The Standards People

ETSI Standards Update

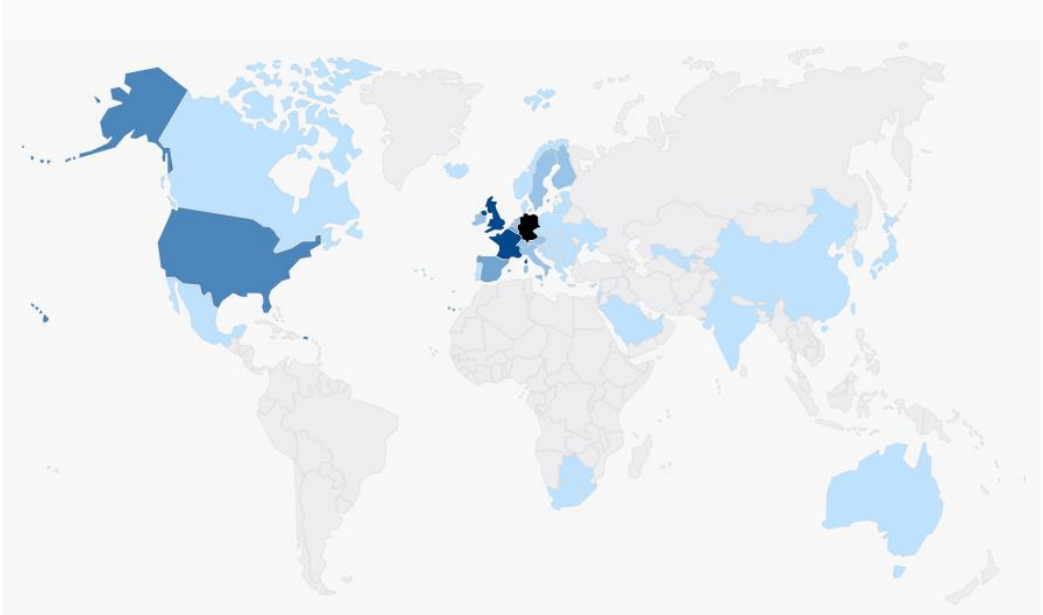
CA/B-Forum #61 New Dehli

Presented by: **Arno Fiedler – Vice Chair ETSI ESI**

arno.fiedler@outlook.com

ETSI – European Standards Organisation with Global Reach

- 900 member organizations worldwide, drawn from over 60 countries and five continents
- Cooperation with India via:
  Telecommunications Standards Development Society https://tsdsi.in/
- Global PKI related partnerships:
  - CA/Browser Forum
  - Asia PKI Consortium
  - Japan Network Security Association
  - Arab-African e-CA Network
  - Cloud Signature Consortium



- Recent Signature Interoperability event:
  - 100+ organisations inside and outside

ETSI & CEN Standards supporting eIDAS – the overall picture

Trust services:
- TSP Audit ✓
- Issuing certificates ✓ ✓ (rev)
- Time Stamping ✓ ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓ (upd)
- Open Banking ✓ (upd)
- Support for NIS 2 (new)
- S/MIME ✓ (new)
- Attribute Attestations (new)

- AdES creation & validation
  - Part 1: procedure ✓ (upd)
  - Part 2: signature validation repo ✓ (rev)

- CC Protection Profiles ✓
  - QSCD - Smart Cards ✓
  - HSM used as QSCD ✓
  - HSM used by TSPs ✓
  - Remote QSCD ✓

119 6xx
Trust service status lists
- Trusted list ✓
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered eDelivery / eMail ✓ (upd)
- Long term preservation ✓

Interop tests

x19 1xx
Signature Creation & Validation

Formats + Interop test:
- XAdES (XM ✓ (rev)
- CAdES (CM ✓ (rev)
- PAdES (PD ✓ (upd)
- ASiC (containers) ✓ (upd)
- JAdES (JSON) ✓ (upd)
- CB-AdES (CBOR) (new)

419 2xx
Signing Devices

119 3xx
Cryptographic suites
- Signature suites ✓ (upd)
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new) ✓

119 0xx
General Framework
- Standards framework ✓ *
- Common definitions ✓
- Guides ✓

✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

Trust services issuing certificates

Trust services:
- TSP Audit ✓
- Issuing certificates ✓ ✓*
- Time Stamping ✓
- Signature creation serv
- Signature validation ser
- Identity proofing ✓*
- Open Banking ✓
- Support for NIS 2 (new)
- Attribute Attestations (new

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validatio

CC Protection Profiles
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

✓ Completed
* Update in pro
(new) New

- EN 319 411-x Cert Policies: ETSI Approved –
  - Part 1: 16 changes to policies for issuing certificates
  - Part 2: 5 changes to policies for issuing qualified certificates
  - Alignment with CA/Browser Forum
- EN 319 412-x Cert Profiles: ETSI Approved –
  - 1 changes to EN 319 412-1 (General) & 7 changes EN 319 412-2 (Certificates issued to natural persons)
  - EN 319 412-4 (Website authentication) CA/Browser Forum alignment
- TR 119 411-5 Co-existence Browser Root store and EU Trust List (QWAC)
  Discussions continue on 2 certificate approach
- TS 119 411-6 alignment with CA/Browser forum S/MIME certificates
  Published

Trust Services – ID Proofing

Trust services:
- TSP Audit ✓
- Issuing certificates ✓*
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓*
- Open Banking ✓
- Support for NIS 2 (new)
- Attribute Attestations

119 6xx

Trust service status lists

Trusted list ✓

Using & interpreting trusted list ✓

d list ✓

il ✓*

✓

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validation

CC Protection Profiles
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

logues (new) ✓

Guides ✓

TS 119 461 Identity Proofing v1.1.1
- Published July 2021
- Incorporated in latest EN 319 411-1/2
- Widely adopted
- Being used a general basis for ID Proofing

TS 119 461 Update including:
- (Qualified) Electronic Attestation of Attribute.
- Identity assurance level 'high'
- Support identity proofing for EUDI Wallet

✓ Completed

* Update in progress

(new) New

Trust Services & NIS 2

Trust services:

- TSP Audit ✓
- Issuing certificates ✓ ✓*
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services
- Identity proofing ✓*
- Open Banking ✓
- Support for NIS 2 (new)
- Attribute Attestations (new)

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validation

CC Protection Profiles

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

✓ Completed

* Update in prog

(new) New

NIS2 and Trust Services:

- Revised EN 319 401: General Policy Requirements for Trust Service Providers, Aim to specify in a way which does not require update to existing trust service standards

under National EN approval until May 2024

More details by Clemens Wanko

Use of Trusted Lists

Revised TS 119 615: Procedures for using and interpreting European Union Member States national trusted lists

- Published
- Further updates planned to take into account Third Country AdES Trusted List e. g- Ukraine

Revised TS 119 172-4: Validation policy for European qualified electronic signatures/seals using trusted lists

General Framework

- Trusted list ✓
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓

Trust services for:
- Registered eDelivery / eMail ✓*
- Long term preservation ✓

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

- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new) ✓

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

✓ Completed
* Update in progress
(new) New

See you:

TSF Forum	25.09.24
CA-Day	26.09.24

Heraklion, Crete

Further information

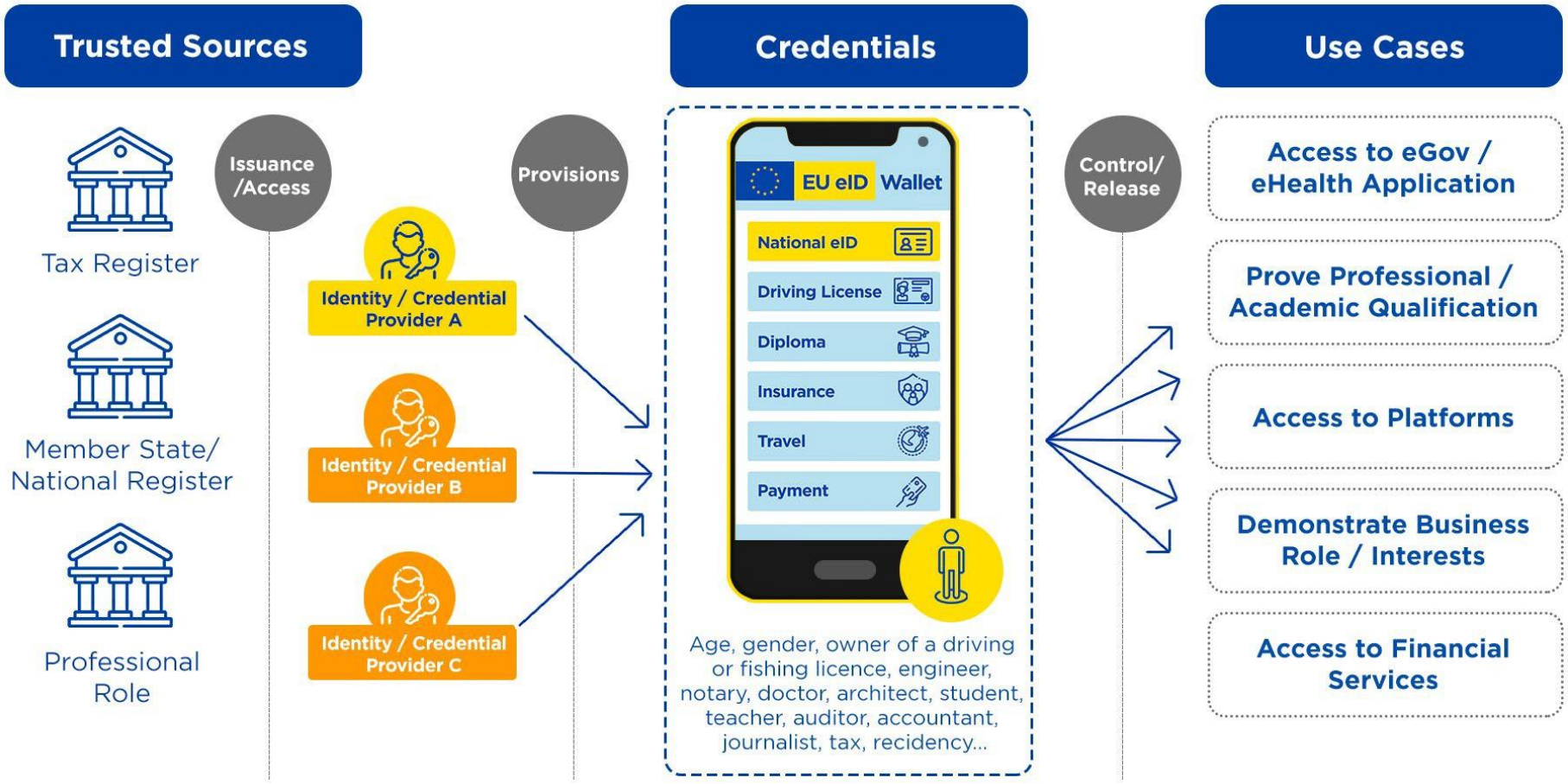
Information on available standards and current activities:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI standards: available for free download
http://www.etsi.org/standards-search

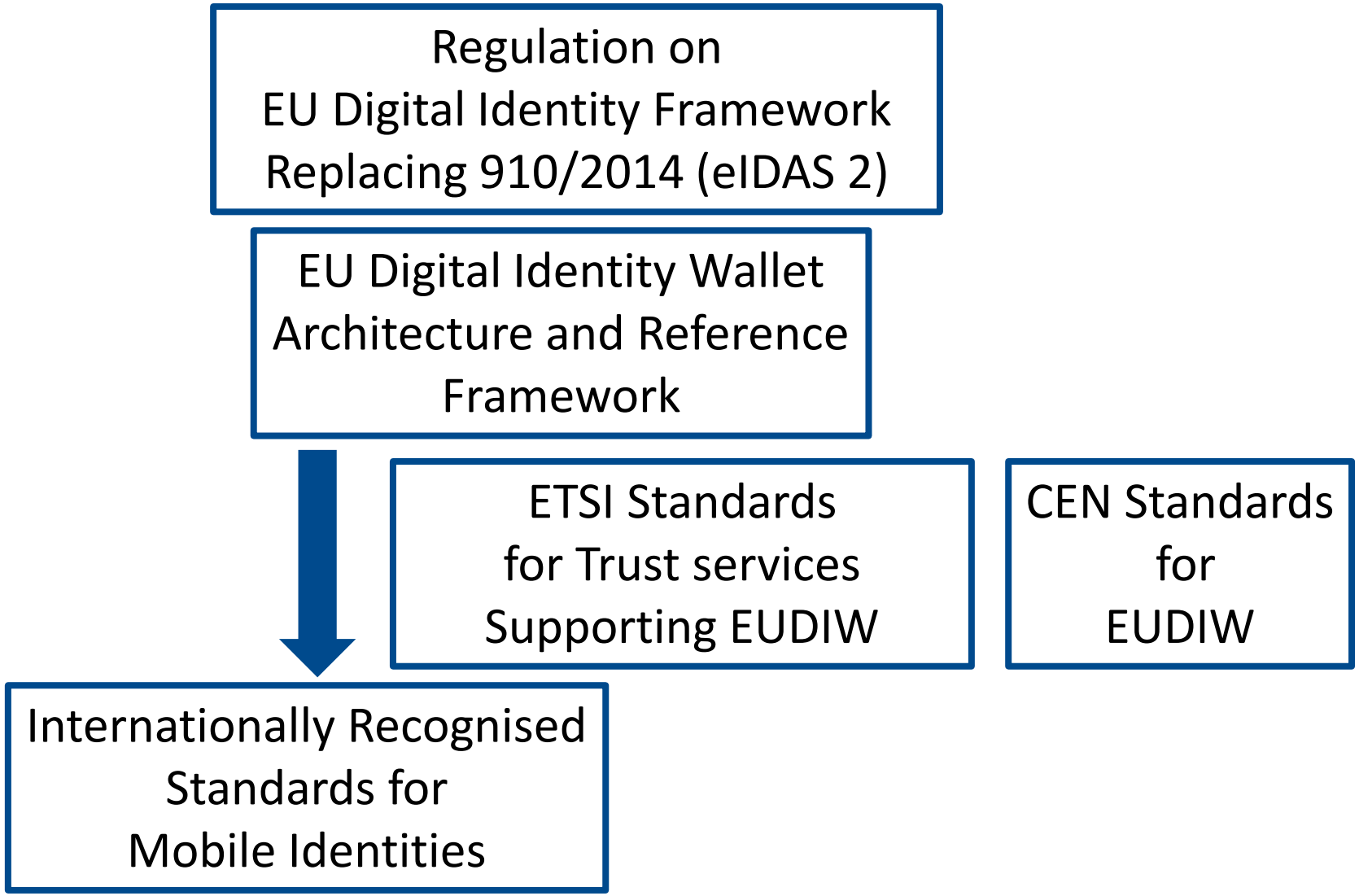
eIDAS 2024 related activities


National eID
TSPs
attestation attributes
EU eID Wallet
National eID
Driving License
Diploma
Insurance
Travel
Payment
SELECTIVE DISCLOSURE
proofs of identity / attributes
SERVICE PROVIDERS
WWW
BANK

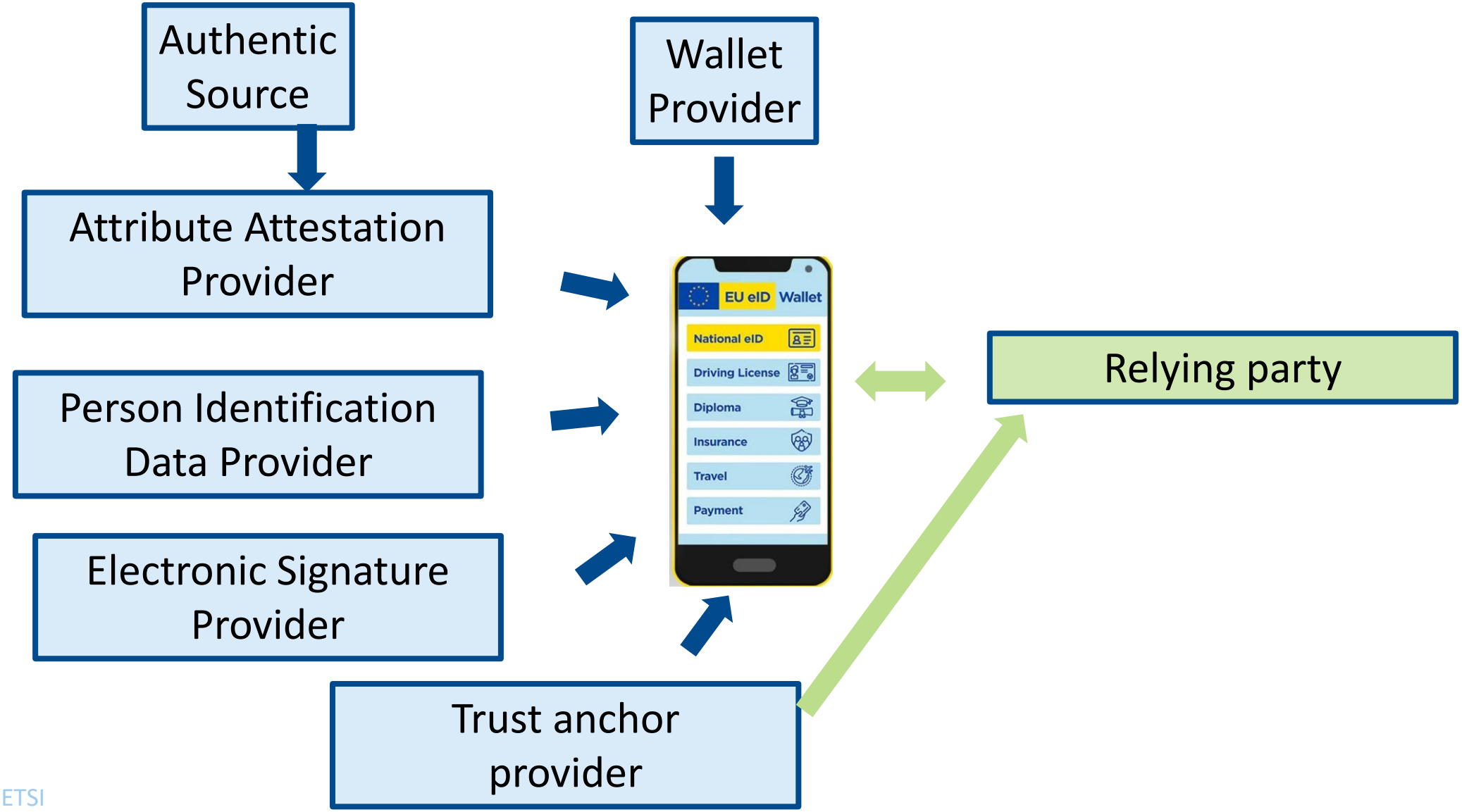
EUeID - Ecosystem



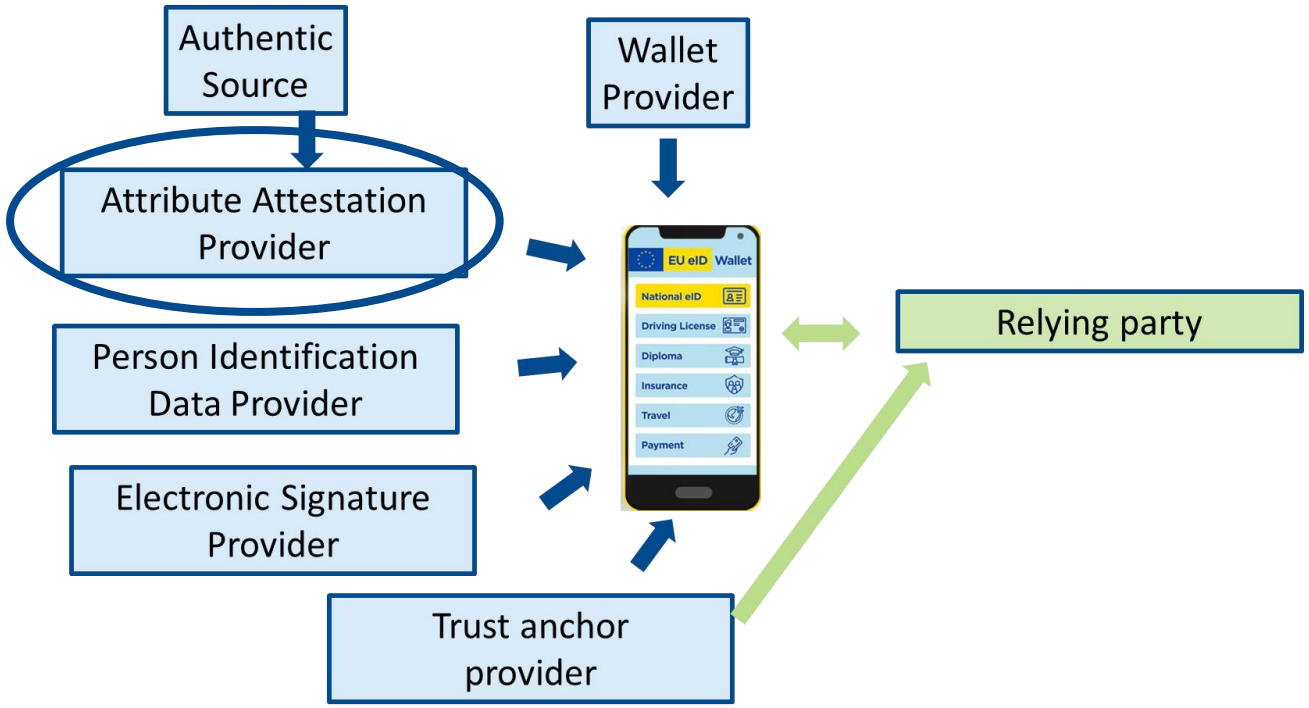
Standards & EU Digital Identity Wallet



Main components and Interfaces for EUDI Wallet



ETSI Standards for Electronic Attestation of Attributes



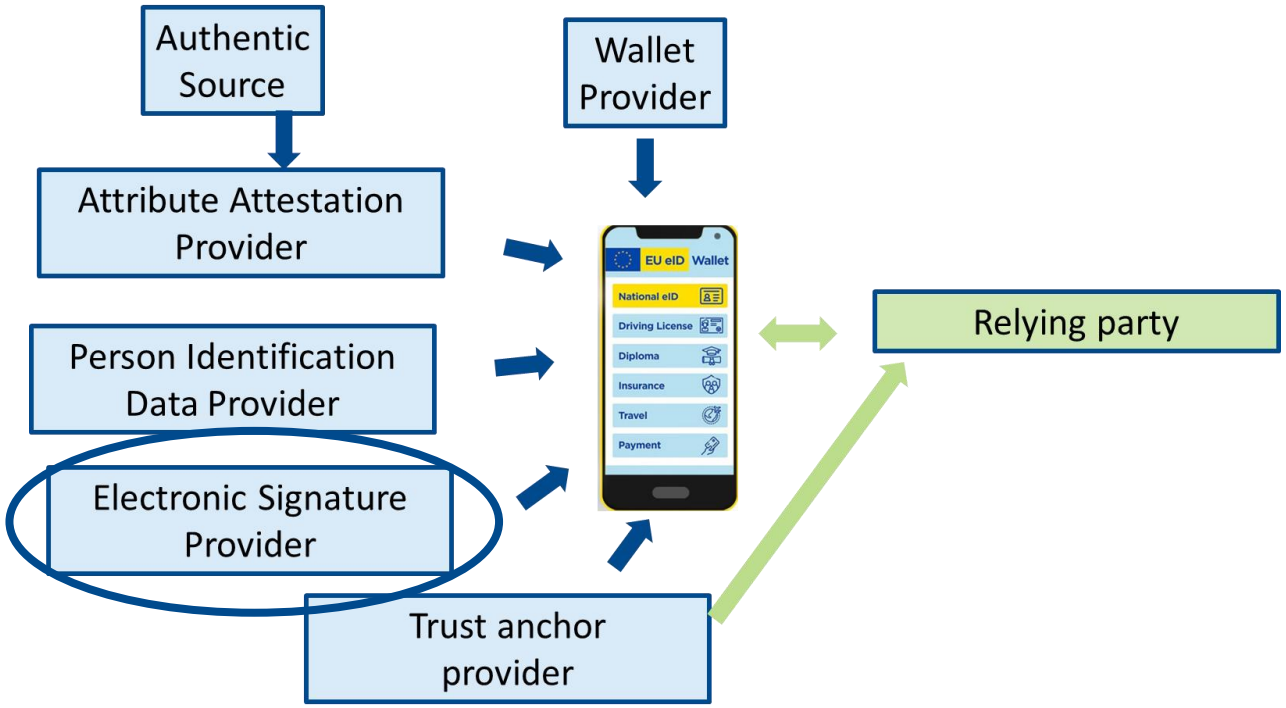
Existing TSP standards

- EN 319 401: General TSP policy & security requirement (NIS2)
- EN 319 403:TSP conformity assessment

To be specified

- Policy and security requirements
- Profile of internationally recognised standards
- Support for selective disclosure
- Interface to wallet

ETSI Standards for Electronic signature



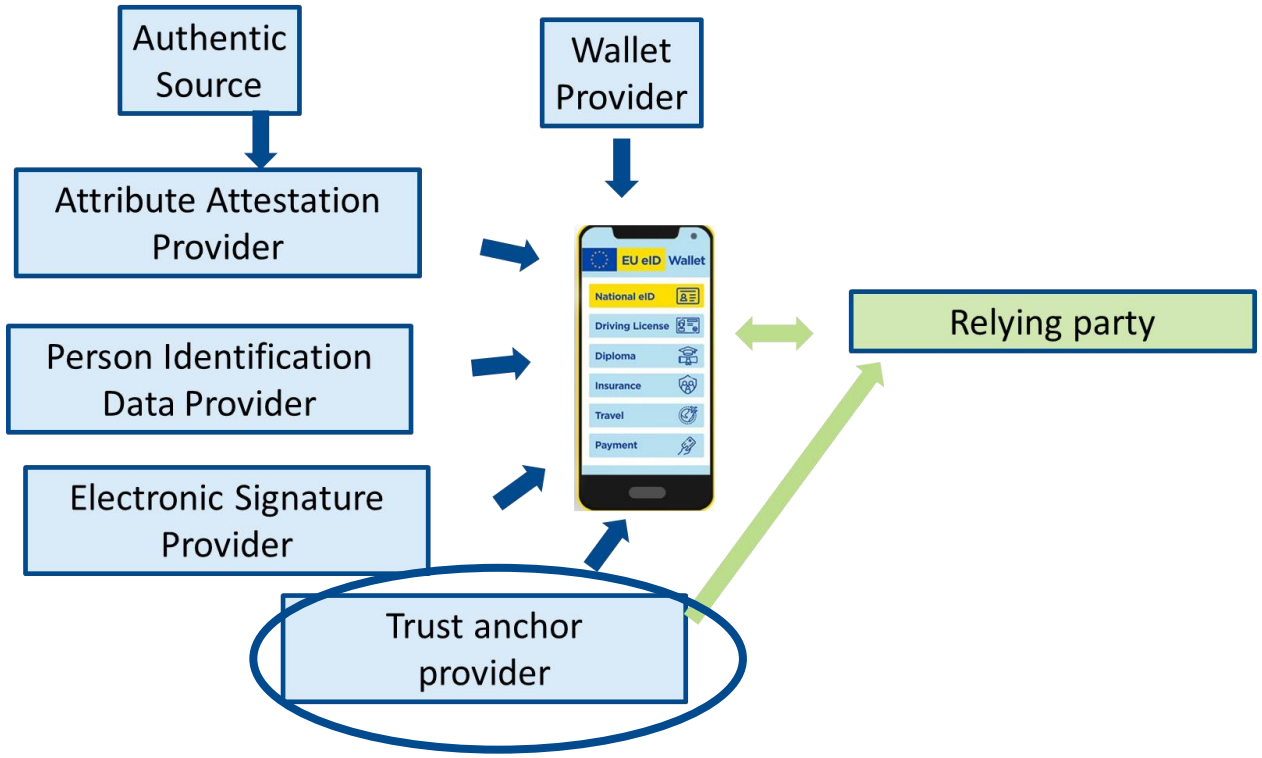
Existing standards

- EN 319 411-1 & -2: Policy & security standards
- EN 319 412-x: Certificate profiles
- TS 119 431 & 432: Remote signing

To be specified

- Wallet interface

ETSI Standards for Trust anchors



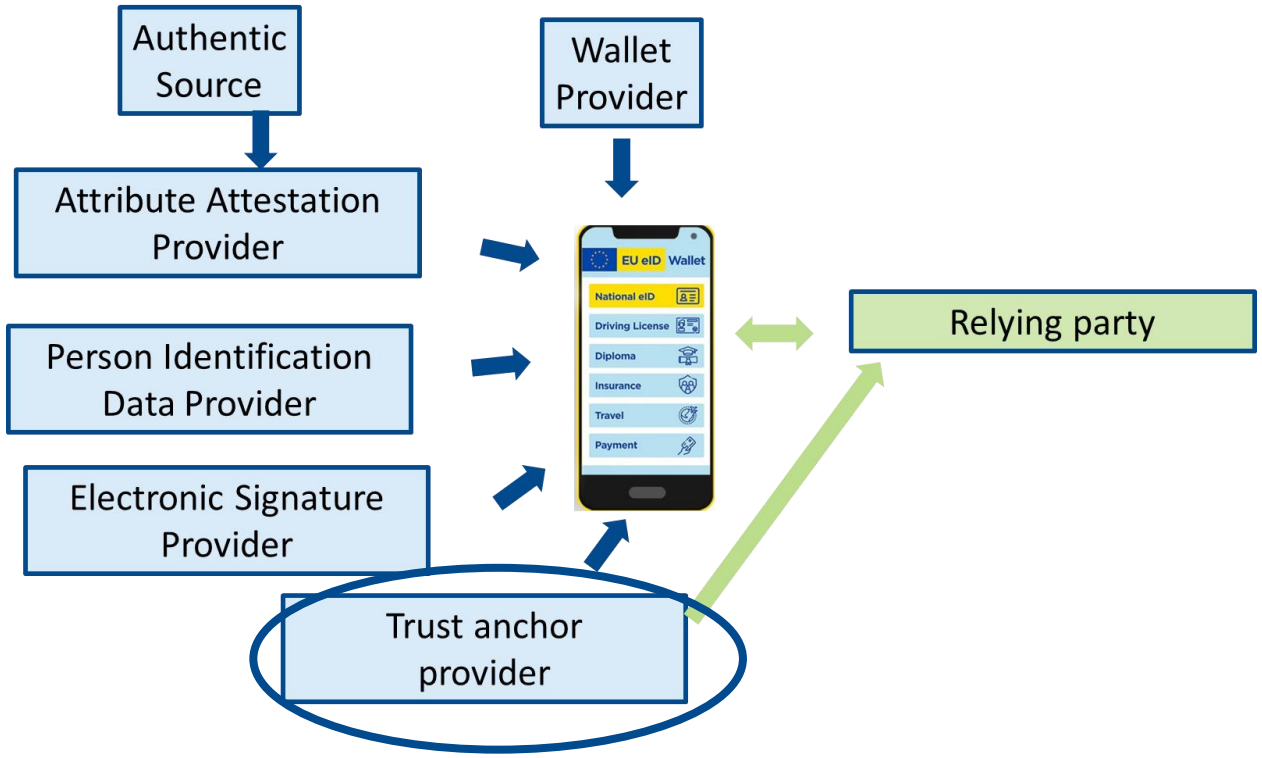
Existing

- TS 119 612: Trusted list
- TS 119 615: Using trusted lists

To be specified:

- Support for new trust services
- Support for other trust anchors

ETSI Standards for Trust anchors



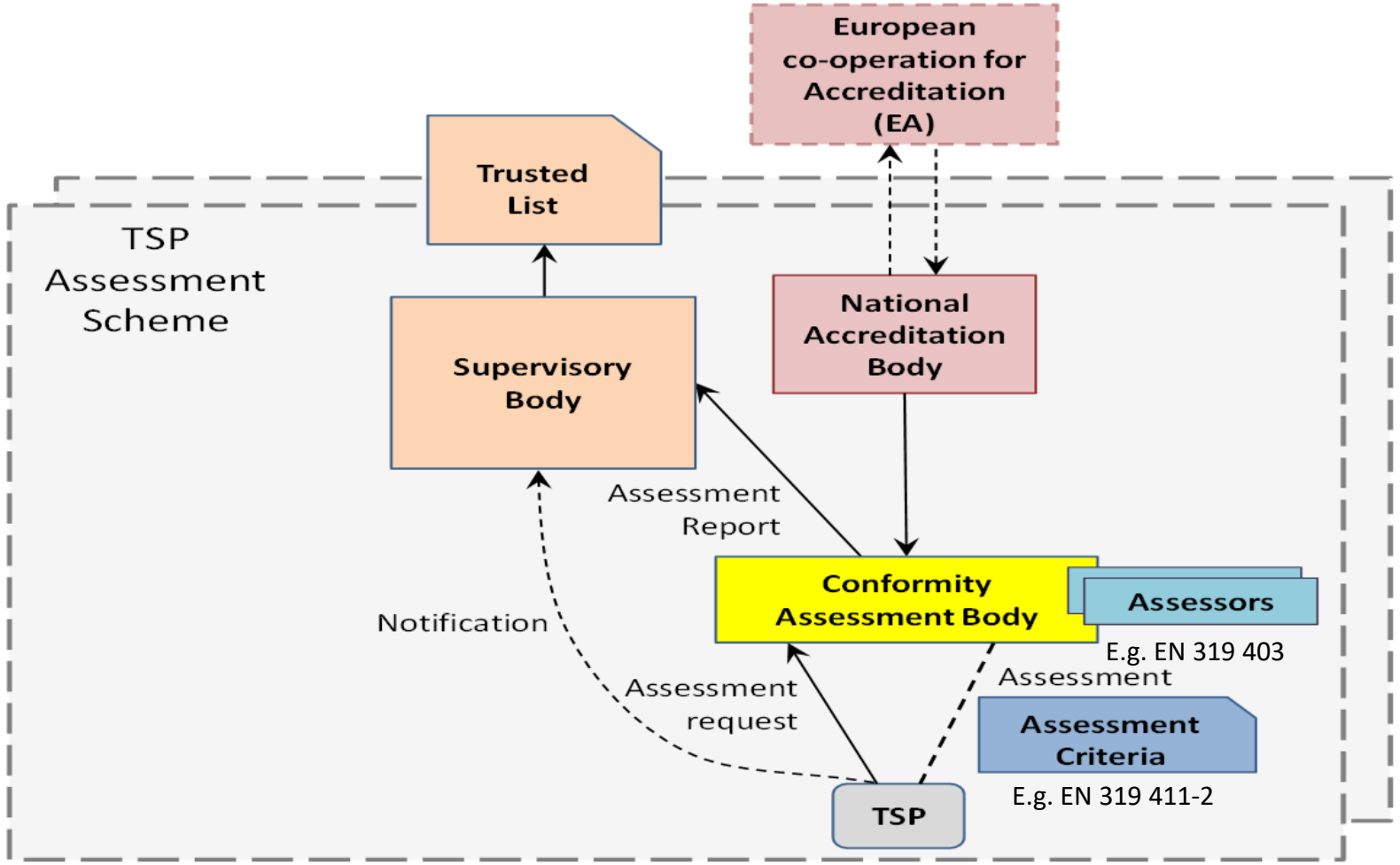
Existing

- TS 119 612: Trusted list
- TS 119 615: Using trusted lists

To be specified:

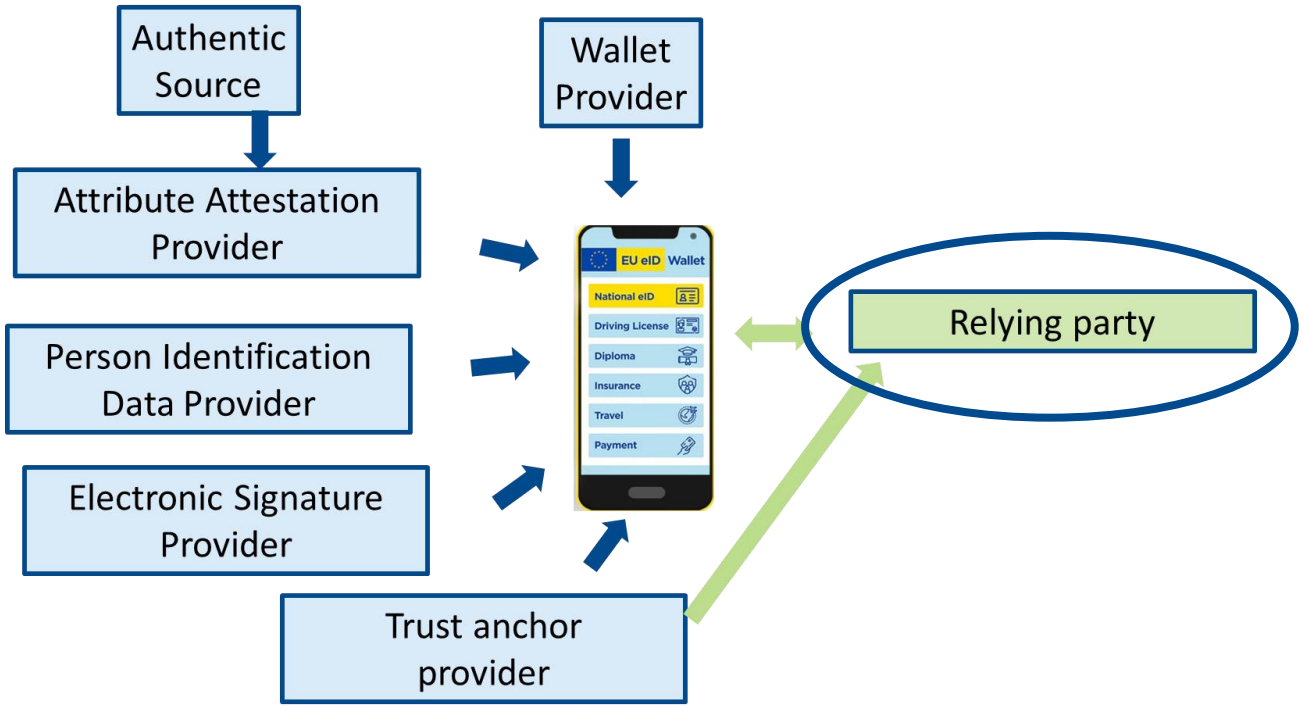
- Support for new trust services
- Support for other trust anchors

eIDAS Audit Framework (Art 17, 18, 19)



TSP+CAB+SB=>TSL

ETSI Standards for relying party use of wallet

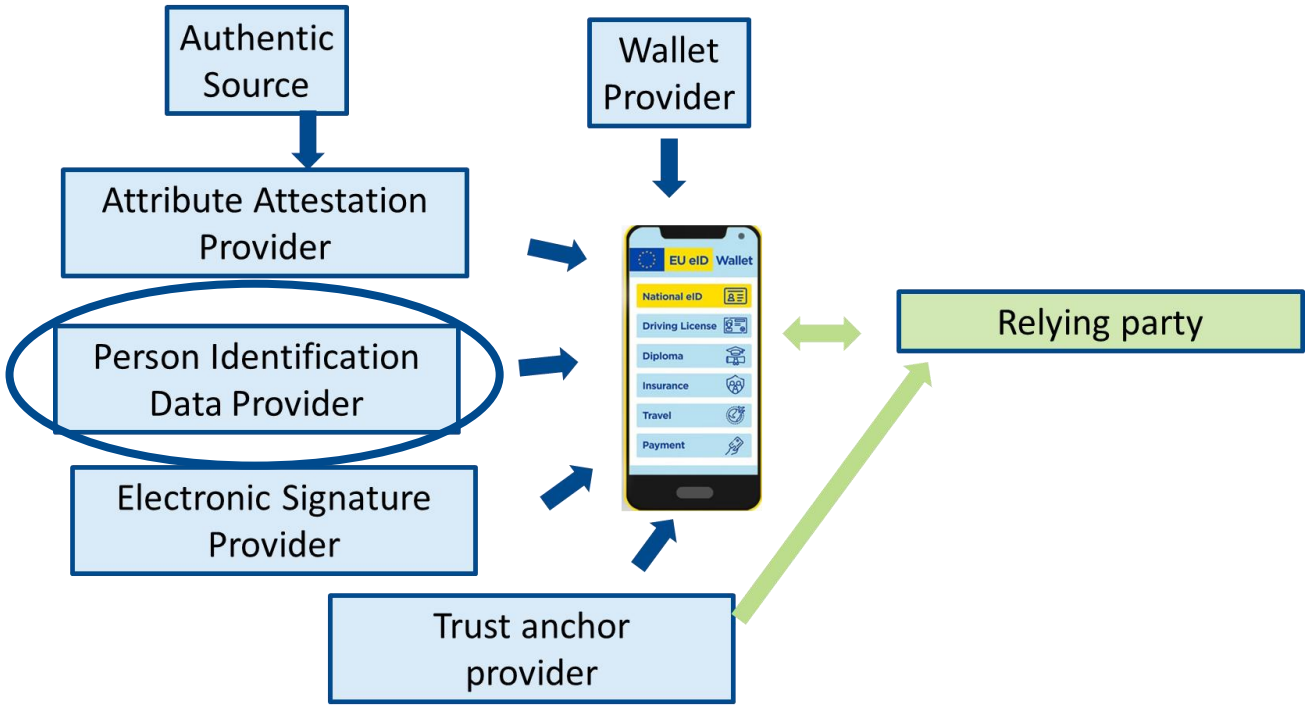


To be specified:

- Relying party authentication
- Wallet authentication
- Presentation of wallet held attributes as selected by the wallet holder

Profile of internationally recognised standards

CEN Standardisation and ETSI overlap



CEN- Draft TS Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets

Overlap:

- Common syntax:
  - CEN: Personal identification data
  - ETSI: electronic attestation of attributes
- Common identity proofing requirements:
  - CEN: Personal identification data
  - ETSI: electronic attestation of attributes
  - ETSI: Signing certificates

ETSI Further information

Information on Signatures and Trust Services standards :
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI standards: available for free download: http://www.etsi.org/standards-search

News list on Signatures and trust services:
https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

EU Pilot for the International Compatibility of Trust Services
https://esignature.ec.europa.eu/efda/intl-pilot/