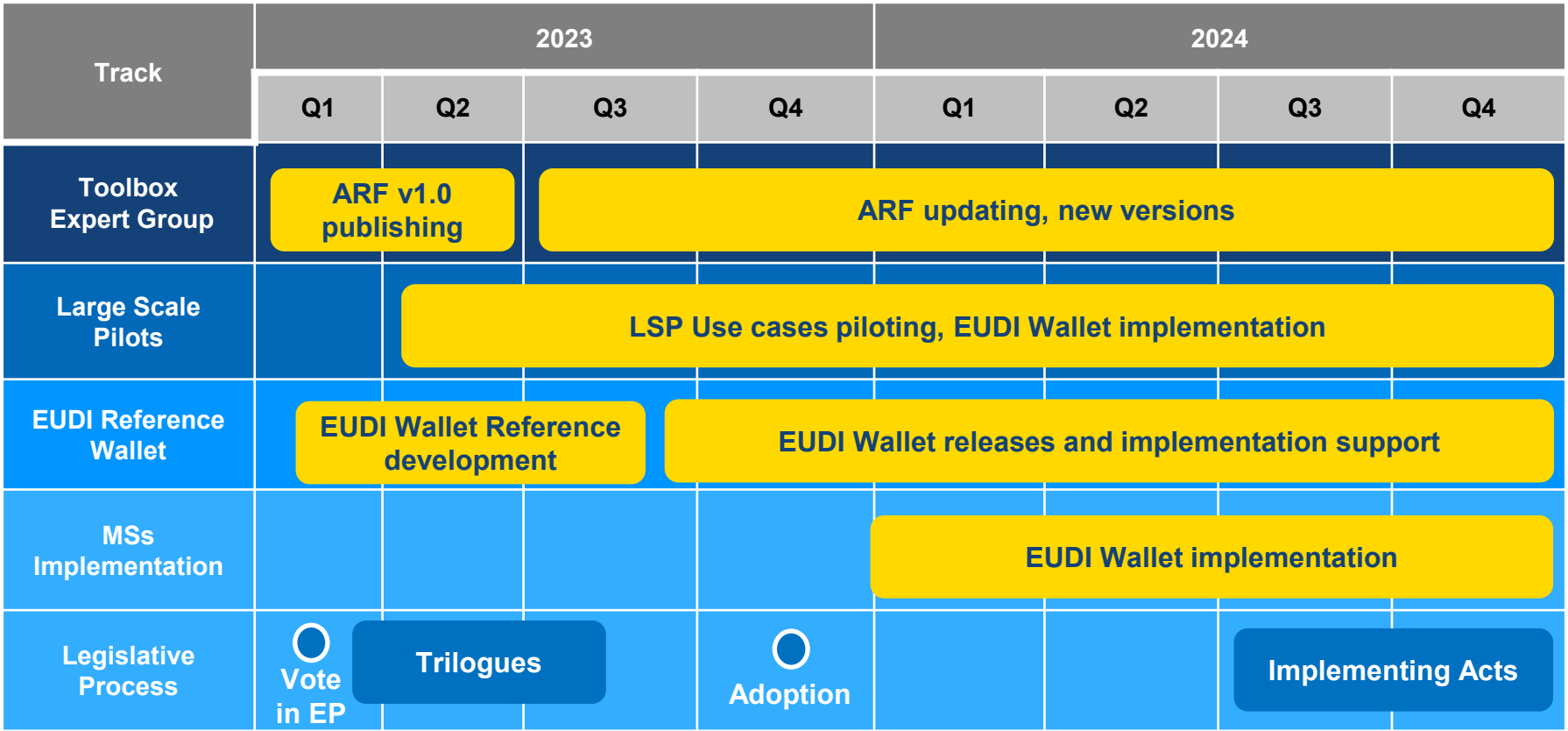
eIDAS 2.0 – Latest developments

Viky MANAILA
Trust Services Director – Intesi Group

March 2023

Implementation Roadmap



Trilogue just started – 21st March 2023

https://twitter.com/vestager/status/1638264599957864452?s=20

First technical trilogue taking place 23rd March, 10:30-13:00. On the agenda are general provisions (Art. 1, 2, 5) + Notified identification schemes (Art. 7, 9, 10, 12a, 12c).

The ARF

The ARF and its legal status

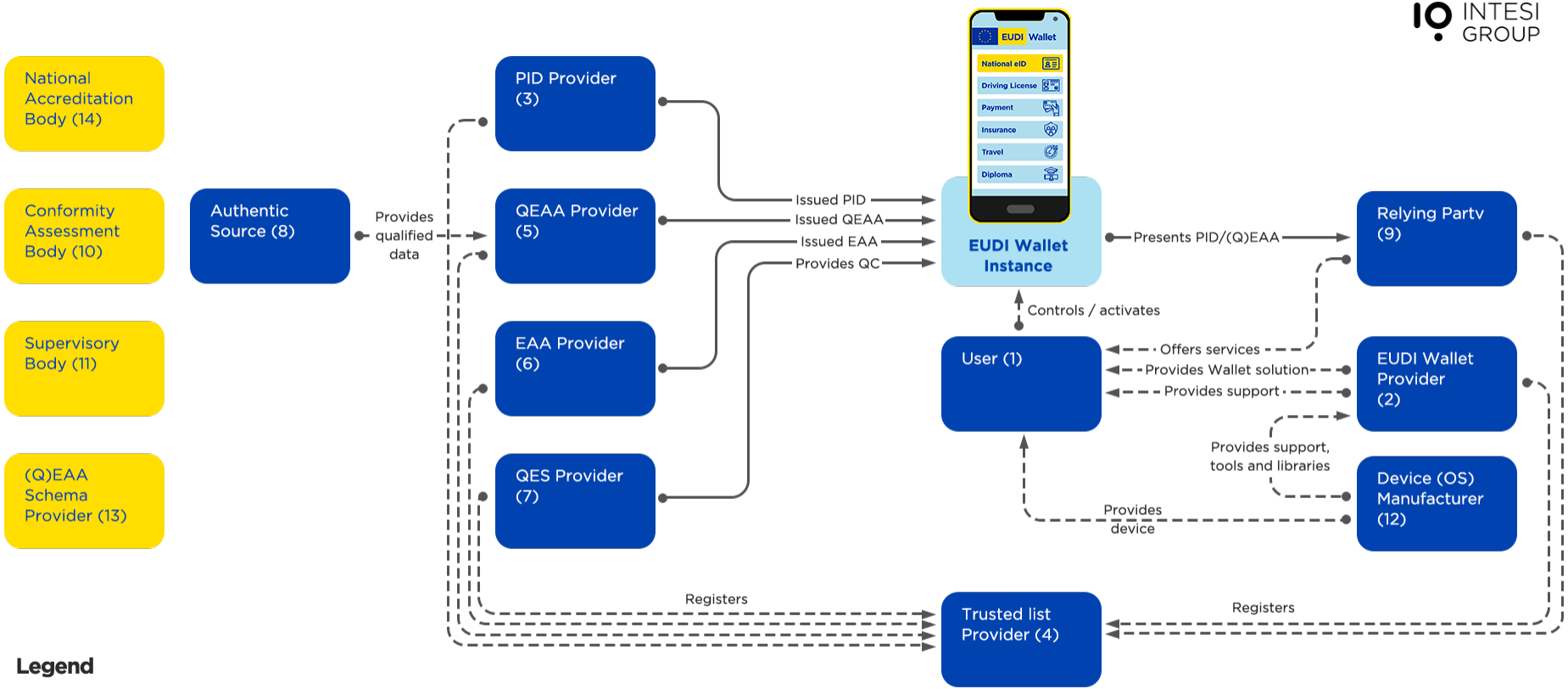
- “The document itself holds no legal value [...] will be aligned to the outcome of the legislative negotiations”.
  - It is the eIDAS 2.0 Regulation, the implementing and delegated acts that are mandatory.
  - The ARF was developed mainly based on the 3 June 2021 eIDAS 2.0 proposal.

Clear LSP focus

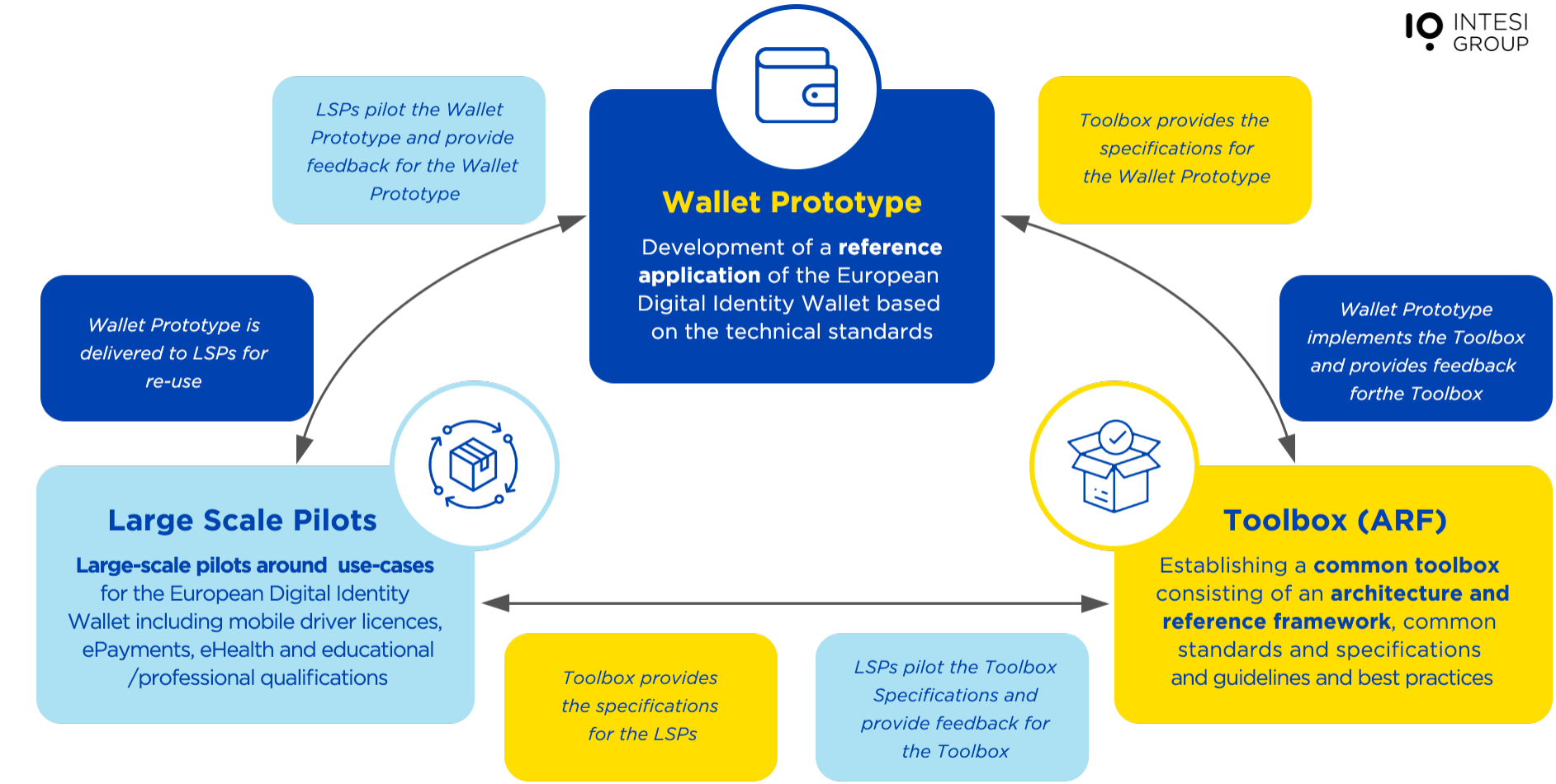
- “meant to be used [for] developing a reference implementation (RI) [and] in the context of Large-Scale Pilots”
- “provide all specifications needed to develop an interoperable EUDI Wallet”
- “This document will be complemented and updated over time” – living document with further iterations

https://github.com/eu-digital-identity-wallet

Demystifying the EUDI Wallet ARF webinar recording:
https://www.youtube.com/watch?v=MvXkh8rBTLw



SOURCE EUROPEAN COMMISSION



SOURCE EUROPEAN COMMISSION

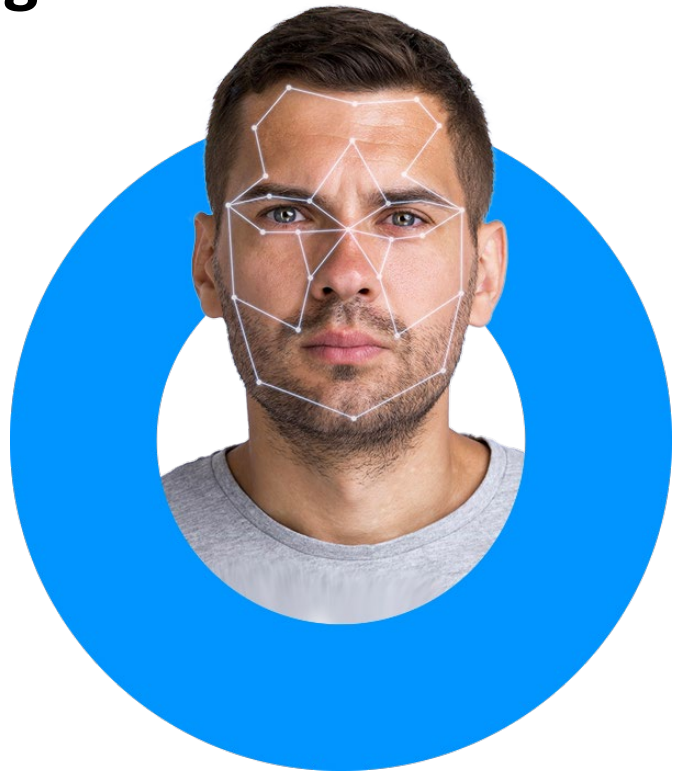
Standards in support of eIDAS 2.0

ETSI ESI

- ETSI TS 119 461 – Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI TS 119 462 – Wallet Interfaces for Trust Services and Signing
- ETSI TS 119 471 – Policy and Security requirements for EAAs
- ETSI TS 119 472 – Profiles for EAAs

ETSI TS 119 461 – Identity proofing

- Published in July 2021, covers identity proofing for qualified and non-qualified trust services
- Must cover eIDAS Article 24.1 on identity proofing for issuing of QES and QEAAs
- Revision started for eIDAS 2.0 alignment



ETSI TS 119 461 – Identity proofing

INTESI GROUP

NOTE: Trilogue negotiations will settle the final version

Current eIDAS allows ‘substantial’ based on physcial presence

Verification of identity for issuing a qualified certificate or QEAA shall be:

a) By European Digital Identity Wallet or notified electronic identification means at assurance level ‘high’.
b) By ~~qualified electronic attestations of attributes or~~ certificate of qualified electronic signature or qualified electronic seal issued in compliance with point a), c) or d).
c) By other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;
d) By physical presence of natural person or authorised representative of legal person by “appropriate procedures and in accordance with national laws”.

«Other» means in practice remote identity proofing by use of identity documents

Parliament suggests removing attribute attestation.

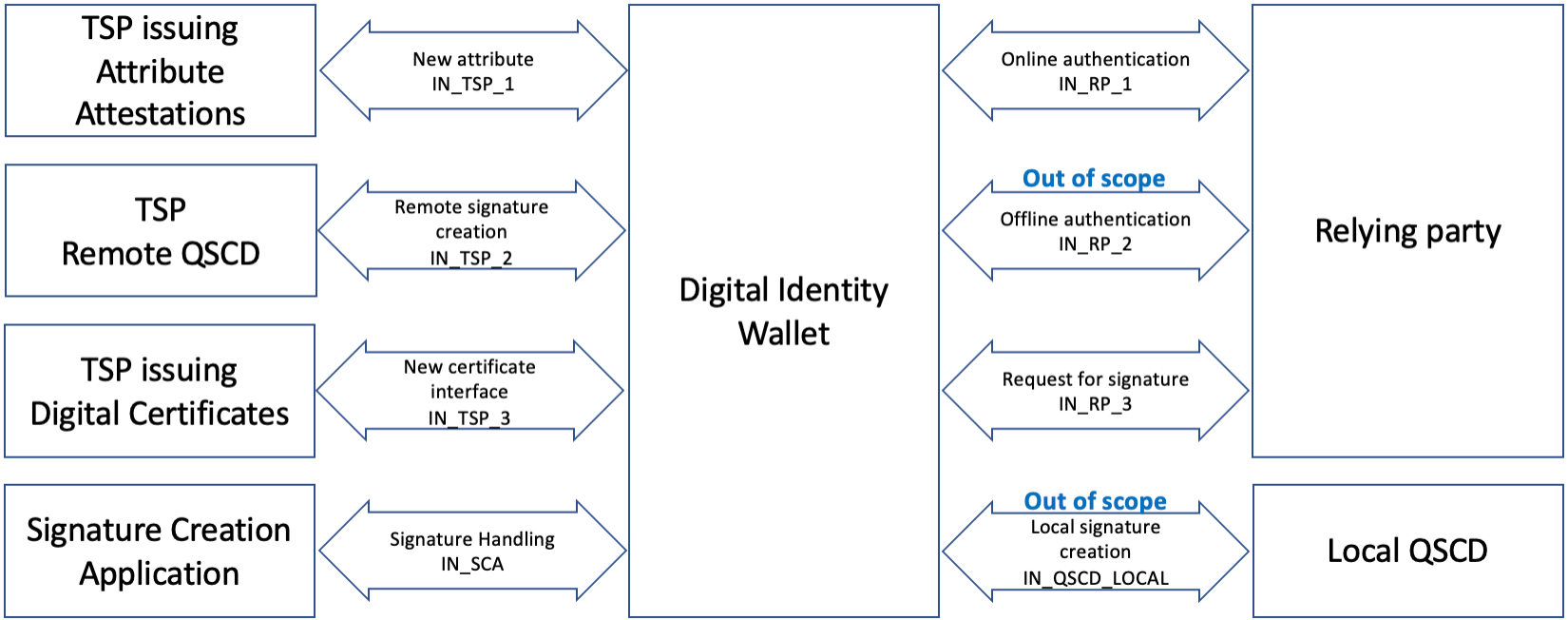
The reference to points a, c, d is technically challenging.

ETSI TS 119 462 – Wallet Interfaces

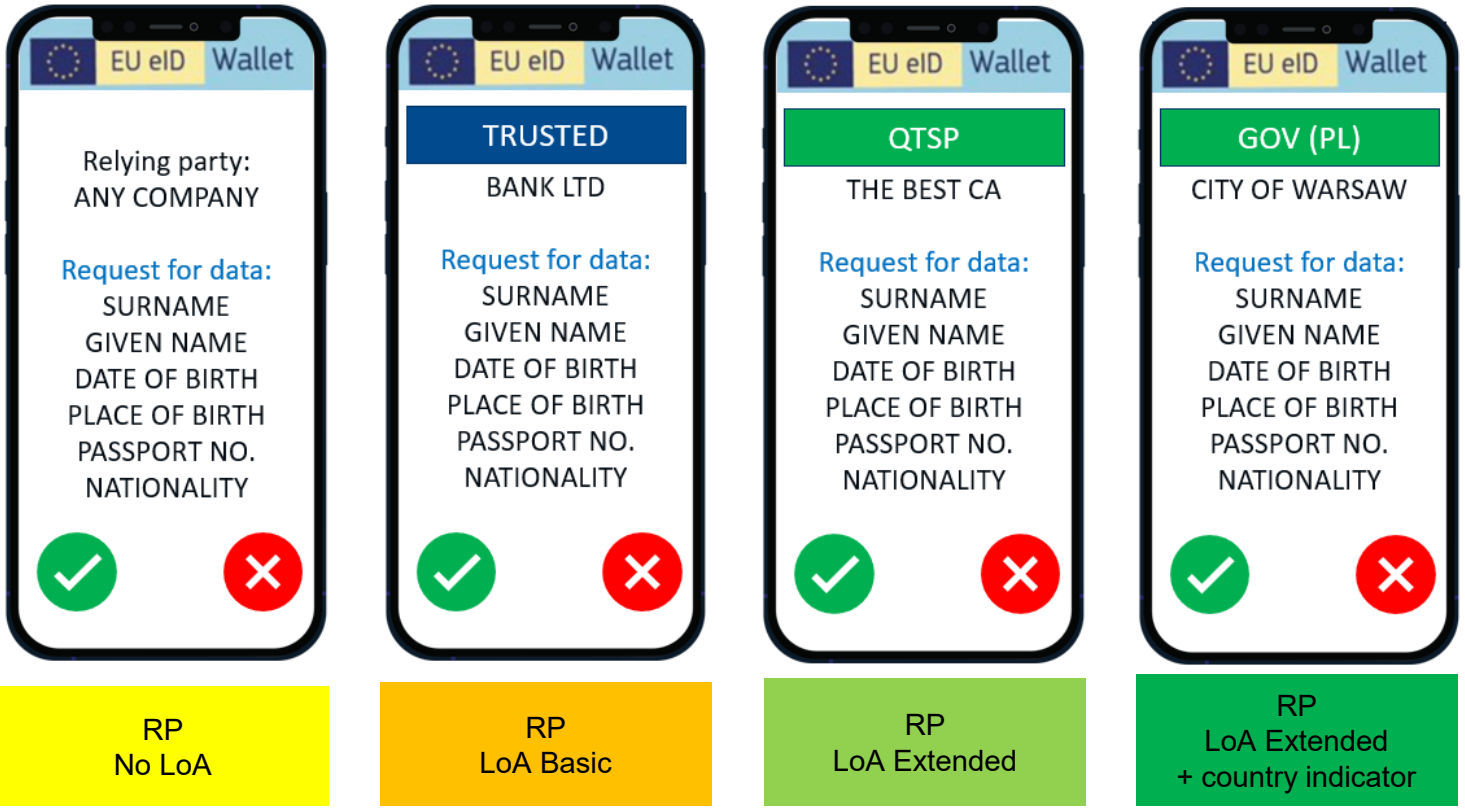
Scope:

- interface for TSPs for the purpose of issuing (Q)EAAs and (Q)ES certificates to the wallet;
- interface to TSPs when acting as Relying Party in providing its services;
- interface for creation of remote QES (the QSCD is managed by TSP);
- Other use cases for the creation of eSig and other trust services;
- **This Work Item is aligned to parallel works on EAA Policies and EAA Profiles standards.**

Interfaces list



RPs – different levels of trust



ETSI TS 119 471 – Policy reqs for (Q)EAA services

Scope:

- Policy and security requirements on EAA generation and verification by the trust service provider;
- Policy and security requirements on EAA status validation services;
- Requirements for assessing the trustworthiness of the EAA; and
- Requirements on personal data processing

ETSI TS 119 472 – EAA profiles

Scope:

- Semantics of EAA: attestation metadata, attributes metadata, signature component
- Bindings for EAA based on W3C VCs: bindings with proofs
- Bindings for EAA based on X.509 Attribute Certificates
- Semantics of Presented EAA

Alignments:

- ISO 23220, ISO 180135
- OpenID
- EBSI

Under reviews:

- ZKP solutions
- Selective Disclosure mechanisms: JWTs (SD-JWT), draft-ietf-oauth-selective-disclosure-jwt-02

ETSI Standards for Trust Services

INTESI GROUP

- EN 319 401 - General Policy Requirements for Trust Service Providers
- EN 319 411-1 - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General Requirements
- EN 319 411-2 - Policy and security requirements for TSPs issuing certificates - Part2: Requirements for TSPs issuing qualified certificates
- TR 119 411-4 Policy and security requirements for TSPs issuing certificates - Part 4: Checklist supporting audit of TSPs
- TS 119 431-1 Policy and security requirements for TSPs, Part1: TSP service components operating a remote QSCD/SCDev
- TS 119 432 - Protocols for remote digital signature creation
- EN 319 421 - Policy and security requirements for TSPs issuing electronic time-stamps
- EN 319 412-1 & TS 119 412-1 - Certificate Profiles, Part 1: Overview and common data structures
- EN 319 412-2 - Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons
- EN 319 412-3 - Certificate Profiles, Part3: Certificate profile for certificates issued to legal persons
- EN 319 412-4 - Certificate Profiles, Part4: Certificate profile for web site certificates issued to organisations
- EN 319 412-5 - Certificate Profiles, Part5: QCStatements
- EN 319 422 - Time stamping protocol and time stamp token profiles

All available on www.etsi.org

ETSI Standards for Trust Services

- TS 119 495 - Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the Payment Services Directive (EU) 2015/2366
- TS 119 612 - Trusted Lists
- TS 119 460 - Survey of technologies and regulatory requirements for identity proofing for trust service subjects
- TS 119 461 - Policy and security requirements for trust service components providing identity proofing of trust service subjects

TS 119 172-4 - Signature Policies, Part4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trust lists

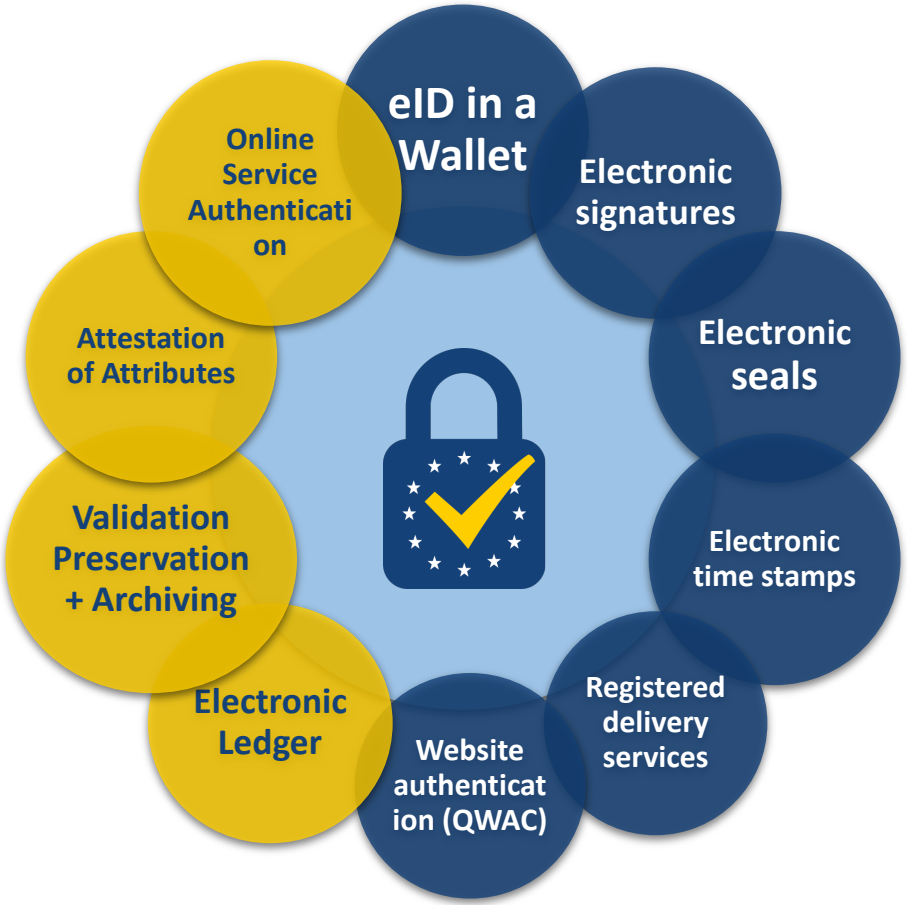
- EN 319 403-1 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing TSPs
- TS 119 403-2 - Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates
- TS 119 403-3 - Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

New standards in support of eIDAS2 - in drafting process:

- TS 119 462 - Wallet interfaces for trust services and signing - all QTSPs
- TS 119 471 - Requirements for TSPs issuing Electronic Attestation of Attributes
- TS 119 472 - Profiles for Electronic Attestation of Attributes

Trust Services

eIDAS 2.0 – Trust Services



Trust Service eIDAS 2.0 - COM 281/2021

Article 1:

‘This Regulations aims at ensuring **the proper functioning of the internal market and providing an adequate level of security of electronic identification means and trust services**. For these purposes, this Regulation:

(a) lays down the conditions under which Member States shall provide and recognise electronic identification means of natural and legal persons, falling under a notified electronic identification scheme of another Member State;

(b) **lays down rules for trust services**, in particular for electronic transactions;

(c) **establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving and electronic attestation of attributes, the management of remote electronic signature and seal creation devices, and electronic ledgers**;

(d)lays down the conditions for the issuing of European Digital Identity Wallets by Member States.’;

Trust Service eIDAS 2.0 - COM 281/2021

INTESI GROUP

Article 2 Scope

1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets issued by Member States and to trust service providers that are established in the Union.

2. **This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants**.

3. This Regulation does not affect national, or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to sector specific requirements as regards form with underlying legal effects.

Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation

Trust Service eIDAS 2.0 - COM 281/2021

(16) ‘trust service’ means an electronic service normally provided against payment which consists of:

(a) **the creation, verification, and validation** of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;

(b) the creation, verification and validation of certificates for website authentication;

(c) the preservation of electronic signatures, seals or certificates related to those services;

(d) the electronic archiving of electronic documents;

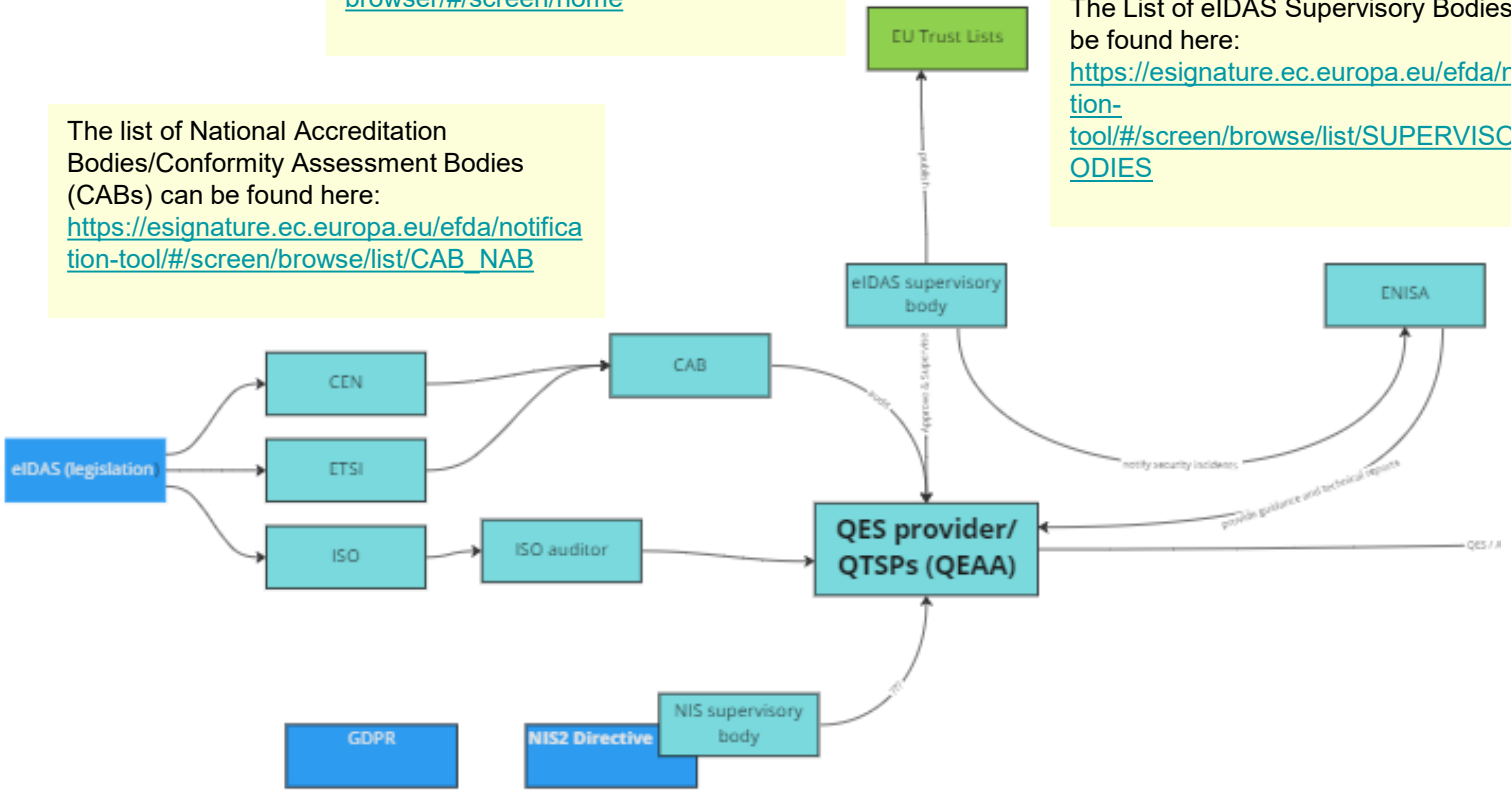
(e) the management of remote electronic signature and seal creation devices;

(f) the recording of electronic data into an electronic ledger.’

EU Trust Lists
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

The list of National Accreditation Bodies/Conformity Assessment Bodies (CABs) can be found here:
https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/CAB_NAB

The List of eIDAS Supervisory Bodies can be found here:
https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/SUPERVISORY_BODIES



QEAA role

INTESI GROUP

QEAA Provider

1. Provided by QTSPs under **existing Trust Framework for QTSPs**
2. Maintain interface for requests and provisioning of QEAA
3. Mutual authentication to EUDIW
4. Where relevant, interface to Authentic Source of attributes
5. Provide validity status check service
6. **MUST NOT learn anything about the use of a QEAA they issue when validity status checks are performed**
    a. W3C Validity Status Lists and various (ZKP) variations thereof
    b. CRL/CRT?

EAA role

INTESI GROUP

EAA Provider

1. Provided by any Trust Service Provider
2. **Supervised under eIDAS but bound by other legal / contractual frameworks**
3. Example areas include mDL, educational credentials, payments etc. even if these can in turn rely also on QEAAs
4. MUST comply with EUDIW interface specifications
5. MAY provide validity status check services
6. **MUST NOT learn about use of EAA if validity status check is performed**
    a. Use case specific and sector specific validity status check services

TSPs vs QTSPs

	TSP	QTSP
Regulatory requirements: eIDAS, GDPR, NIS2	yes	Yes + additional requirements for qualified status
Technical requirements: ETSI, CEN, ISO, sector specific requirements	Yes + subject to national specific requirements	Yes + additional requirements for qualified status
Audit	Yes, recommended	Yes – accredited Conformity Assessment Body (CAB)
Supervision (National Supervisory Body in the EU country where the TSP is incorporated)	Ex-post	Ex-ante
Trust List	Up to the National rules for country TL	Yes

Your input is highly appreciated

INTESI GROUP

(Q)EAA

- authentic sources, authoritative sources: data freshness, data changes propagation to validity status
- How to include (Q)EAA in advanced electronic signatures (XAdES, CAdES, PAdES, JAdES, ASiC…)
- How to verify AdES with (Q)EAA

Relying Parties

- Validation service for multiple (Q)EAA providers to RPs

Q&A

Thank You!

vmanaila@intesigroup.com

Viky Manaila 💯
eIDAS, Digital Identity, Digital Signatures & PKI expert