

TeleTrust-Informationstag

"Elektronische Signatur und Vertrauensdienste"

Berlin, 27.09.2023

Auf dem weiten Weg von Wallet-Visionen zu konkreten Anwendungen – Wie ETSI ESI Standards helfen können

Arno Fiedler, Nimbus Technologieberatung GmbH

Schlüsselemente einer Europäischen Digitalen Identität



- 1. Based on state sovereignty**
- 2. Mutual recognition**
- 3. User ownership of identities, data and certificates**
- 4. Harmonized standards**
- 5. High usability**
- 6. Transparency**
- 7. Safe operation**
- 8. Wide range of services**

Quelle: Dr. Kim Nguyen (D-Trust), 21.09.2021

Einführung – eIDAS 2014

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Verordnung = unmittelbar geltendes Recht in Deutschland

„Diese Verordnung dient der **Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt**, indem eine gemeinsame **Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen** geschaffen wird, wodurch die **Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht** wird.“

Elektronisches Identifizierung

- Gegenseitig in allen Mitgliedsstaaten anerkannte elektronische Identifizierungsmittel .

Vertrauensdienste

- Elektronischer Dienst, zur Erstellung, Überprüfung und Validierung von elektronischen Signaturen und zur Übermittlung betreffender Zertifikate.
- **Qualifizierter Vertrauensdienst:** Vertrauensdienst, der die Anforderungen der Verordnung erfüllt und von einer national ernannten Aufsichtsstelle den Status eines qualifizierten Vertrauensdiensteanbieters erhalten hat.
- 319 qualifizierte TSPs in der European Trusted List aufgeführt



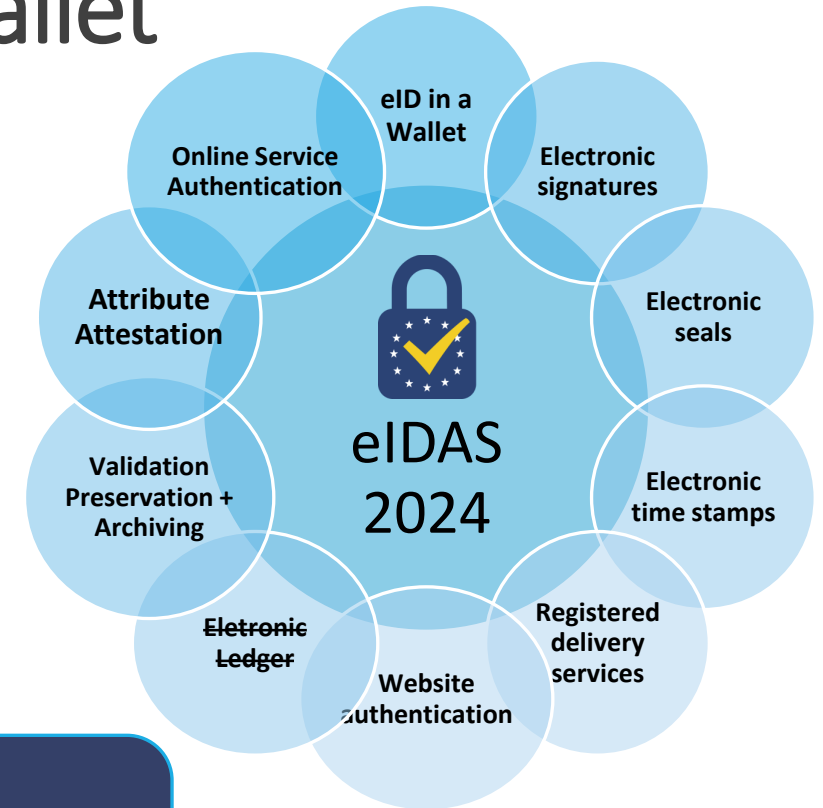
eIDAS 2.0 – European Digital Identity Wallet

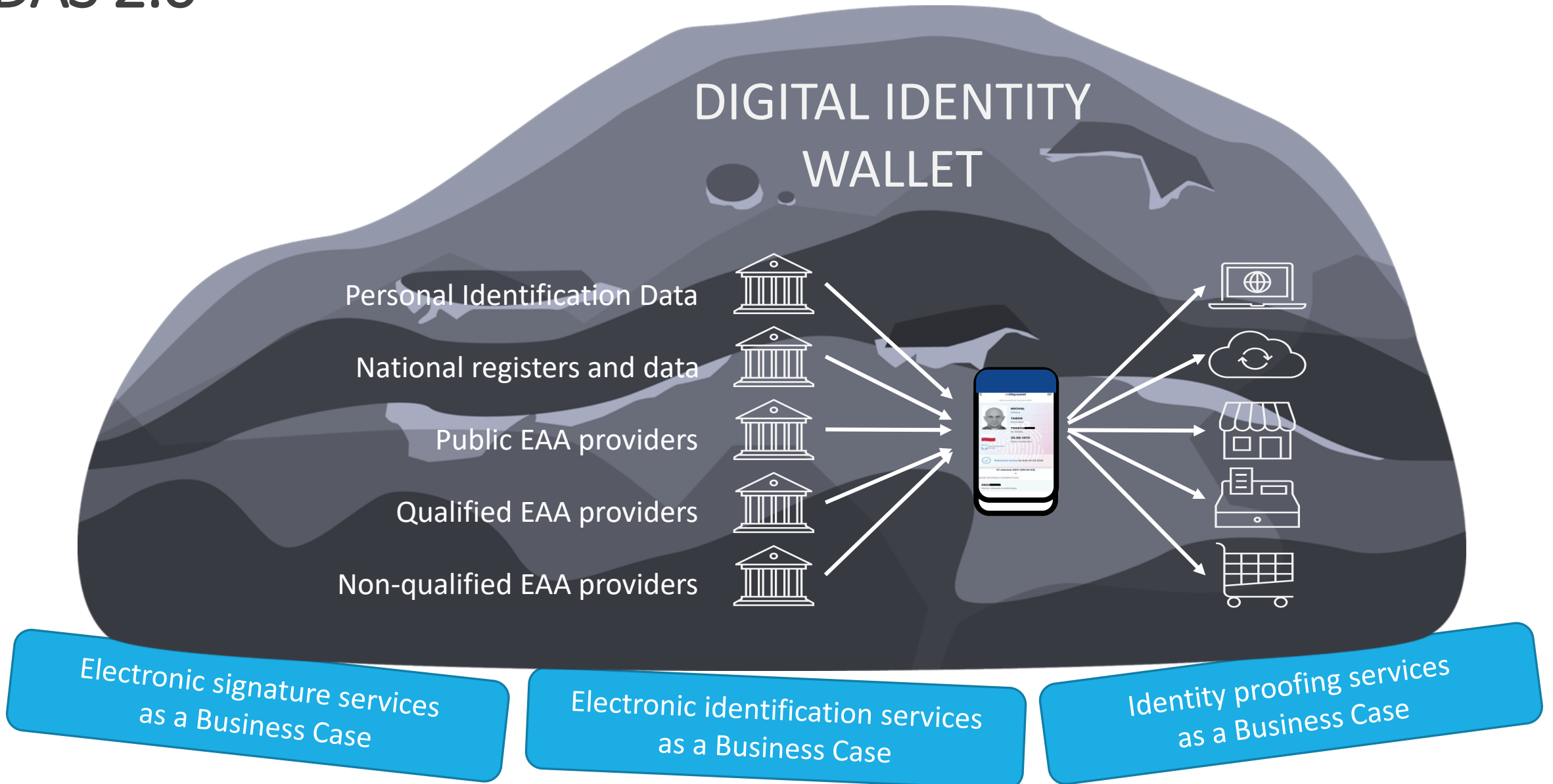
Definition Trust Services eIDAS 2.0

- Scope (Art 3 a): 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.
- Definition (16): ‘Trust Service’ means an electronic service normally provided against payment which consists of 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

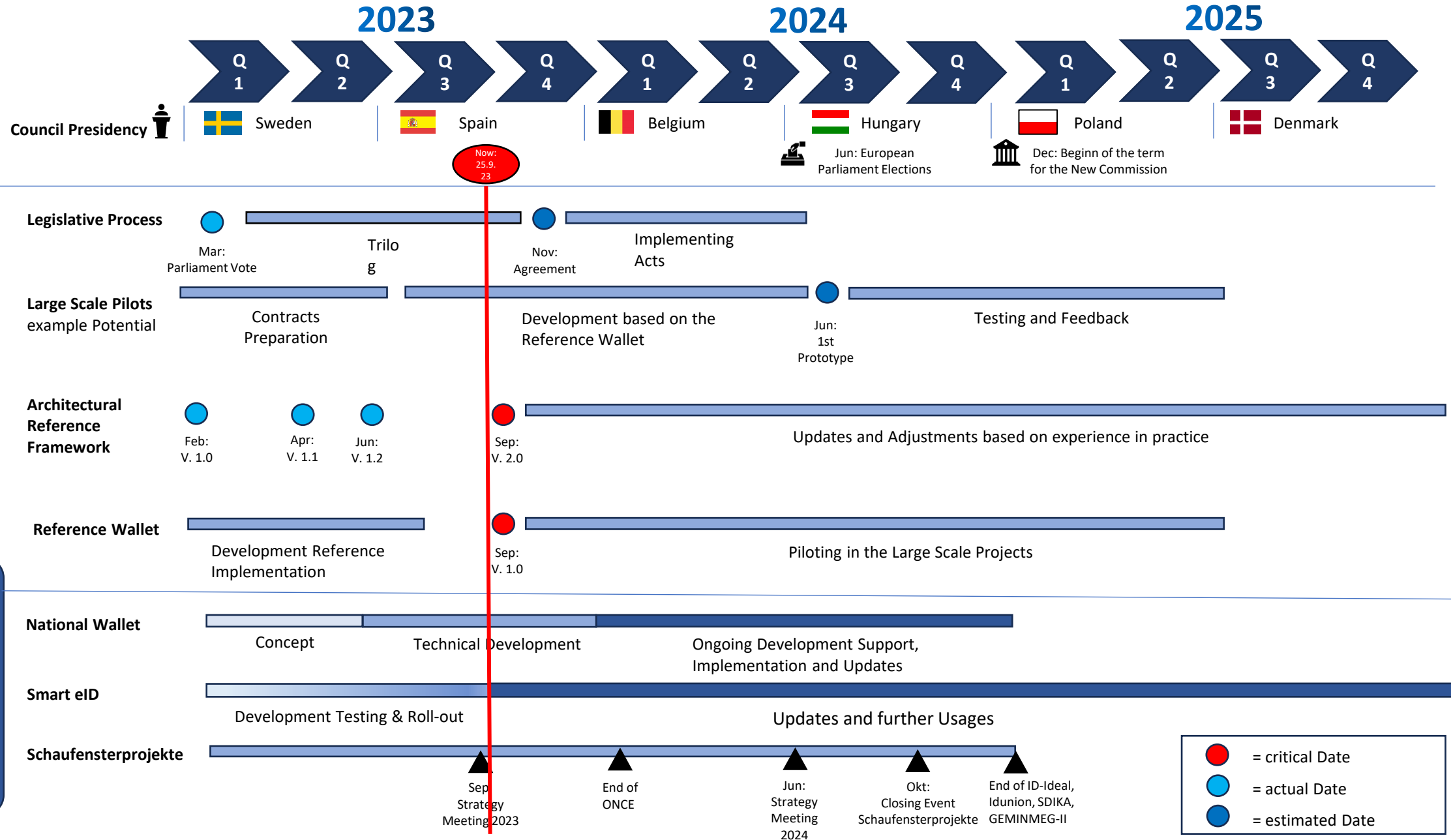
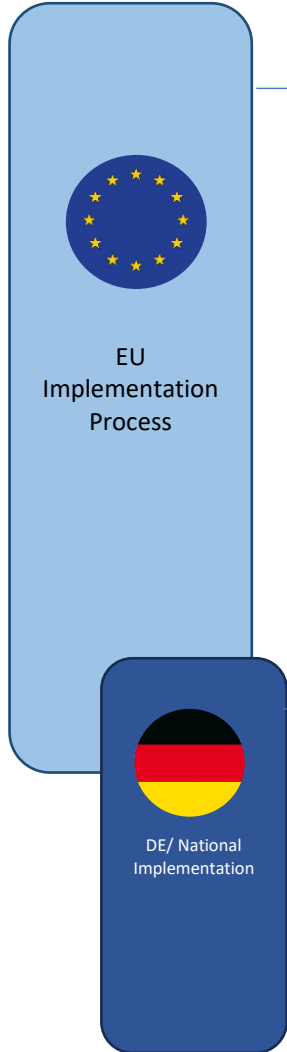
Strengthening Trust Services eIDAS 2.0

- Harmonisation of remote identity verification (on level „high“!)
- Recognition of QWACs - Ensuring the protection of consumers, article 45 has introduced an obligation on the providers of web browsers to accept QWACs and display identity information about the entity behind a website in the browser environment.
- Alignment with the rules applicable to Network and Information Security (NIS/2)





eIDAS 2/ EUDI Wallet / German Wallet – Timeline of Implementation



ETSI & CEN Standards supporting eIDAS – the overall picture



Trust services:

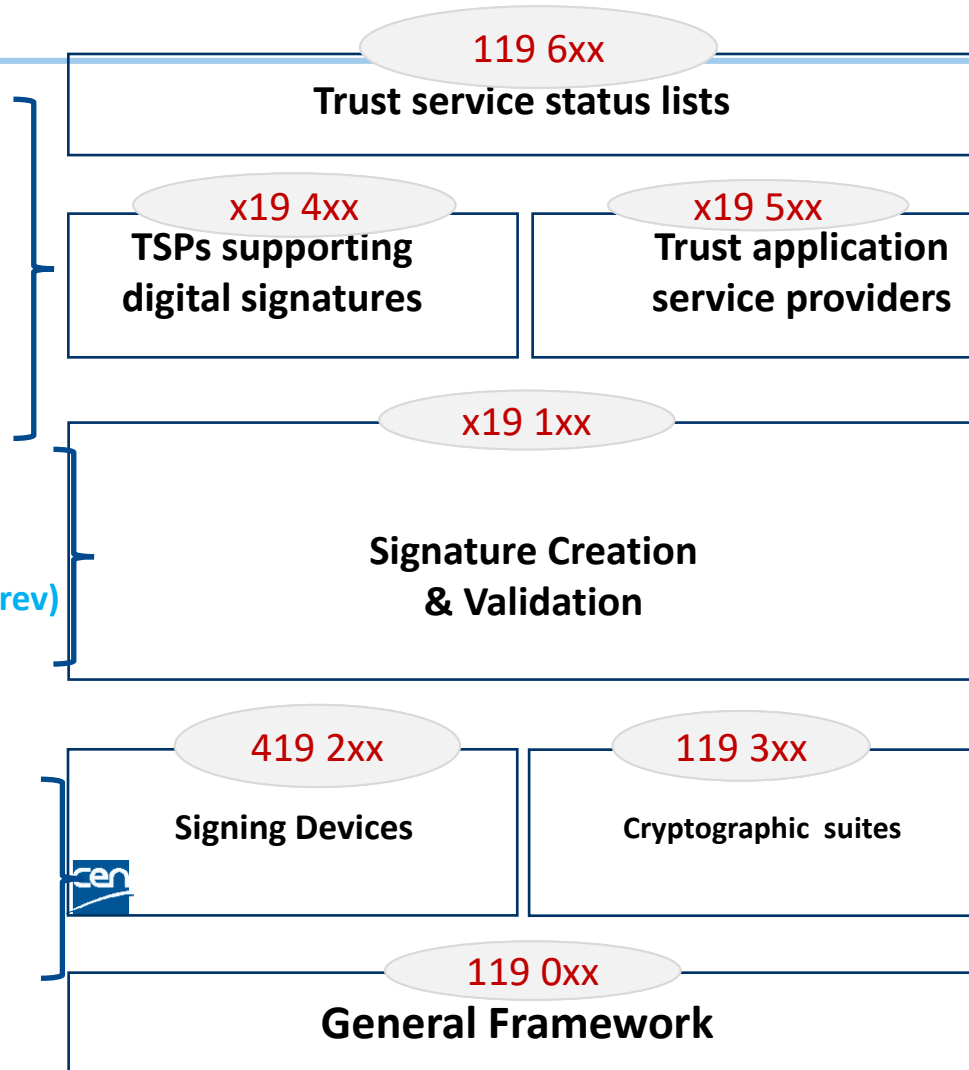
- TSP Audit ✓
- Issuing certificates ✓✓✓ (rev)
- Time Stamping ✓✓✓
- Signature creation services ✓✓
- Signature validation services ✓✓
- Identity proofing ✓✓ (upd)
- Open Banking ✓✓ (upd)
- Support for NIS 2 (new)
- S/MIME ✓✓ (new)
- Attribute Attestations (new)

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 ✓✓✓



Trusted list ✓

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

Trust services for:

- Registered eDelivery / eMail ✓✓ (upd)
- Long term preservation ✓✓
- Interop tests

Formats + Interop test:

- XAdES (XN) ✓✓ (rev)
- CAdES (CN) ✓✓ (rev)
- PAdES (PL) ✓✓ (upd)
- ASiC (containers) ✓✓ (upd)
- JAdES (JSON) ✓✓ (upd)
- CB-AdES (CBOR) (new)

Signature suites ✓✓ (upd)

- Hash
- Asymmetric crypto
- Key generation
- Lifetime

Schema for algorithm catalogues (new) ✓

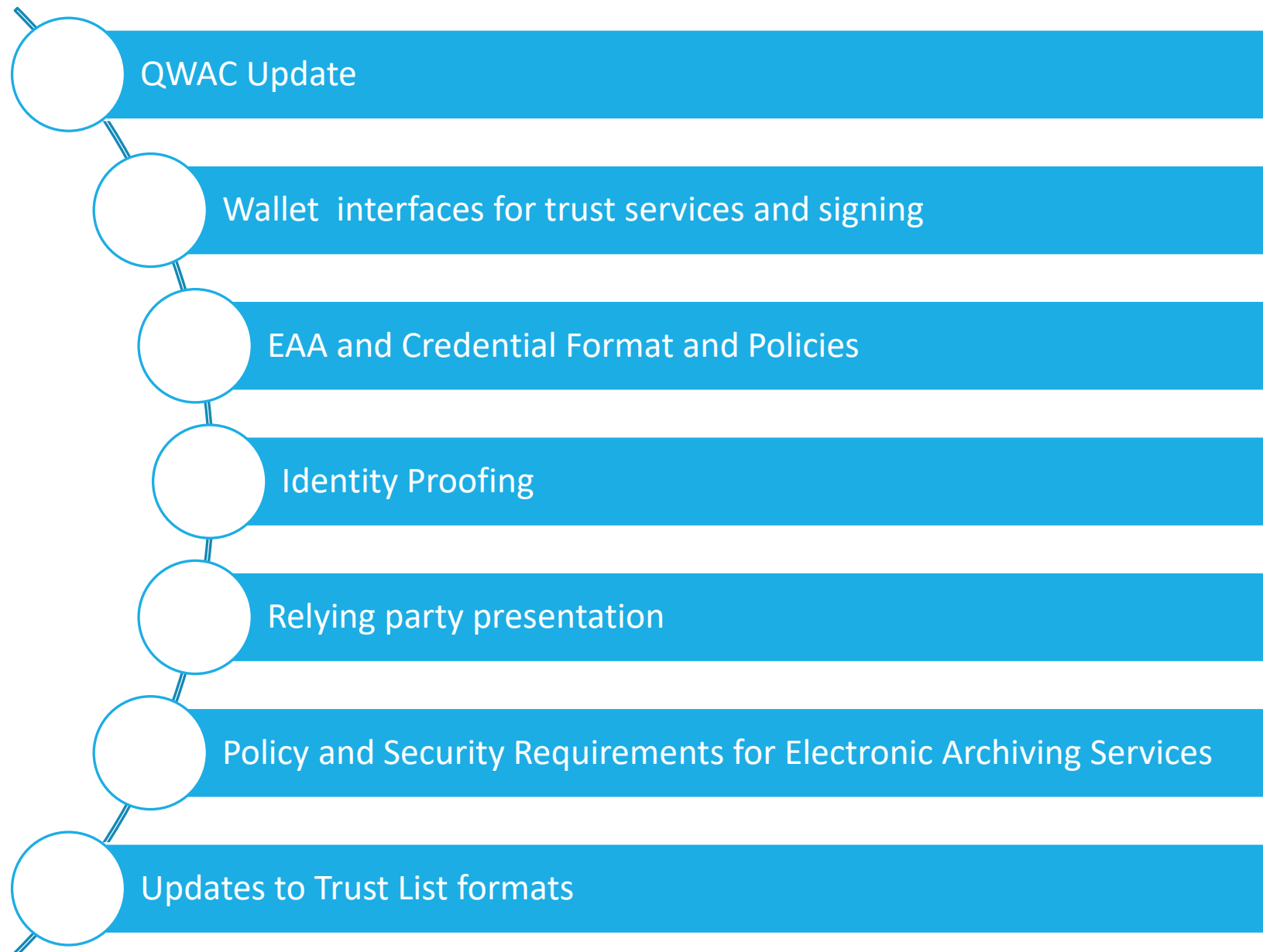
Standards framework ✓✓ *

- Common definitions ✓✓
- Guides ✓✓

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

Aufgabenbereiche von ETSI ESI

- Auf Basis der regulatorischen Vorgaben durch eIDAS 2.0 wird die Standardisierung geprüft.
- Bestehende Standards, die heute schon die Regulierung unterstützen bleiben bestehen und werden ggf. ergänzt.
- Neue Standards für bspw. neue Trust Services werden entwickelt.



EN 319 401 – General requirements for TSP

NIS 2 Alignment



- ✓ Initial draft Distributed to ECATS June 2023
- ✓ Feedback received from ECATS, ACAB's and ETSI experts
 - Includes indication of changes likely needed to align with NIS2 implementing act
- ✓ Processing feedback to agree disposition of comments in process
- ✓ EN 319 401 v2.4.1 Drafting plan
 - stable draft for ETSI November meeting
 - EN approval process initiated by end 2023
 - Final approval Q2 2024
- ✓ Once NIS2 implementing act stable draft available may produce further update to EN 319 401 to fully align with NIS2

TR 119 476: Selective disclosure and zero-knowledge proofs



- Analysis of current technology for selective disclosure and zero-knowledge proofs
- Recommendations on Electronic Attestation of Attributes
- Significant interest and feedback
- Plan revision early 2024

Fazit zu eIDAS 2.0, auch aus den Schaufensterprojekten:

Stand September 2023

- Zielsetzung ist extrem ambitioniert, teilweise nicht realistisch / Schwedische Ratspräsidentschaft hat zwar offiziell den Trilog abgeschlossen, spanische RP aber noch dabei die Einzelheiten mit MG's zu verhandeln. Dies führt auch zu Verzögerungen bei den technischen Entwicklungen.
- Registeröffnung für alle (Qualified) Electronic Attribute Attestation Provider/ Herausforderung u.a. für Deutschland.
- Anhängigkeit von Secure Elements und Betriebssystemen / Wird voraussichtlich beibehalten.....
- „Self-Sovereign Identity“ versus „Identity Matching via PID“ / Weder noch....
- Vorgehensweise stärker national geprägt als bei eIDAS 1 / Harmonisch wird das nicht.....
- NIS2 kommt zusätzlich zu bestehenden Sicherheitsanforderungen auf die TSP zu, der Begriff TSP ist dabei zu weit gefasst. Das blaue Wunder droht...
- Time to Market kritisch, GAFAM reagiert „stark“ und Lobbyiert erfolgreich
- **Allerletzte** Möglichkeit zur Wiedererlangung der Souveränität (eIDAS mit DMA und DSA)



Vielen Dank für Ihre
Aufmerksamkeit!