olivier DELOS
Founder of Sealed



Path to mutual recognition

Background: Pilot for the International Compatibility of Trust Services

Collaboration with Ukraine, leading to the creation of the TC AdES LOTL

TC AdES LOTL-based Signature Applicability Rules

DSS validation process, and the TC AdES LOTL

International recognition in eIDAS

Recognition of qualified trust services

Article 14

- By means of an Art.218 TFEU (Trade) Agreement
- Recognition of 3rd Country trust service (TC-TS) by 3rd Country trust service provider (TC-TSP) as legally equivalent to EU qualified trust service (EU-QTS) by EU qualified TSP (EU-QTSP)
- Provided
- TC-TS and TC-TSP meet the eIDAS requirements for EU-QTS by EU-QTSP
 - Reciprocity

So far not implemented, i.e.

- no TC-TS/TC-TSP recognised as “qualified” in EU
- no TC-Qualified Esignature (QESig) is recognised as legally equivalent to EU-QESig
- ... but what about TC-QESig recognised as EU-AdESig ?

International recognition in eIDAS

Recognition of advanced electronic signatures

Articles 3(11), 26, 25(1), 27(1)

- No territoriality requirement for advanced electronic signatures (AdESig)

Art.3(11), 26

When TC-(Q)Esig meets the requirements of Art.26,

Art.25(1)

they cannot be denied legal effect and admissibility as evidence in legal proceedings solely because electronic or not EU-QESig, and

Art.27(1)

if they comply with standards listed in CID (EU) 2015/1506, Member State public sector online services requiring an AdESig shall recognise them irrespectively from where they originate

Path to mutual recognition

Recognition of qualified trust services

eIDAS 1.0

(Art.14)

- nonEU TSP/TS must meet eIDAS QTSP/QTS requirements
- Reciprocity
- Trade agreement












eIDAS 2.0

(Art.14)

- Trade agreement or **Implementing Act/Decision**
- nonEU TSP/TS must meet eIDAS QTSP/QTS requirements
- Reciprocity

+ Trusted list (MRA cookbook)

- Provision of QC for eSignatures → QESig  
- Provision of QC for eSeals → QESeal  Data integrity & Proof of data origin 
- Provision of QC for website auth° 
- Qualified validation of QESig →  Trustworthy results for validation of QESig/QESeal
- Qualified validation of QESeal
- Qualified preservation of QESig →  Trustworthy assurance of long term evidentiary value of QESig/QESeal
- Qualified preservation of QESeal
- Provision of qualified time stamps →  presumption of the accuracy of the date & time and integrity of the time stamped data
- Qualified electronic registered delivery services →  presumption of integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of date & time of sending and receipt



Above 9 QTs + potentially

- Provision of Qualified electronic attestations of attributes
- Qualified electronic archiving
- Qualified electronic ledgers
- Qualified service for the management of remote qualified electronic signature/seal creation devices

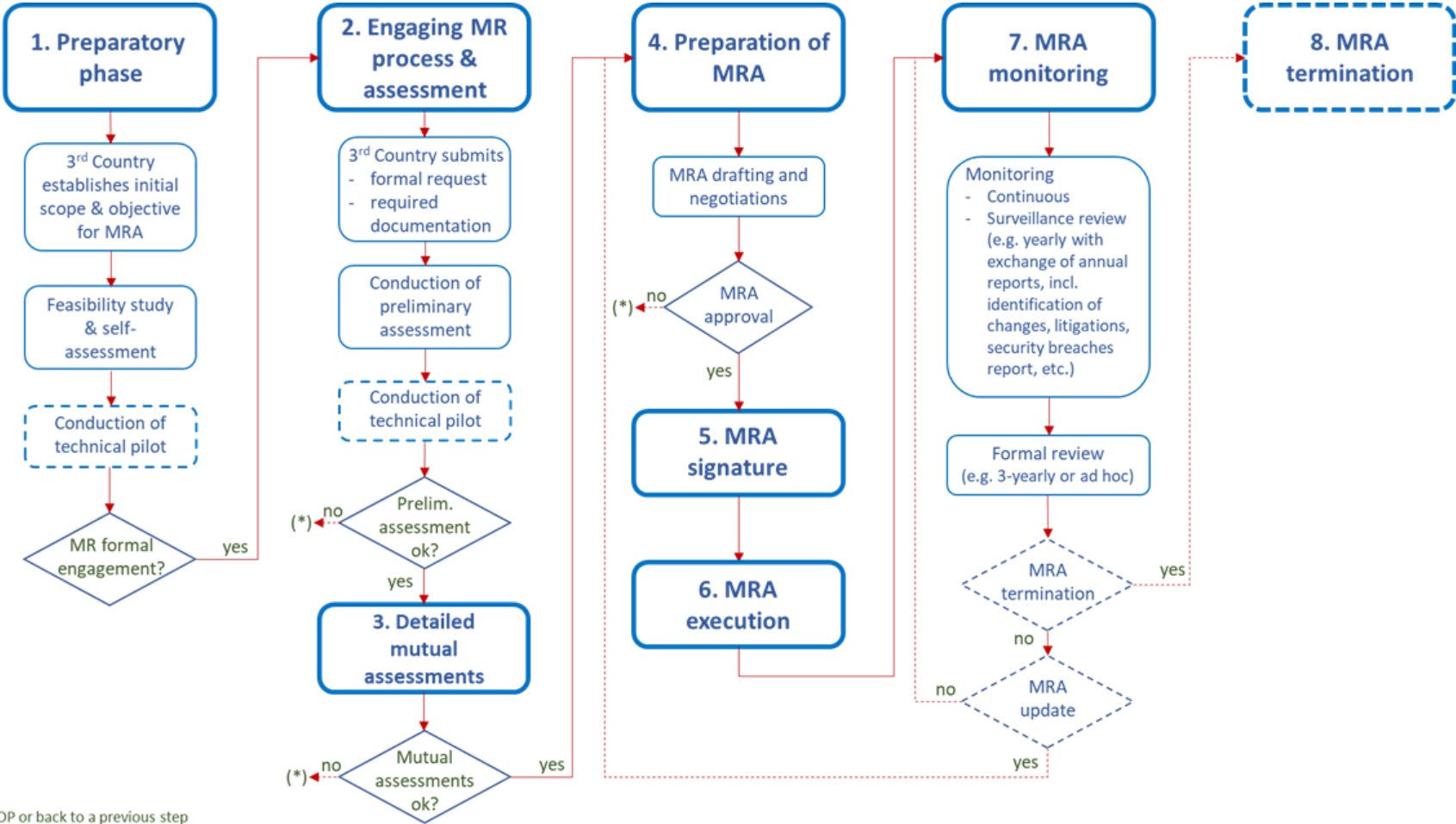
Path to mutual recognition

Recognition of qualified trust services

- Art.14 Mutual recognition agreement (MRA) can be a long journey

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

Note on steps 4 & 5: it is up to Council to decide if/when formal negotiations should be opened for conclusion of a MRA



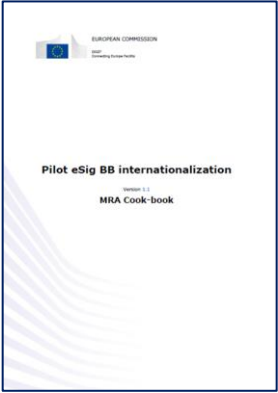
(*) STOP or back to a previous step



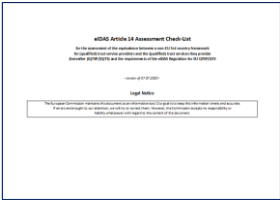
Path to mutual recognition

Recognition of qualified trust services

- EC provides guidance & technical pilot tools to assist 3rd countries
- Assessment on four pillars (Legal, Supervision & auditing, Technical, Trusted List)
- Website on Pilot CEF eSig BB international compatibility
<https://eidas.ec.europa.eu/efda/home/#/screen/international>



MRA CookBook

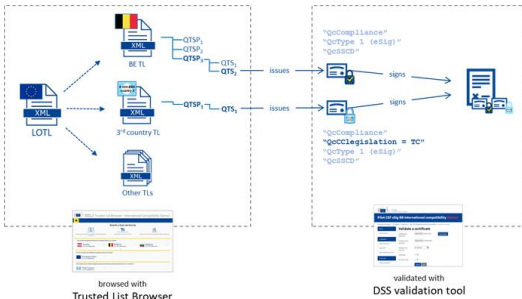


eIDAS Article 14
Assessment
Check-List
(4 pillars)



Trusted List support

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



Technical tools

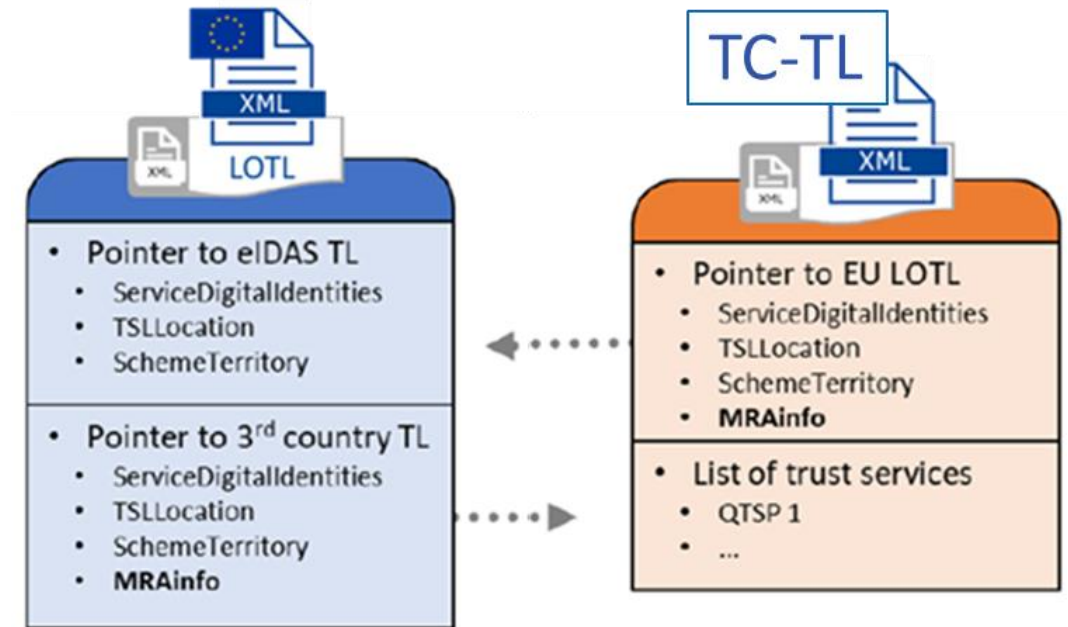
- Test LOTL
- Small test PKI
- Sample signed document
- DSS library based web application to validate signatures/certificates
- Updated TL Browser

Path to mutual recognition

Recognition of qualified trust services

Once Art.14 MRA is *signed*

- EU-LOTL
 - To include a pointer to towards the TC-TL
 - Which pointer includes an MRA-Info element declaring which TC-TS type is recognised equivalent to which EU-QTS type to facilitate validation of the TC-TS outputs as equivalent to the EU ones, with full history
- TC-TL
 - To include a pointer to towards the EU-LOTL
 - Which pointer includes an MRA-Info element declaring which EU-QTS type is equivalent to which TC-TS type to facilitate validation of the EU-QTS outputs as equivalent to the TC ones, with full history



Path to mutual recognition

Recognition of advanced electronic signatures

- No territoriality requirement for eSignatures to be valid EU-AdESig
- COM aims to facilitate the recognition of TC electronic signatures as AdESig by Art.27 Member States public online services
- TC-AdES-LOTL
 - Aims to facilitate the validation and recognition of TC-QESig (*) as meeting the requirements of EU-AdESig by recognising TC-Qualified Certificates for eSignatures issued by TC-QTSP as a means to support valid EU-AdESig **under certain conditions**
- (*) As far as they meet EU-QESig similar requirements
- TC-AdES configuration mode of DSS
 - Validation of TC electronic signatures as meeting the requirements of EU-AdESig based on the TC-AdES-LOTL **under certain validation assumptions**

Path to mutual recognition

Recognition of advanced electronic signatures

- TC-AdES-LOTL – **Conditions for pointing to a TC-TL**
 - TC to establish, maintain and publish a TL with constitutive (or assimilated) value with regards to the listing of TC-QTSP and the TC-QTS they provide
 - TC-QTSP and the TC-QTS they provide to meet similar when not equivalent requirements than those applying to EU-QTSP and EU-QTS
 - Based on TC self-assessment using the MRA-Cookbook
 - TL compliant with ETSI TS 119 612 and MRA-Cookbook requirements
 - E.g. clearly identifies the type of TC-QTS issuing TC-QC_for_eSig
 - TC-QC_for_eSig meet ETSI TS 319 412 part 2 and part 5, in particular include:
 - QcCompliance, QcType and QcCClegislation statements declaring they are TC-QC_for_eSig
 - Either QcSSCD (EU QSCD) or specific CP OID (TC-TL confirmed) declaring use of TC-QSCD meeting similar requirements applicable to EU-QSCD
- TC-AdES-LOTL include pointer to TC-TL with MRA-info element based on above rules
- [option] TC-TL to point to the production EU-LOTL with/without MRA-info

Path to mutual recognition

Recognition of advanced electronic signatures

- TC-AdES configuration mode of DSS - **validation assumptions**
 - Validation of TC electronic signatures based on TC-AdES-LOTL in order to be technical able to reasonably consider them as EU-AdESig
 - Validation based on:
 - The content of the TC signing certificate (i.e. its certificate profile);
 - Supported / confirmed by the content of the TC TL;
 - EU signatures formats (CID 2015/1506 and newer baselines) and EU-recognized signatures algorithms (from SOG-IS); and
 - Following eIDAS Art.32 requirements, as implemented by ETSI TS 119 172-4 (relying on ETSI EN 319 102-1 and ETSI TS 119 615), mutatis mutandis

... not targeting TC-QESig validation rules as applicable in TC

but validating TC eSig for being “as close as possible” to EU-QESig, with the application of EU QESig validation rules, mutatis mutandis, to ensure they meet EU-AdESig requirements

Path to mutual recognition

Background: Pilot for the International Compatibility of Trust Services

Collaboration with Ukraine, leading to the creation of the TC AdES LOTL

TC AdES LOTL-based Signature Applicability Rules

DSS validation process, and the TC AdES LOTL

Introduction to eIDAS QES

What is an eIDAS QES? (1/2)

Article 3(12) of eIDAS states:

Qualified electronic signature (QES) means an advanced electronic signature (AdES) that is:

- 1) created by a **qualified electronic signature creation device** (QSCD), and which is*
- 2) based on a **qualified certificate***
- 3) for **electronic signatures**;*

Annex I (a) and (j) of the eIDAS Regulation on “Requirements for qualified certificates for electronic signatures” states that information (1), (2) and (3) shall be **present in the certificate**.

Then, CID 2015/1505 refers to **ETSI standardized Object Identifiers (OIDs) as a medium of choice for containing information** (1), (2) and (3) in a machine-processable manner in the certificate.

Article 32 of eIDAS sets requirements regarding the process for the validation of qualified electronic signatures.

Introduction to eIDAS QES

What is an eIDAS QES? (2/2)

When opening a certificate used to create an ETSI/eIDAS-compliant QES with an ASN.1 Decoder (<http://lapo.it/>), one can observe that the QES has been:

- 1) *created by a **qualified electronic signature creation device (QSCD)** 0.4.0.1862.1.4, and which is*
- 2) *based on a **qualified certificate** 0.4.0.1862.1.1*
- 3) *for **electronic signatures** 0.4.0.1862.1.6.1 (under 0.4.0.1862.1.6);*

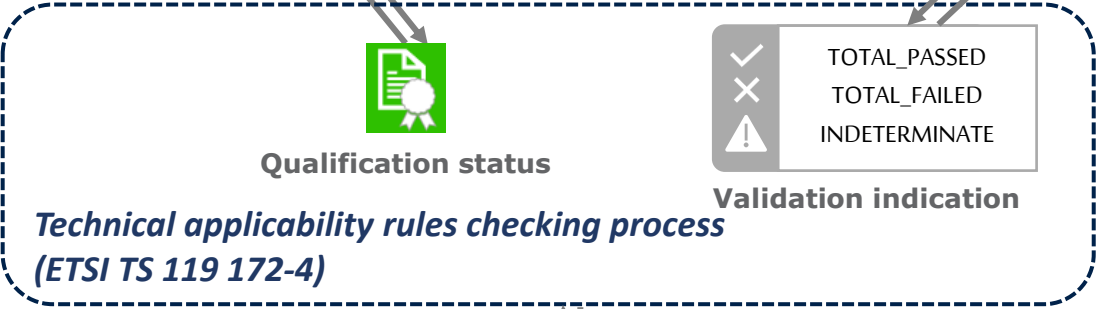
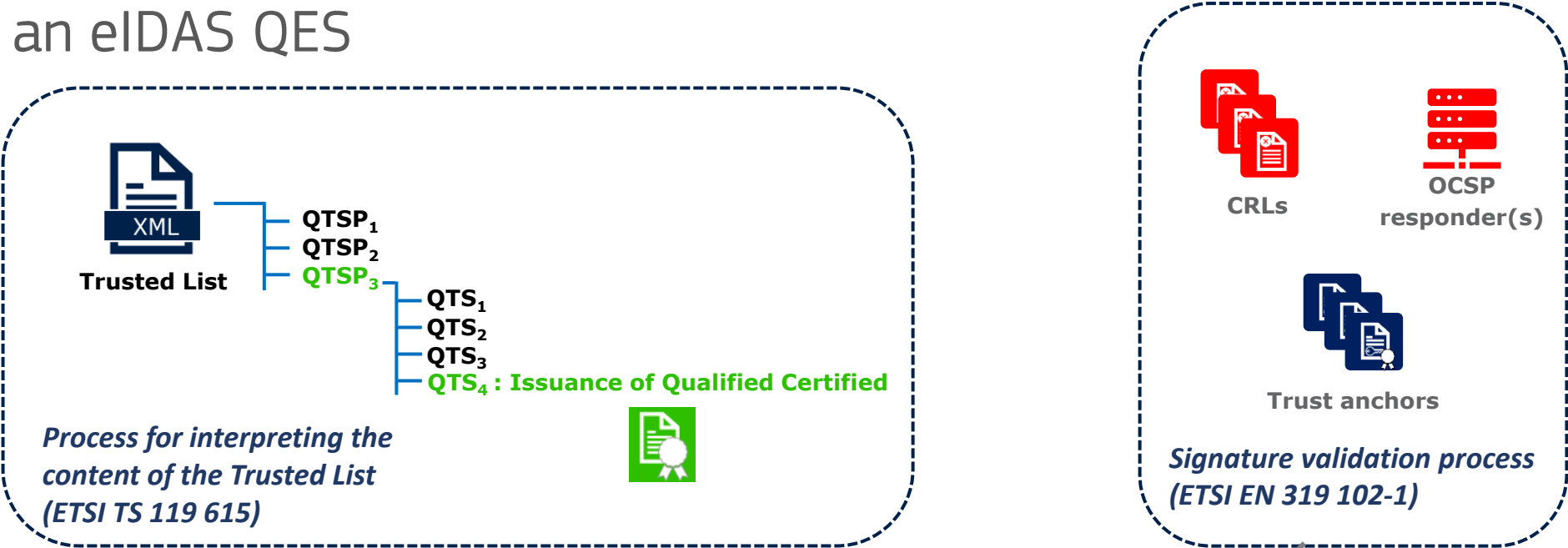
```
SEQUENCE (2 elem)
  OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
  OCTET STRING (117 byte) 30733008060604008E4601013008060604008E4601043048060604008E460105303E3...
  SEQUENCE (4 elem)
    SEQUENCE (1 elem)
      OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862 qualified certificates)
    SEQUENCE (1 elem)
      OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified certificates)
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 0.4.0.1862.1.5
      SEQUENCE (1 elem)
        SEQUENCE (2 elem)
          IA5String
          PrintableString EN
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 0.4.0.1862.1.6 etsiQcsQcType
      SEQUENCE (1 elem)
        OBJECT IDENTIFIER 0.4.0.1862.1.6.1 etsiQct-esign (ETSI EN 319 412-5)
```


2

1

3

Validation of an eIDAS QES

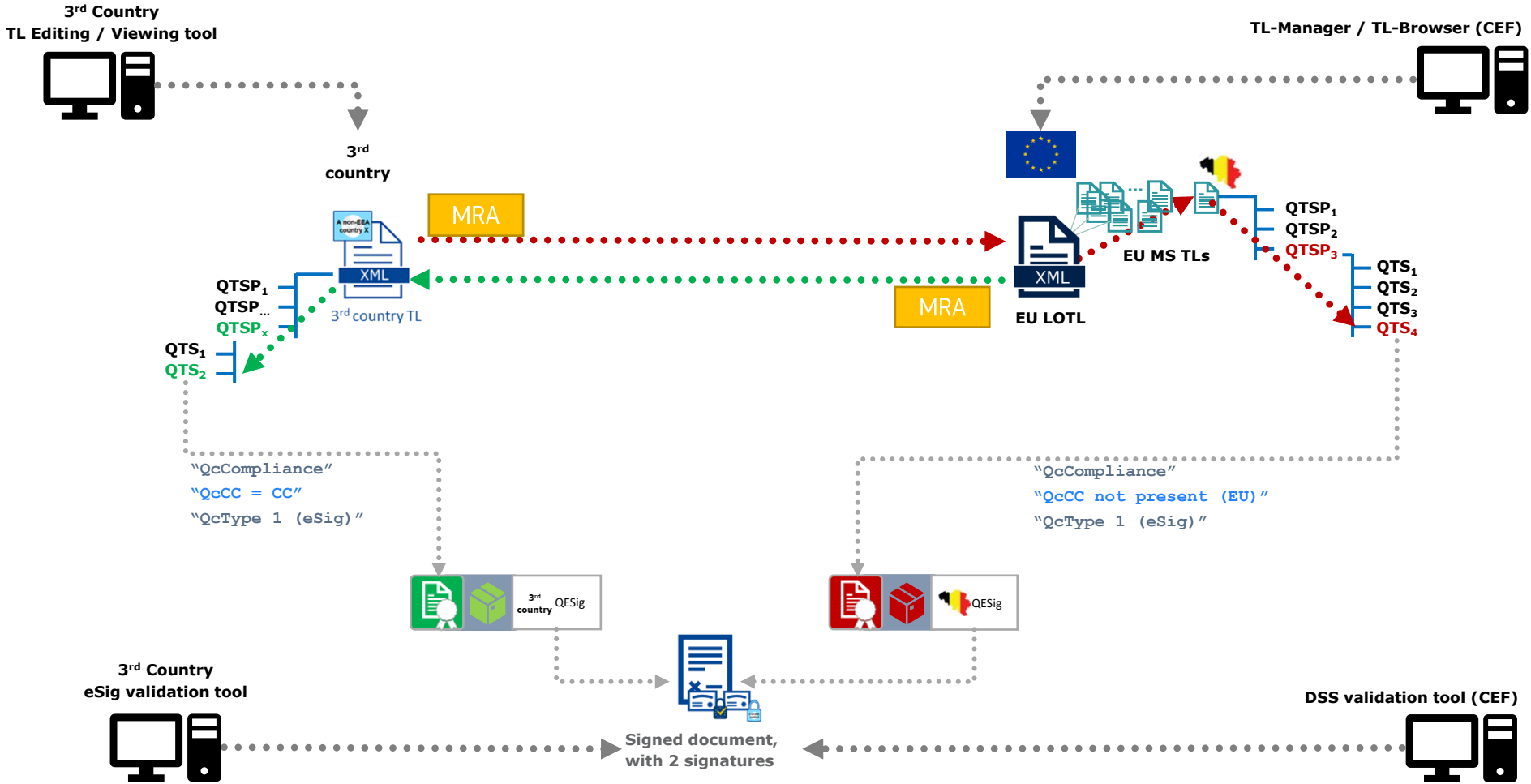



Signed document


Signature creation


Signature validation

Article 14 of eIDAS: Recognition of qualified trust services

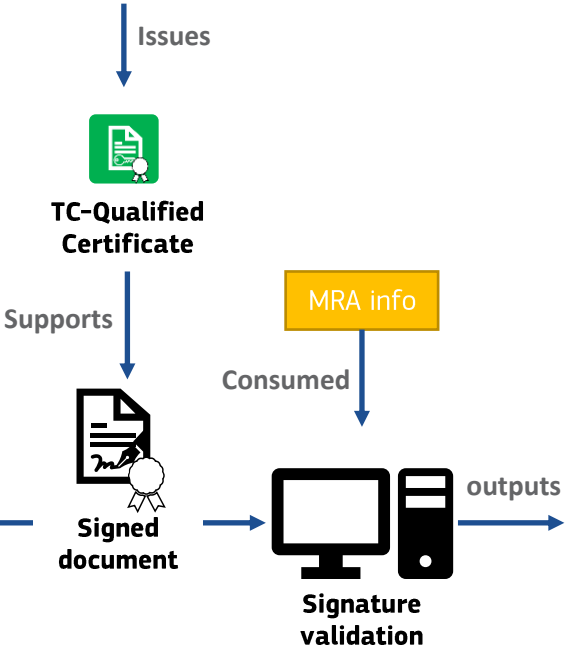


Article 14 of eIDAS: Recognition of qualified trust services



The “**MRAInfo**” element enables trusted list consuming application **to interpret** the content of a third country TL in such a way that TSP/TS listed as **qualified in that third country TL** can be interpreted **as being equivalent** to EU QTSP/QTS

Issuance of TC-qualified certificate for electronic signature



Signature S-
1C0B617512F1856E2623CBD14344EB1DC62D6282CE46F9C1DF4372BE9DD4F25A

Qualification: **QESig** ⓘ

Qualification Details :

- The trusted list validation is supported by an enacted trust service equivalence mapping, in the context of Article 14 of Regulation (EU) No 910/2014.

Signature format: PAdES-BASELINE-B

Indication: **TOTAL_PASSED** ✓

Certificate Chain:

- John Doe
- ZZ eTrust QC for eSignatures CA

On claimed time: 2023-05-10 14:44:26 (UTC)

Best signature time: 2023-05-10 14:44:44 (UTC) ⓘ

Signature position: 3 out of 3

Signature scope: Full PDF (FULL)
The document ByteRange : [0, 90867, 128757, 1132]

Relying party

MRA-Info element specifications

TC AdES LOTL

MRA-enabled TL

MRA element

```
<TrustServiceStatusList xmlns="http://uri.etsi.org/02231/v2#" xmlns:mra="http://ec.europa.eu/tools/lotl/mra/schema/v2#" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" xmlns:ns3="http://uri.etsi.org/02231/v2/additionaltypes#" xmlns:ns4="http://uri.etsi.org/01903/v1.3.2#" xmlns:ns5="http://uri.etsi.org/01903/v1.4.1#" Id="AdES_LOTL" TSLTag="http://uri.etsi.org/19612/TSLTag">
  <SchemeInformation>
    <TSLVersionIdentifier></TSLVersionIdentifier>
    <TSLSequenceNumber>2</TSLSequenceNumber>
    <TSLType>http://ec.europa.eu/tools/lotl/mra/ades-lotl-tsl-type</TSLType>
    <SchemeOperatorName>
      ...
    </SchemeOperatorName>
    <SchemeOperatorAddress>
      ...
    </SchemeOperatorAddress>
    <SchemeName>
      ...
    </SchemeName>
    <SchemeInformationURI>
      ...
    </SchemeInformationURI>
    <StatusDeterminationApproach>http://ec.europa.eu/tools/lotl/mra/ades-lotl-status-detrn</StatusDeterminationApproach>
    <SchemeTypeCommunityRules>
      ...
    </SchemeTypeCommunityRules>
    <SchemeTerritory>EU</SchemeTerritory>
    <PolicyOrLegalNotice>
      ...
    </PolicyOrLegalNotice>
    <HistoricalInformationPeriod>65535</HistoricalInformationPeriod>
    <PointersToOtherTSL>
      <OtherTSLPointer>
        ...
        </OtherTSLPointer>
      </OtherTSLPointer>
      <ServiceDigitalIdentities>
        ...
      </ServiceDigitalIdentities>
      <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
      <AdditionalInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
        <OtherInformation>
          ...
        </OtherInformation>
      </AdditionalInformation>
      <MRA>
        <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:TrustServiceEquivalenceInformation>
          <mra:TrustServiceEquivalenceInformation>
            ...
          </mra:TrustServiceEquivalenceInformation>
          <mra:TrustServiceEquivalenceInformation>
            ...
          </mra:TrustServiceEquivalenceInformation>
          <mra:MutualRecognitionAgreementInformation>
            ...
          </mra:MutualRecognitionAgreementInformation>
        </MRA>
      </AdditionalInformation>
    </PointersToOtherTSL>
    </ListIssueDateTime>
    <NextUpdate>
      <dateTime>2023-07-22T07:00:00Z</dateTime>
    </NextUpdate>
    <DistributionPoints>
      <URI>https://ec.europa.eu/tools/lotl/mra/ades-lotl.xml</URI>
    </DistributionPoints>
    </SchemeInformation>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-0213abe020a0eea8d1eb161285a144e1">
      ...
    </ds:Signature>
  </TrustServiceStatusList>
```

MRA-Info element specifications

Illustration based on a prospective EU LOTL

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 element.

```
<OtherTSLPointer>
+<ServiceDigitalIdentities></ServiceDigitalIdentities>
-<TSLLocation>
  https://eidas.ec.europa.eu/efda/intl-pilot/api/v1/intl-pilot/tl/mra_tl_zz.xml
</TSLLocation>
-<AdditionalInformation>
+<OtherInformation></OtherInformation>
-<OtherInformation>
  <SchemeTerritory>ZZ</SchemeTerritory>
</OtherInformation>
+<OtherInformation></OtherInformation>
+<OtherInformation></OtherInformation>
+<OtherInformation></OtherInformation>
-<OtherInformation>
-<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPartyLegislation="uri/..." pointingContractingPartyLegislation="uri/..." technicalType="1"
  -<mra:TrustServiceEquivalenceInformation>
    <mra:TrustServiceLegalIdentifier>QCForESig</mra:TrustServiceLegalIdentifier>
    -<mra:TrustServiceTSLTypeEquivalenceList>
      -<mra:TrustServiceTSLTypeListPointingParty>
        -<mra:TrustServiceTSLType>
          <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
        -<AdditionalServiceInformation>
          -<URI xml:lang="en">
            http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
          </URI>
        </AdditionalServiceInformation>
```

MRA-Info element specifications

Trust Service Equivalence Information

That contain information about the equivalence mapping :

TrustService**LegalIdentifier**

TrustService**TSLType**EquivalenceList

TrustService**TSLStatus**EquivalenceList

TrustService**TSLQualificationExtension**EquivalenceList

CertificateContentReferencesEquivalenceList

TrustService**EquivalenceStatus**

TrustServiceEquivalenceStatus**StartingTime**

TrustServiceEquivalence**History**

```
<OtherTSLPointer>
+<ServiceDigitalIdentities></ServiceDigitalIdentities>
-<TSLLocation>
  https://eidas.ec.europa.eu/efda/intl-pilot/api/v1/intl-pilot/tl/mra_tl_zz.xml
</TSLLocation>
-<AdditionalInformation>
+<OtherInformation></OtherInformation>
-<OtherInformation>
  <SchemeTerritory>ZZ</SchemeTerritory>
</OtherInformation>
+<OtherInformation></OtherInformation>
+<OtherInformation></OtherInformation>
+<OtherInformation></OtherInformation>
-<OtherInformation>
  -<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPart
  -<mra:TrustServiceEquivalenceInformation>
    <mra:TrustServiceLegalIdentifier>QCForESig</mra:TrustServiceLegalIdentifier>
    -<mra:TrustServiceTSLTypeEquivalenceList>
      -<mra:TrustServiceTSLTypeListPointingParty>
        -<mra:TrustServiceTSLType>
          <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeI
          -<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://zz-trusted-list.go.zz/TrstSvc/Svctype/CA/QC/for-eSig
        </ServiceTypeIdentifier>
      </mra:TrustServiceTSLType>
    </mra:TrustServiceTSLTypeListPointedParty>
```


MRA-Info element specifications

Equivalences between information in the **Pointing Party** and information in the **Pointed Party**

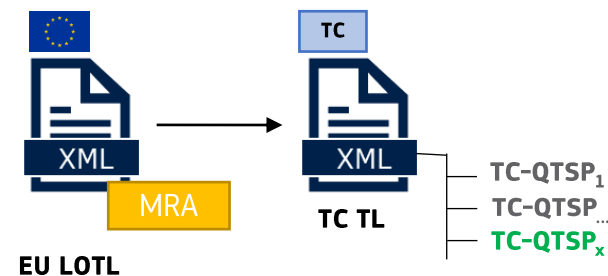
TrustService**TSLType**EquivalenceList

- Identifies the type of TC-QTS, and the corresponding EU QTS

CertificateContentReferencesEquivalenceList

- Identifies QcCompliance, QcType and QcCClegislation or equivalent statements
- Either QcSSCD (EU QSCD) or specific CP OID (TC-TL confirmed) statement, declaring use of TC-QSCD meeting similar requirements applicable to EU-QSCD

**PointingParty - **PointedParty



Tools being made available

- **DSS** supports the MRA element starting from **v5.11**
- A DSS library-based web **demo** to **validate signatures / certificates** (from EU and from the 3rd country)

- **Test material**
- Documentation

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

The screenshot displays the DSS web interface. At the top, a blue information banner states: "For security reasons, the features 'Sign document' and 'Validate signature' can only be used after two-factor authentication. In order to use these features, you must have an EU Login account with a second authentication method. Your account must then be configured with, for example, a mobile phone number or a registered EU Login Mobile application." Below this is a navigation menu with options: "Download center", "Sign a document", "Validate a signature" (highlighted), "Trusted Lists", and "Useful links". The main content area features a document upload section with a blue information banner: "A document that has been signed by a third country qualified certificate for electronic signatures and an EU country qualified certificate for electronic signatures can be downloaded from the 'Download Center'." Below this is a large grey box with a download icon and the text "Drag a PDF document here or click to select the PDF to upload". A yellow "Validate" button is positioned to the right of the upload area. Below the upload section is a list of documentation resources under three categories: "Documentation for 3rd countries looking for an MRA", "Tools to sign and validate signatures in this pilot", and "Technical documentation for the execution of the MRA". Each resource includes a title, a brief description, and a download icon.

Documentation for 3rd countries looking for an MRA

- MRA cookbook (PDF document)**
 - Main document of this pilot that gives an overview of eIDAS and Article 14, the MRA process flow and methodology, the minimal requirements for the MRA, and the technical implications or the assumptions about the technical specifications
- eIDAS Article 14 Assessment Check-List (ODS document)**
 - Check-list for third countries to perform a self-assessment on how compliance against the minimal legal requirements (legal context, supervision and auditing, best practice, trust representation)

Tools to sign and validate signatures in this pilot

- NexU (ZIP containing .bat file)**
 - Application required to sign documents in this pilot
- Keystore / Private key (P12 file)**
 - Keystore containing the private key (password is "password") supported by a qualified certificate for electronic signature issued by a third country QTSP
- Sample document for validation (PDF document)**
 - Document signed with a third country qualified certificate for electronic signatures and an EU country qualified certificate for electronic signatures

Technical documentation for the execution of the MRA

- Version 2.1 of MRA element's specification, usage and XSD (ZIP archive)**
 - Version 2.1 of the bundle. This bundle also contains the specification of the "TC AdES LOTL" supporting the voluntary technical validation by relying parties of electronic signatures and seals supported by certificates issued by trust service providers established in Third Countries as advanced electronic signatures and seals.
- Version 2 of MRA element's specification, usage and XSD (ZIP archive)**
 - Version 2 of the bundle updating the MRA element's prefix URI.
- Version 1 of MRA element's specification, usage and XSD (ZIP archive)**
 - Bundle containing the technical documentation for the execution of the MRA: Specification of the necessary adaptations to the eIDAS LOTL and to the Third Country trusted list to implement the execution of an MRA; XML Schema Definition (XSD) of the MRA element; Description of the necessary adaptation of technical standards for the validation of Third Country electronic signatures/seals based on the MRA element.

COFFEE BREAK

14:40 – 14:50

