BLOCKSTAND

European Trust Model based on EBSI and Reusable eIDAS Attestations

Author: Samuel Gómez (Gataca Labs S.L.U.)
Date: 10-04-2025
Version: 1.0

Table of Contents

Scope and Purpose

The establishment of a secure, scalable, and interoperable European trust model for digital identity is a foundational requirement for the Digital Single Market. As the European Union transitions from the relatively static architecture defined by eIDAS 1.0 to the more dynamic, decentralized, and user-centric framework envisioned under eIDAS 2.0, it becomes imperative to revisit the mechanisms through which **trust** is established, delegated, and resolved.

Under eIDAS 1.0, trust was primarily grounded in centralized notification mechanisms maintained by Member States and the European Commission. These took the form of national and EU-wide trusted lists, which designated recognized trust service providers and authentication schemes. While adequate in controlled environments with a limited number of actors, such an approach cannot be scaled to accommodate the significantly broader and more heterogeneous landscape introduced by the European Digital Identity Wallet (EUDI Wallet) and the European Blockchain Services Infrastructure (EBSI).

The trust model envisioned for eIDAS 2.0 represents a paradigmatic shift. It replaces centralized trust silos with a federated architecture involving thousands of decentralized entities. Universities, public administrations, private companies, and sectoral bodies across Europe may simultaneously act as issuers, verifiers, and holders of verifiable credentials. This multidirectional participation creates a vast and dynamic ecosystem that cannot be supported by static, manually maintained trust lists.

Static trust lists were never designed to support federated accreditation processes, real-time resolution of trust metadata, or automated delegation mechanisms across borders. Their reliance on human intervention and legal formalities renders them unsuitable for a digital identity ecosystem operating at scale, with high-frequency interactions across national and institutional boundaries.

To address these limitations, Europe must adopt a trust infrastructure that is inherently decentralized, dynamic, and resilient. It must enable programmatic discovery, accreditation, and resolution of trusted entities while preserving legal assurance, traceability, and technical interoperability. Within this emerging architecture, EBSI provides the technical and procedural foundation necessary to operationalize this transformation.

At the heart of this infrastructure are four trust registries that collectively support the dynamic operation of the European trust model:

1. **Trusted Entity Registry (TER)** – A canonical registry containing structured metadata about all legal entities participating in the ecosystem. This registry serves as the primary reference for resolving which organizations are authorized to issue or verify credentials under defined conditions.

2. **Trusted Accreditation Registry (TAR)** – A registry dedicated to capturing the legal or sectoral accreditations granted to entities by Member States or other competent

authorities. These accreditations define both the ability to issue specific types of credentials and the legal basis to request or process particular categories of data.

3. **Trusted Schema Registry (TSR)** – This registry provides the semantic and structural definitions of the credential types that circulate within the ecosystem. It ensures that issuers and verifiers operate using harmonized, machine-readable data models, enabling semantic interoperability across jurisdictions.

4. **DID Registry** – A *"decentralized public key infrastructure"* that binds decentralized identifiers (DIDs) to their corresponding cryptographic verification methods. Although DIDs are being analyzed (CEN JTC 19) as compatible with the legal and technical framework of eIDAS 2.0 (ETSI TS 119 612), their use within the trust model remains discretionary. Each entity may choose whether or not to adopt DIDs as part of its credential lifecycle and trust resolution mechanisms. Consequently, the DID Registry, while offering a technically robust solution for secure key management and decentralized resolution, is an optional component. The EBSI trust model is fully operable without it (common PKI), and participation in the ecosystem, whether for federation, accreditation, or credential validation, does not depend on its implementation.

Together, these registries support a machine-readable, legally accountable, and technically interoperable model of trust. They replace the rigid, human-managed processes of eIDAS 1.0 with a flexible and scalable trust framework that aligns with the functional needs of the EUDI Wallet and future digital identity ecosystems.

This document sets out to define the architecture, components, and operational principles underpinning this new trust model. In doing so, it provides a reference framework for Member States, institutions, and service providers to adopt a common, federated approach to digital trust, one that enables legal certainty, supports decentralization, and fosters seamless cross-border interoperability.

Normative References

The trust model described in this document is not conceived in isolation. It builds upon, and aligns with, a comprehensive set of legal, technical, and architectural references established at the European and international levels. These references provide the regulatory foundation, the functional vocabulary, and the architectural principles required to implement a federated, interoperable, and legally trustworthy digital identity ecosystem across the European Union.

At the regulatory level, the model is grounded in the principles and obligations set forth by the original **Regulation (EU) No 910/2014 (eIDAS 1)**, which introduced a pan-European legal framework for electronic identification and trust services. The evolution of this framework is currently embodied in the **Regulation (EU) 2024/1183**, commonly referred to as **eIDAS 2.0**, which expands the scope to include the **European Digital Identity Wallet (EUDI Wallet)** and establishes new obligations around interoperability, decentralization, and user control.

To complement these legal instruments, the trust model draws upon international standards that define the foundational concepts and requirements for digital identity systems. The **ISO/IEC 23042** series, developed under the Joint Technical Committee 1 (JTC 1) of ISO and IEC, plays a central role. Specifically:

- **ISO/IEC 23042-1:2023**, which formalizes core terminology and identity concepts, ensuring semantic alignment across implementations.
- **ISO/IEC 23042-2:2024**, which introduces a reference architecture and defines functional requirements for identity systems, with a focus on decentralization, lifecycle management, and trust interoperability.

From a technological and infrastructural perspective, the **European Blockchain Services Infrastructure (EBSI)** serves as the operational backbone for implementing the trust model in practice. Its published **technical specifications** and **trust model guidance** documents detail how decentralized trust registries, verifiable credentials, and peer-to-peer identity mechanisms can be integrated in compliance with EU policy objectives.

Aligned with these efforts is the **European Self-Sovereign Identity Framework (ESSIF)**, which is built atop EBSI and serves as the canonical architecture for decentralized identity within European institutions. The ESSIF architecture introduces a governance layer on top of W3C Verifiable Credentials, anchoring them in national legal frameworks and enabling cross-border recognition.

On the data modeling side, the trust model adheres to the **W3C Verifiable Credentials Data Model v2.0**, a global standard that defines the structure and semantics of digital credentials in a decentralized environment. This ensures technical compatibility not only within Europe but also with international ecosystems, thereby supporting global interoperability.

Additionally, the trust model benefits from lessons learned through applied innovation. Notably:

- The **EBSI Diplomas** pilot, which demonstrated cross-border issuance and verification of academic credentials between European universities.

- The **ESSPASS project**, funded under the **Connecting Europe Facility (CEF)**, which explored the portability and standardization of identity attestations within the health and mobility sectors.

Further relevant initiatives and frameworks include:

- The **ETSI TS 119 461** standard, which defines policy and security requirements for trust service components that provide identity proofing of trust service subjects. This specification aims to ensure that identity proofing processes are conducted with a high level of security and reliability, supporting the issuance of certificates at various policy levels, including those specified in ETSI EN 319 411-1 and ETSI EN 319 411-2.

- The **ETSI TS 119 612** standard, which defines a standardized framework for the creation and management of trusted lists by Trust List Scheme Operators (TLSOs). These lists provide authoritative information about the status and historical compliance of Trust Service Providers (TSPs) and their services with relevant legal and regulatory requirements, such as those outlined in the European Union's Regulation (EU) No 910/2014 (eIDAS Regulation).

- The **W3C Decentralized Identifiers (DID) Core Specification**, which underpins the optional use of decentralized identifiers in the EBSI trust model.

- The **OpenID for Verifiable Presentations (OIDC4VP)** and **OpenID for Verifiable Credential Issuance (OIDC4VCI)** specifications published by the **OpenID Foundation**, which offer standardized and interoperable mechanisms for the exchange of verifiable credentials within identity wallets.

While not all of these references are formally normative in a legal sense, they constitute the necessary framework of standards, architectural components, and governance conventions required to deploy a pan-European trust infrastructure that is both legally compliant and technologically robust.

Terms and Definitions

For the purposes of this document, the following terms apply:

- **Holder:** The subject in possession of a verifiable credential, typically through a European Digital Identity Wallet.
- **Issuer:** A trusted entity responsible for generating verifiable credentials in accordance with an accredited scheme.
- **Verifier:** An entity authorized to validate the authenticity and integrity of credentials received from holders.
- **Trusted Entity Registry (TER):** A registry of legal entities authorized to issue, verify, or act within the EBSI trust ecosystem. Formerly known as the Trusted Issuer Registry (TIR), it was renamed to Trusted Entity Registry (TER) to reflect the inclusion of verifiers alongside issuers, aligning the terminology with the broader scope of trusted roles under the updated trust model.
- **Trusted Accreditation Registry (TAR):** A dedicated registry containing accreditation information linked to entities listed in the Trusted Entity Registry (TER). The TAR consolidates and extends the data formerly embedded within the original Trusted Issuer Registry (TIR), now split for clarity. In addition to accreditations for credential issuance, it also includes new categories of authorizations, such as the right to request specific data or attributes. The separation between the TAR and the TER is logical rather than operational, aiming to modularize responsibilities within the trust model and to support more flexible authorization semantics across the EBSI ecosystem.
- **Trusted Unit of Verification (TUV):** A formally defined group of entities that share a common accreditation profile for verifying specific types of Verifiable Credentials within designated jurisdictions. Each TUV encapsulates the scope of credential types, schemas, and legal contexts for which its member entities are authorized to perform verification, simplifying governance for sectors or domains with standardized requirements.
- **Trusted Units of Verification Registry (TUVR):** A registry within the EBSI trust architecture that stores and publishes the official definitions of all recognized TUVs. It includes metadata such as group identifiers, supported credential schemas, jurisdictional scope, governance rules, and versioning. The TUVR enables entities to associate themselves with existing verification groups, facilitating streamlined and scalable accreditation processes.
- **Trusted Schema Registry (TSR):** A registry that stores machine-readable definitions (schemas) used across the ecosystem to ensure semantic interoperability of verifiable credentials.

- **DID Registry:** A decentralized registry that associates decentralized identifiers (DIDs) with cryptographic verification methods. While DIDs are compatible with the eIDAS 2.0 legal framework, their use remains optional within the EBSI trust model.
- **Credential Schema:** A machine-readable definition of the structure and semantics of a verifiable credential.
- **Verifiable Credential (VC):** A tamper-evident and cryptographically signed digital assertion about a subject, conforming to the W3C Verifiable Credentials Data Model.
- **Decentralized Identifier (DID):** A persistent identifier that does not require a centralized registry and can be resolved to retrieve public keys and service endpoints.
- **Electronic Attestation of Attributes (EAA):** An attribute-based credential issued by a Qualified Trust Service Provider (QTSP) under eIDAS 2.0, with legal validity equivalent to traditional identification documents.
- **European Digital Identity Wallet (EUDI Wallet):** A personal digital tool, established under eIDAS 2.0, that enables individuals and organizations to securely store, manage, and present verifiable credentials and electronic attestations.
- **Trust Service Provider (TSP):** An entity that delivers digital trust services, such as electronic signatures, timestamps, or attestations, and operates in accordance with eIDAS or equivalent legal frameworks.
- **Qualified Trust Service Provider (QTSP):** A Trust Service Provider that meets the requirements for enhanced legal recognition under eIDAS and is listed in a national trusted list.
- **Accreditation:** A formal recognition, typically issued by a competent authority, that authorizes an entity to perform specific trust-related roles, such as issuing or verifying credentials, in accordance with sectoral or legal mandates.
- **Trust List:** An authoritative list maintained in line with eIDAS 1.0 and ETSI TS 119 612, used to publish and validate the status of qualified trust service providers and their services.
- **Conformity Assessment Body (CAB):** An independent entity designated to evaluate whether Trust Service Providers meet the requirements of applicable standards, including those issued by ETSI.

Drivers for Change in the Trust Landscape

The evolution from eIDAS 1.0 to eIDAS 2.0 introduces a fundamental redefinition of the trust landscape in Europe. While the initial trust model successfully supported a relatively small and static ecosystem of approximately 400 Qualified Trust Service Providers (QTSPs), this scope is no longer sufficient to support the ambitions of the new European Digital Identity framework (https://eidas.ec.europa.eu/efda/home). Under eIDAS 2.0, the trust ecosystem must scale to accommodate not hundreds, but potentially **over 26 million entities**, corresponding to the total number of enterprises currently operating in the European Union (2024).

This exponential growth in the number of actors is driven by the structural principles of eIDAS 2.0: every enterprise, public body, or institution can act not only as a **verifier**, but also as an **issuer** of verifiable credentials. Consequently, the trust model must now account for legal entities across all sectors, including their accreditation status, cryptographic materials, authorization metadata, and associated schemas.

Under the eIDAS 1.0 framework, trust lists were published in accordance with **ETSI TS 119 612**, maintained by National Accreditation Bodies (NABs), and distributed as centralized XML files. These files, typically several megabytes in size, were downloaded and cached by relying parties who used them for verifying digital signatures, timestamps, digital authentications, etc. . Due to the low frequency of change and the relatively small number of entries, the administrative and technical management of such lists remained feasible within a centralized model.

In contrast, the eIDAS 2.0 trust model presents a scenario of **radical complexity and dynamism**. A centralized or monolithic trust list is no longer a viable solution. The file size alone, expected to grow into **multiple gigabytes**, renders it unsuitable for real-time usage or distribution. More critically, the **rate of change** within the ecosystem is expected to be continuous: new entities will enter, accreditations will be updated or revoked, roles will be delegated, and cryptographic keys will be rotated regularly. This level of volatility demands a system capable of real-time, selective, and context-aware resolution.

From an administrative perspective, this shift exacerbates the challenge. Under eIDAS 1.0, modifications to the trust list were infrequent and could be managed centrally by Member States. Under the new model, attempting to coordinate thousands, if not millions, of changes through centralized NABs would result in significant delays, bottlenecks, and governance failures. A centralized administrative structure cannot scale to handle **millions of potential issuers and verifiers**, along with their associated legal and technical metadata.

This is precisely where the **federated and decentralized trust infrastructure** introduced by EBSI becomes necessary. By distributing responsibility across sectoral and national actors, through components such as the **Trusted Entity Registry (TER)**, **Trusted Accreditation Registry (TAR)**, **Trusted Schema Registry (TSR)**, and optionally the **DID Registry**, the ecosystem gains the flexibility to scale dynamically while preserving legal accountability and traceability.

In summary, the unprecedented scale and change dynamics introduced by eIDAS 2.0 render centralized trust list management obsolete. To ensure interoperability, legal certainty, and technical resilience, the trust infrastructure must evolve into a **federated, discoverable, and machine-readable system**. This is no longer a design choice, but an operational necessity for the successful implementation of the European Digital Identity framework.

Conceptual Trust Model Architecture

The conceptual architecture proposed by EBSI for trust management represents a significant departure from the static models of eIDAS 1.0. Instead of relying on centralized trust lists curated by national bodies, the EBSI trust model is designed to operate in a dynamic, federated, and semantically interoperable ecosystem; capable of supporting millions of entities with complex legal and technical attributes.

At the foundation of this architecture are four integrated registries that collectively maintain the metadata required to establish and evaluate trust across borders and sectors. The **Trusted Entity Registry (TER)** serves as the canonical source of truth for identifying which legal entities are authorized to participate in the ecosystem. It contains structured information such as legal identifiers, jurisdiction, and cryptographic material, all of which are made machine-resolvable through public endpoints. Complementing this is the **Trusted Accreditation Registry (TAR)**, which captures the formal authorizations issued by competent national or sectoral authorities. These accreditations define what a given entity may do. What types of credentials it may issue, request, or verify, and under which regulatory scope.

To support semantic interoperability, the model incorporates a **Trusted Schema Registry (TSR)**. This registry provides the formal definitions (data structures, fields, semantics) for the verifiable credentials circulating within the ecosystem. By acting as a canonical source for credential schemas, the TSR ensures that all actors, regardless of jurisdiction or sector, interpret and process data in a consistent and predictable manner. It eliminates ambiguity in credential formats and enables automated validation and processing of claims across different systems. Without such a registry, the risk of mismatched interpretations, fragmented implementations, and failed verifications would significantly increase, undermining the core objective of cross-border interoperability. For this reason, the TSR is not merely an auxiliary component; it is **an indispensable pillar** of the architecture, without which the trusted exchange of verifiable credentials at European scale would not be feasible.

Finally, EBSI offers a **DID Registry**, enabling the resolution of decentralized identifiers to verification methods and service endpoints. Although DIDs are now considered legally compatible with eIDAS 2.0, their adoption is not mandatory. Entities may choose to operate using conventional identifiers or sector-specific PKI solutions, maintaining full compliance with the broader trust model. In the short term, it is not expected that DIDs will play a significant role within eIDAS 2.0 implementations, primarily because the identity and trust market in Europe remains dominated by mature Public Key Infrastructure (PKI) models. Nevertheless, decentralized identifiers have demonstrated clear advantages in other contexts, such as cross-domain interoperability, portability of credentials, and user-centric key management. Their potential for enabling flexible, privacy-preserving trust relationships suggests that they may serve as a valuable complement, if not a future evolution, of the current PKI-centric paradigm.

This architecture embraces the principles of decentralization, machine-readability, and verifiability. Each record, whether representing an entity, its accreditations, or its keys, is

designed to be independently auditable, programmatically accessible, and cryptographically verifiable. Importantly, accreditation, not mere self-assertion, forms the basis of authority: no entity can operate without an explicit, digitally signed accreditation linking its identifier to a role defined in the ecosystem.

Yet this new model does not exist in a vacuum. It must coexist and interoperate with legacy structures, most notably those defined under **ETSI TS 119 612**. This technical specification, which underpins the trusted lists in eIDAS 1.0, assumes a centralized publication model where national authorities distribute signed XML files containing information about qualified trust service providers. The structure is monolithic, the update cadence is infrequent, and the data is consumed as a static snapshot by stakeholder systems.

Herein lies a fundamental tension. EBSI is built for real-time discovery, dynamic resolution, and scalable participation. ETSI TS 119 612, in contrast, reflects a closed, predictable environment with few changes and tightly controlled publication. Attempting to scale TS 119 612 to accommodate the full trust ecosystem envisioned under eIDAS 2.0 would likely result in administrative and technical collapse. The file size alone would grow into multiple gigabytes; the update cycles would become chaotic; and stakeholders would be unable to process the trust data effectively.

Rather than discarding the ETSI framework, the proposed model advocates a bridging approach. National trusted lists may continue to serve as authoritative anchors, establishing the baseline of trust for qualified providers, while the broader ecosystem evolves towards a distributed publication model. Intermediary gateways can translate legacy trust list entries into EBSI-compatible formats, exposing them as records in TER or TAR. Likewise, schema alignment efforts can ensure that XML-based credential definitions are mapped into the JSON-based data structures used across EBSI.

This evolution naturally gives rise to a **hierarchical model of delegated trust**, in which authority flows from a **Root Trust Accreditation Organisation (Root TAO)** to **Trust Accreditation Organisations (TAOs)**, and from them to **issuers**. This layered structure reflects the principle of subsidiarity: trust is managed closer to the entities involved, while auditability and compliance remain anchored in legal and institutional authorities. Where necessary, national or supranational bodies may delegate part of their responsibilities to sectoral institutions, enabling accreditations to be issued and verified locally without compromising the overall legal validity and technical interoperability of the system.

In short, this trust model is not about abandoning established practice, but about expanding its reach. The centralized, monolithic logic of eIDAS 1.0 is no longer sufficient for an environment of this scale and complexity. The conceptual architecture presented here offers a federated alternative, one that distributes trust, maintains legal assurance, and is equipped to handle the operational realities of a digital Europe.

Trust Delegation Hierarchy and Role of TAOs

The operationalization of a federated trust model at European scale requires not only distributed registries and interoperable standards, but also a well-defined system for the **delegation of authority**. This is particularly relevant in the context of high-volume, high-granularity ecosystems, where thousands or millions of entities may need to issue or verify credentials under specific legal or functional mandates.

To address this, the EBSI trust model introduces a three-tiered **trust delegation hierarchy**, consisting of:

- A **Root Trust Accreditation Organisation (Root TAO)**, typically a supranational or national authority, which anchors the entire trust infrastructure by defining the overarching governance rules and accrediting first-level TAOs.
- One or more **Trust Accreditation Organisations (TAOs)**, which may correspond to Member State authorities, sectoral regulators, or pan-European governance bodies. These TAOs are responsible for issuing accreditations to specific issuers or subordinate TAOs, according to the policies inherited from the Root TAO.
- **Issuers**, which may be universities, companies, public administrations, or any other legal entities authorized to issue verifiable credentials within a specific domain or use case. These entities are accredited by a TAO and published in the Trusted Entity Registry (TER), with their scope and capabilities detailed in the TAR.

This structure allows for **multi-level trust delegation**, where each layer maintains accountability while reducing administrative burden at the center. It also facilitates the creation of **domain-specific trust frameworks**. For example, a Ministry of Education acting as a TAO may accredit universities as issuers of diplomas, while a national health agency may act as a TAO for hospitals and laboratories.

The role and implementation of this hierarchical model is further illustrated in the document published by the **EBSI-VECTOR consortium** titled *"The Role of EBSI within eIDAS"* (2025) (https://www.ebsi-vector.eu/wp-content/uploads/2025/02/Role-of-EBSI-within-eIDAS.pdf). This report provides also practical examples of how trust delegation works in real-world scenarios.

Through this architecture, the trust model becomes **scalable, flexible, and legally robust**, supporting high-volume credential exchanges while preserving auditability and conformance with the principles of eIDAS 2.0.

EBSI Trust Model Architecture

Trusted Entity Registry (TER)

The **Trusted Entity Registry (TER)** is one of the foundational components within the EBSI trust architecture. It serves as a verifiable and authoritative source of information on legal entities operating within the European ecosystem of verifiable credentials. The primary purpose of the TER is to register and publish authenticated data regarding organizations that have been recognized by competent authorities as legitimate actors within the decentralized trust model.

Unlike other registries that deal with technical or operational aspects, the TER does not define what credentials an entity may issue or verify, nor does it assign accreditation levels. Instead, it operates as the **initial trust anchor**, providing a validated representation of the legal identity of an entity. All data in the TER is backed by a governmental or sectoral authority and enables the establishment of trusted relationships, especially in cross-border scenarios.

Purpose and Function

The main function of the TER is to **guarantee the legal existence and recognition of entities** within the EBSI ecosystem by serving as a trusted source of verified organizational data. It answers key questions such as:

- Does this organization exist legally within the EU?
- Has it been onboarded by a trustworthy authority under the EBSI governance framework?
- What is its recognized Identifier?
- Where can its accreditations or permitted roles be verified (via the TAR)?

This information is not only essential for human users and organizations, but also for machine-readable trust processes that require dynamic and verifiable data resolution.

Relation to Other Registries

The TER does not operate in isolation. It is **closely linked to the Trusted Accreditation Registry (TAR)**, which describes the formal roles and accreditations associated with each registered entity. A lookup in the TER is generally the **first step** before consulting the TAR to understand an entity's capabilities or permissions within the trust framework.

The TER is conceptually aligned with the **trust model introduced by eIDAS 2.0**, where legal persons must be validated by a trusted authority, be it a National Supervisory Body, academic institution, or public sector authority, in order to issue or verify qualified electronic attestations.

Data Stored in the TER

All information registered in the Trusted Entity Registry (TER) is structured as **Verifiable Credentials** and adheres to the data model defined by the **Legal Person Identification Data (LPID)** schema. This ensures semantic consistency and verifiability across the ecosystem, while aligning with the principles and technical specifications established by EBSI and eIDAS 2.0.

Each credential entry within the TER represents a legal entity and must be **issued and digitally signed by a Trusted Accreditation Organization (TAO)**, a higher authority in the European trust hierarchy. This hierarchical issuance guarantees that the credential benefits from a formally recognized chain of trust. The LPID credential model is designed to express essential legal identity attributes of an organization, and its issuance by a TAO ensures that only vetted and authoritative entities are represented in the registry.

The LPID credential conforms to the schema published in the **Trusted Schema Registry (TSR)** and is accessible here:


```
{
   "$schema": "https://json-schema.org/draft/2020-12/schema",
   "allOf": [
      {
         "$ref":
"https://api-pilot.ebsi.eu/trusted-schemas-registry/v3/schemas/0x0b6c86bd80e1e97f9d461f53
10fc82120049914246002ecf0e14330dbed4f7ef"
      },
      {
         "$ref": "#/$defs/lpid"
      }
   ],
   "description": "Data Type for the Legal Person Identification Data (LPID)",
   "title": "Legal Person Identification Data (LPID)",
   "type": "object",
   "$defs": {
      "lpid": {
         "properties": {
            "authenticSourceId": {
               "type": "string"
            },
            "authenticSourceName": {
               "type": "string"
            },
            "credentialSubject": {
               "description": "Data Type for the Legal Person Identification Data (LPID)",
               "properties": {
                  "legalPersonId": {
                     "type": "string"
                  },
                  "legalPersonName": {
                     "type": "string"
                  }
```

```
            },
            "required": [
               "legalPersonId",
               "legalPersonName"
            ],
            "type": "object"
         },
         "expiryDate": {
            "type": "string"
         },
         "issuanceDate": {
            "type": "string"
         },
         "issuerCountry": {
            "type": "string"
         },
         "issuingAuthority": {
            "type": "string"
         },
         "issuingAuthorityId": {
            "type": "string"
         },
         "issuingJurisdiction": {
            "type": "string"
         },
         "revocationId": {
            "type": "string"
         },
         "revocationLocation": {
            "type": "string"
         },
         "schemaId": {
            "type": "string"
         },
         "schemaLocation": {
            "type": "string"
         },
         "schemaVersion": {
            "type": "string"
         }
      },
      "required": [
         "issuingAuthorityId",
         "issuingAuthority",
         "issuerCountry",
         "issuingJurisdiction",
         "issuanceDate",
         "expiryDate",
         "schemaId",
         "schemaVersion",
```

```
            "schemaLocation",
            "revocationId",
            "revocationLocation",
            "authenticSourceId",
            "authenticSourceName",
            "credentialSubject"
          ],
          "type": "object"
        }
    }
}
```

The core attributes of this schema include:

- **authenticSourceId:** A unique identifier referencing the authoritative data provider or registry from which the legal entity information originates. This ID must correspond to a recognized and accredited source listed in the Trusted Accreditation Registry (TAR).
- **authenticSourceName:** The human-readable name of the authentic source or authority maintaining the original dataset. It helps facilitate transparency and traceability.
- **credentialSchema**
    - **id:** A pointer to the identifier of the schema used to validate the structure of the credential. This ID is often mapped internally to a schema reference in the Trusted Schema Registry (TSR).
    - **type:** Indicates the serialization or schema format, typically JsonSchema for LPID, aligning with the W3C Verifiable Credentials Data Model.
- **credentialSubject:** This object encapsulates the subject of the credential (i.e., the legal entity to which the credential refers)
    - **legalPersonId:** The unique identifier of the legal person, typically a national or sectoral registration number.
    - **legalPersonName:** The full registered name of the legal entity.
- **expiryDate:** The date after which the credential is no longer valid, regardless of revocation status. This ensures temporal control over trust data and enables periodic re-verification of legal status.
- **id:** A unique identifier for the credential instance itself. This may be used for indexing, lookup, or external referencing within registries and trust anchors.
- **issuanceDate:** The date on which the credential was formally issued and cryptographically signed. This is used in trust evaluation and credential freshness assessments.

- **issuer:** A reference to the issuing entity's identifier. In a trusted issuance model, this identifier corresponds to a Trusted Accreditation Organization (TAO), as recorded in the TAR.
- **issuerCountry:** The two-letter ISO 3166-1 alpha-2 code of the country in which the issuing authority is established. It situates the credential legally and jurisdictionally.
- **issuingAuthority:** The formal name of the public authority or trusted institution that issued the credential. This is the entity responsible for guaranteeing the authenticity of the information.
- **issuingAuthorityId:** An internal or external identifier uniquely mapping the issuing authority to its formal representation, possibly aligned with TAR entries or national registers.
- **issuingJurisdiction:** The national or regional legal domain under which the issuer operates and in which the credential is legally effective. This provides contextual clarity for legal interpretation.
- **revocationId:** A unique identifier used to manage the revocation status of this specific credential. It serves as a lookup key in revocation registries or status lists.
- **revocationLocation:** A URI pointing to the endpoint or service where revocation information is made available. This enables verifiers to query whether the credential has been revoked post-issuance.
- **schemaId:** A unique identifier referring to the specific data schema under which the credential was generated. This should correspond to an entry in the Trusted Schema Registry (TSR).
- **schemaLocation:** A URL pointing to the exact location of the credential schema. This allows automatic validation of credential structure during issuance and verification.
- **schemaVersion:** A semantic versioning identifier that specifies the version of the schema used. It is essential for long-term schema governance and migration control.
- **type:** An array of one or more type descriptors defining the credential's classification. In this case, ["lpid"] confirms that the credential follows the Legal Person Identification Data model.
- **validFrom:** The start date from which the credential is considered valid. It works in tandem with expiryDate to determine the credential's active validity window.

Each credential is cryptographically signed and includes metadata enabling **verification of its authenticity, integrity, and issuance provenance**. In practical terms, this structure allows any verifier to resolve the credential to its **issuer (TAO)** and confirm its trust status using the **TAR (Trusted Accreditation Registry)**.

This schema-based approach allows the TER to serve not just as a passive directory but as a dynamic trust anchor capable of powering automated decisions across wallets, verifiers, and relying parties throughout the EBSI trust ecosystem.

Example


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2"
  ],
  "authenticSourceId": "auth-source-001",
  "authenticSourceName": "Bolagsverket Official Records",
  "credentialSchema": {
    "id": "id:2",
    "type": "JsonSchema"
  },
  "credentialSubject": {
    "legalPersonId": "SE5560160680",
    "legalPersonName": "Acme AB"
  },
  "expiryDate": "2025-01-01",
  "id": "id:1",
  "issuanceDate": "2023-01-01",
  "issuer": "issuer:0",
  "issuerCountry": "SE",
  "issuingAuthority": "Bolagsverket",
  "issuingAuthorityId": "bolagsverket-001",
  "issuingJurisdiction": "Sweden",
  "revocationId": "rev001",
  "revocationLocation": "https://bolagsverket.se/revocations/legal-person-id",
  "schemaId": "schema:bolagsverket-lpid",
  "schemaLocation": "https://bolagsverket.se/schemas/legal-person-id",
  "schemaVersion": "1.0.0",
  "type": [
     “lpid”
  ],
  "validFrom": "2024-01-01T00:00:00Z"
}
```


Common Use Cases of the TER

- **Credential validation**: Verifiers consult the TER to confirm whether a credential issuer is a trusted entity.
- **Trust visualization**: Systems can trace the trust relationships and accreditations of an organization using data from TER and TAR.
- **Transparency and compliance**: Public sector registries and national supervisory bodies can publish approved entities under regulatory frameworks like eIDAS 2.0.

- **Wallet and verifier integration**: Digital wallets and verification systems can query the TER in real time to automate trust decisions.

The TER thus serves as a **cornerstone** in the EBSI trust architecture, ensuring that the ecosystem operates based on verified, authoritative identities.

Trusted Accreditation Registry (TAR)

The **Trusted Accreditation Registry (TAR)** is a pivotal component within the European Blockchain Services Infrastructure (EBSI) trust framework. It serves as the authoritative repository for managing and disseminating accreditation information of legal entities registered in the **Trusted Entity Registry (TER)**. The TAR delineates the specific roles and permissions granted to these entities, such as the authority to issue, verify, or request particular types of Verifiable Credentials (VCs). This registry ensures that all operational authorizations within the EBSI ecosystem are transparent, verifiable, and aligned with established governance policies.

Historically, the functionalities of the TAR were encompassed within the former **Trusted Issuer Registry (TIR)**. However, to enhance semantic clarity and accommodate the inclusion of verifiers and requesters alongside issuers, a logical separation was implemented. Consequently, the TIR evolved into the TER, focusing on the legal identities of entities, while the TAR was established to manage their respective accreditations and authorizations.

Purpose and Function

The TAR's primary function is to **map specific accreditations to legally recognized entities** within the EBSI ecosystem. Each entry in the TAR is structured as a **Verifiable Accreditation**, a specialized form of Verifiable Credential that attests to an entity's authorization to perform certain actions. These accreditations are issued and digitally signed by a higher authority in the trust hierarchy, typically a **Trusted Accreditation Organization (TAO)**, ensuring a robust and verifiable chain of trust.

Key functionalities of the TAR include:

- **Authorization Management**: Clearly defines and records the specific roles and permissions granted to entities, such as issuing diplomas, verifying business licenses, or requesting sensitive information.
- **Trust Delegation**: Facilitates the delegation of trust from higher authorities (TAOs) to entities, enabling a scalable and decentralized trust model.
- **Dynamic Trust Evaluation**: Provides mechanisms for verifiers to dynamically assess the validity and scope of an entity's accreditations, ensuring informed trust decisions.

Data Stored in the TAR

Each accreditation entry within the TAR conforms to the **EBSI Verifiable Accreditation Record** schema, ensuring consistency and interoperability across the ecosystem. The core attributes of this schema include:

- **@context**: Specifies the JSON-LD context, typically including "https://www.w3.org/2018/credentials/v1".
- **id**: A unique identifier for the Verifiable Accreditation instance.
- **type**: An array indicating the credential types, such as "VerifiableCredential", "VerifiableAttestation", "VerifiableAccreditation", and specific subtypes like "VerifiableAccreditationToAccredit" or "VerifiableAccreditationToAttest".
- **issuer**: The identifier of the entity issuing the accreditation, usually a TAO.
- **issuanceDate**: The date and time when the accreditation was issued.
- **validFrom**: The date and time from which the accreditation is considered valid.
- **expirationDate**: The date and time after which the accreditation is no longer valid.
- **credentialSubject**: An object detailing the subject of the accreditation, including:
    - **id**: The identifier of the accredited entity.
    - **reservedAttributeId**: An identifier for the specific attribute or role being accredited.
    - **accreditedFor**: An array specifying the schemas and types of credentials the entity is authorized to issue, verify, or request, along with any jurisdictional limitations.
- **credentialStatus**: An object providing information on the revocation status of the accreditation, including:
    - **id**: A URI identifying the credential status.
    - **type**: The type of revocation mechanism, such as "StatusList2021".
- **termsOfUse**: An array detailing any terms and conditions associated with the accreditation, including references to issuance certificates or policies.
- **credentialSchema**: An array specifying the schemas that the accreditation adheres to, including their identifiers and types.

Each Verifiable Accreditation is cryptographically signed by the issuing authority, ensuring its authenticity and integrity. The schema definitions are registered and accessible through the **Trusted Schema Registry (TSR)**, promoting standardization and interoperability.

Integration with the TER

The TAR is **logically dependent** on the TER: every accreditation in the TAR must reference a legal entity that is already present in the TER. This ensures that **only entities with a verified legal identity** can receive operational authorizations. Furthermore, the TAR provides a mechanism to **express delegation**: for example, a ministry of education (TAO) may accredit a university (TER entity) to issue diplomas, and the TAR will formally encode and expose that delegation.

This dual-registry approach supports robust trust chaining and simplifies compliance with eIDAS 2.0 and ETSI 119 612 by decoupling **who** an entity is (TER) from **what** it is allowed to do (TAR).

Functional Role in the Ecosystem

In operational terms, the TAR serves the following ecosystem needs:

- **Credential Issuance Validation** – Before accepting a credential, a verifier can consult the TAR to confirm that the issuer was accredited for that specific credential type.
- **Delegated Trust Management** – TAOs and supervisory authorities can dynamically publish or revoke accreditations, allowing for near real-time updates to the trust topology.
- **Access Control for Requesters** – When sensitive data is requested, e.g., for KYC or regulatory purposes, the TAR can be consulted to validate whether the requesting entity is authorized to make such a request.
- **Audit and Transparency** – TAR entries are publicly accessible, digitally signed, and verifiable using standardized EBSI mechanisms, enabling transparent audit trails for all trust relationships.

<u>Examples of Verifiable Accreditations</u>

To illustrate the structure and content of Verifiable Accreditations within the TAR, consider the following examples:

Accreditation for a Trusted Accreditation Organization (TAO):


```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "id": "urn:uuid:8568b525-a24e-4bc0-9d97-6a8459ec0130",
  "type": [
    "VerifiableCredential",
    "VerifiableAttestation",
```

```
    "VerifiableAccreditation",
    "VerifiableAccreditationToAccredit"
  ],
  "issuer": "did:ebsi:00001234",
  "issuanceDate": "2021-11-01T00:00:00Z",
  "validFrom": "2021-11-01T00:00:00Z",
  "expirationDate": "2024-06-22T14:11:44Z",
  "issued": "2020-06-22T14:11:44Z",
  "credentialSubject": {
    "id": "did:ebsi:zZeKyEJfUTGwajhNyNX928z",
    "reservedAttributeId":
"60ae46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088a8",
    "accreditedFor": [
      {
        "schemaId": "https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0x010110",
        "types": [
          "VerifiableCredential",
          "VerifiableAttestation",
          "DiplomaCredential"
        ],
        "limitJurisdiction": "https://publications.europa.eu/resource/authority/atu/FIN"
      }
    ]
  },
  "credentialStatus": {
    "id":
"https://api-test.ebsi.eu/trusted-issuers-registry/v4/issuers/did:ebsi:zZeKyEJfUTGwajhNyNX92
8z/attributes/60ae46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088a8",
    "type": "StatusList2021"
  },
  "termsOfUse": [
    {
      "id": "https://api-test.ebsi.eu/trusted-issuers-registry/../..xyz",
      "type": "IssuanceCertificate"
    }
  ],
  "credentialSchema": [
    {
      "id":
"https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0xbbdaf273ffe65d497cee8c156
3b48fa2f468e073c77a8a6cbd6fca93ce665436",
      "type": "FullJsonSchemaValidator2021"
    },
    {
      "id":
"https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0x1d7146f8897aa6cd5c59321e
a0756ec61277028e4a8b3c13ec1b310ec47e6495",
      "type": "FullJsonSchemaValidator2021"
    }
  ]
```

```
}
```


Accreditation to Issue a Diploma Credential (Issuer)


```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "id": "urn:uuid:8568b525-a24e-4bc0-9d97-6a8459ec0130",
  "type": [
    "VerifiableCredential",
    "VerifiableAttestation",
    "VerifiableAccreditation",
    "VerifiableAccreditationToAttest"
  ],
  "issuer": "did:ebsi:00001234",
  "issuanceDate": "2021-11-01T00:00:00Z",
  "validFrom": "2021-11-01T00:00:00Z",
  "expirationDate": "2024-06-22T14:11:44Z",
  "issued": "2020-06-22T14:11:44Z",
  "credentialSubject": {
    "id": "did:ebsi:zZeKyEJfUTGwajhNyNX928z",
    "reservedAttributeId":
"60ae46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088a8",
    "accreditedFor": [
      {
        "schemaId": "https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0x010110",
        "types": [
          "VerifiableCredential",
          "VerifiableAttestation",
          "DiplomaCredential"
        ],
        "limitJurisdiction": "https://publications.europa.eu/resource/authority/atu/FIN"
      }
    ]
  },
  "credentialStatus": {
    "id":
"https://api-test.ebsi.eu/trusted-issuers-registry/v4/issuers/did:ebsi:zZeKyEJfUTGwajhNyNX92
8z/attributes/60ae46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088a8",
    "type": "StatusList2021"
  },
  "termsOfUse": [
    {
      "id": "https://api-test.ebsi.eu/trusted-issuers-registry/../..xyz",
      "type": "IssuanceCertificate"
    }
  ],
  "credentialSchema": [
    {
      "id":
```

```
"https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0xbbdaf273ffe65d497cee8c1563b48fa2f468e073c77a8a6cbd6fca93ce665436",
      "type": "FullJsonSchemaValidator2021"
    },
    {
      "id":
"https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0x1d7146f8897aa6cd5c59321ea0756ec61277028e4a8b3c13ec1b310ec47e6495",
      "type": "FullJsonSchemaValidator2021"
    }
  ]
}
```


Accreditation of Verifiers: Types and Trusted Units of Verification (TUV)

Within the EBSI Trust Architecture, the Trusted Accreditation Registry (TAR) plays a central role not only in managing accreditations for credential issuers, but also in governing verifiers. These accreditations are expressed as Verifiable Credentials, conforming to the standardized EBSI Verifiable Accreditation schema. A key structural element in these credentials is the type field, which explicitly defines the role and capabilities of the accredited entity.

To differentiate between these roles, EBSI specifies distinct extensions of the base Verifiable Credential type:

- VerifiableAccreditationToAccredit: authorizes the holder to accredit other entities.
- VerifiableAccreditationToAttest: grants permission to issue credentials of specified types.
- VerifiableAccreditationToRequest: enables the holder to request or verify specific types of Verifiable Credentials.

This last designation, VerifiableAccreditationToRequest, is particularly relevant for verifiers operating under the eIDAS 2.0 framework, which mandates that all actors participating in credential exchange, including those requesting information, must be recognized and listed in the trusted infrastructure.

Example: Accreditation of a Verifier


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "credentialSchema": [
    {
      "id":
```

```
"https://api.ebsi.eu/trusted-schemas-registry/v2/schemas/0xbbdaf273ffe65d497cee8c1563b48fa2f468e073c77a8a6cbd6fca93ce665436",
      "type": "FullJsonSchemaValidator2021"
    }
  ],
  "credentialStatus": {
    "id":
"https://api.ebsi.eu/trusted-issuers-registry/v4/issuers/did:ebsi:zAbC12345EFG67890/attributes/3e9d46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088b1",
    "type": "StatusList2021"
  },
  "credentialSubject": {
    "accreditedFor": [
      {
        "limitJurisdiction": "https://publications.europa.eu/resource/authority/atu/ESP",
        "schemaId": "https://api.ebsi.eu/trusted-schemas-registry/v2/schemas/0x010110",
        "types": [
          "VerifiableCredential",
          "DiplomaCredential"
        ]
      }
    ],
    "id": "did:ebsi:zAbC12345EFG67890",
    "reservedAttributeId":
"3e9d46e4fe9adffe0bc83c5e5be825aafe6b5246676398cd1ac36b8999e088b1"
  },
  "expirationDate": "2026-11-01T00:00:00Z",
  "id": "urn:uuid:12345678-aaaa-bbbb-cccc-1234567890ab",
  "issuanceDate": "2023-11-01T00:00:00Z",
  "issuer": "did:ebsi:00001234",
  "termsOfUse": [
    {
      "id": "https://api.ebsi.eu/trusted-issuers-registry/terms/diploma-verification",
      "type": "IssuanceCertificate"
    }
  ],
  "type": [
    "VerifiableCredential",
    "VerifiableAttestation",
    "VerifiableAccreditation",
    "VerifiableAccreditationToRequest"
  ],
  "validFrom": "2023-11-01T00:00:00Z"
}
```


This example illustrates the direct model, where a verifier receives specific accreditation to request a defined credential type. While clear and precise, this model may introduce scalability challenges, particularly in sectors like finance or healthcare, where many institutions share

identical verification requirements. Managing each verifier individually within the TAR can quickly become inefficient and administratively burdensome.

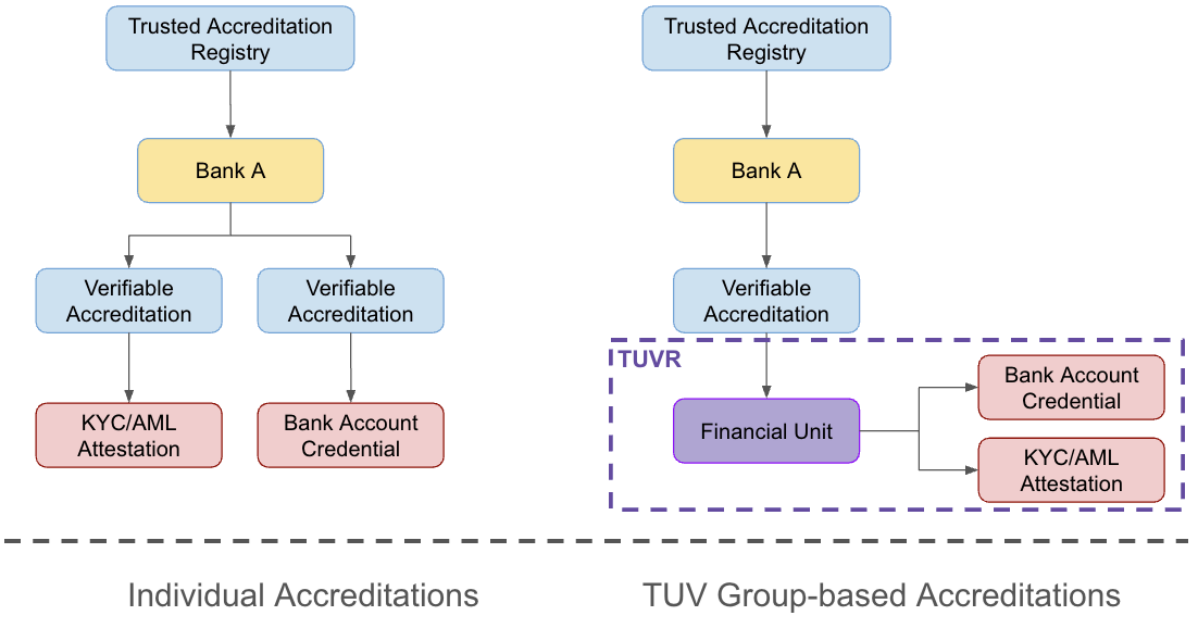
TUV: Trusted Units of Verification – A Scalable Alternative

To address these limitations, an alternative model is proposed through the introduction of **TUVs** (Trusted Units of Verification). These are predefined groups representing common verification profiles across particular domains, such as hospitals, banks, universities, or retail chains. Rather than issuing individual accreditations for each credential type, entities could be affiliated with a TUV that encapsulates their collective verification rights.

Each TUV would define:

- A list of credential types and schemas authorized for verification;
- The jurisdictions where the verification is applicable;
- Internal governance policies regulating group membership and lifecycle.

Instead of repeatedly seeking approval from national or sectoral authorities (TAOs) for each use case, entities would obtain a single Verifiable Accreditation that references the identifier of the TUV they wish to join. The TUV itself becomes the canonical source for the list of verifiable schemas, thereby decoupling entity-specific accreditations from the management of credential type definitions.



Trusted Units of Verification Registry (TUVR)

This group-based model necessitates the creation of a new registry: the **Trusted Units of Verification Registry (TUVR)**. This registry would be responsible for storing:

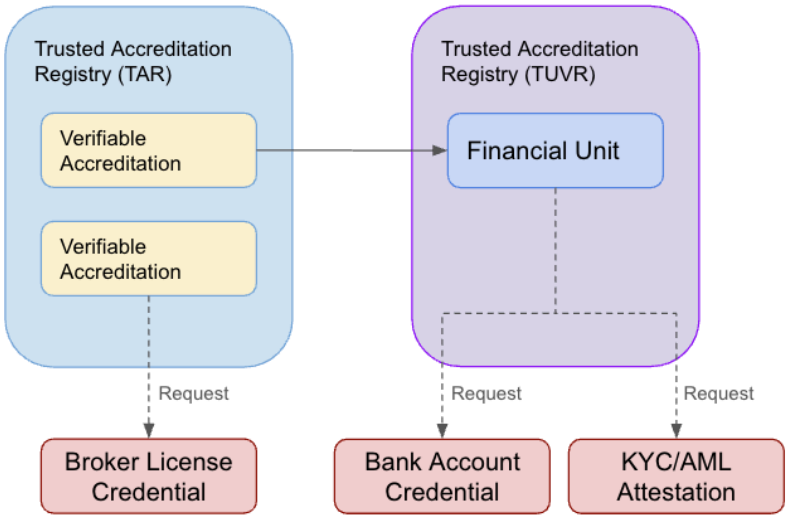
- All officially recognized TUV definitions;
- Group identifiers and names;
- The list of credential schemas each TUV can request;
- Applicable jurisdictions;
- Versioning and governance metadata.

Each TUV record would be structured, discoverable, and public. It would serve as a reference point for accreditations recorded in the TAR. This decouples the operational and semantic burden from national authorities while promoting harmonization across entities with shared requirements.

Balancing Flexibility and Scalability

The coexistence of individual and group-based accreditations preserves system flexibility. Institutions with specific, non-standard requirements can continue to use direct accreditation via VerifiableAccreditationToRequest. Meanwhile, institutions operating within broadly similar contexts, such as all accredited hospitals in a given Member State, benefit from TUV affiliation.

This architecture enhances interoperability and regulatory clarity while reducing redundancy and friction in the accreditation process. It positions the TAR not only as a registry of roles but also as a dynamic interface to verification governance, one that evolves in parallel with the complexity and scale of the European Digital Identity ecosystem.



Trusted Schema Registry (TSR)

Definition and Purpose

The Trusted Schema Registry (TSR) is an essential component of the EBSI trust architecture, serving as the authoritative repository for the schemas that define the structure and semantics of Verifiable Credentials used within the EBSI ecosystem. Unlike the TER and TAR, which store credential instances, the TSR focuses exclusively on the publication, discovery, and validation of the credential *schemas* themselves. This registry guarantees that all Verifiable Credentials (VCs) issued and exchanged on EBSI adhere to standardized, versioned, and publicly available data models.

By referencing a schema in the TSR, credential issuers, verifiers, and relying parties can align on a common semantic and syntactic interpretation of the data fields contained in a VC. This ensures interoperability and reduces ambiguity in credential processing, validation, and presentation.

The TSR supports the traceability of schemas over time through explicit versioning, and allows schemas to be linked with compliance indicators or linked trust levels (e.g., support for EBSI conformity or compatibility with eIDAS requirements).

Registry Functions

The TSR performs several critical functions within the trust model:

- **Schema Publication**: Enables authorized actors to register credential schemas for use within the EBSI framework. These schemas are typically JSON Schema definitions compliant with W3C Verifiable Credentials Data Model, but any kind of schema can be stored.
- **Schema Discovery**: Provides a queryable interface to retrieve schemas by ID.
- **Version Control**: Manages different schema versions and supports backward compatibility.
- **Validation Enablement**: Offers tools and metadata for validating VCs against their declared schemas.

Data Stored in the TSR

Each entry in the TSR consists of a formal schema definition, typically expressed in JSON Schema format (draft 2020-12 or earlier), and accompanied by relevant metadata.

A typical TSR entry contains the following information:

- **Schema ID**: A unique and persistent identifier (URI format) for the schema.
- **Schema payload:** Schema descriptor of information contained into a VC.

DID Registry

Definition and Purpose

The DID Registry in the EBSI ecosystem functions as a decentralized public directory for managing and resolving Decentralized Identifiers (DIDs) and their associated DID Documents. It plays a foundational role in the infrastructure of trust by enabling secure, cryptographically verifiable identity resolution without relying on a centralized intermediary. Each DID resolves to a corresponding DID Document, which contains metadata about the entity's public keys, authentication methods, and capabilities.

While the registry does not operate as a traditional database, it provides a decentralized mechanism for publishing and retrieving identity-related information. This allows legal entities, natural persons, or even services to establish digital identities that can be discovered and verified independently.

The EBSI DID Registry implements the W3C DID specification and supports the use of EBSI-compatible DID methods (notably did:ebsi). The EBSI implementation acts as a decentralized public key infrastructure (DPKI), aligning with the broader goals of self-sovereign identity (SSI) and interoperability across EU member states under eIDAS 2.0.

Registry Functions

The EBSI DID Registry provides the following key capabilities:

- **DID Registration**: Enables entities to create and anchor a DID on EBSI's underlying blockchain infrastructure.
- **DID Resolution**: Offers a publicly accessible method to resolve a DID into its corresponding DID Document.
- **Key Discovery**: Allows third parties to retrieve the public keys associated with a DID for purposes of authentication, credential verification, and encryption.
- **Lifecycle Management**: Supports rotation, deactivation, or revocation of keys and authentication methods, subject to governance constraints.

Data Stored in the DID Registry

Unlike other registries such as the TAR or TER, the DID Registry does not store Verifiable Credentials. Instead, it stores **DID Documents**, which describe how a given DID can be used to verify control over a set of cryptographic keys and interactions.

A DID Document typically includes:

- **@context**: A list of JSON-LD contexts defining the semantics of the document.
- **id**: The unique identifier for the subject of the DID Document.
- **controller**: Entity or entities that control the DID and are authorized to update the document.
- **verificationMethod**: A list of cryptographic public keys associated with the DID, used for various verification purposes.
- **authentication**: References to keys that can be used to authenticate the DID subject.
- **assertionMethod**: Keys authorized to make assertions on behalf of the DID subject.
- **capabilityInvocation**: Keys that can be used to invoke capabilities or access control rights.

Data Model

The DID Document adheres to the W3C DID Core Data Model. Below is a real example of a DID Document registered in the EBSI DID Registry:


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "assertionMethod": [

"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#f2gYeed1K05Z7kd87u4RPaI9TgJoNNZXo9nh5JsjtGU"
  ],
  "authentication": [

"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#vCF0KgYJJvoSiiDrMdR6BlrOWzzckOm7iFakMDPOSWc",

"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#f2gYeed1K05Z7kd87u4RPaI9TgJoNNZXo9nh5JsjtGU"
  ],
  "capabilityInvocation": [

"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#vCF0KgYJJvoSiiDrMdR6BlrOWzzckOm7iFakMDPOSWc"
  ],
  "controller": [
    "did:ebsi:ziDnioxYYLW1a3qUbqTFz4W"
  ],
  "id": "did:ebsi:ziDnioxYYLW1a3qUbqTFz4W",
```

```
  "verificationMethod": [
    {
      "controller": "did:ebsi:ziDnioxYYLW1a3qUbqTFz4W",
      "id":
"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#vCF0KgYJJvoSiiDrMdR6BlrOWzzckOm7iFakMDPO
SWc",
      "publicKeyJwk": {
        "crv": "secp256k1",
        "kty": "EC",
        "x": "Yr5dSC8vVBhz_a_EiIjH63shj1uqPeg8UjtoUXtsVZU",
        "y": "NicHUkZrnM1GgWn1GO4Dl27Q5rD-kG-ODF_jhZYSyQw"
      },
      "type": "JsonWebKey2020"
    },
    {
      "controller": "did:ebsi:ziDnioxYYLW1a3qUbqTFz4W",
      "id":
"did:ebsi:ziDnioxYYLW1a3qUbqTFz4W#f2gYeed1K05Z7kd87u4RPaI9TgJoNNZXo9nh5JsjtG
U",
      "publicKeyJwk": {
        "crv": "P-256",
        "kty": "EC",
        "x": "wcPJTOaQWzGinDY2XAQ47sWm-7QFUFMuHIdbPrc-I4o",
        "y": "LNiGME-6qLagfzc5jVzhcBHuMaNRuNTTcS3gxK7ke1U"
      },
      "type": "JsonWebKey2020"
    }
  ]
}
```

Conclusion

The European Trust Model articulated throughout this document establishes a comprehensive and interoperable digital trust architecture designed to support the issuance, verification, and reuse of verifiable credentials across the European Union. Rooted in the foundational principles of eIDAS 2.0 and operationalized through the European Blockchain Services Infrastructure (EBSI), this model represents a coordinated effort to harmonize technical, legal, and organizational trust across Member States.

At the heart of this architecture are four dedicated registries: the **Trusted Entity Registry (TER)**, the **Trusted Accreditation Registry (TAR)**, the **Trusted Schema Registry (TSR)**, and the **DID Registry**. Each serves a distinct yet interdependent role in enabling trust-based interactions among entities participating in the ecosystem.

The **TER**, formerly known as the Trusted Issuers Registry (TIR), now encompasses not only credential issuers but also verifiers, reflecting a semantic and functional evolution toward inclusivity and transparency. It holds Verifiable Credentials in the Legal Person Identification Data (LPID) format, attested by trusted authorities (TAOs), and ensures that every participating entity can be uniquely and legally identified.

The **TAR** adds a critical layer of semantic authorization by storing accreditations in the form of Verifiable Credentials, specifically EBSI Verifiable Accreditation Records. These records define the scope of an entity's trust function, whether issuing, verifying, or requesting credentials, and bind such authority to a jurisdiction and schema through cryptographically verifiable attestations issued by competent authorities. It includes capabilities inherited from the former TIR while expanding the trust domain to include requesters of information, thus completing the triad of roles in the trust triangle.

The **TSR** provides the essential semantic layer for interoperability by offering standardized Schemas for every type of credential circulating in the ecosystem. By linking each accreditation in the TAR to a schema in the TSR, the model ensures that both the meaning and the structure of credentials are publicly understood, machine-readable, and governed under common rules. This guarantees syntactic and semantic alignment across diverse implementations and jurisdictions.

The **DID Registry**, in turn, serves as the decentralized cryptographic root of the trust model. By storing W3C-compliant DID Documents that associate public keys with decentralized identifiers (DIDs), it provides the necessary cryptographic primitives for authentication, digital signatures, and revocation checking. This registry operates as a decentralized public key infrastructure (DPKI), enabling trust at the protocol level without relying on a central authority.

Together, these registries create a multilayered trust fabric that supports privacy-preserving, legally compliant, and technologically robust credential interactions. Each transaction within the ecosystem—whether it involves issuing a diploma, verifying a license, or requesting access to a digital service—is underpinned by verifiable data, transparent provenance, and role-based

authorization. The model strictly adheres to emerging international standards such as **ISO 23042**, the W3C Verifiable Credentials and DIDs specifications, and aligns with the ongoing policy and pilot efforts led by the **European Digital Identity Framework** and **EBSI-VECTOR**.

Beyond its compliance and technical precision, the model is designed with scalability and reusability in mind. The separation of registries by function allows for targeted governance, modular upgrades, and the integration of additional roles or credential types as digital transformation accelerates across public and private sectors. Moreover, it provides a fertile foundation for cross-border services, pan-European interoperability, and digital sovereignty, ensuring that citizens and organizations alike can operate with trust in the digital single market.

In summary, the European Trust Model as implemented in EBSI is not merely a technical infrastructure, but a systemic enabler of digital trust. It aligns legal identity with verifiable credentials, integrates decentralized cryptography with institutional accountability, and transforms abstract regulatory principles into concrete, actionable mechanisms for cross-border interoperability and secure digital services.

References

1. Regulation (EU) No 910/2014 (eIDAS 1)
2. Regulation (EU) No 2024/1183 (eIDAS 2)
3. ETSI TS 119 612
4. RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
5. ISO/IEC 23042-1:2023 – Digital Identity – Concepts
6. ISO/IEC 23042-2:2024 – Digital Identity – Reference Architecture
7. EBSI Documentation – European Commission https://hub.ebsi.eu/
8. ESSIF Framework – https://blockchain-observatory.ec.europa.eu/
9. EBSI Diplomas Pilot – https://ec.europa.eu/digital-building-blocks/
10. ESSPASS PD A1 Pilot – CEF Telecom Reports
11. W3C Verifiable Credentials Data Model 2.0 – https://www.w3.org/TR/vc-data-model-2.0/
12. Gataca Blog: eIDAS 2.0 and Trust Models – https://gataca.io/blog/
13. EBSI-Vector website – https://www.ebsi-vector.eu/