

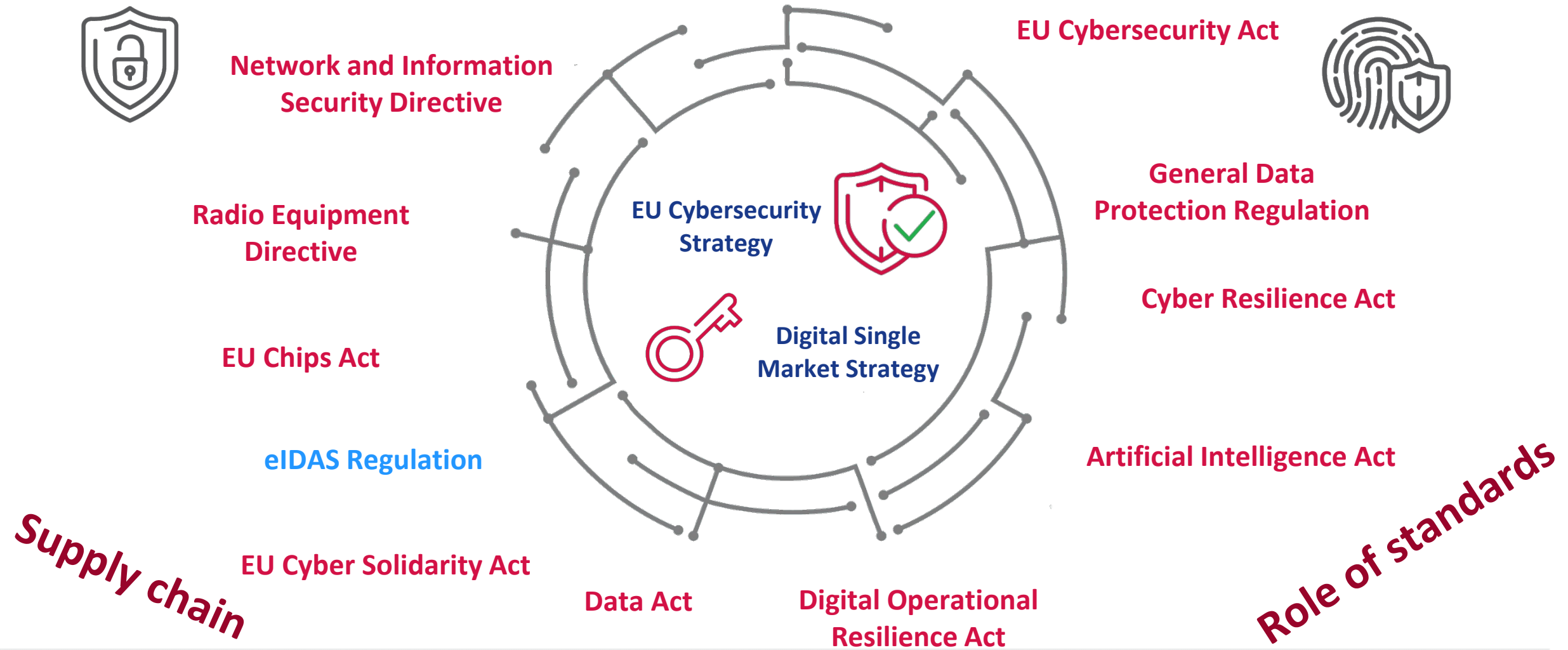
ETSI ESI: Electronic Signatures and Trust Infrastructures Standards Update

CA/B Forum Tokyo— March, 25th 2025

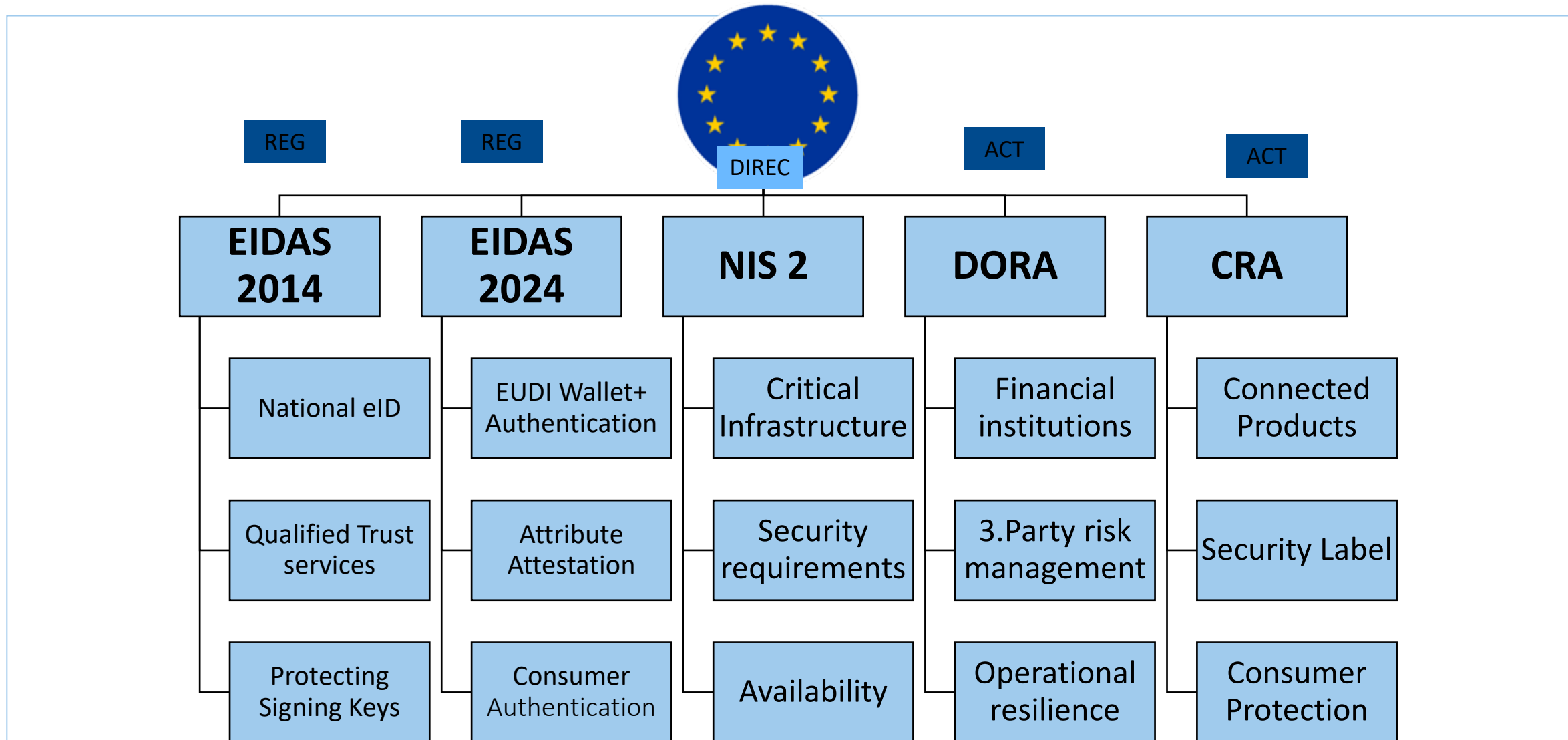
Presented by: Arno Fiedler – Vice chair ETSI ESI



EU LEGISLATION – CYBERSECURITY LANDSCAPE



PKI relevant European Regulations in 2025



First Quarter of 2025: Maintenance of Existing Standards

Trust services general:

- Conformity Assessment ✓
- Policy & security (NIS2) ✓ *
- Identity proofing ✓

Trust services for:

- Issuing certificates ✓ *
- Time Stamping ✓
- Signature creation services ✓ *
- Signature validation services ✓
- Open Banking ✓

AdES creation & validation

- Part 1: procedures ✓ *
- Part 2: signature validation report ✓

CC Protection Profiles

- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

319 40x,
461
Trust services general

119 6xx
Trust service status lists

x19 4xx
TSPs supporting
digital signatures

x19 5xx
Trust application
service providers

x19 1xx
Signature Creation
& Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework

Trusted list ✓

- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓
- General trusted list model and processing (new)

Trust services for:

- Registered eDelivery / eMail ✓
- Long term preservation ✓

Formats:

- XAdES (XML) ✓ *
- CAdES (CMS) ✓
- PAdES (PDF) ✓
- ASiC (containers) ✓ *
- JAdES ✓ *
- CBOR AdES (new)

Signature suites ✓ *

- Hash
- Asymmetric crypto
- Key generation
- Lifetime

Schema for algorithm catalogues ✓

- Standards framework ✓ *
- Common definitions ✓
- Guides ✓

Completed

* Update in progress

(new) New

EN 319 401 – General Policy Requirements for TSPs

Update aimed to align with NIS2

- New version 3.1.1 published 2024-06
- Aims to fully align with NIS2 implementing act
- Updated EN 319 401 incorporated by reference from all TSP Policy standards
- Other standards which follow general topics structure unaffected.

Supports ACAB's strategy for single audit covering NIS2 and eIDAS (and DORA via update in late 2025)

TS 119 461: Identity Proofing finalized

- New Extended LoIP (Level of Identity Proofing)
- Strengthening requirements for threats and risk assessment and for keeping solutions up to date
 - Threats intelligence process, pointing at ENISA “Methodology for sectoral cybersecurity assessments” as a hint towards future cybersecurity certification requirements
- Adding requirements to enhance Baseline LoIP to reach Extended LoIP
- New Annex C on requirements for identity proofing for eIDAS qualified trust services
 - Qualified certificates according to eIDAS v1
 - Qualified certificates and qualified electronic attestation of attributes for eIDAS v2
 - Qualified registered delivery same for eIDAS v1 and eIDAS v2
- References CEN standard on biometric injection attack detection for remote registration

EN 319 411-1/2 Certificate Policy Updates

➤ EN 319 411-1 General Requirements

- Key ceremonies
- Identify last CRL issued (on termination)
- Alignment with EN 319 401 NIS2 version

➤ EN 319 411-2 Qualified

- Support for validity assured / short term certificates
- Alignment with CAB Forum Extended Validation

EN 319 412-x Certificate Profile Updates

➤ EN 319 412-1

- NTR trade identified region identifier
- Alignment with EN 319 401 NIS2 version

➤ EN 319 412-2 Natural person

- Status services for validity assured / short term certificates
- Clarification on identification common name vs given name and pseudonym
- CAB Forum OCSP alignment

➤ EN 319 412-5 QC Statement

- QC Statement on verification method (whether have used QES)
- ASN.1 encoding of non-EU QSCD

- EN 319 142-1 PadES : Updates to align with the latest version of ISO 32000 (pdf)
- EN 319 132-1 XAdES (XML): Changes includes update to archive timestamp
- EN 319 162-1 Associated Signature Container (ASiC):
Adding alternative forms (e.g. time assertion),
- TS 119 182 JAdES (JSON) Changes includes replacing claimed signing time:
sigT with *iat* to facilitate IETF alignment
- TS 119 152 CB-AdES (CBOR):
Adopting IETF allocation of numbers to new header parameters
- EN 319 102-1: AdES Signature creation and Validation : 17 Detailed changes
- TS 119 172-4 -1: Validation Policy on EU Qualified e-Seals and e-Signatures:
Remain open issue on revocation checks on preserved signatures

QWACs Spec ETSI TS 119 411-5 finalized

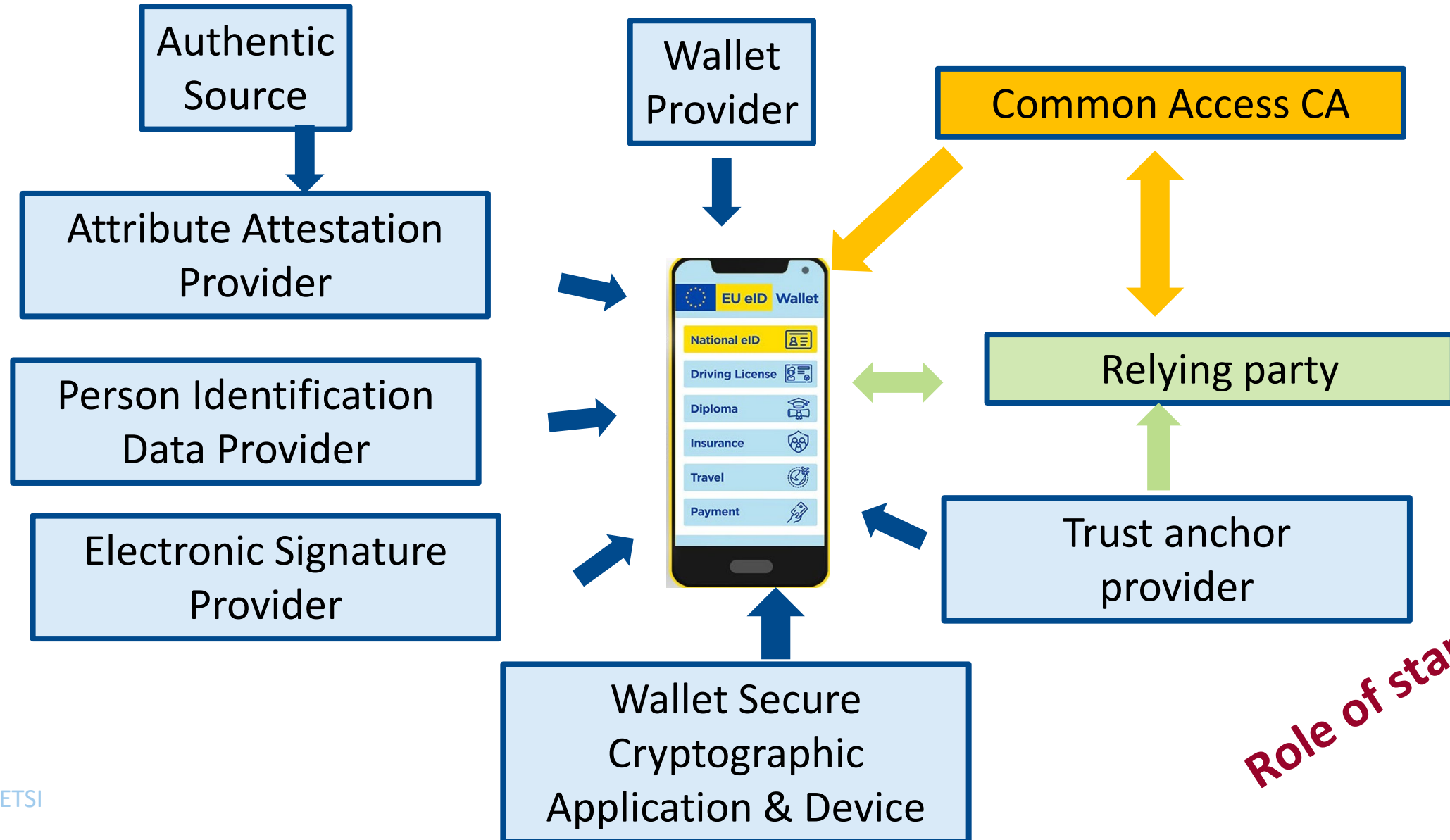
The TS defines multiple approaches for issuing qualified certificates for website authentication, deploying them to websites, and their consumption by user agents.

- 1. “1-QWAC Approach”: Single certificate that meets both browser root store **and** EU Qualified requirements both aligned with CA/Browser Forum requirements
- 2. “2-QWAC with Certificate Binding Validation Approach”
 - EU Qualified Certificate signed binding to TLS Certificate
 - + TLS Certificate meets browser root store requirements aligned with CA/Browser Forum requirements
 - Browser validates TLS Certificate against binding

EU Certificate Transparency Ecosystem: NWI at ESI

- Title:
Requirements on a Certificate Transparency (CT) Ecosystem to make the issuing of certificates transparent and verifiable
- Scope and Field of Application:
Report on existing Certificate Transparency approaches and on standardisation requirements for equivalent of Certificate Transparency as specified in RFC 6962 and concepts such as Static Certificate Transparency supporting log of certificates, as defined in amended Regulation (EU) 910/2014
- Supporting Organizations:
Microsec Ltd, Nimbus Technologieberatung, Google Ireland Limited, DigiCert, Sectigo, ESD, D-TRUST (Enrico Entschew)

Main components and Interfaces for EUDI Wallet:



Role of standards !

[←](#) [→](#) [↺](#) [🏠](#) [https://github.com/orgs/eu-digital-identity-wallet/projects/29/views/2](#) [🔍](#) [★](#) [📧](#) [A](#) [📌](#) [☰](#)

☆ ELSTER - Login mit Per... 🌐 SAP Ariba Sourcing 🔄 ETSI - ESI Training 🌐 OpenID4VC High Assu... ⚙️ CLAYS. Mein Körper... 🗣️ DeepL Übersetzer: Der... 🕒 Time Converter and W... 🇩🇪 Nimbus Technologieb... ➡️

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing 🔍 Sign in Sign up

🌐 STS Roadmap Increased items preview [Feedback](#)

Board ▾ List | Roadmap | Gap status

Responsible body ▾

- ISO 46
- CEN 12
- ETSI 65
- W3C 3
- OIDF 6
- IETF 17
- CSC 1
- EC 15
- ENISA 3

🔍 -label:wontfix 193 ✕ Discard

○ 📋 **Backlog** 57

The STS has been identified as relevant to EUDI Wallet requirements, but no suitable standard is currently available.

🟡 🛠️ **In progress** 67

A relevant STS exists, but gaps have been identified, or the document is incomplete. Work is actively being done to address the gaps.

🟢 ✅ **Done** 69

The identified STS has reached a stable version and is currently considered a Candidate, meaning no gaps have been identified, but final assessment is pending.

▼ **01. Milestone 1** 96 ...

Item ID	Title	Status	Labels	Due Date
eudi-doc-standards-and-technical-specifications #24	EC (4.2.12) Data Portability and Download (export)	In Progress	Art 5a(4)(f), Art 5a(4)(g), Fn: Utilities, gap	Nov 30, 2025
eudi-doc-standards-and-technical-specifications #268	EC (4.2.16) Zero-Knowledge Proof (ZKP) Implementation in EUDI Wallet	In Progress	Art 5a(23) ICF, Fn: Privacy, gap, locked	Nov 30, 2025
eudi-doc-standards-and-technical-specifications #327	EC (4.2.17) Relying Party Registration Certificates	In Progress	Art 5b, gap, locked	Nov 30, 2025
eudi-doc-standards-and-technical-specifications #17	EC (4.2.4) Specification of the Wallet Unit Attestation (WUA)	In Progress	Art 5a(23) ICF, Essential, Fn: WUA, gap	

Sep 30, 2024

🟢 eudi-doc-standards-and-technical-specifications #25
BSI: PP-0104 - CSP: Cryptographic Service Provider EAL4+

Art 5c, Fn: SE, locked, std: PP, sts: ready

MSP Pending, BSI, Feb 28, 2019

Sep 30, 2024

Further information

Information on available standards and current activities:

<https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx>

ETSI standards: available for free download

<http://www.etsi.org/standards-search>

CEN standards: available through National Standards Organisations

Updates on standardisation:

https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

Next ESI Meetings:

25.-28.05.25 Sophia Antipolis, France

16.-18.09.25 Bilbao, Spain

24.-25.09.25 Split Croatia, CA-Day+TSF,

