ascertia | IDENTITY PROVEN TRUST DELIVERED

eIDAS 2.0

The Future of Digital Identity & Trust Services

Fábio Rego

Business Solutions and Compliance Manager

STRUCTURE

- Regulatory Development
- European Union Digital Identity Wallet (EUDIW)
- ARF & LSPs
- EUDI Wallet and Very Large Platforms
- New Trust Services under eIDAS 2.0
- Implementing Acts
- Standardization updates
- Wallet Demo
- Wrap up

Regulatory Development

1 eSIGNATURE DIRECTIVE

1999

- First regulatory framework for eSignatures Across the EU
- Only eSignatures and no definition of trust services
- Not directly applicable in the EU MS i.e. National legislation required for the provisions to be applicable;

2 eIDAS

2014

- Introduction of eIDs schemes and eIDAS Nodes
- Introduction of trust services in addition to eSignatures.

i) eSeals
ii) Timestamps
iii) eDelivery
iv) Website Authentication (QWACS)

- Possibility of Management of Signature Creation on Behalf of the Signatory i.e. Remote Signature
- Directly applicable in the EU Member States, with elements left to different national implementations on specific topics (e.g., Remote Signature and Remote Identification)
- Centralized identity models

3 eIDAS 2.0

2024

- Introduction of the European Digital Identity Wallet (EDIW) as User-centric, wallet-based digital identity recognised anywhere in the EU (public & private sectors);
- Introduction of new trust services:

i) Electronic attestations of attributes (EEA);
ii) Management of remote electronic signature and seal creation devices;
iii) Electronic archiving services;
iv) Electronic ledgers;

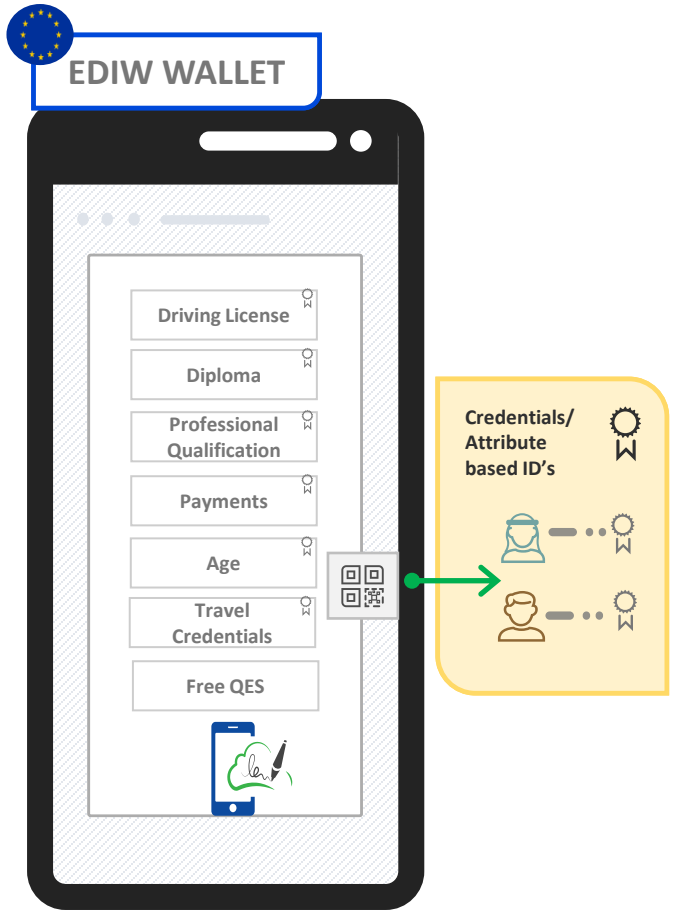
- Uniform policies, standards, and requirements for electronic identification and trust services with more than 40 implementing acts:
- Fines for QTSP infringements up to 5M or 1% Global Turnover

European Digital Identity Wallet (EUDIW)

Definition: Mobile application for citizens, residents and businesses, provided for free by all Member States on a voluntary use basis.

Concept: with a broader range of digital attributes/virtual credentials, such as mobile driving license, Diploma, ePrescriptions, travelling credentials, Professional Capacity, Organizational Attributes.

Mandatory: All MS are obliged to provide a EUDIW to its citizens, although it's use is voluntary by the citizens.



Functionalities: Store and manage digital credentials (Attributes), user control of its digital identity, and serve as an interface for Payment Initiation Services (PIS) and Qualified Electronic Signature (QES).

Free QES capacity: Offer the ability to sign by means of qualified electronic signatures to all natural persons by default and free of charge, for non-professional uses.

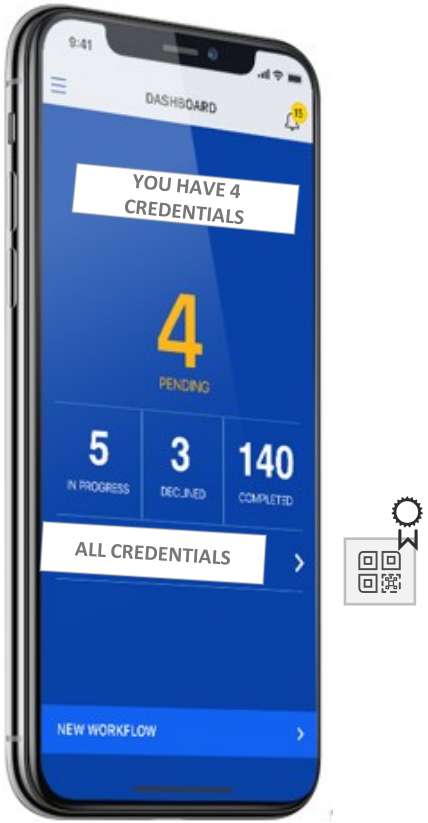
Level of Assurance High: the onboarding process should guarantee a level of assurance high with regards to identity proofing.

European Digital Identity Wallet (EUDIW) II

Common Protocols and Interfaces: Support common protocols and interfaces for issuing person identification data (PID) and management electronic attestations of attributes (EEA) to the EDIW.

Zero Knowledge Proofs (ZKP): Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the EDIW. This goes in line with the ETSI standard ETSI TR 119 476 - analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes

Selective Disclosure: concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information that is necessary for the provision of a service requested by a user.



Open Source: In a move towards transparency and collaboration, the application software components of the EDI Wallet will be open source.

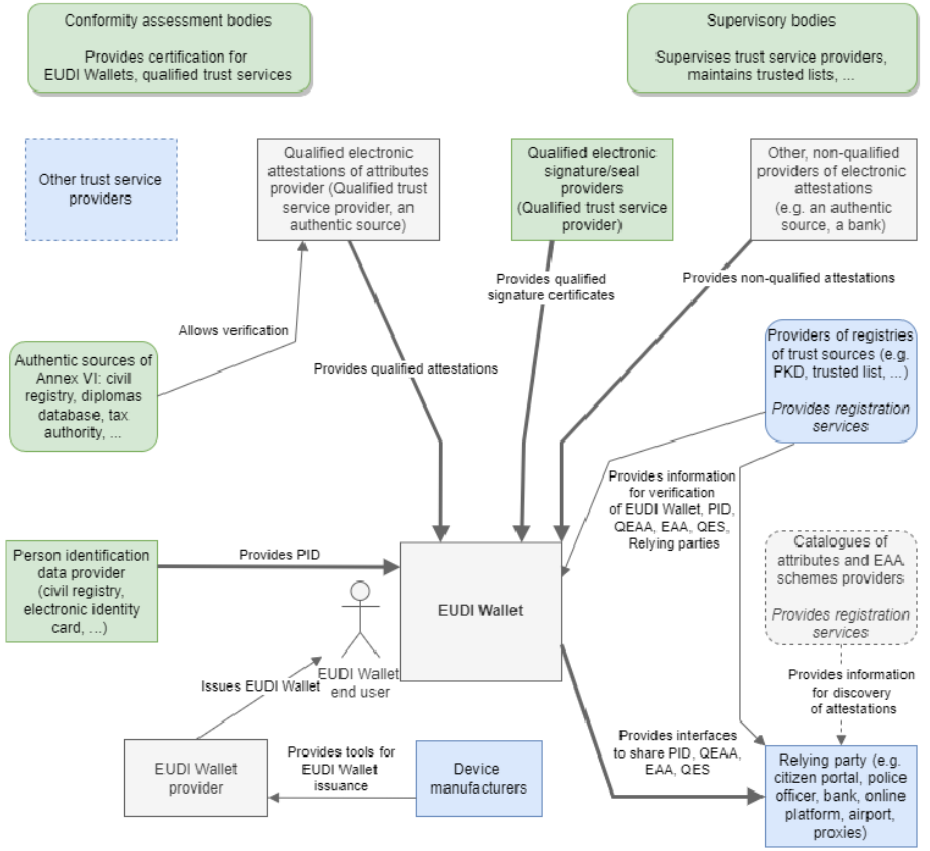
Relying parties: Provide protocols for relying parties to request and validate person identification data and electronic attestations of attributes. Very Large Platforms (VLPs) will be obliged to accept the EDIW.

Secure Elements: EUDIWs should benefit from the potential offered by tamper-proof solutions such as secure elements, and must ensure data minimization, user consent, security-by-design and certified.

Architecture and Reference Framework (ARF)

[European Digital Identity Architecture and Reference Framework (ARF) (link)]

The document serves as an outline provided by the eIDAS expert group, outlining their understanding of the European Digital Identity Wallet (EUDI Wallet) concept. The key focus is on the objectives, roles of ecosystem actors, functional and non-functional requirements, and potential building blocks. Importantly, it is part of the broader initiative spurred by the Commission's Recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.



Roles In The Ecosystem Laid Down In The ARF

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

Large Scale Pilots

- 4 Large Scale Pilots for the EDIW were funded in €46 million by the European Commission (link)

- Digital Credential for Europe (DC4EU) Consortium (link)

Use cases:

- **Applying for a job**
- **Accessing Social Security benefits**

- EU Digital Identity Wallet Consortium (EUWC) (link)

- **Travelling credentials**
- **Organisational Digital Identities**
- **Initiating Payments**

- Nobid Consortium (link)

- **Initiating Payments**

- Potential (link)

- **Identify to and access a digital public service:**
- **Opening a bank account**
- **Applying for a SIM**
- **Receive and store the mobile driving licence**
- **Signing contracts**
- **Claiming Prescriptions**

Large Scale Pilots – Second Round

WE BUILD is led by the Dutch and Swedish government authorities Ministry of Economic Affairs (Netherlands), KVK Netherlands) and Bolagsverket (Sweden)

https://www.webuildconsortium.eu/

EUDI Business Wallets:

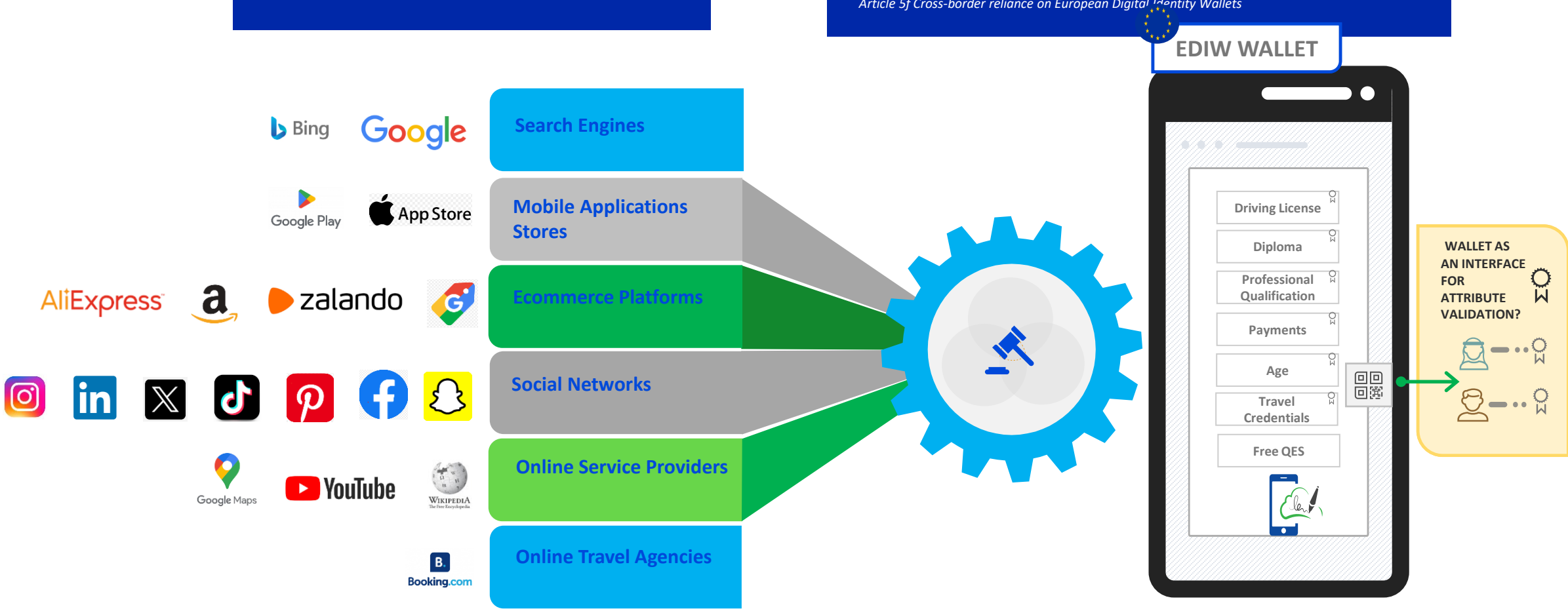
-European Unique Identifier
-Digital Power of Attorney
-EU Company Certificate
-Business Licenses
-Environmental certificates

- Digital Signatures and Seals
-Qualified EEA
-Timestamping Services
-Most Probably Qualified Delivery Services

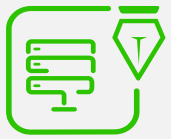
EDI Wallet and Very Large Platforms

Very large online platforms as defined in Article 25(1) of Regulation (EU) 2022/2065 require users to authenticate to access online services, those platforms should be mandated to accept the use of EDIWs upon voluntary request of the user.

*"Private relying parties providing services such as in the areas of **transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education** should accept the use of EDIWs for the provision of services where strong user authentication for online identification is required by Union or national law or by contractual obligation."*
Article 5f Cross-border reliance on European Digital Identity Wallets



New Trust Services In eIDAS 2



Management of remote electronic signature and seal creation devices (MQSCD)

- Only QTSPs can manage remote QSCDs
- Back up only under certain conditions
- Certification will not exceed 5 years
- Implementing act will lay down the technical requirements

Electronic attestations of attributes (EEA)

- Legally equivalent to paper-based credentials;
- Revocation mechanisms will be required;
- All Attestations will be QSealed/Qsigned by the issuing organization suitable for automated processing;

NEW TRUST SERVICES

Electronic archiving services (EAS)

- Legal Validity: Electronic data preserved by archiving services is legally recognized in proceedings, irrespective of format.
- Presumed Integrity: Qualified archiving services presume the integrity and origin of electronic data throughout the preservation period.

Electronic ledgers

- Qualified electronic ledgers should establish a legal presumption.
- Unique and accurate sequential chronological ordering and integrity of data records.

New Trust Services In eIDAS 2 – MRSCD

- **QTSPs only:** The remote generation or management of electronic signatures and their creation data is restricted to qualified trust service providers acting on behalf of the signatory.
- **Specific conditions:** Qualified providers must adhere to specific conditions, including the duplication of signature creation data for backup, subject to security standards and limitations on the number of duplicates. Additionally, there are requirements outlined for the qualified service managing remote electronic signature creation devices.
- **Certification maximum validity:** The validity of a certification referred to in paragraph 1 shall not exceed 5 years, subject to a regular 2-year vulnerabilities assessment.
- **Vulnerabilities:** If vulnerabilities are identified and not remedied, the certification shall be cancelled.

Related Legal Definitions

- ‘remote qualified electronic signature creation device’ means a qualified electronic signature creation device managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;
- ‘remote qualified electronic seal creation device’ means a qualified electronic seal creation device managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;

Management of remote electronic signature and seal creation devices (MRSCD)

New Trust Services In eIDAS 2 – (EA)

- **Preservation of Electronic Data:** Electronic data and documents stored using electronic archiving services should not be denied legal effect or admissibility in legal proceedings simply because they are in electronic form or not preserved using a qualified electronic archiving service.
- **Presumption of Integrity and Origin:** If electronic data and documents are preserved using a qualified electronic archiving service, there is a presumption of their integrity and origin for the duration of the preservation period by the qualified trust service provider.
- **Provider Qualifications:** Qualified electronic archive services must be provided by qualified trust service providers.
- **Durability and Legibility:** Services must use procedures and technologies ensuring the durability and legibility of electronic data beyond technological validity, throughout the legal or contractual preservation period, while maintaining integrity and accuracy of origin.
- **Preservation Safeguards:** Electronic data must be preserved to safeguard against loss and alteration, except for changes related to medium or electronic format.
- **Automated Report for Relying Parties:** Authorized parties should be able to receive an automated report confirming the presumption of integrity of electronic data retrieved from a qualified electronic archive. This report must be provided reliably and efficiently and bear the qualified electronic signature or seal of the archiving service provider.

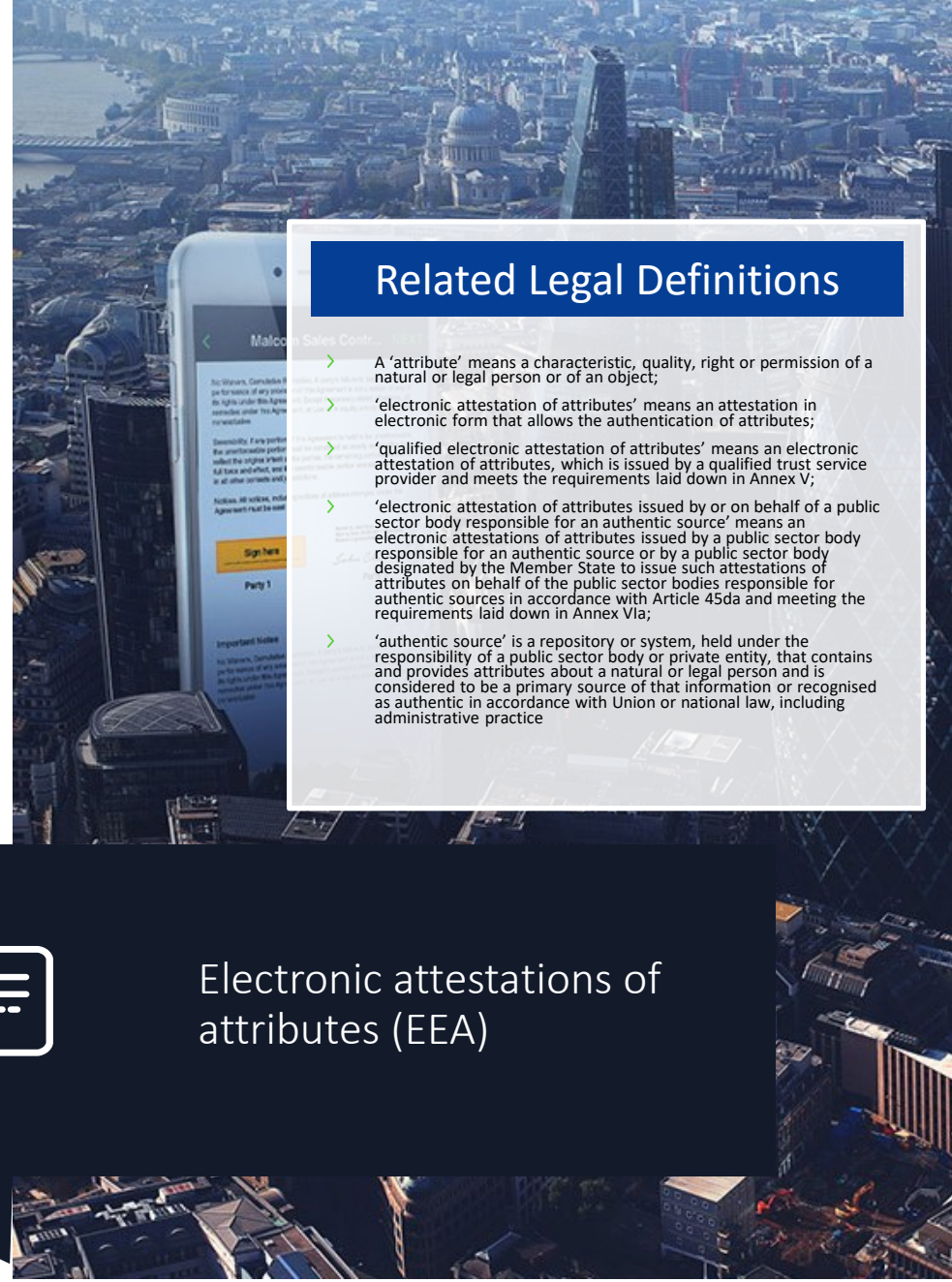
Related Legal Definitions

- ‘electronic archiving’ means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;
- qualified electronic archiving service’ means an electronic archiving service that meets the requirements laid down in Article 45ga;

Electronic Archiving

New Trust Services In eIDAS 2 - EEA

- **Legal effect:** A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.
- **Revocation:** Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.
- **Non combination of data:** Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners
- **Data segregation:** Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes.
- **Attributes Qseal/Sig:** The qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body identified as the issuer, shall contain a specific set of certified attributes in a form suitable for automated processing



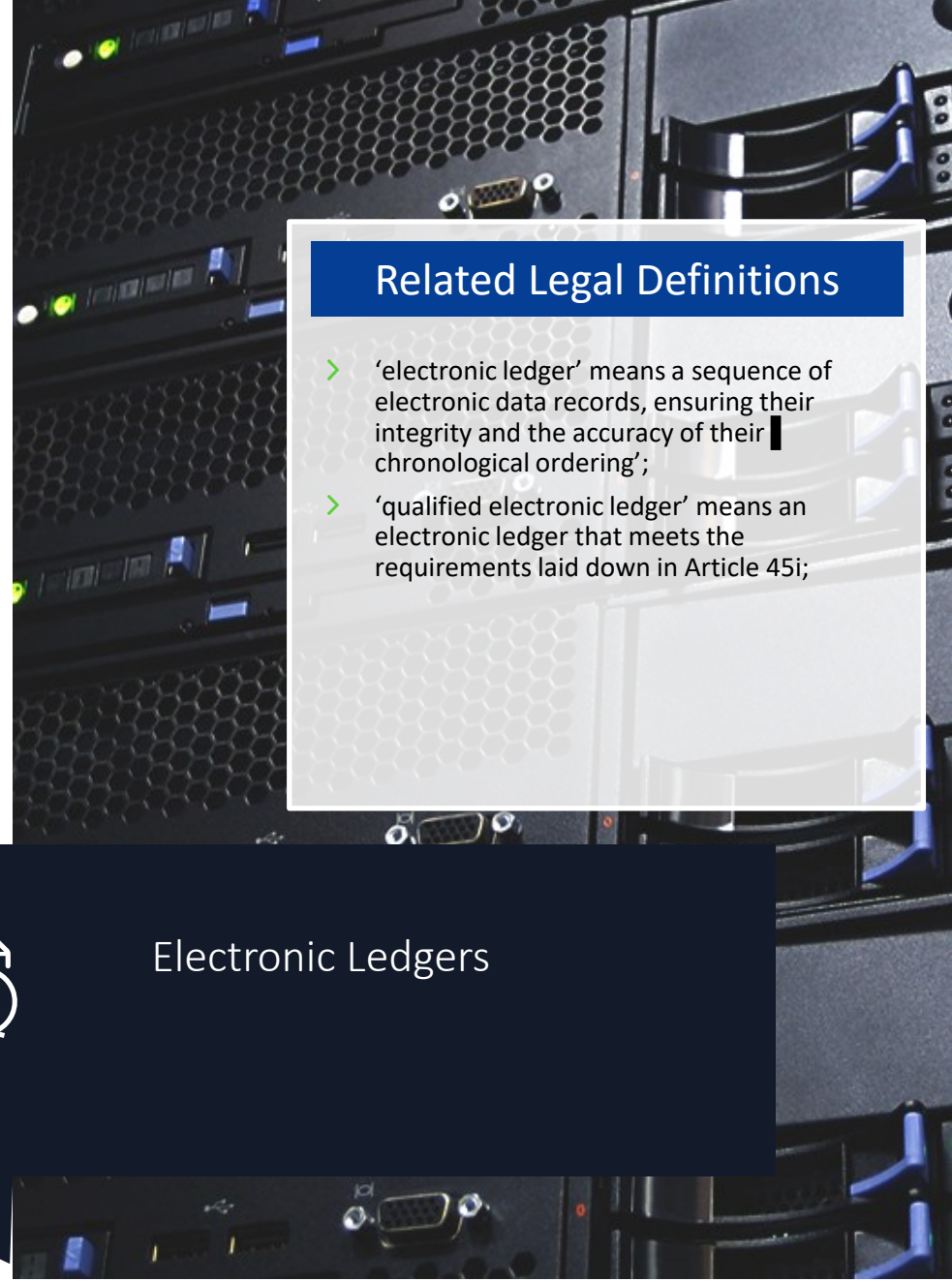
Related Legal Definitions

- A 'attribute' means a characteristic, quality, right or permission of a natural or legal person or of an object;
- 'electronic attestation of attributes' means an attestation in electronic form that allows the authentication of attributes;
- 'qualified electronic attestation of attributes' means an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;
- 'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' means an electronic attestations of attributes issued by a public sector body responsible for an authentic source or by a public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45da and meeting the requirements laid down in Annex VIa;
- 'authentic source' is a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person and is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice

Electronic attestations of attributes (EEA)

New Trust Services In eIDAS 2 - EL

- **Concept:** Electronic ledgers are a sequence of electronic data records which should ensure their integrity and the accuracy of their chronological ordering. Electronic ledgers should establish a chronological sequence of data records.
- **Use cases:** In conjunction with other technologies, they should contribute to solutions for more efficient and transformative public services such as e-voting, cross border cooperation of customs authorities, cross border cooperation of academic institutions, or the recording of ownership for real estate in decentralised land registries.
- **Legal Presumption:** Qualified electronic ledgers should establish a legal presumption for the unique and accurate sequential chronological ordering and integrity of the data records in the ledger.
- **European Legal Framework:** To ensure legal certainty and promote innovation, a pan-European legal framework should be established that allows for the cross-border recognition of trust services for the recording of data in electronic ledgers. This should sufficiently prevent that the same digital asset is copied and sold more than once to different parties. The process of creating and updating an electronic ledger depends on the type of ledger used (centralised or distributed).
- **TSP Role:** Trust service providers for electronic ledgers should be mandated to ascertain the sequential recording of data into the ledger.



Related Legal Definitions

- ‘electronic ledger’ means a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological ordering’;
- ‘qualified electronic ledger’ means an electronic ledger that meets the requirements laid down in Article 45i;

Electronic Ledgers

Regulatory Structure

1 Regulation

- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

2 Implementing Acts

- More than 40 implementing Acts that will define the specific implementation rules for open provision laid down in eIDAS 2

3 Standards

Work on market standards is currently underway. ETSI and CEN are collaborating to develop a range of standards that will support the new regulatory framework, drawing on the most recent globally recognized standards for website authentication, open identity systems, and mobile-based wallets.

LIST OF IMPLEMENTING ACTS - European Digital Identity Wallets

Article	Topic
Article 5a (23)	European Digital Identity Wallet standards
Article 5b (11)	European Digital Identity Wallet-Relying Parties
Article 5c (6)	Certification of European Digital Identity Wallets
Article 5d (7)	List of certified European Digital Identity Wallets
Article 5e (5)	Security breach of European Digital Identity Wallets
Article 11a (3)	Cross-border Identity Matching
Article 45d (5)	Qualified Attestation of Attributes
Article 45e (2)	Verification of Attributes against Authentic Sources
Article 45f (6)	Issuing of Electronic Attestation of Attributes by or on behalf of public Authentic Sources
Article 45f (7)	Notification and List of Issuers of Electronic Attestation of Attributes

LIST OF IMPLEMENTING ACTS – Trust Services

Article	Topic
Article 19a (2)	Policies for Non-Qualified Trust Service Providers
Article 20 (4)	Conformity Assessment and Accreditation
Article 21 (4)	Initiation of Qualified Trust Service
Article 24 (1c)	Identity Verification
Article 24 (5)	Requirements for Qualified Trust Service Providers
Article 28 (6)	Qualified Certificates for Electronic Signatures
Article 29a (2)	Management of Remote Qualified Electronic Signature Creation Devices
Article 31 (3)	List of certified Qualified Electronic Signature Creation Devices
Article 32 (3)	Validation of Qualified Electronic Signatures
Article 32a (3)	Validation of Advanced Electronic Signatures based on Qualified Certificates
Article 33 (2)	Qualified Validation Service for Qualified Electronic Signatures
Article 34 (2)	Qualified Preservation Service for Qualified Electronic Signatures

Article	Topic
Article 38 (6)	Qualified Certificates for Electronic Seals
Article 42 (2)	Qualified Electronic Time Stamps
Article 44 (2)	Qualified Electronic Registered Delivery Services
Article 45 (2)	Qualified Certificates for Website Authentication
Article 45j (2)	Qualified Electronic Archiving Service
Article 45l (2)	Qualified Electronic Electronic Ledgers
Article 46a (7)	Report of Supervisory Bodies to the EU Commission
Article 46b (7)	Guidelines for Supervisory Bodies
Article 46d (4)	Guidance on Mutual Assistance (every two years)
Article 46e (7)	European Digital Identity Cooperation Group
Article 26 (2)	Advanced Electronic Signatures (Assessment of Necessity)
Article 36 (2)	Advanced Electronic Seals (Assessment of Necessity)

LIST OF IMPLEMENTING ACTS – Dates , Reviews and Delegated Acts

Article	Topic
Article 5a (1)	Availability of European Digital Identity Wallets in all EU Member States
Article 45e (1)	Verification of attributes against Authentic Sources
Article 5f (2)	Cross-border reliance on European Digital Identity Wallets
Article 5f (5)	Assessment of Demand, Availability and Usability of European Digital Identity Wallets
Article 49 (1+3)	Review Report (every four years)
Article 5a (24)	European Digital Identity Wallet Onboarding Procedures
Article 14 (1)	Recognition of non-European Trust Service Providers
Article 44 (2b)	Interoperability Framework for Qualified Electronic Registered Delivery Services

Article	Topic
Article 12 (6)	Procedural Arrangements for Peer Reviews (cf. CID (EU) 2015/296)
Article 12 (8)	Interoperability Framework (cf. CIR (EU) 2015/1501)

Standardization Updates

2025-05-19 **Work Programme** Version 2.3.3

Simple Search | Advanced Search | Pre-Defined Reports | Help

Work Item Progress Report: All Active Work Items For ESI For Current Status: Up to 'Waiting - see "Remarks"'

View As Work Item Summary List | View As Work Item Plan Legend: On Time Late

Found 36 items...
Displaying items 1 to 36 ...

	Work Item	Title	Current Status	Planned Next Status	Planned Procedure
ESI					
1.	EN 319 142-2 REN/ESI-0019142-2v121	**Electronic Signatures and Trust Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles** PAdES part 2 Additional PAdES signatures profiles	2025-03-27 Start of EN Approval Procedure	2025-06-25 End of EN Approval Procedure	2025-10-17 V
2.	TS 119 152-1 DTS/ESI-0019152-1	**Electronic Signatures and Trust Infrastructures (ESI); CB AdES (CBOR-AdES) digital signatures Part 1: Building blocks and CB-AdES baseline signatures** CB-AdES	2025-04-14 Stable draft	2025-03-25 Final draft for approval	2025-05-13 PU
3.	EN 319 162-1 REN/ESI-0019162-1v121	**Electronic Signatures and Trust Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers** ASiC part 1 Building blocks and ASiC Baseline containers	2025-01-13 Stable draft	2025-04-30 Final draft for approval	2025-06-27 AP
4.	TS 119 172-4 RTS/ESI-0019172-4v121	**Electronic Signatures and Trust Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists** Signature applicability rules (validation policy) for European qualified electronic signatures/seals	2024-02-20 Stable draft	2025-05-31 Final draft	2025-09-11 PU
5.	TS 119 322 RTS/ESI-0019322v131	**Electronic Signatures and Trust Infrastructures (ESI); Schema for machine-readable cryptographic algorithms, and cipher suites catalogues** Schema for machine-readable cryptographic algorithm catalogues	2025-02-21 Start of work	2025-05-22 Early draft	2025-05-11 PU
6.	EN 319 401 REN/ESI-0019401v321	**Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers** General Policy Requirements for Trust Service Providers	2025-05-15 Final draft	2025-05-30 Final draft endorsed by the Technical Group	2025-07-13 AP
7.	EN 319 411-2 REN/ESI-0019411-2v261	**Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates** Policy requirements for certification authorities issuing QC	2025-04-04 Start of Vote	2025-06-03 End of Vote	2025-06-17 PU
8.	TR 119 411-4 RTR/ESI-0019411-4v131	**Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2** Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2	2025-05-05 Start of work	2025-08-03 Early draft	2025-10-25 PU
9.	TR 119 411-7 DTR/ESI-0019411-7	**Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 7: Security Considerations on use of QWACs** Security Considerations on use of QWACs	2025-02-04 Start of work	Early draft	2025-12-11 PU
10.	TS 119 411-8 DTS/ESI-0019411-8	**Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 8: Common Access Certificate Policy for EUDI Wallet Relying Parties** Common Access Certificate Policy for EUDI Wallet Relying Parties	2025-05-05 Early draft	2025-05-19 Stable draft	2025-11-14 PU
11.	TR 119 411-9 DTR/ESI-0019411-9	**Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 9: Requirements on a Certificate Transparency (CT) Ecosystem to make the issuing of certificates transparent and verifiable** Requirements on a Certificate Transparency (CT) Ecosystem to make the issuing of certificates transp	2025-02-03 Early draft	2025-05-30 Stable draft	2025-12-13 PU
12.	EN 319 412-1 REN/ESI-0019412-1v161	**Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures** Certificate Profiles part 1 overview and common data structures	2025-03-14 Start of EN Approval Procedure	2025-06-12 End of EN Approval Procedure	2025-10-04 V
13.	EN 319 412-2 REN/ESI-0019412-2v241	**Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons** Certificate Profile for Natural Persons	2025-03-14 Start of EN Approval Procedure	2025-06-12 End of EN Approval Procedure	2025-10-04 V
14.	EN 319 412-4 REN/ESI-0019412-4v141	**Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates** Certificate profile for web site certificates	2025-03-14 Start of EN Approval Procedure	2025-06-12 End of EN Approval Procedure	2025-10-04 V
15.	EN 319 412-5 REN/ESI-0019412-5v251	**Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements** QCStatements	2025-03-14 Start of EN Approval Procedure	2025-06-12 End of EN Approval Procedure	2025-10-04 V
16.	TS 119 412-6 DTS/ESI-0019412-6	**Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles:**	2025-04-28 Early draft	2025-06-03 Stable draft	2025-08-16 PU

[Link for ETSI website]

Standardization Updates II

Electronic Attestation of Attributes

- TS 119 471 EAA Policy and security requirements
- TS 119 472-1: EAA Profile of recognised standards
- TR 119 476: Support for selective disclosure
- TS 119 462: Wallet interfaces for trust services and signing
- TS 119 477: Electronic Attestation of Attributes with Signatures

Electronic Signature

- TS 119 431 TSPs operating QSCDs
- TS 119 432 CSC API 2.x alignment
- TS 119 462 Wallet interfaces for trust services and signing

Remote IDV & Trust Lists

- ETSI 119 461 Identity proofing of trust service subjects
- TS 119 602: General trusted list model
- TS 119 605: General trusted list processing

Relying Parties

- TS 119 472-2:Profile of recognised standards
  - ✓ Relying party authentication
  - ✓ Wallet authentication
  - ✓ Presentation of wallet-held attributes as selected by the wallet holder
- TS 119 475: Relying party authorisation

Third Countries - Mutual Recognition

'Article 14

International aspects

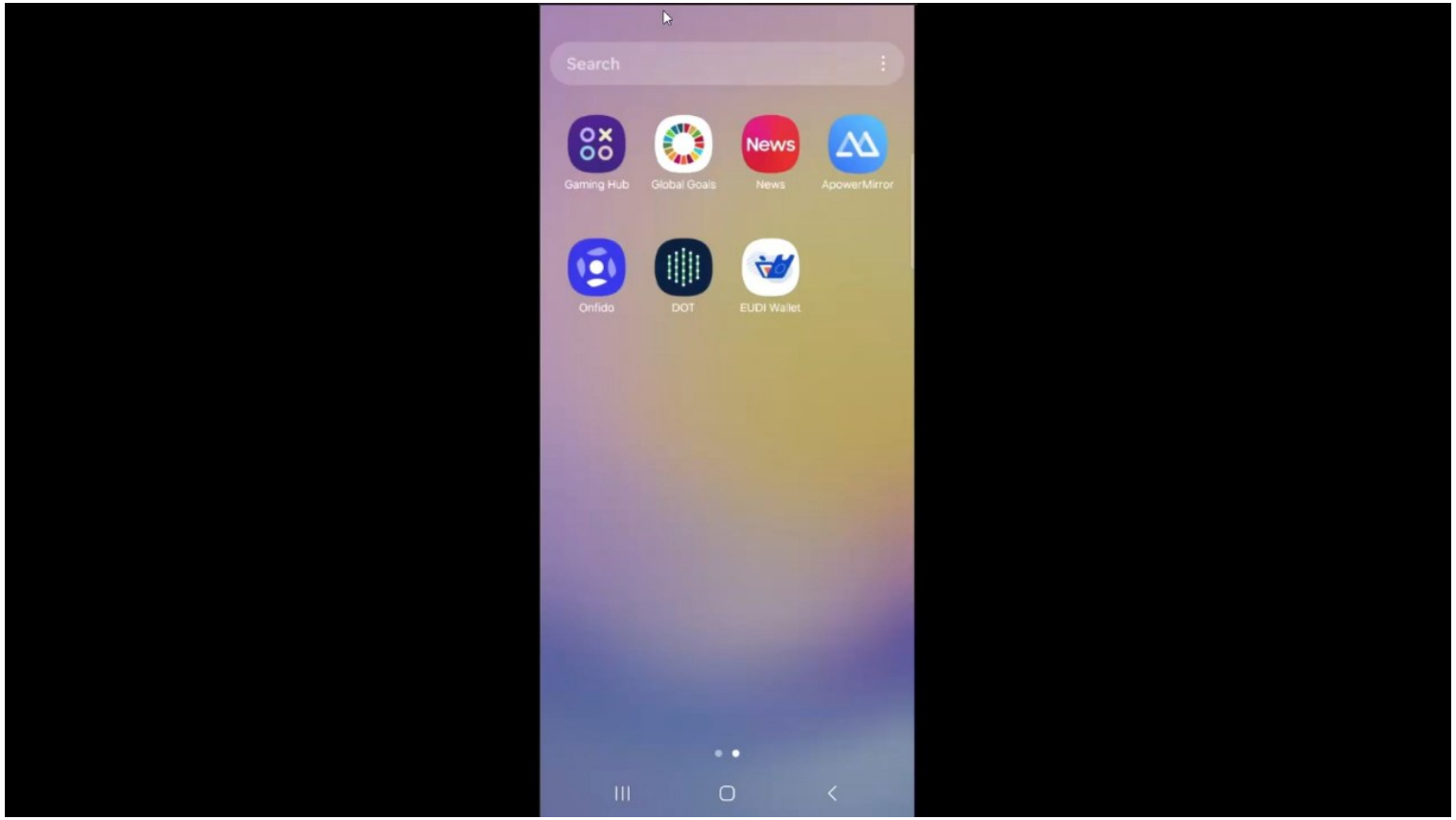
1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU.

The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).

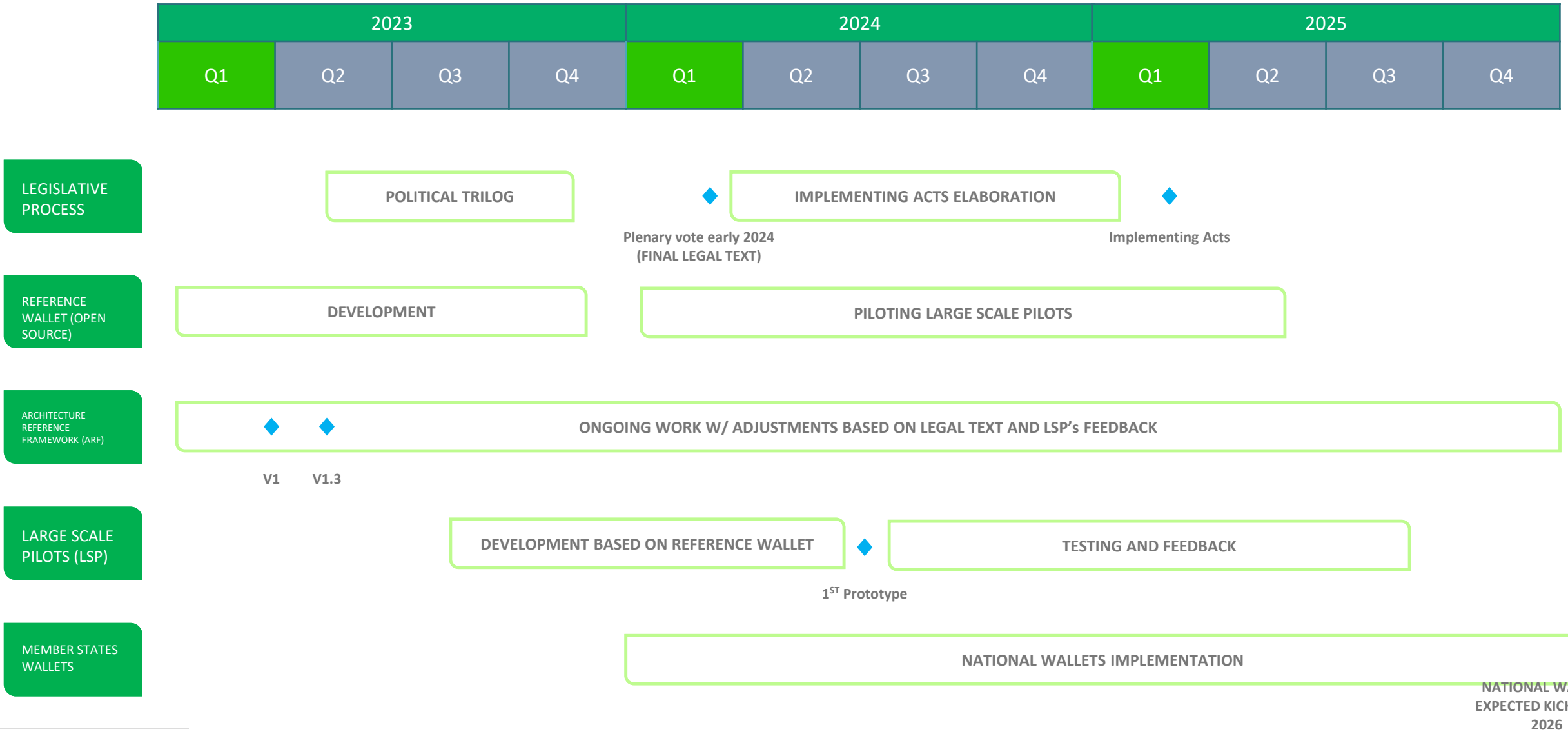
2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.

3. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.

Wallet and VC issuance



Timelines



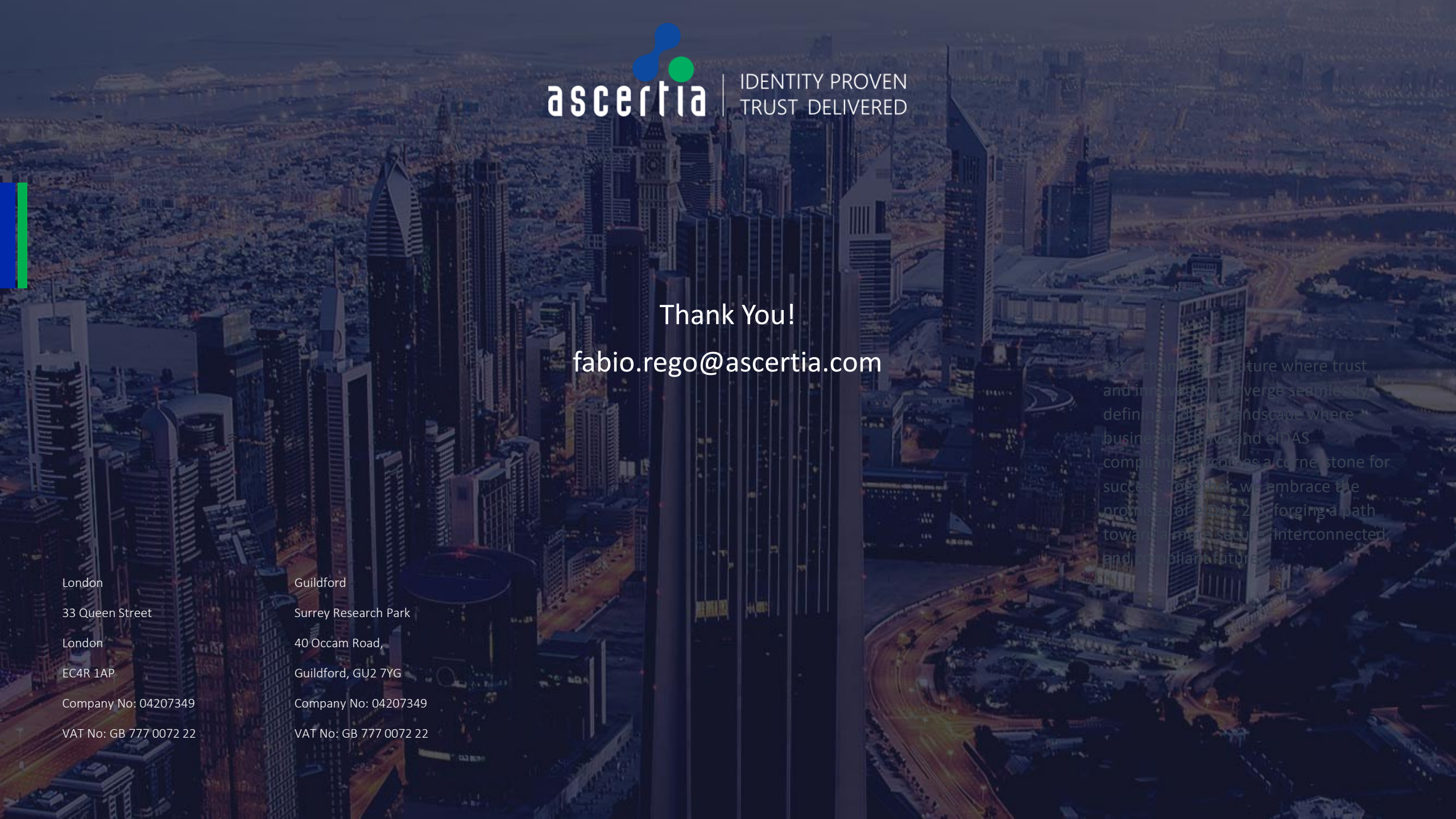
Conclusion & Strategic Takeaways

•The **European Digital Identity Wallet (EUDI Wallet)** empowers citizens and businesses with **secure, sovereign control** over their digital interactions.
•By anchoring digital identity in **state-issued and verifiable attributes**, the EU reduces dependency on non-EU tech platforms.
•eIDAS 2.0 reinforces **trust, interoperability, and resilience** in the European Digital Single Market.

•Adoption success depends on strong partnerships:
•**Public Sector:** Trusted issuance, regulation, and infrastructure.
•**Private Sector:** User-centric innovation, service integration, and broad use case development.
•Incentivizing ecosystem participation ensures real-world relevance and rapid scaling

•eIDAS 2.0 sets a precedent for harmonized digital identity frameworks worldwide.
•Aligns with international movements: W3C verifiable credentials, ISO/IEC standards, and G7 digital trust principles.
•Positions the EU as a global leader in secure, privacy-first digital identity.

•As AI agents become more embedded in daily life—managing tasks, initiating transactions, or even representing users digitally—the need for secure, consent-based identity control grows exponentially. eIDAS 2 and the EUDI Wallet provide the tools to ensure that these agents can act on behalf of individuals safely, verifiably, and within legal boundaries, without compromising identity integrity. This marks a shift toward a user-centric identity architecture, where the user—not platforms—decides how identity is shared, used, and delegated.


ascertia
IDENTITY PROVEN
TRUST DELIVERED
Thank You!
fabio.rego@ascertia.com
London
33 Queen Street
London
EC4R 1AP
Company No: 04207349
VAT No: GB 777 0072 22
Guildford
Surrey Research Park
40 Occam Road,
Guildford, GU2 7YG
Company No: 04207349
VAT No: GB 777 0072 22