EBSI-VECTOR
Education and work reloaded

T3.1

Project title:	**EBSI-VECTOR** - EBSI enabled VErifiable Credentials & Trusted Organisations Registries
Grant Agreement No.	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Deliverable Title	Role of EBSI within eIDAS 2.0
Version:	0.5
Date:	01.06.2024
Responsible Partner:	Logalty, msg
Authors:	Dr. Ignacio Alamillo (Logalty), Steffen Schwalm (msg)
Contributing Partners:	Laia Bota (Logalty)
Reviewers:	name of person (organisation) name of person (organisation)
Dissemination Level:	SEN – Sensitive/ PU – Public

Co-funded by the European Union

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Document Change History

Version	Date	Author (organisation)	Description
0.1	05.03.2024	msg	Initial Creation
0.2	15.04.2024	msg, Logalty	Legal framework
0.3	28.05.2024	Dito	Integration results from Blockchain Sandbox
0.9	01.06.2024	Dito	Final draft
1.0	01.10.2024	Dito	Final version

Co-funded by the European Union

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Table of Contents

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

List of Figures

List of Tables

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

1 Introduction

The document describes the fundamentals to integrate the European Blockchain Service Infrastructure into the eIDAS Trust Framework. Based on an introduction into eIDAS 2.0 the document shows the role of Electronic Ledger within eIDAS 2.0 and in next step how this relies to EBSI and gives recommendation to integrate EBSI into eIDAS 2.0 including possible steps for migration.

The annexes contain a comprehensive overview on existing standards related to eIDAS as well as a template for risk assessment on needed Level of Assurance for certain use cases based on Art. 8 eIDAS 2.0 and 2015/1502.

The document is intended as comprehensive introduction into and description of the subject as a basement for further analysis and steps based on the recommendations given in the document.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

2 Role of EBSI in eIDAS 2.0

2.1 Fundamentals on EUDI Wallet and Qualified Trust Service Providers

2.1.1 Electronic Identification

2.1.1.1 Introduction

eIDAS 2.0 defines (Art. 6a) the obligation for every member state to notify one eID scheme within 12 months after the regulation will become applicable. Mandatory implementing acts referencing European technical standardization shall be published by the European Commission within six months after the new regulation is published, means appr. November 20024. The new regulation requires that at least one identity scheme from each member state shall be notified (Art. 10 and following). This applies even more because any notified eID scheme must ensure the possibility of unique identification with the proposed EU Digital Identity Wallet (EUDIW)1.

Beside government eID schemes relevant for notification, the eIDAS also introduces (Art. 12a) private identification schemes together with the possibility for a national certification against LoA. The certification scheme shall be based on the EU Cybersecurity Act and performed by dedicated CAB listed transparently by the EC. An implementing act is currently not stipulated.

The presumable biggest change in eIDAS 2.0 is the requirement for every member state to provide an EUDIW to its citizens. Such an EUDIW could be published:

- By a member state
- Under authority of a member state
- Recognized by a member state.

This makes also private wallets possible under the recognition of a member state. Any EUDIW will contain Personal Identification Data (PID) for natural persons or Organizational Digital Identity (ODI) for legal entities as wallet holders. Based on the notified eID scheme on LoA

[1] I. Alamillo, S. Schwalm. 2021, S. Schwalm: The possible impact s of the eIDAS 2.0 digital identity approach in Germany and Europe. Open Identity Summit 2023. DOI: 10.18420/OID2023_09. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-729-6. pp. 109-120. Regular Research Papers. Heilbronn, Germany. 15.-16. June 2023

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

"high" it must achieve LoA "high" itself. This does not mean, that in every use case LoA "high" is really necessary, this has to be assessed by the Relying party interacting with the EUDIW or another identification mean.

Directly corresponding with the EUDIW are the new qualified attestation services (Art. 45a-e). Qualified Electronic Attestations of Attributes (QEAA) are additional attributes as a driver's license, diploma, or vaccine passport of the EUDIW holder, but with a qualified seal from the issuing QTSP. This means that EUDIWs will contain the core identity (PID/ODI) established by e.g., government eID as well as additional attributes. The data to be attested in QEAA will be provided from authentic sources provided by member states, practically these sources represent existing companies or public authorities which will send them to a QEAA provider for attestation. It has to be mentioned that acc. eIDAS 2.0 Public Sector Bodies can directly issue QEAA from the authentic source they provide without becoming QTSP for QEAA.

Recognizing this close relationship between qualified attestation services and the EUDIW, eIDAS 2.0 contains the same requirements for mandatory implementing acts referring to European standards for both wallet and attestation service. So only the issuer into the EUDIW must be qualified attestation service. Consequently, eIDAS 2.0 crosses digital identity means and qualified trust services, they determine each other.

Technical details as well as security requirements are defined within the eIDAS Toolbox Group as well as the ongoing European standardization at ETSI and CEN. The fulfilment of these requirements on EUDIWs and QTSPs will be certified by CAB based on further defined certification schemes which must be compliant to the EU Cybersecurity Act (Art. 6c). The responsibility for the assessment itself is with the issuing member state, with execution by the CAB. Within six months, mandatory implementing acts will define the requirements by referencing the relevant European standards. A list of all certified EUDIWs will be published by the European Commission, which is a de facto EUDIW Trust List, i.e., the wallet will be integrated in the now extended eIDAS trust framework. Any certified EUDIW will be, similar to any qualified trust service listed in the national trust list of each member state which are compiled onto the List of the Lists (LOTL) of the European Commission. Current Trust List:

- https://webgate.ec.europa.eu/tl-browser/

In accordance with the SSI principles, eIDAS 2.0 also contains requirements (Art. 6b) on the verifier, i.e., the relying party. They must notify usage and register in public lists provided by

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

member states. The elimination of any security assessment, in contrast to former drafts of eIDAS 2.0, introduces the risk of competition about lowest standards, potentially increasing the privacy risks for holders.

Equivalent to the dedicated requirements on the EUDIW, the qualified attestation services as well as the identification schemes, eIDAS 2.0 also defines concrete obligations on acceptance of the wallet. Not only public services, also any critical infrastructure provider (which means financial sector, utilities, health care etc.) as well as the big internet companies such as Google, Apple, Facebook, or Amazon are forced to accept the EUDIW (Art. 5f). Like eIDAS 1.0, the member state is fully liable for the provided EUDIW as well as the eID scheme. A qualified attestation service takes the full liability risk like all QTSPs (Art. 13). This means that eIDAS continues to limit the risks for users significantly

eIDAS 1.0 was underpinned by mandatory implementing acts which are still valid. In the context of digital identities especially 2015/1502 has to be mentioned which defines the requirements on Level of Assurance. It`s technical defined further e.g., in ETSI TS 119 461. In summary the current eIDAS Regulation follows the approach of a centralized digital identity *de facto* issued by member state or under its control. This means that eIDAS acts on the assumption of a government trust anchor for each digital identity so that a trustworthy third party issuing the eID is always needed. A digital identity without government trust anchor is not covered by eIDAS.

The trust model of eIDAS is described in section 3.

2.1.2 Qualified Trust Service Providers

Along with digital identities eIDAS also defines (qualified) trust services. They contain:

- Creation (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps
- Validation of (qualified) electronic signatures, seals and/or timestamps
- (qualified) Electronic registered mail/ delivery services
- (qualified) Preservation of (qualified) electronic signatures and/or seals
- (qualified) website certificates

Additionally, to the new qualified attestation services eIDAS 2.0 also introduces the following new trust services:

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

- Electronic Ledger (Section 11)
- Management of secure signature creation devices (Art. 29a)
- Archiving (Art. 45h)

Another change is the binding of QTSPs on the EU NIS2 (Network and Information Security 2) directive. As a result, QTSPs become part of critical infrastructure, hence must fulfil foreseeably higher security requirements than under eIDAS 1.0.

Any QTSP underlie the conditions Section III eIDAS (Art. 13–14 for all (Q)TSP, 20 following acc. to kind of trust service). Means:

- supervision by National Supervisory body (in German BNetzA)
- obligation on collaboration with National Data Privacy Officers for National Supervisory Body
- certified by independent Conformity Assessment Body (which is accredited by independent accreditation body) against European standards (eIDAS 1 acc. to M460 from European Commission we speak about ETSI and CEN standards: https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers and e.g. CEN EN 419 241
- after successful Conformity Assessment any QTSP will be listed publicly in national trust list which is consolidated to List of the Lists (LOTL) from EC: https://webgate.ec.europa.eu/tl-browser/#/
- periodical repetition of Conformity Assessment of any QTSP every 24 month, Remember: The National Supervisory Body can request additional Conformity Assessments if necessary.
- full liability for QTSP
- obligation to inform about any security or privacy breach within dedicated time to relevant authority by QTSP including affected person
- obligation to fulfil all requests for change in case of non-conformities by QTSP
- Especially the requirements from Art. 24 have to be mentioned:
- (a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.
- (b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards.

- c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law
- (d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use.
- (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
- (f) use trustworthy systems to store data provided to it, in a verifiable form so that:
- (I) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,
- (ii) only authorised persons can make entries and changes to the stored data,
- (iii) the data can be checked for authenticity.
- (g) take appropriate measures against forgery and theft of data.
- (h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically.
- (I) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (I) of Article 17(4);
- (j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;
- (k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.
- (l) provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

Furthermore, further in the context of trust services 2015/1506 should not be forgotten which defines the mandatory signature formats for mutual recognition according to Art. 27 of the eIDAS Regulation and is also still valid under eIDAS 2.0.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

The trust model of eIDAS is described in Section 3.

2.1.3 Relationship between eIDAS and technical framework

Concerning EUDIW as well as QTSP eIDAS is underpinned through technical framework of European standardization bodies. Those standards will be foreseeably referenced within the Implementing Acts and basement for the conformity assessment of the CAB. The picture below shows the basic approach on the conformity assessment by example of (qualified) trust services. This means:

1. Assessment of fundamental requirement agnostic from certain (qualified) trust service against ETSI EN 319 401 which include e.g., overall security, risk management, business continuity, records management, service management, termination plans)
    a. Stage 1: Documents
    b. Stage 2: Onsite
2. Assessment of specification requirements depending on type of (qualified) trust service to be qualified
    a. Stage 1: Documents
    b. Stage 2: Onsite

The picture below shows the approach by example.

.

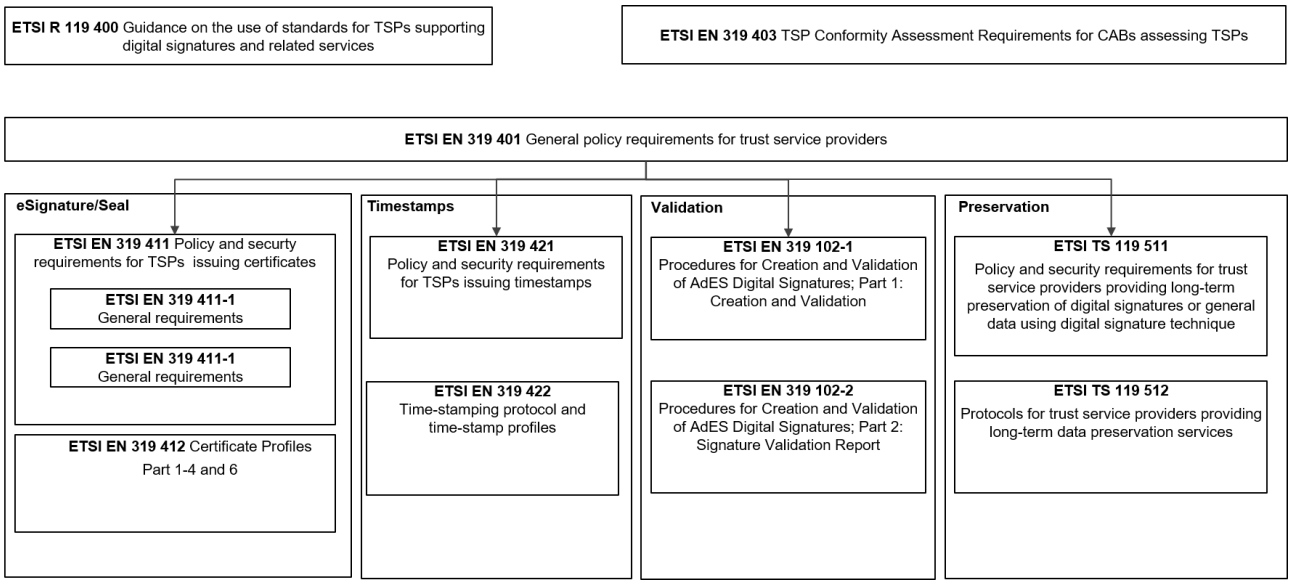

Figure 1: Fundamentals on relationship between eIDAS-standards

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

2.1.4 Governance to become EUDIW-Provider and QTSP

2.1.4.1 EUDIW-Provider

Basically, the process for wallet providers to become EUDIW Provider is as following:

1. Decision by Member State about Issuance Model:
    a. Member State
    b. On behalf of Member State
    c. Acceptance of Private Wallets

    Only in case b) and c) a private wallet provider is possible.
2. In case of b) and c): endorsement by Member State
3. In all cases: successful conformity assessment by Conformity Assessment Body
    a. Application at National Supervisory Body: Applicant for EUDIW Provider
    b. Selection of CAB: Applicant for EUDIW Provider
    c. Conformity Assessment: CAB
        i. Stage 1: Document Audit
        ii. Stage 2: Onsite Audit
    d. Submission Assessment Report to National Supervisory Body: CAB
    e. Approval EUDIW Provider: National Supervisory Body
    f. List in National Trust List: National Supervisory Body
    g. Compilation in LOTL: European Commission

The PID Provider will be defined by each Member State in own responsibility. The PID of a user is issued into the EUDIW in communication PID-Provider and EUDIW during issuance process of the EUDIW for each user.

2.1.4.2 QTSP

Basically, the process for wallet providers to become EUDIW Provider is as following:

1. Application at National Supervisory Body: Applicant for certain qualified trust service
2. Selection of CAB: Applicant for certain qualified trust service
3. Conformity Assessment: CAB
    a. Depending on kind of (qualified) trust service: necessity for certified product e.g., QSCD (Annex II eIDAS 2.0, CEN EN 419 241) in case issuing qualified certificates for QES/QSeal

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

   b. Stage 1: Document Audit
   c. Stage 2: Onsite Audit
4. Submission Assessment Report to National Supervisory Body: CAB
5. Approval EUDIW Provider: National Supervisory Body
6. List in National Trust List: National Supervisory Body
7. Compilation in LOTL: European Commission

2.2 Electronic Ledger in eIDAS 2.0

2.2.1 Terminology

The term "Ledger" is defined in ISO 22739 which was adopted as CEN EN into European standardization Framework and is so mandatory in terms of European standardization. In order to ensure a coherent European standardization framework as requested by CEN Internal Regulation Part 1 as well as ETSI Directive it`s recommended to follow this definition:

- Ledger 3.54.
  information store that keeps records of transactions that are intended to be final, definitive and immutable
- Distributed Ledger
  ledger that is shared across a set of distributed ledger technology (DLT) nodes and synchronized between the DLT nodes using a consensus mechanism

This means that DLT is technical only a special kind of ledger and the basic properties like immutability as well as the fact that on ledger records are final per definition are valid for any kind of ledger. The only difference between a ledger and a distributed ledger is the distributed provision – all other properties are similar as describe in section 3.2

ISO 22739 is standardized in ISO Tc 307 for which CEN JTC 19 is the European mirror committee.

2.2.2 Ledger in eIDAS 2.0

The eIDAS 2.0 establishes a pan-European legal framework on (de-centralized digital identities and (qualified) trust services as an amendment of the already implemented eIDAS 1.0. As the regulation is technology neutral it`s possible to use DLT as infrastructure for or by any component or actor within the eIDAS 2.0 ecosystem:

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

This means also that it has to be differentiated between:

- EUDI Wallet and/or (qualified) trust services using electronic ledger as well as any subcomponent like Trust lists (Trusted issuer registries etc.)
- QTSP for Electronic Ledger

There`s no dependency between EUDI Wallet, QTSP using Ledger and a certain QTSP for Electronic Ledger intended by the regulation. The following table shows the differentiation in detail:

#	Subject	Role of Ledger	Section 11 applicable

1	EUDI Wallet	• Infrastructure for
		  ○ PID
		  ○ (Q)EAA (with QTSP)
		  ○ QES (with QTSP)
		• Trusted Issuer Registries
		• TrustList/Trust Anchors
		• Verifiable Data Registry
			no

2	Other QTSP using Ledger	• QES • QSeal • QTimestamp • eDelivery and registered mail • Remote signing • Validation • Preservation • Archiving • Trusted Issuer Registries • TrustList/Trust Anchors	no
2	QTSP for Electronic Ledger	Infrastructure • Nodes • Validator Nodes • Consensus Mechanism • SmartContract Machine Applications	yes

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

#	Subject	Role of Ledger	Section 11 applicable
		• Cryptocurrencies • Supply chain • Data traceability • Product traceability • Document traceability	
3	Use cases in non-regulated domains	• Dito	yes

Table 1: Role of Electronic Ledger within eIDAS

2.2.3 EUDI Wallet and QTSP using Ledger

2.2.3.1 Fundamentals

EUDI Wallet and QTSP using Ledger means that an EUDIW Provider or provider of one of the following (qualified) trust services.

- Creation (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps
- Validation of (qualified) electronic signatures, seals and/or timestamps
- Issuance of (qualified) attestations of attributes
- (qualified) Electronic registered mail/ delivery services
- (qualified) Preservation of (qualified) electronic signatures and/or seals
- (qualified) website certificates
- Management of secure signature creation devices
- Archiving

use an Electronic Ledger as infrastructure for the certain EUDI Wallet or (qualified) trust service but not provide the Ledger as (qualified) trust service.

The security and compliance of the ledger will be in this case audited by the Conformity Assessment Body during the conformity assessment acc. Art. 5c and 20 eIDAS 2.0 of the certain EUDI Wallet or (qualified) trust service. It´s possible that an EUDIW Provider or QTSP of the (qualified) trust services mentioned above might use a QTSP for Ledger to provide the necessary infrastructure but in this case the QTSP for Ledger is a 3rd party provider on behalf of

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

the actual EUDIW Provider or QTSP using it, similar e.g. to providers of HSM acc. CEN EN 419 241 as e.g. requested for (qualified) trust services issuing (qualified) certificates for QES or QSeal acc. ETSI EN 319 411 and 412. But there`s no mandatory requirement for certain EUDIW Provider nor QTSP using Ledger to integrate a QTSP for Ledger or in this case qualified ledger.

2.2.3.2 Relevant technical framework

Standardization on EUDIW and QTSP using Ledger is currently done on one hand by eIDAS Toolbox Group on the other hand by ETSI ESI (QTSP except Archiving and Electronic Ledger) and CEN (Tc 224 on hardware security of EUDIW, Tc 468 on QTSP for Archiving and foreseeable CEN JTC 19 on QTSP for Ledger). Annex 1 contain an overview of existing ETSI and CEN standards on (qualified) trust services. Those standards are under revision according eIDAS 2.0. The following table shows main existing standardization projects on EUDIW and new (qualified) trust services

(qualified) trust service	**Standardization project**
EUDIW	ETSI TS 119 472 ETSI TS 119 475
Qualified Attestations of attributes	ETSI TS 119 471 ETSI TR 119 476

Table 2: Main standards on EUDIW and QEAA

2.2.4 Qualified Trust Service Provider for Electronic Ledger

2.2.4.1 Fundamentals

With Section 11 eIDAS 2.0 also introduces (qualified) trust services on Electronic Ledger (Art. 45h following). [eIDAS2] defines that qualified ledgers “are created and managed by one or more qualified trust service provider or providers, establish the origin of data records in the ledger, ensure the unique sequential chronological ordering of data records in the ledger and record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time”. Although eIDAS 2.0 is technology neutral the description in Art. 45i is in line with the definition of DLT in international standards as ISO 22739 and contains core properties of DLT. Since the requirements on QTSP also apply for QTSP for Ledger these standards will also be the basement for certification by independent conformity assessment body and so ensure proven security and trust in DLT. It has to be stated that Section 11 focus on

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

all use cases not covered by EUDIW or all other (qualified) trust services mentioned in section 3.2. This means that a QTSP for Ledger may provide services like:

- Technology
  - Whole DLT network
  - Validator Nodes
  - Consensus mechanism
  - Smart contract machine
- Applications
  - Traceability
  - Tokenization
  - Digital Currencies

For the European Blockchain Service Infrastructure the different roles of Electronic Ledger within eIDAS 2.0 contains several options to be integrated in the eIDAS ecosystem.

2.2.4.2 Relevant Technical Framework

The standardization on Ledger is mainly in the responsibility of ISO Tc 307 (worldwide) and CEN JTC 19 (Mirror Committee in Europe). The main standards relevant in the context of ledger and eIDAS, so identity, trust and their certification contain following table:

Committee	Standard	Scope	Status
ISO Tc 307	ISO 22739	Terminology	Final
	ISO TR 22349	Overview of existing DLT systems for identity management	Final
	ISO 23257	Reference Architecture	Final
	ISO TS 23635	Guidelines for governance	Final
	ISO TR 23644	Overview of trust anchors for DLT-based identity management	final
	ISO DTR 24332	Blockchain and DLT in relation to authoritative records, records systems, and records management	Final draft Publication appr. Q4/2024

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Committee	Standard	Scope	Status
	ISO TS 23353	Auditing Guidelines	Stable draft Publication appr. Q1/2025
	ISO TS 23516	Interoperability Framework	Stable draft Publication appr. Q1/2025
CEN JTC 19	New Work Item	Policy and security requirements on QTSP for Ledger Basement: ISO TS 23353, ISO 23257, ISO 22739, ISO TS 23635 Compliance to: ETSI	Proposed Publication appr. Q1/2025

Table 3: Relevant Technical Framework on Electronic Ledger

2.2.5 Summary

In summary it can be stated:

- Electronic Ledger within eIDAS 2.0 means any kind of ledger:
  - Centralized ledger
  - Distributed Ledger
- Electronic Ledger has to be considered in two different categories
  - EUDIW and QTSP using Ledger, where the ledger is only the infrastructure for certain wallet and/or (qualified) trust service.
  - QTSP for Ledger
- EUDIW/QTSP using Ledger are not covered by Section 11 eIDAS and do not depend on a QTSP for Ledger
- Only QTSP for Ledger is covered by Section 11
- The provisions for any EUDIW and/or QTSP given in eIDAS 2.0 apply also in case of Electronic Ledger
- Technical Framework on eIDAS has to be adjusted to integrate Electronic Ledger

Co-funded by the European Union

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

2.3 Possible Role of EBSI

2.3.1 Fundamental

EBSI is special kind of DLT network. The EDIC as basically an organization owned by the participating Member States acts as the fundamental operation authority. This means that the fundamental components of the DLT network owned and provided by and in final responsibility of Member States taking part in EDIC so e.g.:

- Main nodes
- Consensus mechanism
- Governance
- Basic identity-, access- and authorization management
- Basis security on core infrastructure reg. ISO 27001
- Risk management acc. ISO 31.000
- Service management including service levels acc. ISO 20.000
- Business Continuity acc. ISO 22301.

In case EBSI is used as infrastructure for EUDIW and/or QTSP using the EUDIW as well as the (qualified) trust service would be application or services build on top of the infrastructure so:

- Identity Management (EUDIW)
- Trust Service

These applications together with the infrastructure they use form the actual wallet and especially (qualified) trust service as subject of conformity assessment of the CAB. This leads to the conclusion that in case EBSI is used as infrastructure for EUDIW or QTSP using Ledger both will achieve additional trust in comparison to other EUDIW/QTSP not using EBSI because the EUDIW/QTSP using Ledger will always rely on governmental trust – exactly the basic infrastructure provided by EDIC on which the EUDIW/QTSP using Ledger is implemented and operated as de facto application/service. EUDIW/QTSP not using EBSI rely on an infrastructure:

- EUDIW
    - Provided by Member State or
    - Provided by Private Entity (in case MS use issuance option that EUDIW provided by private entities endorsed by MS)
- QTSP

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

- Provided by private entity.

Although those infrastructures always part of the conformity assessment they represent, especially if provided only by provided entity, only one trust layer without governmental trust anchor (except the PID based on notified eID Scheme), means the user relies on private entity only. In case EBSI is used the user of certain EUDIW/QTSP using Ledger relies on provider of EUDIW/qualified trust service including the infrastructure provided through EDIC and so the Member States.

Beside the utilization of Electronic Ledger as infrastructure for EUDI Wallet or QTSP using Ledger the ledger can also be used as Trusted Registry meaning:

- Issuer Registry
- Verifier Registry.

This would mean an Electronic Ledger could technically replace the existing TrustList acc. Art. 22 eIDAS resp. ETSI TS 119 612 which is currently implemented in XML. As with the new (qualified) trust services like QEAA the number of QTSP will foreseeably increase the current XML may not fulfill the required scalability across Europe.

2.3.2 Trusted Registry

The already existing Trusted Issuer Registry of EBSI could be reused as solution for a scalable Trust List in eIDAS 2.0. This would mean that EBSI will be the infrastructure and the Trusted Issuer Registry could be extended towards all QTSP, so also issuance of qualified certificates or provision of preservation services, means the Registry will be used as evidence for the trusted status of the certain QTSP. The status itself could be issued as QEAA by the national Supervisory Bodies using EBSI or other infrastructures. Beside the Trusted Issuer Registry EBSI could also provide the registration for Relying Parties acc. Art. 5b eIDAS 2.0.

In the final consequence this means that EBSI could be used to build up complete trust chains in order to automize the trust framework of eIDAS 2.0 and ensure the real-time provability of e.g.:

- Status of QTSP
- Trustworthiness of conformity assessment reports
- Needed certificates for conformity assessment.
- Identity of Supervisory Bodies, CAB, QTSP etc.

Details on how this could be automized contains Section 4.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

The following Recommendations are made in order to use EBSI as Trusted Registry within eIDAS 2.0.

- Adjustment EBSI Governance acc. TrustList reg. Art. 14 and 22 eIDAS
- Segregation of responsibilities (organizational and technical) between EDIC and National Supervisory Bodies[2] and European Commission
- Assessment
- Adjustment of related EBSI and ETSI/CEN technical framework[3] according eIDAS to improve TrustList on scalability.

2.3.3 Electronic identification/EUDI Wallet

2.3.3.1 Fundamentals

As described in section 3.2 an electronic ledger can be used as infrastructure for a certain EUDI Wallet for natural and/or legal entities (Enterprise Wallet). This may include e.g., a decentralized PKI for DID-Management as done currently with EBSI, but also for key management of certain PID. In any case the endorsement of the certain EUDIW and/or PID by certain member state is needed. This includes:

- PID for natural entities
- PID for Legal Entities (Organizational Identities)

In case EBSI is used as infrastructure for the EUDIW and to ensure the migration of existing wallets certified against EBSI technical framework it`s required to integrate the EBSI specific requirements into the relevant standards on EUDIW[4] to be referenced by implementing acts acc. Art. 5a and c eIDAS 2.0. The reason is that the Conformity Assessment Body will use those standards for certification of the EUDIW.

Like described in Section 3.1.1 the EUDIW has to fulfil LoA “high” acc. Art. 8 eIDAS 2.0. This does not mean that in every use case this LoA is really needed. According to a well-grounded risk analysis in practice most of the use cases require max. LoA “substantial”. This means that also existing EBSI wallet can be used as long as the personal identification data (See Art. 24 eIDAS) issued e.g., as (Q)EAA into the wallet fulfil at least LoA “substantial”.

[2] See Section 3
[3] Trust Model | EBSI hub
[4] See Section 3.2.3

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Annex 2 contain the template for a risk management to assess the needed LoA for use cases. The risk management is based on the mythology of ISO 27005 and can so easily adopted into the existing ISMS in certain organizations. An exemplary analysis for the application area of EBSI VECTOR so Social Security and Education lead to the result that:

- -80–85% LoA “substantial”
- 10–15 % LoA “low”
- 5–10 % Loa “high”

Means, in most cases no LoA “high” needed. On the other hand it`s possible to use a Qualified Attestation of Attributes also for identification purposes as long as the Relying Party does not replace the EUDI Wallet. This analysis matches with results done on the 52 most important e-government services in Germany which one of the authors of the present document did. This analysis delivered same results for areas like construction affairs, social affairs, health care, environmental affairs, economic development, mobile driver licenses, public transport etc. Only in case of psychological evidences or vehicle registration (where it´s required by law in Germany) LoA “high” was needed.

With regard to the obligations to issue and accept an EUDIW for member states and defined relying parties it´s also recommended to enable EUDIW using EBSI to store not only the PID on LoA “high”, but additionally other Attestation used for personal identification which could be executed using (Q)EAA. In this case an EBSI Wallet which is certified as EUDIW can be used in 2 modes: LoA “high” and LoA “substantial” – recommended especially in case LoA “high” may limit the user-friendliness of the EUDIW. As existing EBSI wallet in most cases fulfil LoA “substantial”, the described approach could ensure an easy migration and growth of the EBSI ecosystem within eIDAS 2.0.

2.3.3.2 EBSI Wallets as EUDI Wallets

In order to ensure that existing EBSI certified wallets may be used as EUDIW in eIDAS 2.0 the wallet provider have to follow the process described in Section 3.1.4.

Additionally, the certification framework for EUDIW should contain optional parts, means if certain applicant for EUDIW wants to become EBSI compliant at same time, the CAB shall assess the related conditional requirements too.

The following measures are recommended to integrate EBSI in the EUDIW-Framework of eIDAS.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Category	Subject

Fundamental	Definition of business model and related roles, responsibilities and processes of EDIC correlated with eIDAS (EUDIW)
	Adjustment of EBSI act, Section 3.3.1 so
	- Security
	  o Main nodes
	  o Consensus mechanism
	  o Governance
	- Basic identity-, access- and authorization management
	- Basis security on core infrastructure reg. ISO 27001
	- Risk management acc. ISO 31.000
	- Service management including service levels acc. ISO 20.000
	- Business Continuity acc. ISO 22301.
	Strategy Development for migration of existing EBSI-Wallets into eIDAS:
	• Endorsements of Member States on EUDIW
	• Assessment EBSI use cases on LoA.
	• Approach for additional "PID" on LoA lower than "high"

Governance	Adjustment of EBSI governance to eIDAS so: • Integration EBSI requirements in EUDIW Conformity Assessment • Adjustment EBSI certification framework
Technology	Ensuring that ARF contains EBSI core subjects. Adjustment EBSI VC and Certification Framework acc. ARF and ETSI/CEN Standards

Table 4: Recommendations Integration EBSI in EUDIW

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

2.3.4 QTSP using Ledger.

2.3.4.1 Fundamentals

As described in Section 3.2.3 EBSI could be used as infrastructure for following (qualified) trust services:

- Creation (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps
- Validation of (qualified) electronic signatures, seals and/or timestamps
- Issuance of (qualified) attestations of attributes
- (qualified) Electronic registered mail/ delivery services
- (qualified) Preservation of (qualified) electronic signatures and/or seals
- (qualified) website certificates
- Management of secure signature creation devices (Art. 29a)
- (qualified) Archiving (Art. 45h)

Especially the QEAA stuff would serve the current use cases of EBSI which are mainly focused on issuance and verification of verifiable credentials as identity attributes such as diploma, social security, digital product passport etc. using EBSI certified wallet which might be migrated into the eIDAS ecosystem as described in Section 3.3.2.

The aims could be:

(qualified) Trust Service	**Role of EBSI**
Issuance (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps,	Decentralized PKI
Issuance (qualified) timestamps only	Delivery of DLT native (qualified) timestamps
Validation of (qualified) electronic signatures, seals and/or timestamps	Decentralized PKI
Issuance of (qualified) attestations of Attributes	Decentralized PKI
(qualified) Electronic registered mail/ delivery services	Audit Trail Decentralized PKI for the QES/QTS

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

(qualified) Trust Service	Role of EBSI
(qualified) Preservation of (qualified) electronic signatures and/or seals	Audit Trail Integrity preservation
Issuance of qualified) website certificates	Decentralized PKI
(qualified) Archiving	Integrity protection and proof

Table 5: Role of EBSI in QTSP using Ledger.

In any case EBSI or those part relevant for the certain QTSP would be part of the related conformity assessment executed by certain CAB and subject to the requirements on QTSP acc. Art. 20 ff. as described in Sections 3.1.2 and 3.1.3. As EDIC provides EBSI the QTSP using the Ledger will need at least an agreement with the EDIC which covers distribution of tasks between both parties regarding obligations from the relevant technical framework for certain type of QTSP which may be related to EDIC.

2.3.4.2 Integration EBSI in QTSP using Ledger

In case EBSI is used through a QTSP it is basically a component for a certain (qualified) trust service. The component can be expressed in two variants:

- EBSI native provided through EDIC
- EBSI provide through a QTSP for Ledger, which could be EDIC or another 3rd party

In any case EBSI or parts of it would become part of the QTSP using the ledger as infrastructure. This means an agreement between EDIC/ QTSP for Ledger and the QTSP using it has to be established.

The steps for certain applicant to become (qualified) trust service provider contains Section 3.1.4. The specifics in case EBSI used as infrastructure or component are:

- EBSI native provided through EDIC
  - No specifics in processes to 3.1.4
  - Security of EBSI proven in conformity assessment by CAB acc. to the specific standards of the intended (qualified) trust service
  - possibly: Specific component certification equivalent to Annex II eIDAS 2.0
- EBSI provide through a QTSP for Ledger
  - No specifics in processes to 3.1.4

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

- Security of considered as existing during conformity assessment by CAB, as long as qualified status of ledger documented (proven in Stage 1)

The following measures are recommended to achieve the utilization of EBSI for QTSP using Ledger:

Category	**Subject**

Fundamental	Definition of business model and related roles, responsibilities and processes of EDIC correlated with eIDAS.
	
	Clarification of renumeration as QTSP always provided for renumeration.
	
	Adjustment of EBSI act, Section 3.3.1 so
	
	- Security
	  - Main nodes
	  - Consensus mechanism
	  - Governance
	- Basic identity-, access- and authorization management
	- Basis security on core infrastructure reg. ISO 27001
	- Risk management acc. ISO 31.000
	- Service management including service levels acc. ISO 20.000
	- Business Continuity acc. ISO 22301.

Governance	Segregation of responsibilities between QTSP using EBSI and the EDIC Adjustment of EBSI Governance acc. eIDAS 2.0[5]
Technology	Assessment and Adjustment of ETSI/CEN-Standards on QTSP for • Creation (qualified) certificates for (qualified)

[5] See Section 3 ff.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Category	Subject
	electronic signatures, seals and/or timestamps • Validation of (qualified) electronic signatures, seals and/or timestamps • Issuance of (qualified) attestations of attributes • (qualified) Electronic registered mail/ delivery services • (qualified) Preservation of (qualified) electronic signatures and/or seals • (qualified) website certificates • Management of secure signature creation devices • (qualified) Archiving Adjustment of related EBSI technical framework[6] according eIDAS so especially relevant ETSI/CEN standards on trust services and related implementing acts (QEAA November 2024, all other April 2025) as well as qualification of DLT native timestamps Definition the Ledger to be use by QTSP has to fulfil certain functional requirements from European Standard for Ledger to product certification of QSCD to ensure common security on ledgers Definition that certain European Standard for Ledger has to ensure the interoperability with worldwide standardization framework

Table 6: Recommendation on using EBSI for QTSP using Ledger.

[6] Trust Model | EBSI hub

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

2.3.5 QTSP for Ledger

2.3.5.1 Fundamentals

For QTSP for ledger EBSI or those part relevant for the certain QTSP would be part of the related conformity assessment executed by certain CAB and subject to the requirements on QTSP acc. Art. 20 ff. as described in Sections 3.1.2 and 3.1.3.

With regards to the specific governance of EBSI after which the EDIC as fundamental operating organization always provides main nodes always the following questions occurs to define the concrete design of the role of EBSI in case of QTSP for Ledger:

- Portfolio of QTSP, means: What provides the QTSP?
- Provider of QTSP, means: Who is the QTSP?

2.3.5.2 Portfolio

The main role of EBSI within eIDAS 2.0 could be the provision by a qualified trust service provider for ledger. The possible portfolio of such a QTSP can be focused on 2 categories.

- Technology and infrastructure
- Applications

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

The categories can e.g., include the following specific subjects:

Category	**Content (examples)**
Technology and infrastructure	• Validator Nodes • Consensus Mechanism • Smart contract machines
Applications	• Traceability • Tokenization • Cryptocurrencies

Table 7: Possible Portfolio QTSP for Ledger

2.3.5.3 Provider

As described in section 3.3.1 EBSI is special kind of DLT Network as it`s provided through EDIC and any qualified trust service will be de facto a service build on top of the basic infrastructure.

Against this background and the possible portfolio mentioned in previous section there are several options for the possible provider of a (qualified) trust service for Ledger with given advantages and disadvantages.

- EDIC as QTSP (EDIC or parts of EDIC)
  - Takes all responsibilities given in section 3.1.2
  - Takes additionally all responsibilities independently from the eIDAS subject.
- Another Public or Private Entity as QTSP
  - Takes all responsibilities given in section 3.1.2
  - Use the infrastructure provided by EDIC.
  - EDIC acts as 3rd party provider to the QTSP
  - EDIC may provide building blocks to support interoperability for certain subjects e.g.:
    - Smart Contracts
    - Traceability Toolbox
    - Tokenization Toolbox

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Category	Role QTSP	Advantages	Disadvantages
Technology and infrastructure	EDIC	- Combination of all duties in one organization - Liability ensured by governments. - Less effort in correlation of governance eIDAS and EBSI	- Limitation of EDIC due to liability risks of QTSP - Restriction of competition as EDIC only infrastructure provider - High complexity especially in case of smart contract machines - High effort for EDIC on conformity assessment - Limited segregation of duties

	Private entity which relies on EDIC	- EDIC only 3rd party provider for QTSP decrease effort for EDIC.
		- Additional trust layer for QTSP
		- Technical flexibility and room for improvement
		- Economical risk mainly at private company
		- No restrictions on competition
		- EDIC could provide building blocks to ensure
			- Surrender of control for EDIC
			- Addiction of EDIC to QTSP[7]
			- Complexity on business model for EDIC
			  ○ QTSP
			  ○ Non QTSP subjects
			- Higher effort on interoperability

[7] Would be there anyway in case EUDIW/QTSP using Ledger

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Category	Role QTSP	Advantages	Disadvantages
		interoperability	
Applications	EDIC	- Combination of all duties in one organization - Liability ensured by governments. - Easier to ensure interoperability as only one QTSP possible	- Limitation of EDIC due to liability risks of QTSP - Restriction of competition as EDIC only infrastructure provider - High complexity as application areas is de facto unlimited - High effort for EDIC on conformity assessment - Limited segregation of duties
	Private entity which relies on EDIC	- EDIC only 3rd party provider for QTSP decrease effort for EDIC. - EDIC could provide building blocks to ensure interoperability. - Additional trust layer for QTSP - Technical flexibility and room for improvement - Economical risk mainly at private company - No restrictions on	- Surrender of control for EDIC - Addiction of EDIC to QTSP[8] - Complexity on business model for EDIC ○ QTSP ○ Non QTSP subjects Higher effort on interoperability

[8] Would be there anyway in case EUDIW/QTSP using Ledger

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Category	Role QTSP	Advantages	Disadvantages
		competition	

Table 8: Assessment Provider Options for QTSP for Ledger

2.3.5.4 EBSI as QTSP for Ledger

In case EBSI provided by QTSP for Ledger (Technology or Applications) the Electronic Ledger is basically the portfolio of the (qualified) trust service. This can be provided as mentioned in section 3.3.5.3.

In any case EBSI or parts of it would become de facto the (qualified) trust service In case EDIC is not the QTSP itself this means an agreement between EDIC and the QTSP for Ledger has to be established.

The steps for certain applicant to become (qualified) trust service provider contains Section 3.1.4. The specifics in case EBSI used as infrastructure or component are:

- No specifics in processes to 3.1.4
- Security of EBSI proven in conformity assessment by CAB acc. to the specific standards for Electronic Ledger acc. Section 11 eIDAS 2.0

The following measures are recommended to achieve the utilization of EBSI becoming QTSP for Ledger

Category	Subject
Fundamental	Definition of business model and related roles, responsibilities and processes of EDIC correlated with eIDAS: • Definition who becomes QTSP for Ledger • Portfolio QTSP for Ledger • Billing models • Necessary contracts Clarification of renumeration as QTSP always provided for renumeration. Adjustment of EBSI act, Section 3.3.1 so - Security o Main nodes

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Category	Subject
	○ Consensus mechanism ○ Governance - Basic identity-, access- and authorization management - Basis security on core infrastructure reg. ISO 27001 - Risk management acc. ISO 31.000 - Service management including service levels acc. ISO 20.000 - Business Continuity acc. ISO 22301.
Governance	Segregation of duties between EDIC and QTSP Adjustment EBSI Governance acc. eIDAS
Technology	Development dedicate European Standard for Electronic Ledger (rec. CEN JTC 19) in compliance with existing European Standards on QTSP Standard shall recognize EBSI Technical Framework and ensure interoperability with worldwide standards ISO TS 23353, ISO 23258, ISO TS 23635

Table 9: Recommendation for EBSI in QTSP for Ledger

2.3.6 Summary

2.3.6.1 Role of EBSI within eIDAS 2.0

Basically, EBSI could fulfil following roles within eIDAS 2.0:

Subject	Role of EBSI
Fundamental	Trusted Registry to provide scalable alternative to XML-based TrustList acc. Art. 14 and 22 eIDAS so: - Trusted Issuer Registry - Trusted Verifier (Relying Party) Registry

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Subject	Role of EBSI
EUDIW	3rd party infrastructure provider (decentralized PKI) for EUDIW Infrastructure for wallets on EBSI certified to be used in case with LoA "Substantial" or lower. EBSI wallets endorsed by Member States as EUDIW for natural and/or Legal Entity so especially EBSI Enterprise Wallet Infrastructure for QTSP issuing personal identification data as QEAA on LoA "substantial" additionally to PID to provide bridge for EBSI Wallets
QTSP using Ledger	3rd party Infrastructure for certain QTSP so especially QEAA for EBSI use cases like diploma
QTSP for Ledger	Subject of (qualified) trust services which focus on: - Technology and infrastructure - Applications QTSP: - EDIC - Private entities

Table 10: Summary Role of EBSI within eIDAS

2.3.6.2 Necessary Measures

So that EBSI can fulfil the possible roles the following measures are recommended

Role of EBSI	Measures
Fundamental	Definition of business model and related roles, responsibilities and processes of EDIC correlated with eIDAS for EUDIW, QTSP using Ledger and QTSP for Ledger Adjustment of EBSI Governance according eIDAS Trust

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Role of EBSI	Measures
	Framework[9] Automatization eIDAS Trust Framework with EBSI acc. Section 4 Adjustment of EBSI and EDIC with subjects acc. Section 3.3.1
Trusted Registry	Adjustment of related EBSI technical framework[10] according eIDAS so especially ARF and relevant ETSI Standards (e.g., ETSI TS 119 612) and related implementing acts (April 2025) Segregation of responsibilities (organizational and technical) between EDIC and National Supervisory Bodies[11] and European Commission
EUDIW	Alignment with Member States on endorsement for EUDIW using EBSI, especially EBSI Enterprise Wallet and issuance of PID for legal entities segregation of responsibilities between EUDIW Provider using EBSI, Member States issuing the EUDIW and the EDIC Adjustment of related EBSI technical framework[12] according eIDAS so especially ARF and relevant ETSI Standards as well as related implementing acts (November 2024) Assessment of use cases against Art. 8 eIDAS (LoA) Correlation EBSI certification framework and eIDAS

[9] Proposal contains Section 4
[10] Trust Model | EBSI hub
[11] See Section 3
[12] Trust Model | EBSI hub

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Role of EBSI	Measures
	conformity assessment Technical bridge for EBSI certified wallets
QTSP using Ledger	Segregation of responsibilities between QTSP using EBSI and the EDIC Adjustment of related EBSI technical framework[13] according eIDAS so especially relevant ETSI/CEN standards on trust services and related implementing acts (QEAA November 2024, all other April 2025) Adjustment ETSI/CEN standards on trust services using EBSI
QTSP for Ledger	Definition of responsibility for QTSP (Who is the QTSP) Definition and detailing of possible portfolio for QTSP Segregation of responsibilities between QTSP and the EDIC Definition of Technical Framework for QTSP for Ledger aligned with EBSI to be referenced by implementing acts (April 2025) and correlated with worldwide standardization so especially ISO TS 23353, ISO 23258, ISO TS 23635

Table 11: Summary necessary measures for integration EBSI in eIDAS

3 Trust Model eIDAS 2.0

eIDAS 2.0 complements the well-known trust model from eIDAS 1.0. This means that any EUDIW will be certified by a CAB against technical requirements provided within European standards referenced by mandatory implementing acts. The eIDAS Toolbox Group, a group of experts from different member states together with European standardization bodies, develops the framework of technical requirements, the EU Architecture and Reference Framework (ARF).

[13] Trust Model | EBSI hub

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Every EUDIW will be provided under responsibility of a member state, logically expanding the trust chain. The same holds true for PID providers accepted by the member state. Comparable to eIDAS 1.0, a trustworthy digital identity, no matter if it is a PID, an EAA or any other eIDAS trust service, always requires proof and supervision by a trusted third party. There is no trust by default. Trust is established on European law, supervised by European and national supervisory bodies, accreditation of CAB under European standards, certification of trust services by CAB under supervision of national supervisory bodies and verifiable via Europe-wide Trust Lists – based on democratically created law, mutual control and certification but also transparent verifiability. EUDIW, (Q)EAA and electronic ledger as well as decentralized identities are only integrated in this trust model following the known and proven trust approach in Europe14. The picture below illustrates these extended trust chains15:

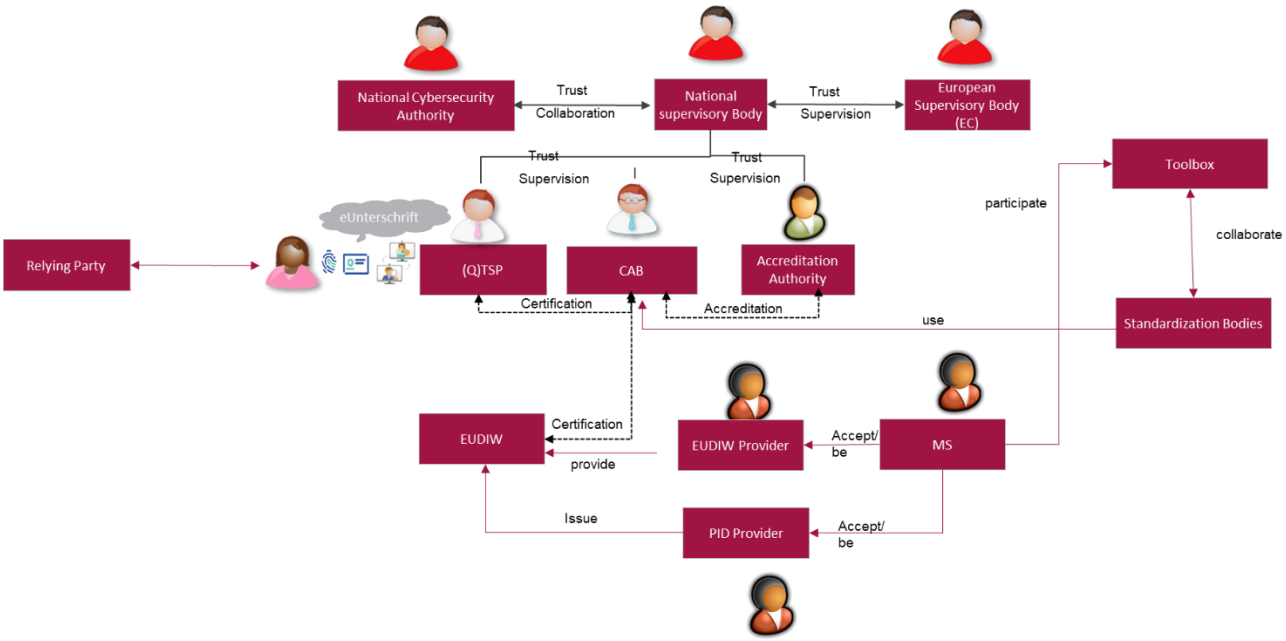

Figure 2: Trust Model eIDAS

[14] I. Alamillo, S. Schwalm 2021. S. Schwalm: Trusted transaction in Electronic Ledger? Overview on international standardization in DLT. Seeblock Webinar Blockchain Education & Standardisation: Navigating (beyond) the European Landscape. 2023. https://seeblocks.eu/events/blockchain-education-standardisation-navigating-beyond-european-landscape

[15] S. Schwalm: EU Digital Wallet Chances and challenges for EU Digital Identity a German perspective. MyData Conference 2023. Helsinki 2023.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

The section below describes the roles and responsibilities in detail.

3.1 Roles and Responsibilities

3.1.1 Fundamentals

Roles	**Responsibilities**
National Ministry	eID Issuance and endorsement EUDI Wallet Strategic responsibility for notification eID Scheme and decision PID Provider
National Cybersecurity Body (Can be practically same institution as National Supervisory Body)	eID Coordination of notification eID Scheme Requirements on eID Scheme and Wallet Cybersecurity requirements on EUDI Wallet Certification authority for PID Provider QTSP Defines requirements on cybersecurity related subjects. Typically, responsible for adoption and national requirements reg. NIS 2 (relevant for QTSP)
National Supervisory Body (can be represented by 1-n authorities)	Supervision for: • EUDI Wallet Provider • Qualified Trust Service Provider • Conformity Assessment Bodies Includes: • Approval of Conformity Assessment Reports as basement for listing in Trust List

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Roles	Responsibilities
	• Responsibilities acc. Section 2 eIDAS 2.0 Art. 20 eIDAS 2.0
National Accreditation Body	Accreditation of Conformity Assessment Bodies including withdrawal (in collaboration with National Supervisory Body)
Conformity Assessment Body (CAB)	Conformity Assessment of EUDI Wallet Providers and any QTSP
EUDI Wallet Provider	Provision of EUDI Wallet endorsed my Member State Responsibilities acc. Art. 6 eIDAS 2.0 Underlies supervision by National Supervisory Body Certified by CAB
PID Provider	Provision of endorsed by Member State Certified and approved by Member State provided PID relies on requirements acc. Section II eIDAS 2.0
Qualified Trust Service Provider	Provision of certain (qualified) trust service acc. Chapter III eIDAS 2.0 Underlies supervision by National Supervisory Body Underlies Conformity Assessment by National Supervisory Bodies against standards from ETSI ESI and/or CEN CENELEC Fully liable of its business acc. Art. 13 eIDAS
Toolbox Group	Provides fundamental technical requirements on EUDI Wallet, PID and other Attestations as well as Relying Parties in the Architecture and Reference

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Roles	Responsibilities
	Framework
Standardization Bodies	Provide standards on QTSP, EUDI Wallet and related components. Technical Framework for Conformity Assessment by CAB
Member State	Provides EUDI Wallet acc. Art. 6 eIDAS 2.0. Endorse EUDI Wallet Provider Provides notified eID Scheme for PID acc. Section II eIDAS 2.0. Approves PID Provider Appoints National Supervisory Body and National Cybersecurity Body
Trust List Provider	Provision of Trust List acc. Art. 22 eIDAS 2.0 Currently typically (by national law) • National Supervisory Body (National TL) • European Commission (LOTL)
Authentic Source	Registry for provision of data to be attested by (qualified) Attestation Provider Announced by Member State (typically Ministry responsible for QTSP)

Table 12: Fundamental roles in eIDAS

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

3.1.2 Dependencies

3.1.2.1 EID and EUDI Wallet

Notification eID Scheme (necessary for PID Issuance)

Authority	Responsibility
National Cybersecurity Authority with responsible Ministry	Development eID Scheme
National Cybersecurity Authority	Application for notification at EC
European Commission	Provision for Peer Review
National Cybersecurity Authorities of Member State	Peer review and report
European Commission	Check reports and grant notification

Table 13: Roles in Notification eID Schemes

PID/ODI Provider (Natural and legal entities)

Authority	Responsibility
National Cybersecurity Authority with responsible Ministry	Definition legal and technical requirements
PID Provider	Application for certification
National Cybersecurity Authority	Start Certification
Certification Body	Audit and submit report
National Cybersecurity Authority	Check reports and grant certification

Table 14: Roles reg. PID Provider

Issuance EUDI Wallet (natural entities and Enterprise Wallet for legal entities)

Authority	Responsibility
Responsible Ministry	Decision about issuance Model
EUDIW Provider	Application for certification

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

National Supervisory Body	Inform CAB
EUDIW Provider	Contract CAB
Conformity Assessment Body	Conformity Assessment and submit report
National Supervisory Body	Check report and grant certification. Integration in trust list Consolidate trust list to EC
European Commission	Consolidate LOTL

Table 15: Roles Issuance EUDI Wallet

3.1.2.2 Qualified Trust Service Provider

Accreditation Conformity Assessment Body

Authority	**Responsibility**
Applicant	Apply for accreditation
National Accreditation Body	Checks application Contracts certification Body
Certification Body	Audit and report
National Accreditation Body	Check report and grant accreditation. Inform National Supervisory Body
National Supervisory Body	List CAB Inform EC
European Commission	List CAB

Table 16: Roles Accreditation CAB

Establish Qualified Trust Service

Note: The Conformity assessment has to be repeated every 2 years, for new (qualified) trust services the re-audit has to be done 1 year after the initial one.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Authority	**Responsibility**
QTSP	Apply for qualification
National Supervisory Body	Inform to engage CAB
QTSP	Contract CAB
Conformity Assessment Body	Conformity Assessment and submit report
National Supervisory Body	Check report and grant certification. Integration in trust list Consolidate trust list to EC
European Commission	Consolidate LOTL

Table 17: Roles to establish QTSP.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

4 Trust Model of EBSI within eIDAS 2.0

4.1 Introduction

The following description aims to map the EBSI Trust model to eIDAS 2.0 with focus on:

- QTSP
- Products for QTSP

As the trust chain for EUDIW is not defined yet, a mapping will be postponed. Taking into account the different roles within eIDAS 2.0 described in section 3 and the EBSI Trust Model[16]. The processes describe the fundamental flow, the acting authorities in terms of eIDAS and their roles in terms of EBSI Governance. As a result, the explanations can also be used to automize the issuance, verification and revocation of certain status of the certain actors (e.g., CAB, QTSP, EUDIW Provider etc.) within the Trust Framework.

Since the eIDAS Trust Framework is highly complex it`s divided into several trust chains those interaction enables the functionality of the framework.

4.2 Mapping EBSI Trust Model to eIDAS 2.0

4.2.1 Trust Chain Qualified Trust Service Provider

[16] https://hub.ebsi.eu/vc-framework/trust-model/issuer-trust-model-v3

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

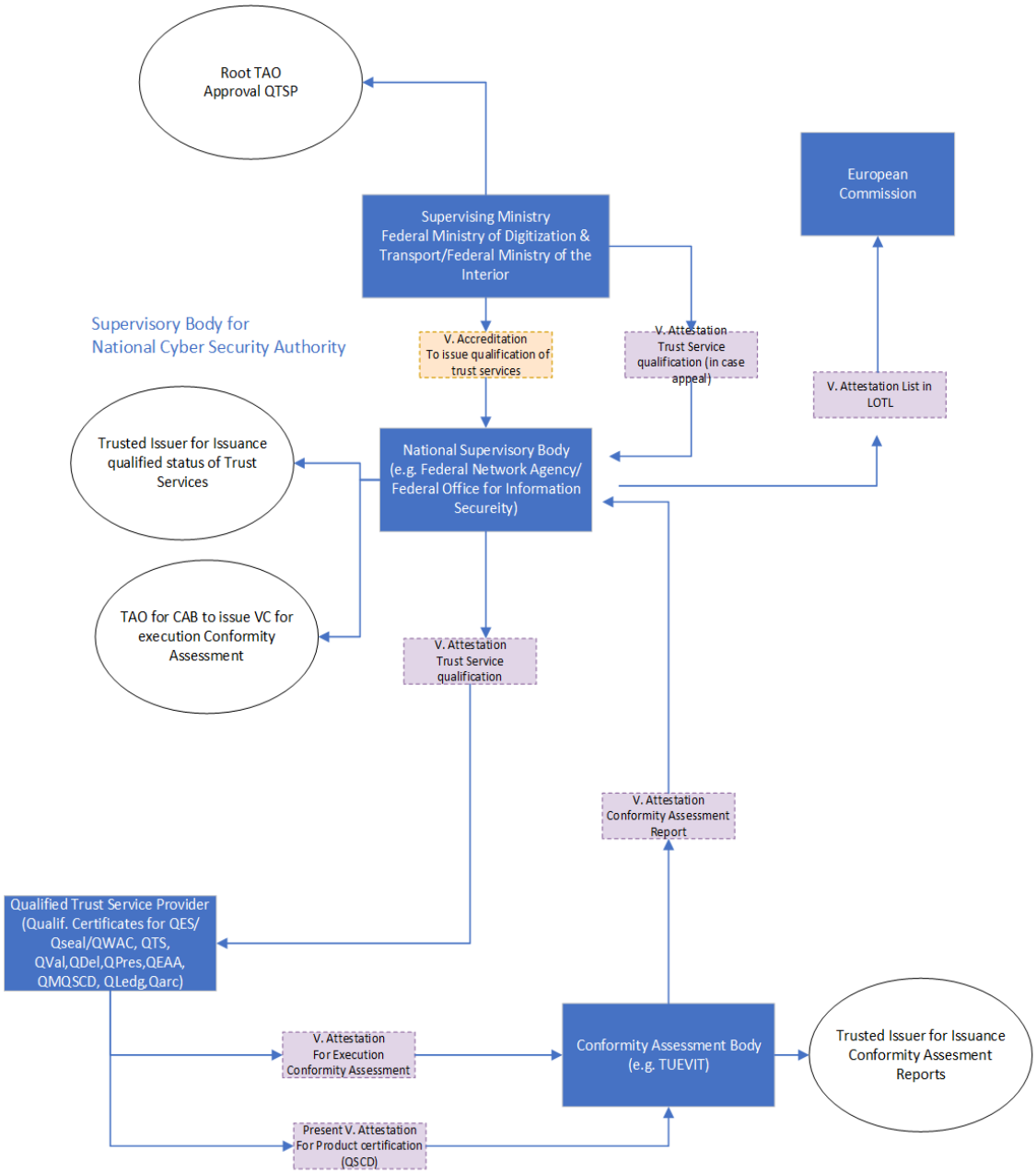

Figure 3:Trust Chain QTSP

Co-funded by the European Union

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Process Flow

Role acc. eIDAS	Role acc. EBSI	Task
Supervisory Ministry	Root TAO	Accreditation National Supervisory Body as Trusted Issuer Attestation QTSP in case of appeal of QTSP against decision of National Supervisory Body
National Supervisory Body	Trusted Issuer	Issuance Attestation Trust Service qualification to applicant (possible QTSP) Issuance (or revocation) qualified status of Trust Services Issuer for Attestation to be listed in TrustList
	TAO	Accreditation applicant on QTSP to issue attestation to QTSP to start conformity assessment
CAB	Trusted Issuer	Issuance Conformity Assessment Report
	User	Presentation Conformity Assessment Report to National Supervisory Body
Applicant for QTSP	Trusted Issuer	Issuance Attestations for Attestation for Execution Conformity Assessment
	User	Presentation Attestation for Product certification (QSCD in case QTSP for QES/QSeal/QWAC)

Table 18: Process Flow Trust Chain QTSP

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

4.2.2 Trust Chain Accreditation of Conformity Assessment Body

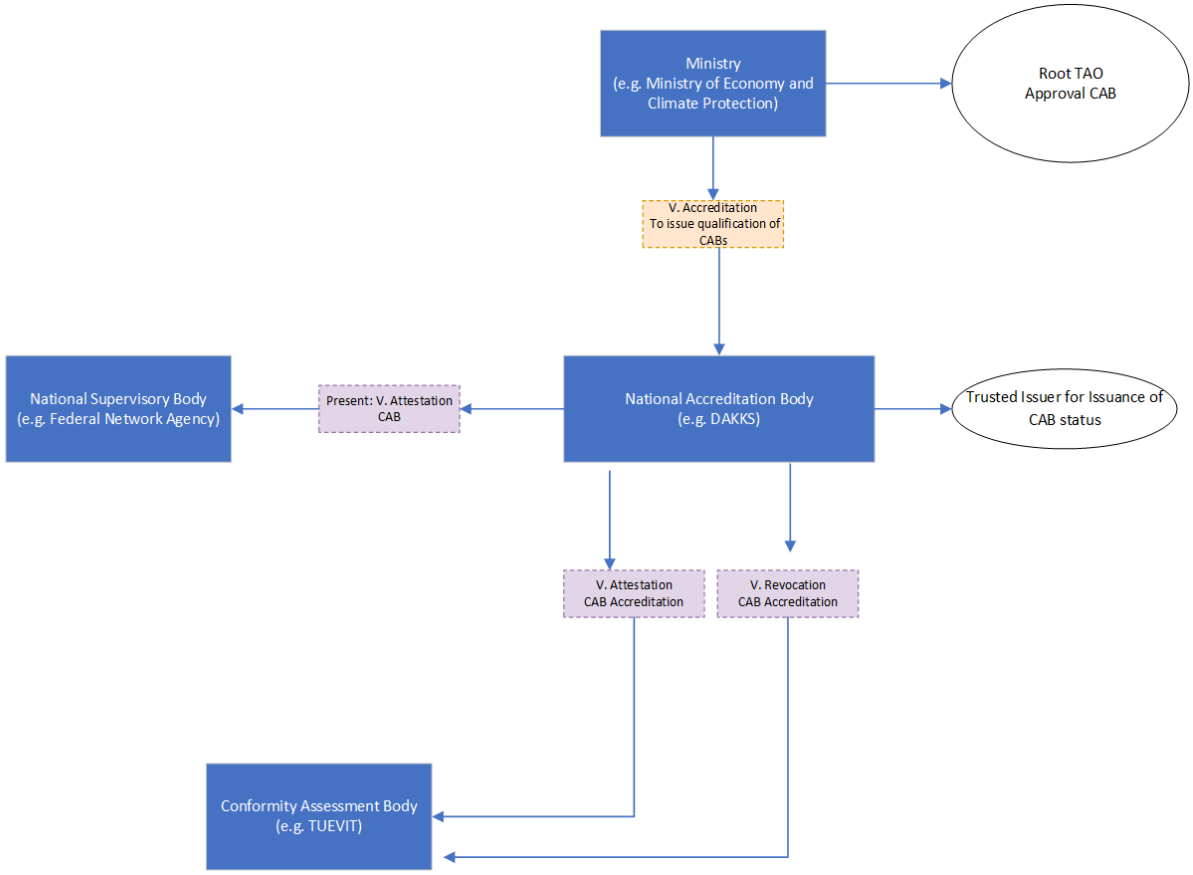

Figure 4: Trust Chain Accreditation

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Process Flow

Role acc. eIDAS	Role acc. EBSI	Task
Ministry	Root TAO	Accreditation of National Accreditation Body
National Accreditation Body	Trusted Issuer	Issuance and Revocation of CAB status
	User	Presentation Attestation CAB status to National Supervisory Body
Conformity Assessment Body	User	Gets Issuance and Revocation of CAB status

Table 19: Process Flow Trust Chain Accreditation CAB

4.2.3 Trust chain Product Certification related to QTSP.

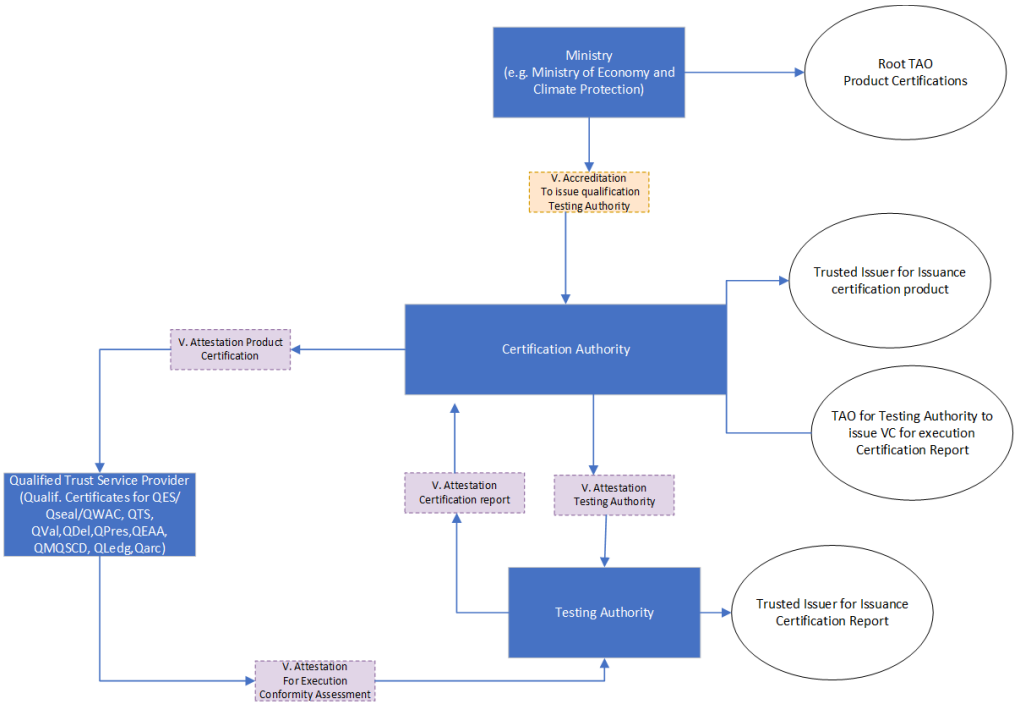

Figure 5: Trust Chain Product Certification

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Process Flow

Role acc. eIDAS	Role acc. EBSI	Task
Ministry	RootTAO	Accreditation to issue qualification Testing Authority
Certification Authority	TAO	TAO for Testing Authority to issue attestation for Certification Report
	Trusted Issuer	Issuance attestation product certification to Product Provider Issuance Attestation Testing Authority
Test authority	Trusted Issuer	Issuance attestation for Certification Report
Product Provider	User	Present Attestation to Test Authority execute the audit. Gets attestation product certification to Product Provider

Table 20: Trust Chain Product Certification

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

5 Conclusions and Recommendations

5.1 Overview

The advent of eIDAS 2.0 and the introduction of qualified electronic ledgers mark a significant milestone in the evolution of digital identity and trust services. These ledgers, with their unique ability to ensure the uniqueness, authenticity, and correct sequencing of data entries, are poised to revolutionize various sectors, from cross-border trade to public services, and even extend their influence beyond the EU.

On the other hand, the European Blockchain Service Infrastructure is established and EDIC as the operating authority founded. This leads to the need to refine the role of EBSI within eIDAS recognizing and migrating the existing EBSI Governance, technical framework as well as wallets and use cases in danger. At same time Electronic Ledger are integrated in eIDAS 2.0, first of all as possible infrastructure for EUDIW or certain qualified trust service providers, second as explicit qualified trust service provider for Electronic Ledger.

The role of Electronic Ledger within eIDAS 2.0 has to be differentiated as given below:

#	Subject	Role of Ledger	Section 11 applicable

1	EUDI Wallet	• Infrastructure for
		  ○ PID
		  ○ (Q)EAA (with QTSP)
		  ○ QES (with QTSP)
		• Trusted Issuer Registries
		• TrustList/Trust Anchors
		• Verifiable Data Registry
			no

2	Other QTSP using Ledger	• QES • QSeal • QTimestamp • eDelivery and registered mail • Remote signing • Validation • Preservation • Archiving • Trusted Issuer Registries • TrustList/Trust Anchors	no

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

#	Subject	Role of Ledger	Section 11 applicable
2	QTSP for Electronic Ledger	Infrastructure ● Nodes ● Validator Nodes ● Consensus Mechanism ● SmartContract Machine Applications ● Cryptocurrencies ● Supply chain ● Data traceability ● Product traceability ● Document traceability	yes
3	Use cases in non-regulated domains	● Dito	yes

Table 21: Role of Electronic Ledger in eIDAS

Against this background especially the following subjects and recommendations shall be considered.

5.2 Fundamental

EBSI can basically play following roles within the eIDAS ecosystem:

- Trusted Registry so scalable technical alternative to current XML-based TrustList
- Infrastructure for EUDIW/PID
- Infrastructure or component for QTSP using Ledger.
- Object of QTSP for Ledger (Section 11)

With regard to the fact that EDIC is owned by the Member States it has to be stated that in any case EBSI is used within eIDAS it provides always a higher level of Trust than EUDIW or QTSP using other technology.

Background: In case of EBSI the EUDIW or QTSP using it, is build on top of the EBSI and so the governmental infrastructure provided by EDIC – it always relies on governmental trust anchor. In case of

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

EUDIW/QTSP using another technology, they rely on only one structure without government trust anchor.

Independently from this it has to be recognized that eIDAS 2.0 follows its own mandatory Trust Framework which directly determines the integration of EBSI. As described in section 3 and 4 this can be automized using EBSI and so EBSI bring added value and additional trust in the eIDAS Ecosystem.

The following recommendations for concrete measures are made.

- Definition of business model and related roles, responsibilities and processes of EDIC correlated with eIDAS for EUDIW, QTSP using Ledger and QTSP for Ledger
- Adjustment of EBSI Governance according eIDAS Trust Framework (section 3)
- Automatization eIDAS Trust Framework with EBSI acc. Section 4
- Adjustment of EBSI and EDIC with subjects acc. Section 3.3.1

5.3 Trusted Registry

The already existing Trusted Issuer Registry of EBSI could be reused as solution for a scalable Trust List in eIDAS 2.0 (Art. 14 and 22). In the final consequence this means also that EBSI could be used to build up complete trust chains in order to automize the trust framework of eIDAS 2.0 and ensure the real-time provability of e.g.:

- Status of QTSP
- Trustworthiness of conformity assessment reports
- Needed certificates for conformity assessment.
- Identity of Supervisory Bodies, CAB, QTSP etc.

Details on how this could be automized contains Section 4.

The following Recommendations are made in order to use EBSI as Trusted Registry within eIDAS 2.0.

- Adjustment EBSI Governance acc. TrustList reg. Art. 14 and 22 eIDAS
- Segregation of responsibilities (organizational and technical) between EDIC and National Supervisory Bodies[17] and European Commission
- Assessment

[17] See Section 4

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

- Adjustment of related EBSI and ETSI/CEN technical framework[18] according eIDAS to improve TrustList on scalability.

5.4 EUDI Wallet

The eIDAS 2.0 requests the Member States to issue EUDIW mandatorily with following options:

- By a member state
- Under authority of a member state
- Recognized by a member state.

Only Wallets endorsed by certain Member State can become EUDIW. Any EUDIW has to be certified by CAB during Conformity Assessment against European Standardization Framework and listed in the Trust List acc. eIDAS. Any EUDIW has to contain a PID for natural or legal entities (depending on if wallet for natural entity or Enterprise Wallet) from Member State and to fulfill LoA "high" acc. eIDAS.

This sets the related EBSI Governance as EBSI contains own wallet certification and as there are EBSI wallets already in use which mainly fulfill eIDAS LoA "substantial" maximum. As in not all use cases LoA "high" and so EUDIW is needed it`s necessary to assess the relevant use cases with the template given in Annex 2. Based on this the migration scenarios for EBSI Wallets can be defined. As EBSI contains own certification scheme for wallets also the related governance has to be adjusted including the role of EDIC in case EBSI used as infrastructure for certain EUDIW.

The following recommendations are made:

- Alignment with Member States on endorsement for EUDIW using EBSI, especially EBSI Enterprise Wallet and issuance of PID for legal entities
- segregation of responsibilities between EUDIW Provider using EBSI, Member States issuing the EUDIW and the EDIC
- Adjustment of related EBSI technical framework19 according eIDAS so especially ARF and relevant ETSI Standards as well as related implementing acts (November 2024)

[18] Trust Model | EBSI hub
[19] Trust Model | EBSI hub

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

- Assessment of use cases against Art. 8 eIDAS (LoA)
- Correlation EBSI certification framework and eIDAS conformity assessment
- Technical bridge for EBSI certified wallets
- Endorsement from Member State

5.5 QTSP using Ledger.

Qualified Trust Service Provider using Ledger means that QTSP providing one of the following qualified trust services would use EBSI as infrastructure or component:

(qualified) Trust Service	Role of EBSI
Issuance (qualified) certificates for (qualified) electronic signatures, seals and/or timestamps,	Decentralized PKI
Issuance (qualified) timestamps only	Delivery of DLT native (qualified) timestamps
Validation of (qualified) electronic signatures, seals and/or timestamps	Decentralized PKI
Issuance of (qualified) attestations of Attributes	Decentralized PKI
(qualified) Electronic registered mail/ delivery services	Audit Trail Decentralized PKI for the QES/QTS
(qualified) Preservation of (qualified) electronic signatures and/or seals	Audit Trail Integrity preservation
Issuance of qualified) website certificates	Decentralized PKI
(qualified) Archiving	Integrity protection and proof

Table 22: Role of EBSI in QTSP using Ledger.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

Any QTSP has to fulfill the requirements given in section 3.1.4 and will be certified by CAB in Conformity Assessment against European Standardization Framework[20]. In order to enable QTSP using EBSI the following recommendations are made:

- Segregation of responsibilities between QTSP using EBSI and the EDIC
- Adjustment of related EBSI technical framework[21] according eIDAS so especially relevant ETSI/CEN standards on trust services and related implementing acts (QEAA November 2024, all other April 2025)
- Adjustment ETSI/CEN standards on trust services using EBSI

5.6 QTSP for Ledger

With regards to the specific governance of EBSI after which the EDIC as fundamental operating organization always provides main nodes always the following questions occurs to define the concrete design of the role of EBSI in case of QTSP for Ledger:

- Portfolio of QTSP, means: What provides the QTSP?
- Provider of QTSP, means: Who is the QTSP?

The following portfolio could be possible:

Category	Content (examples)
Technology and infrastructure	• Validator Nodes • Consensus Mechanism • Smart contract machines
Applications	• Traceability • Tokenization • Cryptocurrencies

Table 23: Possible Portfolio QTSP for Ledger

Against this background and the possible portfolio mentioned in previous section there are several options for the possible provider of a (qualified) trust service for Ledger with given advantages and disadvantages.

[20] eIDAS Governance s. Section 3
[21] Trust Model | EBSI hub

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.
Co-funded by the European Union

- EDIC as QTSP (EDIC or parts of EDIC)
    - Takes all responsibilities given in section 3.1.2
    - Takes additionally all responsibilities independently from the eIDAS subject.
- Another Public or Private Entity as QTSP
    - Takes all responsibilities given in section 3.1.2
    - Use the infrastructure provided by EDIC.
    - EDIC acts as 3rd party provider to the QTSP
    - EDIC may provide building blocks to support interoperability for certain subjects e.g.:
        - Smart Contracts, Traceability Toolbox
        - Tokenization Toolbox

In any case the following measures are recommended to integrate EBSI into QTSP for Ledger

- Definition of responsibility for QTSP (Who is the QTSP)
- Definition and detailing of possible portfolio for QTSP
- Segregation of responsibilities between QTSP and the EDIC
- Definition of Technical Framework for QTSP for Ledger aligned with EBSI to be referenced by implementing acts (April 2025) and correlated with worldwide standardization so especially ISO TS 23353, ISO 23258, ISO TS 23635

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Abbreviations

See https://medium.com/@schwalm.steffen/collection-of-eidas-identity-related-terms-and-abbreviations-d14eada34364

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Bibliography

[AlSc22] Alamillo, Dr. I., Schwalm S.: Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of [eIDAS2]. European Review of Digital Administration & Law - Erdal2021, Volume 2, Issue 2, pp. 89-108

[ALStScTh24] Alamillo, Dr. I., Schwalm S., Stoecker, C., Thiermann, R.: Qualified Ledgers: Bridging the Gap between Blockchain Technology and Legal Compliance. 2024.

[ArchGER23] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v1

[ARF23] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. The European Digital Identity Wallet Architecture and Reference Framework. December 2023; https://github.com/skounis/architecture-and-reference-framework/blob/80d00cf5ad1c3930235e4140b1fc8a975638f787/docs/arf.md

[BSI19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019

[BSI21] Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Bundesamt für Sicherheit in der Informationstechnik. Bonn 2021

[BSI23] Federal Office for Information Security (BSI): Basics of Digital Signature Techniques and Trust Services. Legal Framework, Technical Aspects. 2023

[CENTR17982] European Digital Identity Wallets standards Gap Analysis

[CyberSecAct] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[DINTS31648] DIN TS 31648:2021. Criteria for trusted transaction. Records Management and Evidence Preservation in Distributed Ledger Technologies and Blockchain.

[EBSI] EBSI, European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI, accessed: 30/03/2020

[eIDAS1] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

[eIDAS2] 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

[ETSIEN319411] ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSITS119471] ETSI TS 119 471 Policy and Security requirements for Providers of Electronic Attestation of Attribute Services

[ETSITS119612] ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists.

[ETSITR119476] ETSI TR 119 476 Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes

[GDPR] Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.

[HKH20] Hellwig, D., Karlic, G., & Huchzermeier, A. Build Your Own Blockchain. Springer International Publishing.

[IDW21] [ISO22739] ISO 22739:2020: Blockchain and distributed ledger technologies - Terminology, 2020

[ISOTR24332] ISO DTR 24332. Information and documentation — Blockchain and DLT in relation to authoritative records, records systems, and records management

[Ko20] Korte, U. et. al.: Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation. OpenIdentity Summit 2020. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2020 S. 49-60

[Ko21] Korte, U. et. Al.: Records Management and Long-Term Preservation of Evidence in DLT. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2021. Bonn: Gesellschaft für Informatik e.V.. (131-142)

[NIS2] DIRECTIVES DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[RCG19] Reddick, C. G., Cid, G. P., & Ganapati, S. Determinants of blockchain adoption in the public sector: An empirical examination. Information Polity, 24(4), 379–396.

[Sc23] Schwalm S.: Trusted transaction in Electronic Ledger?. Overview on international standardization in DLT. Seeblock Webinar DLT Standardization. 10.11.2023.

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

[SoAl21] Sobolewski, M., & Allessie, D. Blockchain Applications in the Public Sector: Investigating Seven Real-Life Blockchain Deployments and Their Benefits. In M. P. and S. H. J. Reddick Christopher G. and Rodríguez-Bolívar (Ed.), Blockchain and the Public Sector: Theories, Reforms, and Case Studies (pp. 97–126). Springer International Publishing.

[W3VC] W3C VC Data Model v2.0. 2023

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Annex 1 Overview of existing standards on QTSP

See Section 2 of following document:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile&v=6

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union

Annex 2: Template Risk Analysis on Level of Assurance

·oject co-funded by the European Union under the Digital Europe Programme under Grant Agreement n°)1102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect ıose of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European nion nor the granting authority can be held responsible for them.

Co-funded by the European Union