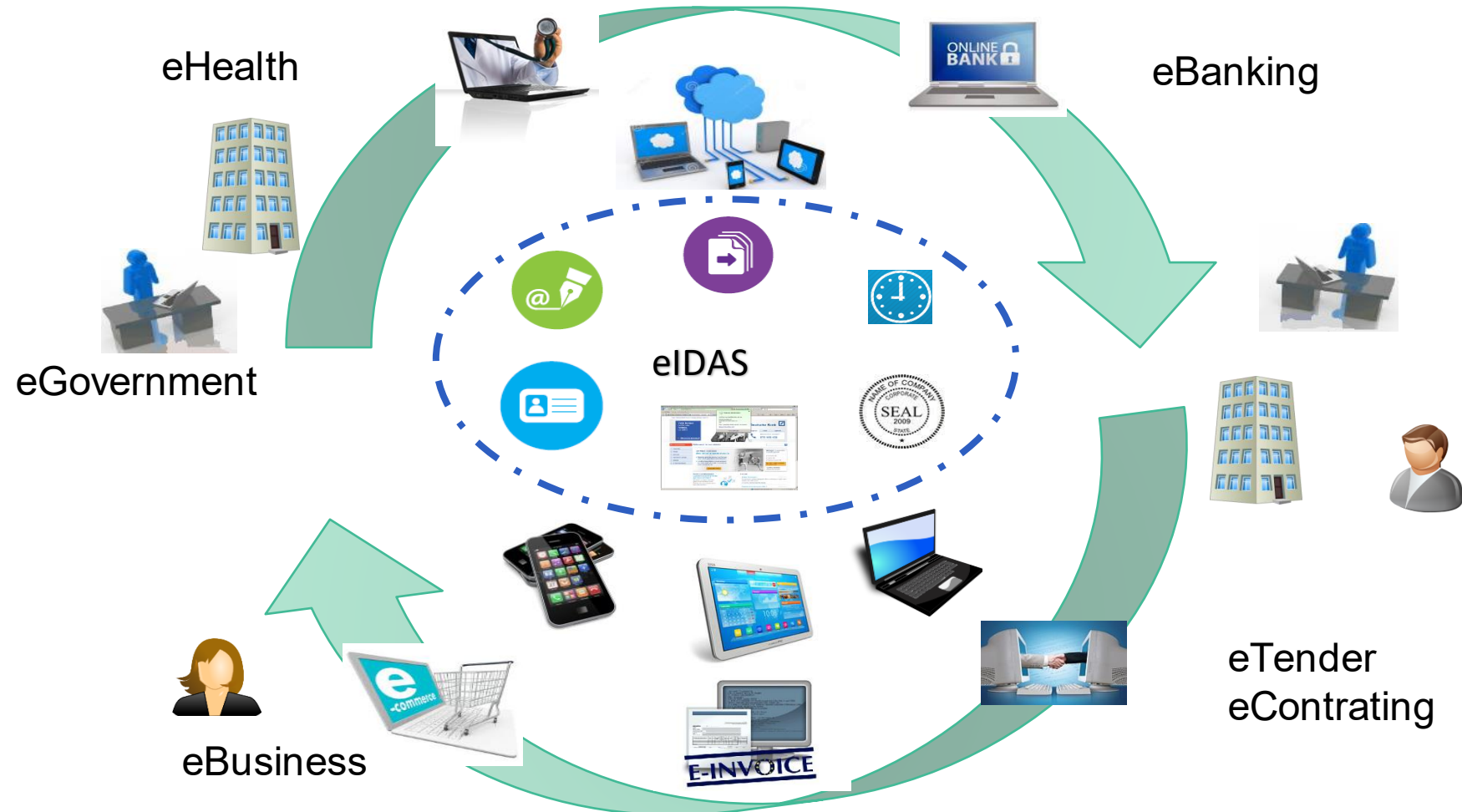


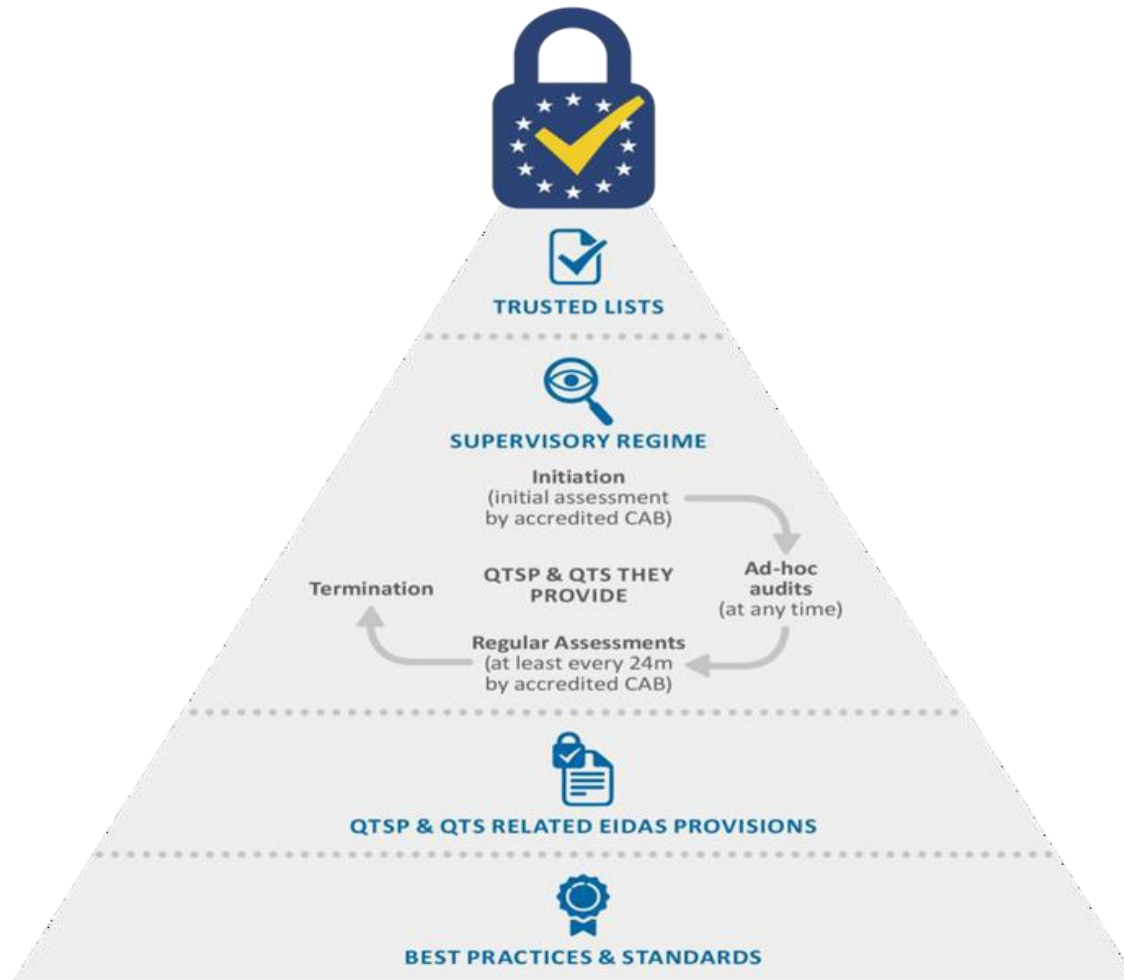
Trust Services with the EUDI Wallet

ARNO FIEDLER

NIMBUS TECHNOLOGIEBERATUNG GMBH

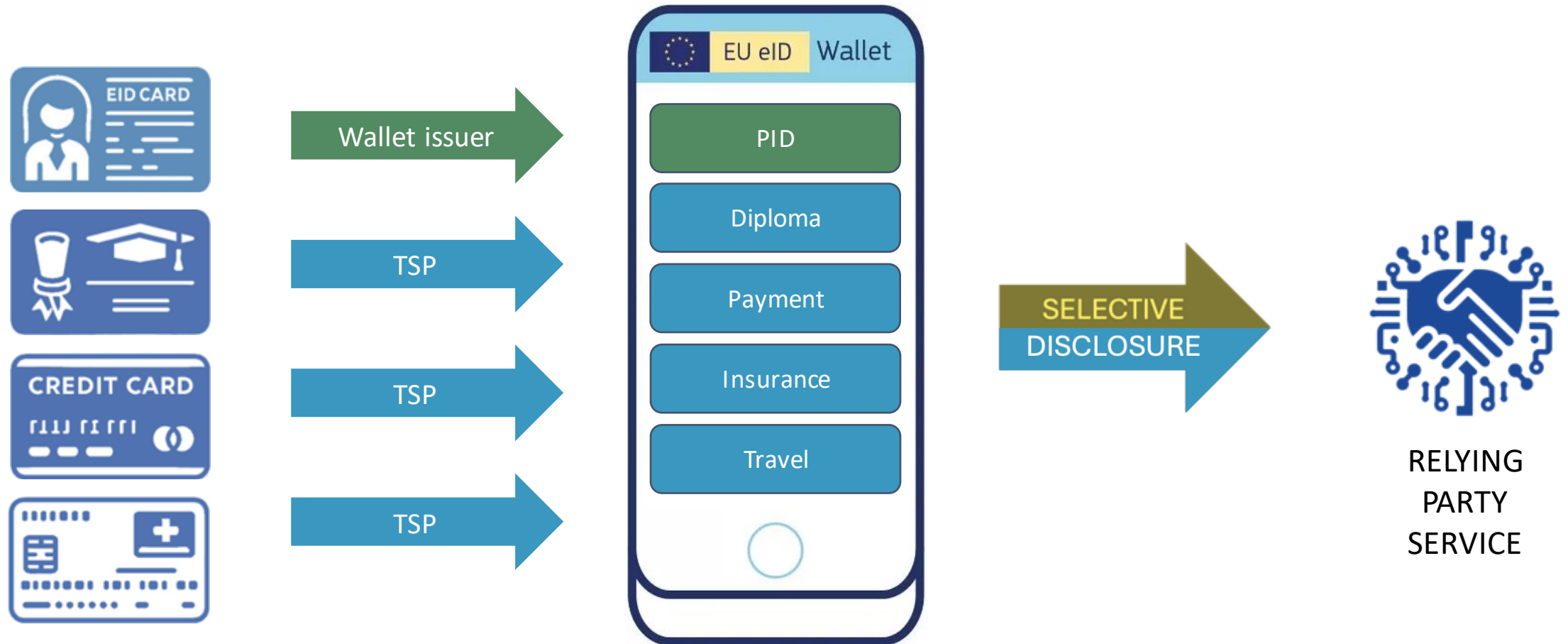
eIDAS 2014: Vision to enable “EU Digital Single Market via Pan-European Trust Services”





- The harmonization of trust services has been achieved through Mandate/460 to CEN and ETSI
- The relevant standards are accepted, sufficiently secure and detailed and sufficiently testable
- Trust services can be used “freely” in the European market; PSD2 is a good example of authorization.
- The TSL as a technical trust space has proven itself
- Some member states have further security-related policies that lead to market disadvantages of some providers; e.g. in the field of identification

eIDAS 2024: European Digital Identity Wallet

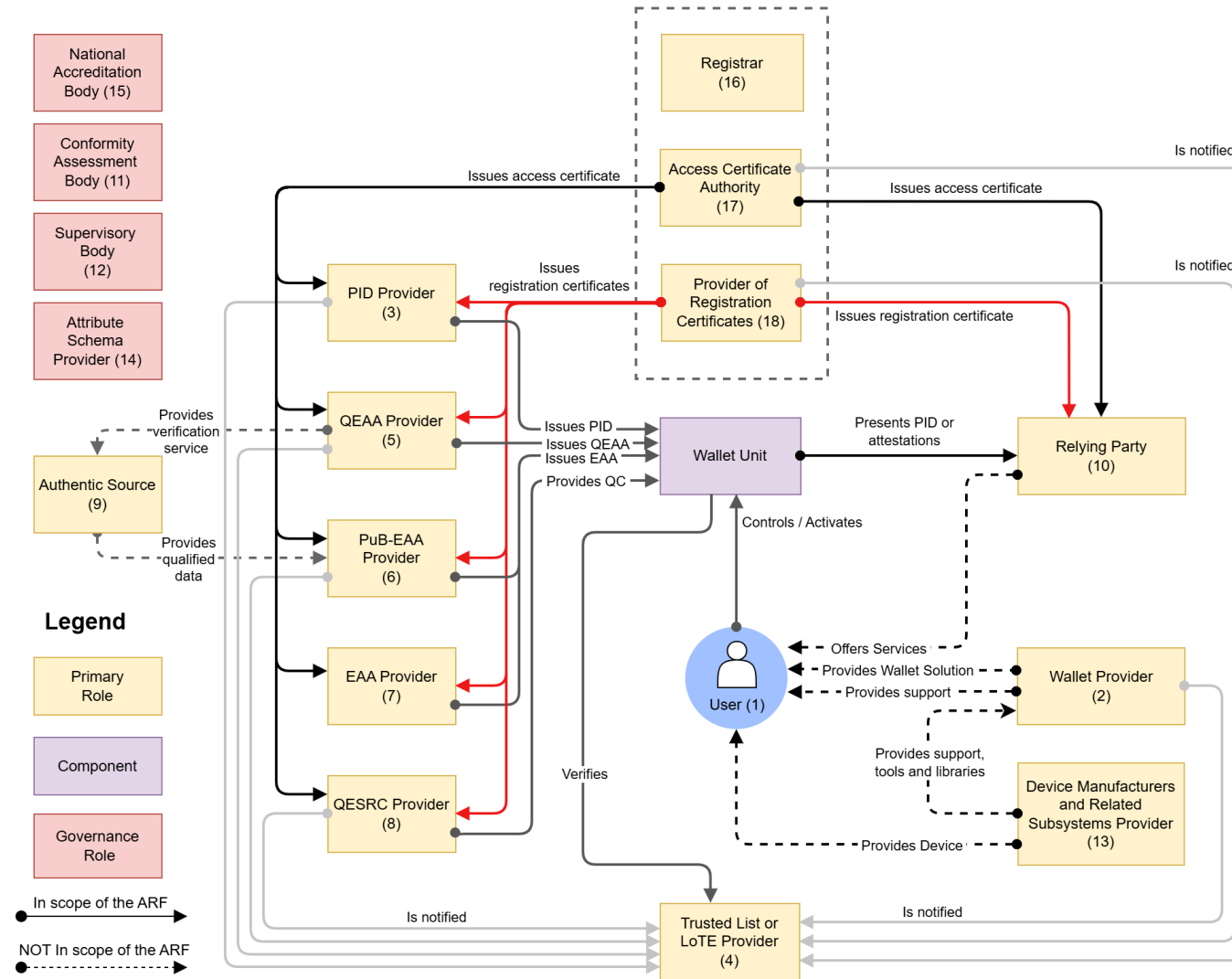


eIDAS 2.0 – Key Changes

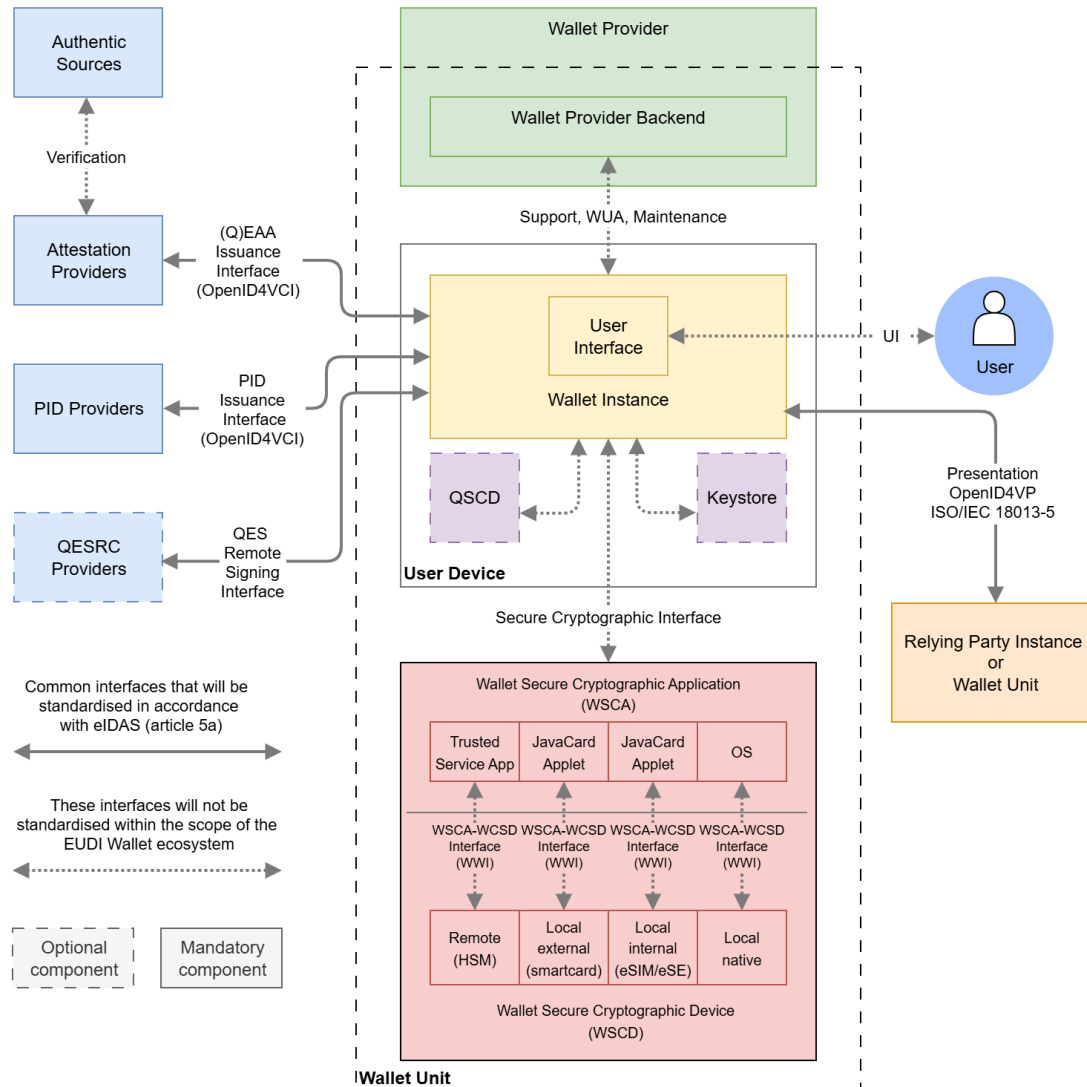
- Adopted: 11 April 2024 – in force from 20 May 2024
- Mandatory EUDI Wallet provision by all Member States
 - Member States must offer at least one EUDI Wallet by November 2026
 - Private sector relying parties in regulated sectors must accept it
- Expanded scope of trust services:
 - Electronic attestation of attributes (EAA)
 - Qualified EAA (QEAA) with qualified status
 - Electronic archiving (now a qualified trust service)
 - Electronic ledger services (eLedger)
- New actors in the ecosystem:
 - Wallet providers, PID providers, Authentic Sources, QEAA providers, Relying Party
 - Relying party registration and obligations
 - Certification of wallets
- Stronger enforcement: private sector must accept eID (for SCA)
- Enhanced data minimisation and unlinkability requirements



New roles within the eIDAS 2 ecosystem

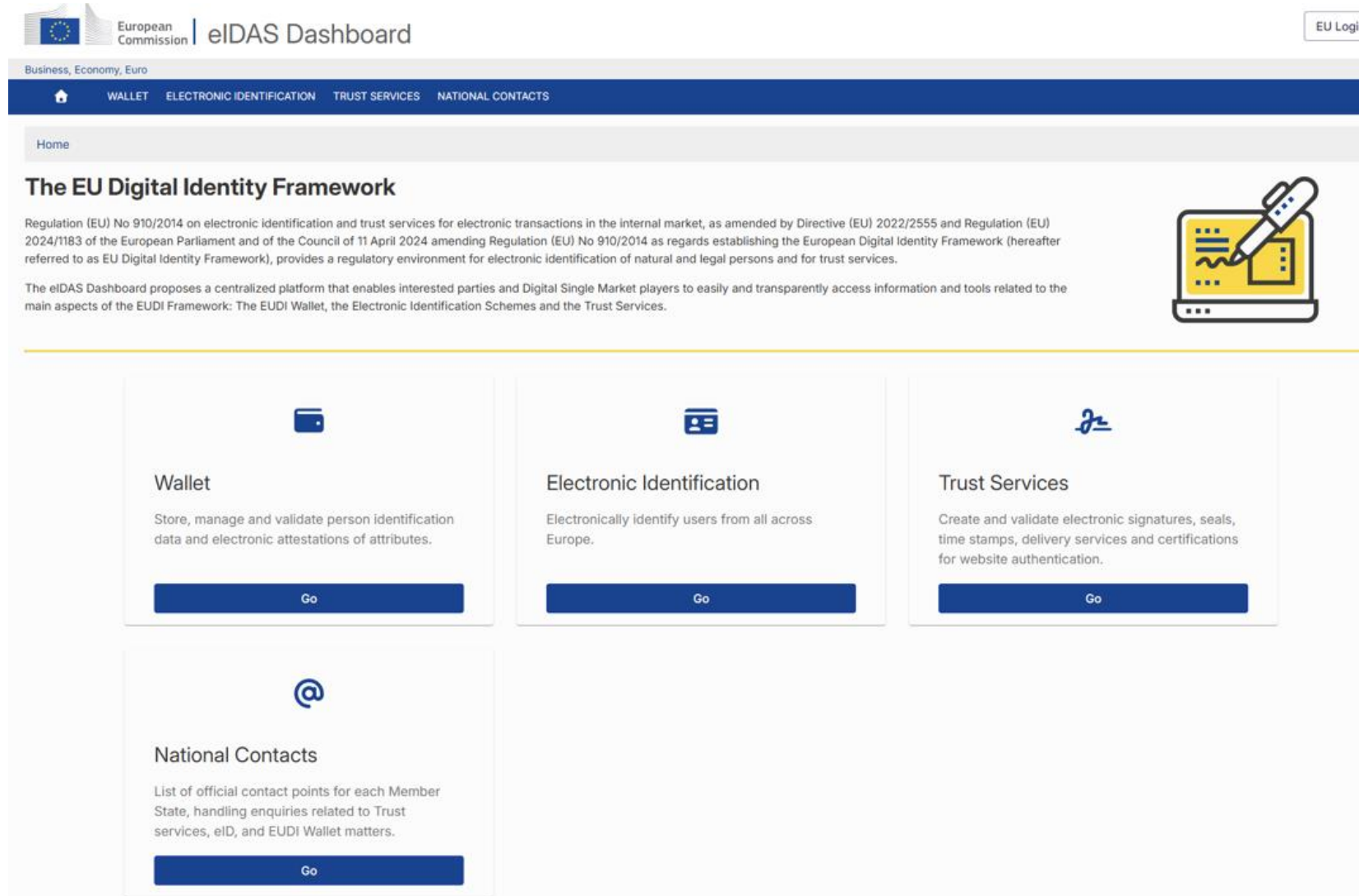


EUDI Wallet Architecture



What is the ARF?

- Technical blueprint for the EUDI Wallet ecosystem
- Developed by European Commission + Member State experts
- Published on GitHub (eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework)
- Versioned document
- Covers: architecture, data models, protocols, security
- Informs CIRs and standards development
- Not legally binding itself – implemented via CIRs



eIDAS Dashboard: Wallet Space Toolbox

Wallet Space toolbox

PID Providers

Access the list of Providers of Person Identification Data allowing users to onboard with their EUDI Wallet unit.

[Go](#)

Wallet Providers

Access the list of Wallet Providers.

[Go](#)

WRPAC Providers

Access the list of Providers of Wallet Relying Party Access Certificates that are necessary to ensure and verify the authenticity and validity of European Digital Identity Wallets.

[Go](#)

Registrars & Registers

Access the list of Registrars & Registers allowing users to access and verify the lists of parties relying upon the EUDI Wallet.

[Go](#)

mDL Providers

Access the list of Mobile driving license Providers allowing relying parties to verify the mobile driving licences.

[Go](#)

Other tools

Discover the Trust Services domain

Learn about the Trust Services domain: Electronic Signatures and Seals, Website authentication, Trusted Lists, International collaboration, and more...

[Go](#)

EU/EEA Trusted Lists Browser

Browse the Member States Trusted Lists containing their (Q)TSPs and the (Q)TSs they provide, including for the issuance of (Qualified) Electronic Attestations of Attributes.

[Go](#)

eIDAS-Network

Learn about the European Network enabling the cross-border Electronic Identification of the European Citizens.

[Go](#)

Overview of qualified trust services

[Home](#) / [Trust Services](#) / [Browse the eIDAS Lists](#) / [EU/EEA Trusted Lists](#) / [Search by type of service](#)

Search by type of service



Service status

☒ All services ☐ Exclude inactive services

Qualified trust services ☐ Check all

- | | | |
|--|---|---|
| ☐ Qualified certificate for electronic signature | ☐ Qualified certificate for electronic seal | ☐ Qualified certificate for website authentication |
| ☐ Qualified validation service for qualified electronic signature | ☐ Qualified preservation service for qualified electronic signature | ☐ Qualified validation service for qualified electronic seal |
| ☐ Qualified preservation service for qualified electronic seal | ☐ Qualified time stamp | ☐ Qualified electronic registered delivery service |
| ☐ Qualified remote management of qualified electronic signature creation device | ☐ Qualified remote management of qualified electronic seal creation device | ☐ Qualified electronic attestation of attributes |
| ☐ Qualified electronic archiving service | ☐ Qualified recording service of electronic data in qualified electronic ledgers | |

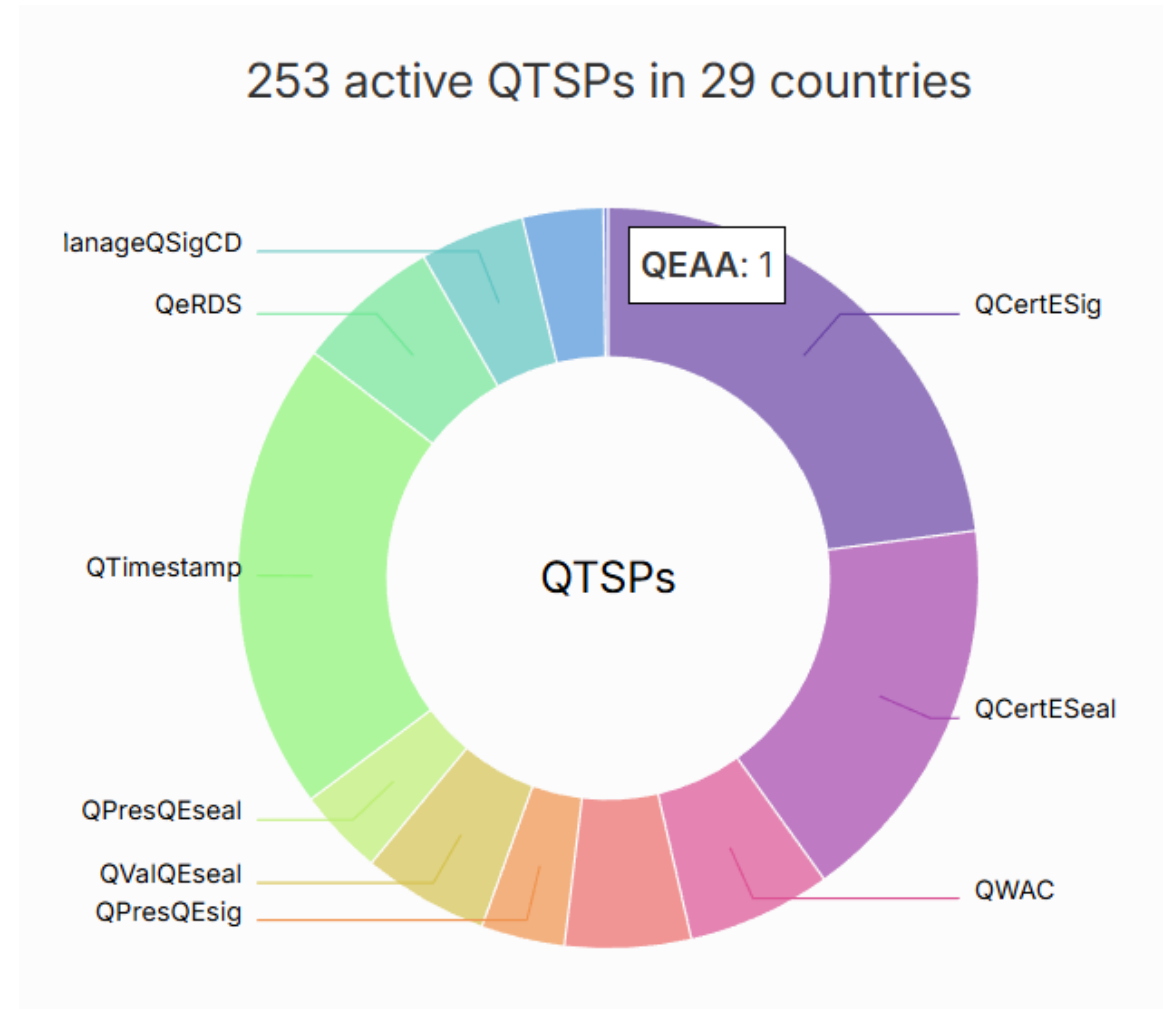
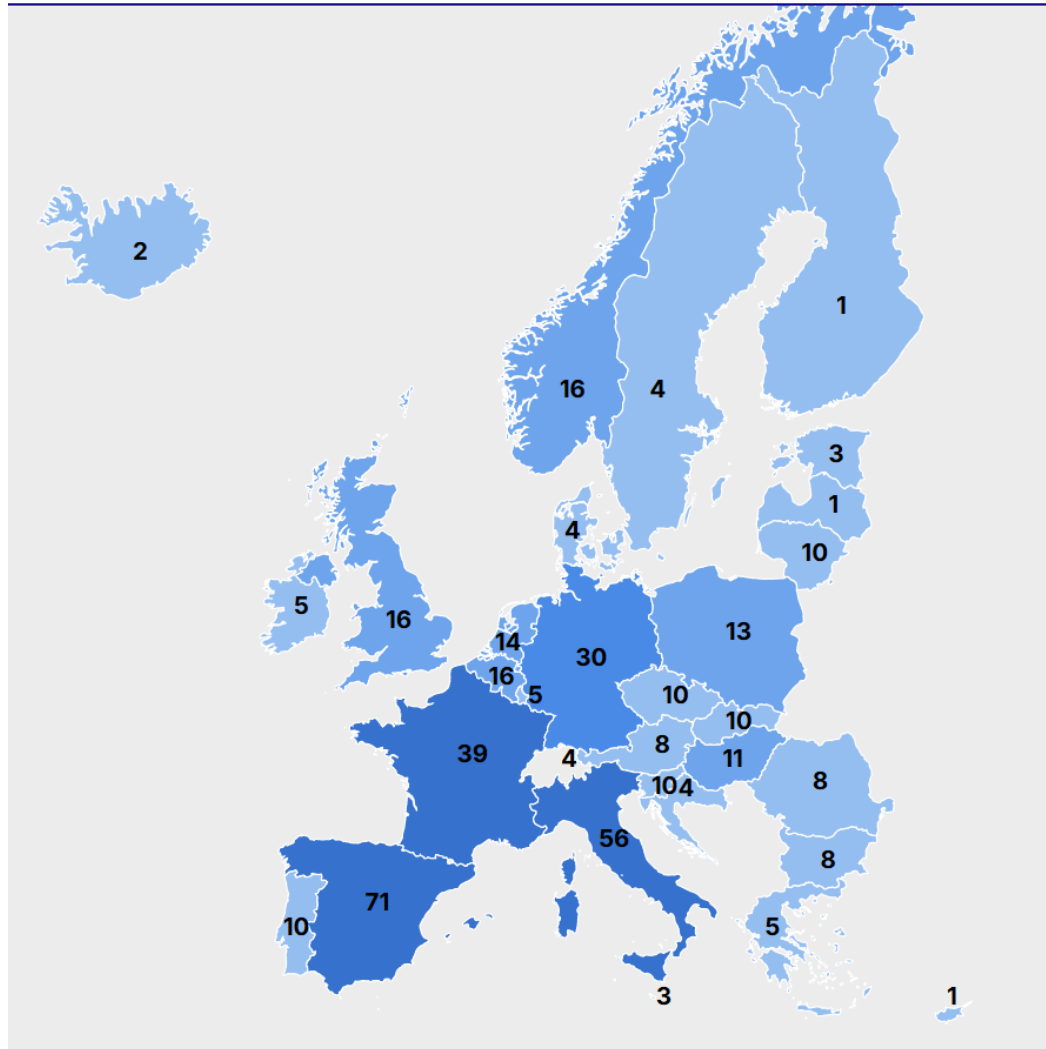
Current search

All services

No service selected

No country selected

Active QTSPs in Europe



Trust Service Providers – Roles & Responsibilities

Non-Qualified TSPs

- Provide trust services without qualified status
- No mandatory audit
- Not subject to supervisory body oversight
- No mandatory entry in Trusted Lists (TSL)
- No legal presumption of compliance
- Subject to general data protection / liability rules
- May offer AdES-level services (e.g. Advanced eSignature)
- Compete in open market without qualification overhead

Qualified TSPs (QTSPs)

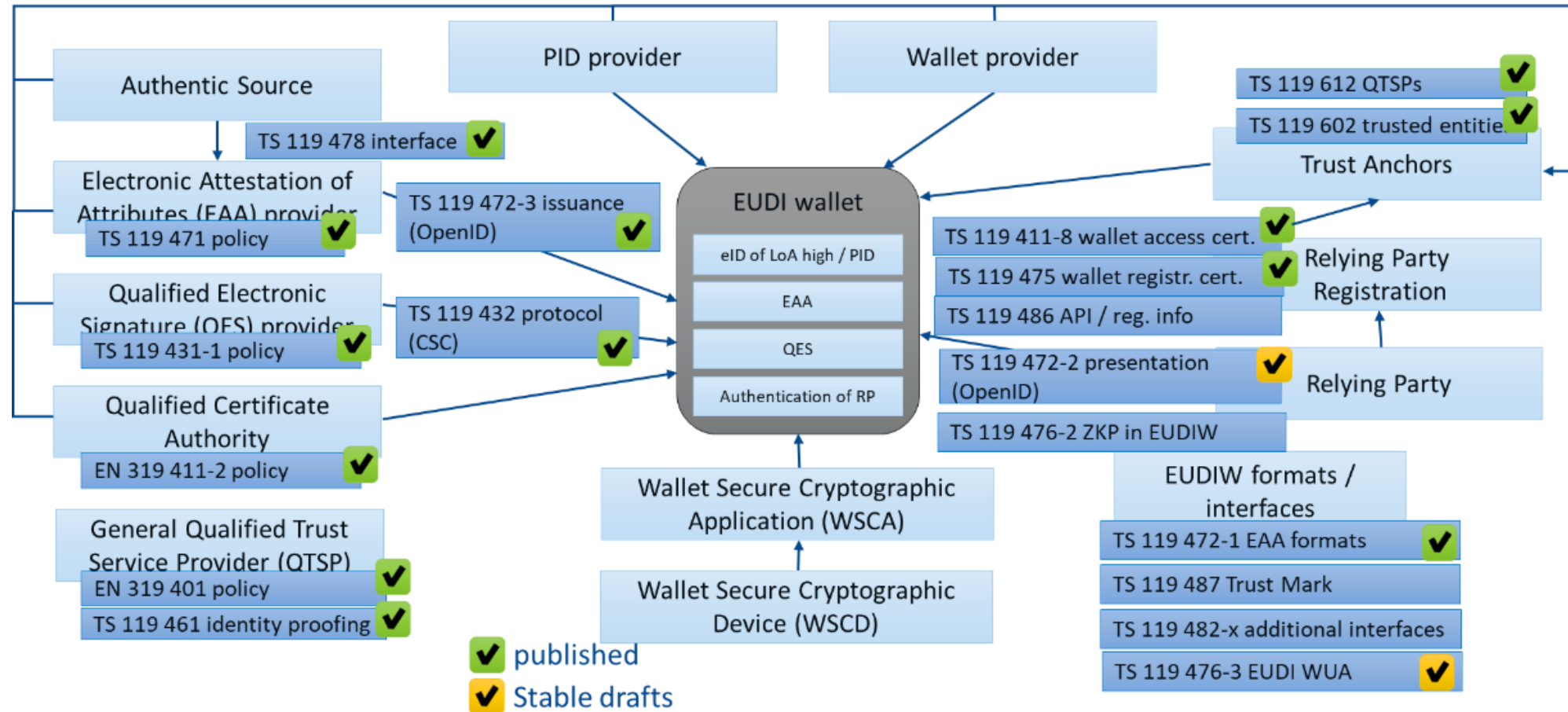
- Granted qualified status by supervisory body
- Listed in national Trusted List (TSL)
- Undergo conformity assessment by accredited CAB
- Annual audits (EN 319 401 + service-specific standards)
- Strict requirements: security, personnel, infrastructure
- Services carry full legal presumption of compliance
- Entitled to use EU Trust Mark
- Must notify supervisory body of security breaches

General Requirements

- EN 319 401 – General Policy Requirements for TSPs
 - Covers: security management, operations, human resources, physical security
- EN 319 411 – Policy and security requirements for Trust Service Providers issuing certificates
- TS 119 461 – Policy and security requirements s for trust service components providing identity proofing

+ Service-Specific Standards

Already available ETSI standards for the EUDIW ecosystem



Qualified, motivated, cross-competency team with a strong background and experience in:

- Law (national, European and international framework conditions)
- Technology (full stack, wallets, HSM, trusted cloud, standards)
- Procedural (certification guidelines, governance, remote procedures, audit, relevant standards)
- Security and availability (inside the perimeter and web-based status services)
- Trusted applications and best practice
- Crypto (performance, long-termism, agility, PQC, key generation)
- Team-oriented project management



Arno Fiedler,
Managing
Director &
Senior Expert



**Franziska
Granc,**
Principal
Consultant



Thank you!