Prepared by DigitalTrade4.EU

Towards a Trusted Digital Trade Framework: The Role of the European Trade Indexes Registry (EUTIR)

Summary of Feedback
to the European Commission

September 2025, v8.10 [GLOBAL]

Table of Contents

Cover Letter To the European Commission

Over the past six months, ***DigitalTrade4.EU*** *has submitted* ***96 feedback documents*** *across consultations, calls for evidence, and draft acts. This work shows how strongly EU initiatives connect to the opportunities and challenges of* ***digitalisation****.*

A clear conclusion emerges: alongside sector-specific laws, the EU needs a ***common technological framework*** *to ensure interoperability, legal certainty, and efficient use of resources. Such a framework allows the same digital trust principles to be applied across sectors from* ***agriculture and energy to customs, finance, sustainability, and defence****, while meeting high security requirements and remaining interoperable with global trade infrastructures.*

Through dialogue with several Commission Directorates-General, we are convinced that ***coordination and interoperability*** *are indispensable. A harmonised digital trust infrastructure such as the* ***European Trade Indexes Registry (EUTIR)*** *can:*

- *uphold* ***high security*** *and global interoperability,*
- *let each DG focus on its domain while contributing to a* ***shared, future-proof foundation****,*
- *reinforce the EU's role as a* ***global standard-setter*** *for trusted digital trade.*

This document consolidates our key insights. It presents a ***List of Top 34 Feedback Topics*** *distilled from our 96 submissions and explains how EUTIR can serve as a* ***unifying framework*** *connecting sectoral regulations into a coherent, secure, and globally interoperable ecosystem.*

We remain at your disposal to deepen the dialogue—both technically and at policy level—to help Europe lead the next stage of the ***green and digital transition****.*

Respectfully submitted,

Riho Vedler
DigitalTrade4.EU Consortium
EU Transparency Register: 355266197389-94

Strategic Feedback Topics

This section consolidates the **34 most important topics** covered in the 96 feedback documents submitted by DigitalTrade4.EU. They reflect the **strategic intersections of the EU's green and digital transitions** and show how the **European Trade Indexes Registry (EUTIR)** can serve as a **cross-cutting trust infrastructure**. These topics were submitted in the framework of the European Commission's *Have your say – Public Consultations and Feedback* platform, ensuring transparency and alignment with the Union's better regulation principles.

A. Core to NLF Revision (Product, Metadata, Trust Infrastructure)

1. **Omnibus Regulation – Aligning product legislation with the digital age.** Integrates digital trust, metadata, and interoperability rules directly into product legislation.
2. **European Innovation Act.** Provides a unifying policy basis for interoperability and innovation frameworks like EUTIR.
3. **Circular Economy Act**. Links product lifecycle traceability (DPP, CBAM, CSRD) with NLF compliance structures.
4. **Carbon Border Adjustment Mechanism (CBAM) – downstream extension, anti-circumvention and electricity rules**. Ensures trusted reporting and registry-based validation of emissions and trade flows.
5. **CO_2 Emission Standards for Cars and Vans (2019/631 revision / Clean corporate vehicles)**. Connects NLF product conformity rules with DPP and transport sustainability standards.
6. **Electronic Freight Transport Information (eFTI) requirements**. Embeds metadata and registry logic into logistics compliance processes across the Union.
7. **Critical Raw Materials Act – strategic project application template**. Strengthens supply chain trust and traceability for high-risk, high-value raw materials.
8. **Consumer Agenda 2025–2030 and action plan on consumers in the Single Market**. Uses transparency and metadata to reinforce consumer trust in digital and green products.
9. **Farm Sustainability Data Network (FSDN)**. Introduces registry-based traceability for agricultural sustainability reporting.
10. **Fisheries Control Regulation – Implementing Act (2026)** Applies NLF-compatible registry and audit requirements to fisheries compliance.

B. Climate & Green Transition Framework

11. **European Climate Law amendment.** Aligns climate neutrality obligations with digital traceability and registry verification.
12. **European strategy to boost global climate and energy transition.** Positions the EU as a leader in global green-digital infrastructures.
13. **European Climate Resilience and Risk Management Framework.** Links resilience reporting to interoperable registry systems.
14. **Simplification of administrative burdens in environmental legislation.** Proposes reducing costs by digitising environmental compliance processes.
15. **Measures related to specific plant pests.** Requires rapid, interoperable reporting of phytosanitary risks.

C. Finance, Competitiveness & Trade

16. **Markets in Financial Instruments Regulation (MiFIR) – post-reform changes**. Ensures metadata traceability and ESG-linked financial reporting.
17. **Multiannual Financial Framework (MFF) – competitiveness pillar**. Directs funding towards interoperable digital trust infrastructures.
18. **Multiannual Financial Framework (MFF) – civil protection & crisis preparedness**. Strengthens shared infrastructures for resilience and risk monitoring.
19. **Multiannual Financial Framework (MFF) – external action**. Extends EU's global reach through interoperable trade registries.
20. **Multiannual Financial Framework (MFF) – education, youth, culture, civil society**. Includes digital infrastructures as horizontal enablers.
21. **Burden reduction and simplification for small mid-cap enterprises (Omnibus Regulation)**. Proposes easing SME compliance by leveraging registry automation.
22. **28th Company Law Regime – harmonised rules for innovative companies**. Creates cross-border legal certainty for innovative SMEs.
23. **Trade defence: global excess capacity in the EU steel sector**. Uses registry-based monitoring to counter unfair global trade practices.

D. Security, Border & Justice

24. **Cybersecurity – peer review of National Cybersecurity Certification Authorities.** Aligns certification with NLF-level trust service rules.
25. **EU cybersecurity certification – amendment to the scheme on common criteria.** Updates cross-border assurance frameworks for interoperability.
26. **Passenger Name Record (PNR) Directive evaluation.** Links transport security data to registry-based verification.
27. **European Border and Coast Guard – update of EU rules.** Uses registry verification for coordinated EU border operations.
28. **Requests for customs enforcement of intellectual property rights – updated forms.** Digitalises IPR enforcement for customs authorities.
29. **EU Customs Code reform (future linkage).** Introduces registry-driven customs declarations aligned with WCO standards.
30. **European antitrust procedural rules (revision).** Improves legal certainty in competition enforcement via trusted metadata.
31. **Digitalisation of justice: 2025–2030 European judicial training strategy.** Ensures that registry-based records are admissible and trusted in judicial proceedings.

E. Sectoral & Strategic Policies

32. **Organic product imports – recognised control authorities.** Requires validation of organic certifications via registries.
33. **European strategy for housing construction.** Connects sustainability and lifecycle traceability in construction.
34. **Technical updates of the Emissions Trading Scheme (ETS) State aid guidelines.** Adds metadata requirements for emission and state aid monitoring.

Executive Summary

The **European Trade Indexes Registry (EUTIR)** is a proposed framework designed as a **strategic enabler for the European Union's digital and green transition**, supporting not only the ongoing revision of the **New Legislative Framework (NLF)** but also a wide range of related Union initiatives. Its central purpose is to provide a **horizontal digital trust layer** for product, trade, financial, and sustainability data, addressing weaknesses in fragmented digital integration, inconsistent compliance signals, and excessive administrative burdens identified in the Commission's 2022 evaluation.

By ensuring that **electronic documents, data sets, and associated metadata are authentic, traceable, and machine-readable**, EUTIR strengthens **market surveillance**, reinforces **consumer and business trust**, and enables **secure interoperability** across CBAM, DPP, eFTI, MiFIR, FiDA and other sectoral frameworks. In this way, EUTIR not only supports the EU's internal governance but also enhances Europe's role as a **global standard-setter for trusted digital trade infrastructures**.

EUTIR creates **synergies across multiple flagship EU initiatives**, including the **Digital Product Passport (DPP)**, **electronic freight transport information (eFTI)**, and the **Carbon Border Adjustment Mechanism (CBAM)**. This non-exhaustive list also extends to instruments such as the **EU Deforestation Regulation (EUDR)**, the **Corporate Sustainability Due Diligence Directive (CSDDD)**, and the upcoming **Forced Labour Regulation**. It strengthens legal certainty, reduces costs for SMEs by automating compliance verification, and positions the EU as a frontrunner in **global digital trade governance** by linking the **Economic Operator Registration and Identification (EORI)** system with the globally recognised **Legal Entity Identifier (LEI)** and its secure digital counterpart, the **verifiable LEI (vLEI)**. Importantly, EUTIR should be scoped in close alignment with the ongoing **EU Customs Code reform** and its planned **Customs Data Hub**, ensuring that both authorities and economic operators benefit from seamless and fully digital data exchange. By relying on existing trusted infrastructures, including qualified trust services under **eIDAS 2.0**, EUTIR ensures **technical feasibility** while enhancing **digital sovereignty**.

The governance model follows a **hybrid approach**: decentralised infrastructure nodes (e.g. the **European Blockchain Services Infrastructure, EBSI**) combined with centralised supervision led by the **European Securities and Markets Authority (ESMA)** and the competent national authorities. This balance ensures both resilience and legal consistency. EUTIR's architecture is designed for integration with **Artificial Intelligence (AI)** and **Machine Learning (ML)**, supporting real-time risk assessment and proactive interventions to combat fraud and non-compliance.

EUTIR is more than a regulatory tool—it is an **enabling infrastructure** for cross-border trade, sustainability, and competitiveness. Its successful implementation will:

1. Reduce **administrative burden** and duplication, especially for **SMEs**;
2. Provide **legal certainty**, including clearer **liability allocation** across the logistics chain, and strengthen **consumer trust**;
3. Support the **circular economy** by linking compliance and sustainability data;
4. Enable **interoperability** with international trade and financial systems;
5. Position the EU as a **global standard-setter** for **digital trade;**
6. Build the foundation of a **trusted** and **resilient digital economy**, strengthening Europe's global competitiveness.

*Looking ahead, the European Trade Indexes Registry (EUTIR) may be further developed into a broader **European Trusted Infrastructure for Registries**, while retaining the same acronym (EUTIR). Such an evolution would allow the Registry to go beyond trade indexes and serve as a common backbone for multiple trusted registries across the Union — including certificates, permits, sustainability data, agricultural policy instruments, and other sectoral frameworks. Considering this option in the future would ensure that the EU maintains a flexible and scalable infrastructure that can seamlessly integrate with the **Digital Business Wallet** and reinforce strategic initiatives such as the DPP, eFTI, CBAM, and the CAP.*

1. EU Strategic Digital Models for Trade, Logistics and Sustainability

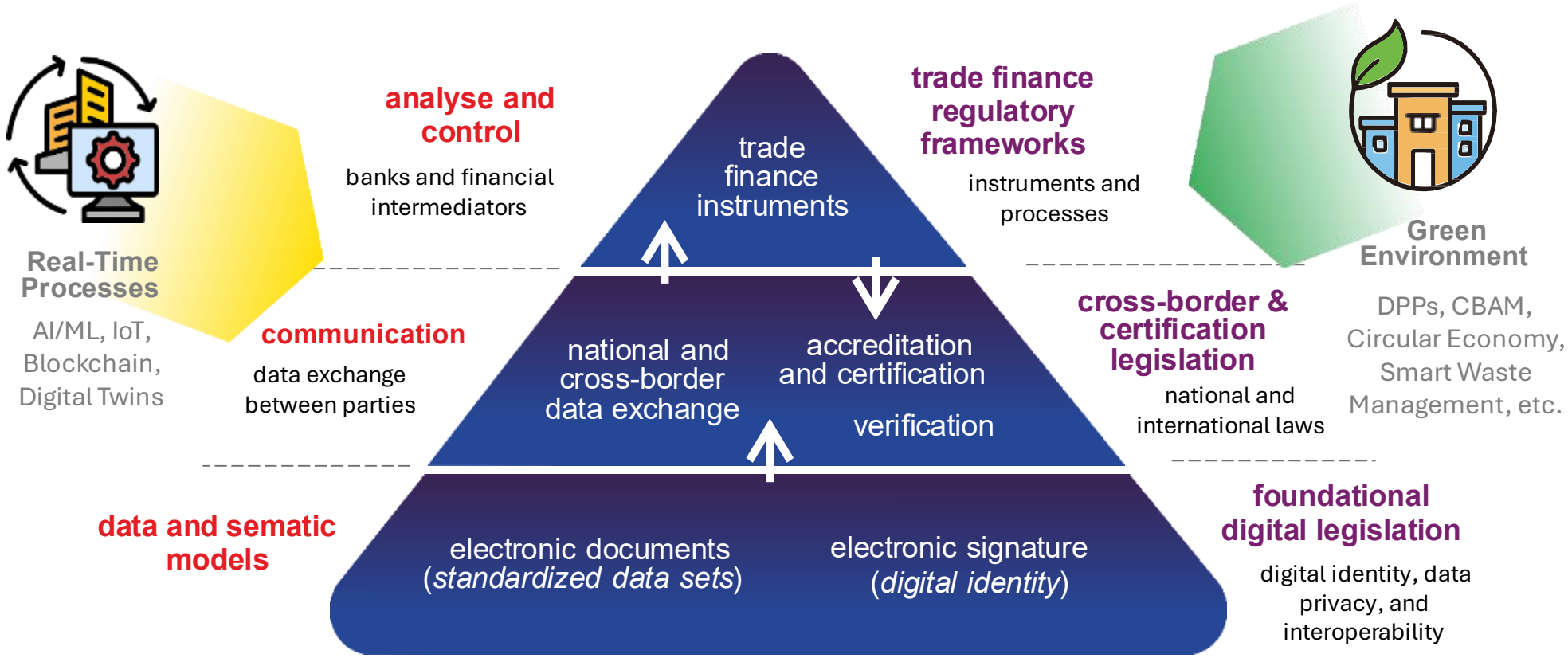


Figure 1. This visual model bridges the European Commission's strategic objectives with the proposed regulatory and operational solutions, illustrating how digital requirements and compliance mechanisms can be implemented in a technologically neutral and future-proof manner. Companies remain free to select and reuse their preferred IT solutions, ensuring flexibility and innovation. The diagram was prepared by Riho Vedler on behalf of the DigitalTrade4.EU consortium (icons by Flaticon).

2. Strategic Alignment: EUTIR Framework and Future EU Legislation

2.1. EUTIR as a Solution for the Revision of the New Legislative Framework (NLF)

The ongoing review of the NLF is a **critical opportunity** to update EU product legislation in light of new challenges related to **digitalisation**, the **circular economy**, and **sustainability**. The Commission's 2022 evaluation highlighted the need to adapt the framework to new realities, identifying shortcomings in fragmented digital integration, underutilised circular economy potential, and insufficient consumer awareness of product compliance signals. **EUTIR** has been proposed as a solution that acts as a **"trust anchor"** for trade-related data verification, providing the missing **technical and administrative layer** that enables the NLF revision to fully embrace digitalisation while avoiding fragmentation.

The system's value lies in its ability to **synergistically support** other major EU initiatives, such as the **Digital Product Passport (DPP)** under the **Ecodesign for Sustainable Products Regulation (ESPR) – Regulation (EU) 2024/1781**, **electronic Freight Transport Information (eFTI) – Regulation (EU) 2020/1056**, and the **Carbon Border Adjustment Mechanism (CBAM) – Regulation (EU) 2023/956** registries. The EUTIR proposal supports the NLF objectives of **harmonisation**, reduction of **regulatory burdens**, digital integration, enhanced **market surveillance**, and the integration of **circular economy** and **sustainability principles**. The table below illustrates EUTIR's contribution to the objectives of the NLF revision.

Table 1: EUTIR contribution to NLF revision objectives

#	NLF Revision Objectives	EUTIR Contributions	Shared Interest / Added Value
1	**Harmonisation of EU product legislation**	Provides a single, trusted registry for trade-related datasets (DPP, eFTI, CBAM, permits)	Avoids fragmentation across Member States; ensures consistency of compliance verification

2	**Reduction of regulatory burdens, especially for SMEs**	Automates verification through metadata and machine-readable identifiers (LEI/vLEI, EORI)	Cuts administrative costs, reduces duplication of filings, supports SME participation in cross-border trade
3	**Digital integration (e.g. Digital Product Passport)**	Anchors and verifies product lifecycle and compliance datasets in real time	Ensures that DPP and other product data are authentic, traceable, and interoperable
4	**Strengthened market surveillance and consumer trust**	Grants Competent Authorities direct access to verification services	Improves legal certainty, increases consumer confidence, enables faster detection of non-compliance
5	**Circular economy and sustainability objectives**	Links ESG/CE compliance datasets with traceability mechanisms	Guarantees that refurbished, remanufactured, and sustainable products remain compliant and transparent
6	**Future-proof regulatory framework**	Built on interoperable, decentralised, and AI/ML-ready architecture	Provides resilience, innovation capacity, and long-term adaptability for the Single Market

2.2. "Trust Anchor" in Digital Trade: Strategic Value and Global Leadership

EUTIR's strategic value stems from its role as a **"trust anchor"** for **economic operators**, **service providers**, and **competent authorities**. The registry ensures that all registered datasets—whether related to freight, product lifecycle, sustainability, or licences—are **authentic**, **traceable**, and **machine-readable**. This is achieved by building a system that does not store complete documents but only the **metadata necessary for verification**, such as cryptographic hashes, timestamps, and unique identifiers.

EUTIR's distinctive feature is the **dual identifier model**, combining the EU-specific **Economic Operators Registration and Identification (EORI)** number with the globally recognised **Legal Entity Identifier (LEI)** and **verifiable LEI (vLEI)**. This approach, adopted from the **Markets in Financial Instruments Regulation (MiFIR)**, enables seamless **interoperability** with international **trade** and **financial networks**. It is not just a technical choice but a **strategic step**

to ensure **digital sovereignty**. By relying on a globally recognised system (LEI/vLEI), the EU avoids the need to create a new, separate global identification framework, while maintaining control over its internal market through the EORI number. This balanced approach positions the EU as a **leader in global digital trade**, promoting interoperability without compromising regulatory integrity. In addition, EUTIR's architecture is designed to support **artificial intelligence** and **machine learning** tools, creating a structured data environment essential for **data-driven risk assessment** and **trade facilitation**, thus providing the EU with a **competitive edge** globally.

The EUTIR framework reflects the Pull-Based Data Model as described in UN/CEFACT's paper *Globally Unique Identifiers in Supply Chains*[1]. Instead of exchanging full documents, only identifiers and metadata are shared, while authorized parties may securely pull the precise data they need through EUTIR. This enforces the "Need-to-know" and "Minimum Privilege" security principles, ensures immutability and traceability, promotes ESG transparency, prevents fraud, and supports SME inclusion.

2.3. Exclusive Control as a Foundational Principle

One of the foundational principles of the EUTIR is the recognition and enforcement of **exclusive control** over Metadata Records, which acts as a bridge between functional requirements and international legal alignment. Exclusive control means that at any given time, only one identified party holds the full right to exercise the entitlements associated with a Metadata Record, to prevent others from exercising such rights, and to lawfully transfer them to another party. This ensures that electronic records function in a manner comparable to traditional paper-based documents, while exceeding them in traceability and security.

From a legal perspective, this principle guarantees that digital trade documents managed within the EUTIR carry the same evidentiary value as their paper equivalents. The transfer of exclusive control is critical in commercial and financial transactions: it ensures that records are transferable and can be reliably used as collateral, in financing arrangements, or in risk management practices. In this way, **small and medium-sized enterprises (SMEs)** benefit from

[1] https://unece.org/trade/documents/2025/06/standards/white-paper-globally-unique-identifiers-supply-chains

enhanced access to finance, as banks and insurers may rely on EUTIR-verified records with the same confidence as they do with traditional documents.

From a technical perspective, Certified Service Providers (CSPs) are required to implement reliable and verifiable mechanisms to demonstrate the existence and transfer of control. Such mechanisms must remain **technologically neutral** and support **international interoperability**. This may include cryptographic linkages, status changes, or unique identifiers (e.g. LEI/vLEI), which enable the system to track at all times who the lawful controller of a record is.

From an international perspective, the principle of exclusive control creates common ground with other jurisdictions that regulate possession and transfer of rights in electronic documents. While the EUTIR does not replicate the legal framework of any third country, it reflects **international best practices** to ensure that records can be recognised and relied upon in cross-border transactions. This lays the foundation for future **Mutual Recognition Agreements (MRAs)**, which are necessary for achieving global legal certainty and trusted data exchange.

2.4. Institutional Coherence and Governance

The EUTIR proposal foresees coordinated efforts among several **Commission Directorates-General (DGs)** to ensure **policy coherence** and **technical interoperability**. Project governance should be led by **DG FISMA** (financial stability, financial services, and Capital Markets Union), **DG TRADE, and DG TAXUD**, ensuring synergies between the NLF revision, the ongoing Customs Code reform (including the planned Customs Data Hub), and MiFIR.

The governance model is built on the **EBSI infrastructure**, using **Distributed Ledger Technology (DLT)** to guarantee the **immutability** of document metadata. This hybrid model combines a **decentralised technological backbone**, managed by **accredited service providers (CSPs)**, with **centralised supervision** and control exercised by **EU bodies (e.g., ESMA)** and **national accreditation authorities**. However, this creates a tension between **centralised oversight** and the **resilience** inherent in a decentralised network. While central supervision ensures **legal consistency**, it may also potentially undermine **DLT advantages**, such as **censorship resistance** and resilience. This contradiction is a critical aspect the Commission must manage clearly in the long term.

3. In-Depth Evaluation of EUTIR's Operational Backbone

3.1. Accreditation and Certification Framework (Annex II): Critical Review

Annex II outlines a comprehensive framework for the **accreditation** and **certification** of EUTIR-certified **service providers (CSPs)**, which is critical to the operational integrity of the system.

Table 2: Functional rights by participant role

ID	Participant Role	Authorised Actions	Restrictions
1	**Certified Service Provider (CSP)**	Creation and amendment of new **Metadata Records** within their authorised scope (e.g., trade, transport, product, insurance, customs). All CSP actions are logged in immutable audit trails.	Limited strictly to the domains for which the CSP is accredited and certified. Cannot impose or alter statuses beyond their scope of authorisation.
2	**Competent Authority (CSP with extended rights)**	Status change of **Metadata Records** (e.g., flagged, locked, released, cancelled). Cannot change the content of the underlying Data Set or Electronic Document, only its status.	Powers derive exclusively from **Union or national legislation** applicable to the authority's domain. No right to amend substantive business data.
3	**Financial Institution (CSP with extended rights)**	Creation and amendment of financial and payment-related **Metadata Records** under obligations linked to AML/CTF legislation. These entries must be linked to parent trade **Metadata Records** and verified through EUTIR.	Restricted to financial and payment-related metadata. No authority to alter trade, transport, or product Metadata Records.

3.1.1. Strengths and Legal Foundations

One of the framework's main strengths is the **mutual recognition** of accreditation decisions issued by a **Member State accreditation body** in line with **Regulation (EC) No 765/2008**. This ensures that CSPs accredited in one Member State can operate across the Union without additional national requirements, thereby addressing **single market fragmentation**. The framework also mandates that all CSPs are uniquely identified with a valid **LEI or vLEI**, and an **EORI number** within the EU, guaranteeing **global identity assurance** and **interoperability** with international trade systems. Furthermore, the framework requires all CSPs to use **qualified trust services** under the **eIDAS 2.0 Regulation (EU) 2024/1183**, ensuring **data authenticity** and **non-repudiation**. Importantly, **ESMA** is tasked with maintaining and publishing the **public registry** of all CSPs linked to EUTIR. This registry is **machine-readable** and interoperable with other EU registries, which is critical for **real-time verification** and **trust**.

3.1.2. Gaps and Considerations for Legal Integrity

While Annex II provides a strong accreditation framework, certain **gaps** require clarification. The framework distinguishes three roles (**Certified Service Provider**, **competent authority**, **financial institution**), but the technical implementation of their differentiated rights is delegated to Annex III. This raises the question of whether this separation provides sufficient **legal clarity** to avoid overlaps or gaps in authority, particularly since **competent authorities** hold specific rights such as **data Metadata Record locking**. Although **ESMA** is designated as the **supervisory body**, its precise mandate across multiple domains within EUTIR should be defined more clearly to avoid duplication of oversight responsibilities with other **supervisory authorities**.

3.2. Data Submission and Lifecycle Rules (Annex III): Functional Analysis

Annex III sets out the core principles of EUTIR's **data Metadata Record lifecycle** and **management**, which is a key strength in meeting **authenticity** and **traceability** requirements.

3.2.1. Immutable and Auditable Lifecycle Model

The core of the system is the **immutable** and **auditable** data lifecycle model. Annex III clearly stipulates that **"no data Metadata Record may be deleted or overwritten."** Instead, all Metadata Records remain in the registry, linked chronologically, with each new version or amendment including the **cryptographic hash** of the relevant document or dataset. This creates an **unbroken audit trail** essential for **trust** and **accountability**. The model represents a major step forward by shifting the focus of **legal validity** from **paper documents**, which can be manipulated, to **immutable, verifiable data Metadata Records**. However, legal certainty must also include a clear allocation of liability, especially in cases where actors later in the value chain possess more accurate or updated information. In such cases, responsibility for corrections and their legal effects must be explicitly defined. Based on this model, the **EUTIR registry** itself becomes the **legal proof** of **authenticity** and **validity**.

Table 3: EUTIR data Metadata Record lifecycle statuses and legal implications

Id	Status	Definition	Legal Effect
1	**active (submitted)**	Status assigned when a new record is created for a new document or initial data set.	The record is legally valid and has full effect until it is amended, terminated, cancelled, or expired.
2	**superseded**	Status assigned to a record when a new version has been registered referencing it.	The record remains preserved for audit and traceability but no longer has legal validity. Only the most recent version is legally valid.
3	**transferred (controlled)**	A status indicating that exclusive control over a Metadata Record has been lawfully transferred to a new party. This status confirms that the transfer is completed and that the record is now associated with the new controller.	Upon application of this status, the previous holder permanently loses all rights associated with the Metadata Record. The new controller obtains exclusive and enforceable rights to the record, with the same legal certainty as if the record had been originally issued to them.
4	**flagged**	Status applied when a record is marked for irregularities, pending review by a Competent Authority.	The record remains legally valid but is subject to regulatory review. Its use may be restricted depending on applicable Union or national law.
5	**locked**	Status imposed by a Competent Authority to prevent further amendments or supplements.	No new linked records may be created until the lock is released. The locked record itself remains preserved in its prior state.

6	**released**	Status update applied by a Competent Authority lifting a previous lock or flag.	The record regains the status it held before being locked or flagged (typically active), unless it has since been superseded, terminated, or cancelled.
7	**cancelled**	Status applied when a record is invalidated due to error, withdrawal, or regulatory order before it takes legal effect.	The record remains preserved for audit but has no legal validity.
8	**terminated**	Status applied when the underlying legal or contractual process has concluded (e.g., contract ended, shipment completed).	The record ceases to have legal effect from the time of termination, but remains preserved in EUTIR.
9	**expired**	Status automatically applied when a predefined validity period lapses.	The record ceases to have legal effect after the expiry time but remains preserved for audit purposes.

3.2.2. Functional Rights and Implementation Adequacy

Annexes III and II operate together to define specific **functional rights** for each participant role (**CSP**, **competent authority**, **financial institution**). Only **competent authorities** may **lock** or **flag** data Metadata Records, while **financial institutions** may create and modify **metadata** related to financial transactions. This strict **rights system** is crucial for **security** and **governance**, preventing **unauthorised manipulation**. The model is **flexible** enough to accommodate diverse actors and transactions, but its implementation details depend on **sector-specific delegated acts**, which must ensure alignment with core principles.

4. From Theory to Practice: Implementing the EUTIR Framework

4.1. Model Validation Through Use Cases (Annex V)

The use cases presented in Annex V provide practical examples of how the rules described in Annexes II and III operate in real life. The analysis shows that these cases demonstrate the functionality and resilience of the EUTIR conceptual framework.

- **Supply chain and finance integrity:** Use Case 4 (shipment custody chain) and Use Case 5 (financial amendment) illustrate how EUTIR's **immutable Metadata Record chain** maintains the **custody of goods** even when carriers or owner change in transit. The model allows a **financial institution** to add a **verifiable financial reference** to a shipment Metadata Record, preventing **multiple pledges** of the same document.
- **Real-time data-driven supervision**: Use Case 6 shows how a **customs authority** can change a Metadata Record status to **"flagged"** or **"locked"** to prevent further modification until an investigation is completed. This marks a shift from **reactive paper-based checks** to **proactive, data-driven interventions**, significantly strengthening **market surveillance** and reducing **fraud risks**.
- **Multiple applications and document tree:** Use Case 9 (AML investigation) shows how EUTIR can also function as an **anti-money laundering tool**, demonstrating its **broader applicability** beyond trade. Use Case 10 illustrates the **"document tree" model**, where a base document (e.g., bill of lading) can be linked with related Metadata Records (e.g., customs declaration) without affecting the validity of the base document, ensuring **traceability** and **validity** across the chain.

These use cases are **illustrative examples**: the data fields, identifiers, and statuses shown are not exhaustive or prescriptive, but are included to demonstrate the flexibility of Metadata Records, versioning, and parent–child relationships. Their primary purpose is to showcase the potential of managing a **decentralised technical infrastructure** through the EUTIR environment in a transparent and auditable way across the Union.

4.2. Interoperability and AI/ML Integration

EUTIR is not intended to replace other registries (**CBAM**, **DPP**, **eFTI**) but to act as an **index layer** that provides a single **trusted point** for **data verification**. This **federated approach** supports **interoperability** without centralising all data. Moreover, EUTIR's framework is designed for integration with **artificial intelligence (AI)** and **machine learning (ML)**, which are critical for **risk assessment** and **fraud detection**. Annex III establishes strict rules requiring compliance with the **AI Act** and **GDPR**, ensuring that automated data use does not undermine **privacy** or **regulatory integrity**. **AI systems** may only process **machine-readable metadata**, not full documents or personal data.

4.3. Global Dimension: International Nodes and Mutual Recognition Agreements (MRAs)

The EUTIR proposal also addresses the **international dimension**, which is essential for the system's **long-term success**. Annex II sets out the framework for **Mutual Recognition Agreements (MRAs)**[2], providing the **legal** and **technical basis** for connecting **third-country registries** to the **EUTIR network**. This approach aligns with broader EU initiatives such as **Global Gateway** and the **Digital Economy Partnership Agreement (DEPA)**[3], which aim to extend **EU digital norms** and **influence globally**.

Table 4: EUTIR use cases and their regulatory connections

Use Case	Description	Link to Regulatory Rules
Use Case 1	New version, where the old hash is superseded by a new one.	Aligns with the amendment rules in Annex III, Section 4, which ensure that only the most recent **Metadata Record** is valid.
Use Case 4	Tracking the chain of custody of a shipment between carriers.	Illustrates the **Metadata Record chain** principle from Annex III, ensuring that each change in the chain of custody corresponds to a new, immutable **Metadata Record**.

[2] European Commission. Mutual Recognition Agreements https://single-market-economy.ec.europa.eu/single-market/goods/international-aspects/mutual-recognition-agreements_en

[3] Digital Economy Partnership Agreement (DEPA) https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

Use Case 5	Financial amendment added to an eBL by a financial institution.	Implements the functional rights model of Annexes II and III, which grants financial institutions the authority to add financial **Metadata Records**.
Use Case 6	A customs officer flagging and locking a **Metadata Record**.	Establishes the rules for flagging and locking in Annex III, Section 5, giving Competent Authorities the right to real-time intervention.
Use Case 9	AML suspicion and investigation.	Shows how the role models and rules in Annexes II and III allow a financial institution to identify and flag data in case of AML suspicion, notifying the Competent Authorities.
Use Case 10	Linking a T-document to a Consignment Note.	Proves the "document tree" concept, where supplementary documents are linked to a base **Metadata Record** without affecting the base document's validity.
Use Case 11	Submission of a Digital Product Passport (DPP) with lifecycle, sustainability, and repairability data.	Aligns with ESPR Regulation (EU) 2024/1781 and Annex IV CTS rules (JSON-LD/RDF + XBRL), ensuring semantic interoperability and extended retention (10–15 years).
Use Case 12	Submission of a CBAM report with embedded CO_2 emissions data, verified by an accredited body.	Aligns with CBAM Regulation (EU) 2023/956 and Annex IV CTS rules (XBRL + liabilityReference), ensuring traceable verification and audit retention of 84 months.

5. Conclusions and Recommendations

5.1. Overall Assessment of Framework Integrity

In conclusion, the **EUTIR framework**—particularly its **operational backbone** in Annexes II and III—is notably **comprehensive**, **coherent**, and **legally robust**. The proposal sets out a clear model for **immutable data lifecycles** and strictly defined **functional rights**, which are critical for building **trust** and **accountability**. The **technical approach**, based on **cryptographic hashing** and **Distributed Ledger Technology (DLT)**, together with the **legal framework** granting the **registry itself evidentiary value**, creates an **innovative** and **reliable system**. The framework succeeds in establishing a **horizontal, digital trust layer** that enables **proactive real-time supervision** and facilitates **cross-border trade** by linking **physical goods** with **digital data**. **5.2a Cybersecurity as a Horizontal Principle**

5.2. Policy Recommendations for the Commission

- **Clarify governance**: While the model is hybrid, the division of authority between **centralised supervision (ESMA)** and **decentralised EBSI nodes** must be defined more clearly. An official **governance structure** with explicit mandates is recommended to prevent **overlaps** and **gaps**.
- **Strengthen legal mandate**: Competent authorities' rights to **lock Metadata Records** should be explicitly linked to relevant **EU legislation**, ensuring **legal certainty** and **due process** for economic operators.
- **Standardise technical requirements**: Although the proposal references **international standards** (e.g., **ISO**, **WCO**), the Commission should issue more detailed **implementing acts** to ensure **technical interoperability** and a consistent **user experience** across CSPs.

5.3. Cybersecurity as a Horizontal Principle

The IISD report *Cybersecurity and International Trade Policy* (August 2025)[4] stresses that **strong cybersecurity** is now a **prerequisite for resilient global trade**. **Weaknesses in one jurisdiction** undermine the integrity of entire supply chains. The EUTIR framework **is designed to integrate** key safeguards—immutability of records, qualified trust services under eIDAS 2.0, NIS2 compliance, and a strict accreditation framework—that directly address these risks. Making **cybersecurity** an explicit **horizontal principle** within EUTIR would strengthen **legal certainty** and demonstrate that EU measures are **proportionate and WTO-compatible**.

Linking the EUTIR **certification framework** with **international standards** (ISO/IEC 27001, Common Criteria) and **mutual recognition agreements** would enhance **global interoperability**. In addition, **international nodes** could become channels for **capacity-building in partner countries**, helping to close **cybersecurity gaps** highlighted in the IISD analysis. Embedding **cybersecurity** visibly into the **EUTIR proposal** would reinforce **institutional coherence**, enable **AI-driven risk monitoring**, and strengthen the EU's position as a **global benchmark for secure digital trade infrastructures**.

5.4. Long-Term Perspective

EUTIR is not a standalone project but a **strategic preventive measure**. Its successful implementation is critical to supporting the EU's **green and digital transition**, providing the foundation for **sustainable, AI-enabled supply chains**. In addition, its **MRA framework** and alignment with **global identification systems (LEI/vLEI)**, as well as its potential for **"dual-use applications"**, position the EU as a **global leader** in creating **transparent**, **interoperable**, and **innovation-friendly** digital trade ecosystems.

Recommendations, strategic implementation and further development of EUTIR:

1. **Implement Specific Measures for SMEs**: While the EUTIR project mentions reducing the regulatory burden on SMEs, these measures should be clearly highlighted and implemented. In the coming years, **support programmes** for SMEs should be established to help them adapt to new digital requirements, including training on

[4] Mishra, N. (2025, August). *Cybersecurity and International Trade: Understanding the policy landscape*. International Institute for Sustainable Development.

DPPs and **carbon accounting**. **Tiered compliance thresholds** could also be offered to avoid a disproportionate burden.

2. **Promote Global Interoperability**: For the EU to maintain its **leadership** in **digital trade**, the EUTIR framework should be integrated with global initiatives, such as the **UNECE recommendations** and the **eIDAS 2.0 framework**. Negotiations for **Mutual Recognition Agreements (MRAs)** with third countries and regional registries should be accelerated to ensure seamless **cross-border data exchange**. By embedding pull based models, it is ensured only necessary data is shared, improving efficiency and enabling trusted and compliance data exchange.

3. **Clarify the Technical and Legal Framework**: Although the fundamental principles of EUTIR are strong, it is essential to clarify its **technical** and **legal aspects**. The Commission should issue **implementing acts** that provide more detailed guidance on **technical interoperability** and **data submission standards**. This would prevent **fragmentation** among Member States and ensure that **AI and ML systems** can reliably use EUTIR data in compliance with the **General Data Protection Regulation (GDPR).**

4. **Integrate Financial and Sustainability Data**: EUTIR offers a unique opportunity to connect **trade** and **financial data**. Rules for adding **financial data** (e.g., guarantees) and **ESG/CE compliance data** (e.g., DPPs) to data-derived Metadata Records should be further developed. This would strengthen **trust** among **financial institutions** and enable new financing models that offer lower interest rates to companies using **sustainable supply chains**.

5. **Strengthen Institutional Coordination**: The successful implementation of EUTIR depends on close cooperation among **DG FISMA**, **DG TRADE**, and other relevant **Directorates-General**. A permanent **inter-institutional task force** should be established to ensure the project's **coherence** and **alignment** with all EU policy areas, including **financial stability**, **consumer protection**, and **environmental goals**.

5.4. Key reasons for establishing EUTIR

EUTIR is a strategic enabler for Europe's future competitiveness, sustainability, and security. By providing a trusted, decentralised verification environment, it accelerates trade,

strengthens resilience, and supports the EU's green and digital ambitions. Its adoption would not only modernise cross-border processes but also position Europe as a global leader in transparent, ML/AI-ready trade ecosystems.

1. **Global Unique Identification**: International trade involves vast flows of data across multiple stakeholders, systems, and jurisdictions. Without globally unique identifiers, there is a high risk of duplication, misassociation, and fraud.

2. **Interoperability Across Platforms**: Modern trade relies on multiple specialised registries and platforms (eFTI, DPP, CBAM, permit registries). EUTIR functions as the **index layer**, enabling automated cross-referencing between systems without requiring manual reconciliation.

3. **Traceability & Accountability**: EUTIR maintains a full custody chain, showing the entire lifecycle of a document or shipment, including transfers between different Certified Providers, enabling transparent compliance checks.

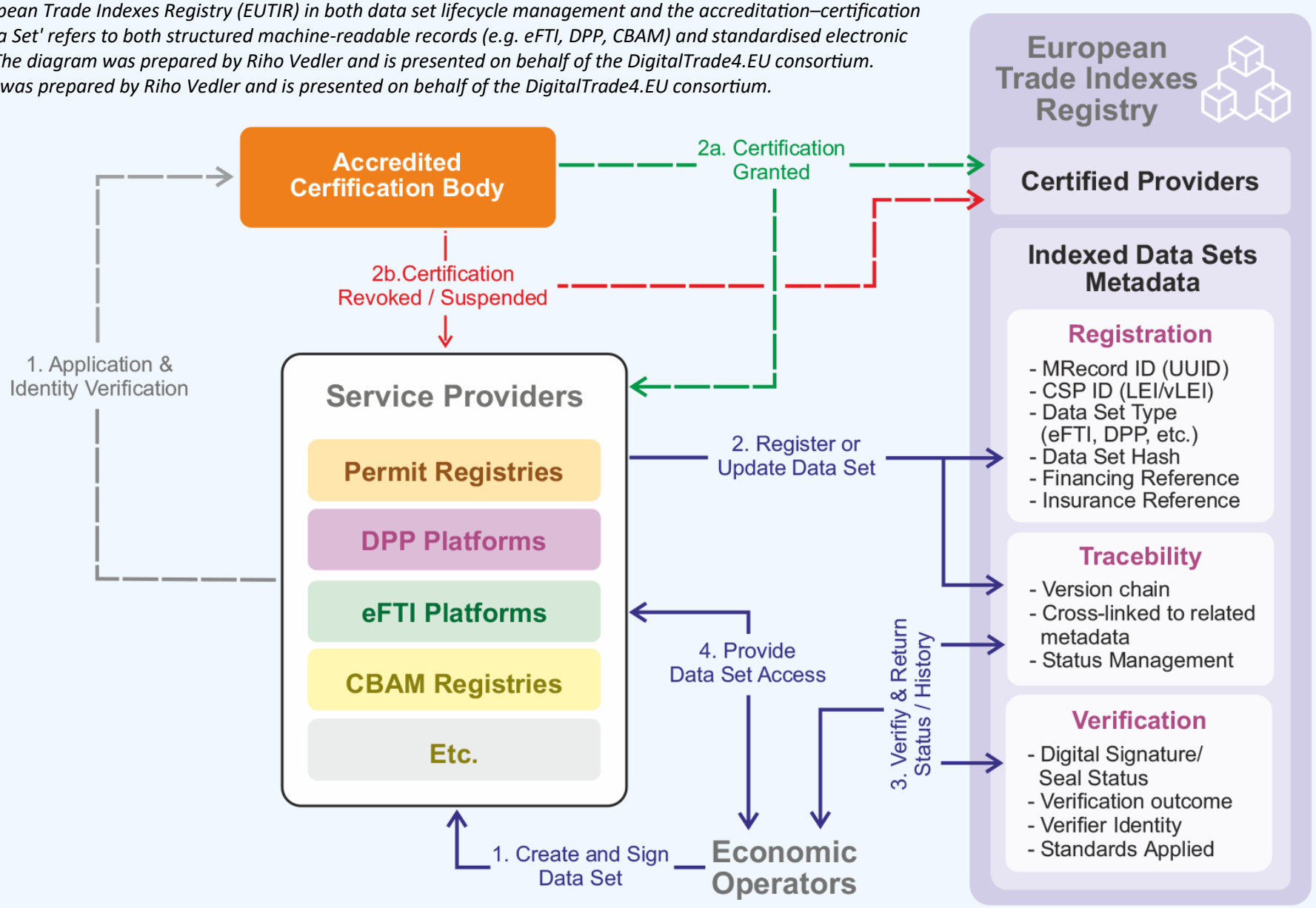
4. **Single Source of Truth**: By acting as the authoritative reference, EUTIR ensures that both authorities and market actors can confirm that the information they use is the latest, valid, and authentic version. At the same time, in cross-border contexts, incidents occurring outside the Union are governed by the applicable legislation of the jurisdiction concerned (e.g., Japan), interpreted in light of relevant international conventions and established practices. EUTIR therefore provides a harmonised audit trail that supports recognition across jurisdictions, while respecting the primacy of local law.

5. **Support for Digital Trust Infrastructure**: Full interoperability with **Global Legal Entity Identifier Foundation (GLEIF) LEI/vLEI** framework and EBSI-based DLT creates a trust environment that extends beyond the EU, enabling recognition and interoperability in global supply chains and finance networks.

Now is the time to integrate EUTIR into the EU's digital policy framework and make it a cornerstone of the Single Market's next evolution.

Annex I. EUTIR Environment: Data Set Lifecycle and Accreditation–Certification Flow

Figure 2. This diagram illustrates the interaction between Economic Operators, Service Providers, Accredited Certification Bodies, and the European Trade Indexes Registry (EUTIR) in both data set lifecycle management and the accreditation–certification process. 'Data Set' refers to both structured machine-readable records (e.g. eFTI, DPP, CBAM) and standardised electronic documents. The diagram was prepared by Riho Vedler and is presented on behalf of the DigitalTrade4.EU consortium.
The diagram was prepared by Riho Vedler and is presented on behalf of the DigitalTrade4.EU consortium.



Annex II. Accreditation and Certification Framework for Service Providers

DRAFT

1. Definitions

1.1. Core Registry Concepts & Processes

a) **"European Union Trade Index Registry (EUTIR)"** means the Union-wide digital infrastructure based on a distributed ledger technology (DLT) network, created for the secure submission, indexing, verification, and retrieval of trade-related Metadata Records. EUTIR is operated by Certified Service Providers (CSPs) and authorised stakeholders through national nodes, ensuring interoperability with other Union digital systems.

b) **"Node"** means a technical instance participating in the EUTIR distributed ledger infrastructure, maintaining a synchronised copy of the registry and executing validation and consensus functions in accordance with Union interoperability and security standards. Nodes may be operated by Member States, Certified Service Providers (CSPs), or, subject to international agreements, third countries ("international nodes").

c) **"Metadata"** means structured descriptive information associated with an Electronic Document or Data Set, including unique identifiers, cryptographic hashes, timestamps, status fields, and references (e.g., financing or insurance links). Metadata enables verification of authenticity, integrity, and traceability across platforms and jurisdictions, while avoiding the storage of full document contents in EUTIR.

d) **"Metadata Record (Record)"** means the registered unit of information in the EUTIR. A Metadata Record represents the authoritative and legally valid reference to an Electronic Document or Data Set, consisting solely of metadata elements (hash, timestamp, identifiers, status). Each Metadata Record is immutable, auditable, and preserved for at least the same legal retention period as its associated Electronic Document or Data Set. Metadata Records constitute legal

proof of authenticity and validity, while never storing the full content of the underlying document.

e) **"Record Relationship"** means the structural link between Metadata Records, covering both versioning (supersede relationships) and parent–child relationships. The detailed rules and categories (including dependent and independent inheritance, recursive descendant chains, and applicability to version sequences) are defined in the **Common Technical Specifications (CTS)**.

f) **"Submission"** means the act of transmitting metadata into EUTIR by a Certified Service Provider (CSP).

g) **"Control"** means the exclusive ability of a person or entity to exercise rights associated with a Metadata Record, including the ability to prevent others from exercising such rights and to transfer those rights lawfully to another party. Control shall be demonstrated through reliable and verifiable technical means, ensuring technological neutrality and international interoperability.

h) **"Verification"** means the process of confirming, through the EUTIR, that an **Electronic Document or Data Set** corresponds to its registered Metadata Record and meets the applicable requirements of Union or national legislation. Verification establishes that the Electronic Document or Data Set is authentic, intact, and legally valid. Detailed rules for verification services are set out in **Chapter 16** of this Annex.

1.2. Documents and Data

a) **"Electronic Document (eDocument)"** means any digital file or dataset, including but not limited to trade, transport, customs, financial, environmental, or compliance documents, created, transmitted, or stored in electronic form. Electronic Documents may exist in both structured formats (e.g., XML, JSON, XBRL) and unstructured formats (e.g., PDF). **For the purposes of EUTIR, full Electronic Documents are not stored in the registry; only their metadata is referenced.**

b) **"Data Set"** means a structured, machine-readable electronic document consisting of standardised fields and formats, in line with Union or international data

exchange standards (e.g., ISO 20022, WCO Data Model, UN/CEFACT Core Components). Where Union sectoral legislation requires the use of structured electronic records, such documents shall be treated as Data Sets and may serve as the basis for creating Metadata Records in EUTIR.

c) **"Cryptographic Hash (Hash)"** means a unique, fixed-length value generated by a cryptographic hash function representing the content of a digital document or dataset. Any alteration of the original content results in a different hash, ensuring integrity and enabling traceability without storing the full content in EUTIR.

1.3. Actors and Roles

a) **"Certified Service Provider (CSP)"** means an entity accredited in accordance with Union or national law to perform technical functions in EUTIR, including the secure submission, creation, and validation of Metadata Records. A CSP acts solely in its certified technical role and does not assume liability for the legal, regulatory, or economic content of the underlying Electronic Document or Data Set. The responsibility for the correctness and legal validity of the content remains with the Economic Operator or the party creating the document.

b) **"Actor"** means any entity authorised to interact with the EUTIR registry under this Regulation, including but not limited to Certified Service Providers (CSPs), Competent Authorities, Financial Institutions, and Economic Operators, each within the scope of their designated roles.

c) **"Economic Operator"** means any natural or legal person who, in the course of business, is required under Union law to submit, maintain, or rely on records linked to compliance, customs, trade, sustainability, or product-related obligations within the EUTIR framework. This includes, where applicable, manufacturers, importers, exporters, distributors, freight forwarders, and other supply chain participants, but excludes Certified Service Providers acting solely in their technical role.

d) **"Financial Institution"** means a credit institution, payment service provider, insurance undertaking, investment firm, or other entity authorised under Union or

national law to provide financial services, including banking, payments, guarantees, collateral, insurance, and supply chain finance. Financial Institutions under EUTIR are subject to regulatory supervision by competent financial or supervisory authorities.

e) **"Parties"** means all actors interacting with EUTIR in relation to a transaction or record, including Economic Operators, Certified Service Providers (CSPs), Financial Institutions, and Competent Authorities, each within the scope of their designated roles.

f) "Competent Authority" means an authority or body designated by a Member State, or by Union law, to exercise regulatory, supervisory, or enforcement functions in relation to EUTIR. Competent Authorities may include, depending on their mandate:

i. logistics and transport authorities, including customs, border, and transport administrations;

ii. environmental and climate authorities, including bodies supervising the Carbon Border Adjustment Mechanism (CBAM), carbon registries, and sustainability regulators;

iii. financial and tax authorities, including VAT authorities, payment supervision authorities, and financial market regulators.

Each Competent Authority shall exercise oversight only within its designated legal mandate.

1.4. Identifiers and Trust

a) **"Legal Entity Identifier (LEI)"** means a 20-character alphanumeric code compliant with ISO 17442, ensuring the clear and unique identification of legal entities engaged in financial transactions and other official interactions. The LEI connects to key reference data enabling interoperability across jurisdictions. The Global Legal Entity Identifier Foundation (GLEIF) oversees the governance and operational framework of the LEI system.

b) **“Verifiable Legal Entity Identifier (vLEI)”** means, in accordance with ISO 17442-3, digitally trustworthy version of the 20-digit LEI code which is automatically verified, without the need for human intervention and interoperable with Regulation (EU) 2024/1183 (eIDAS 2.0), enabling secure and automated identification and authorisation of legal entities.

2. Accreditation Bodies

2.1. Accreditation bodies shall be designated by the Member States in accordance with Regulation (EC) No 765/2008 and shall operate in full independence and impartiality.

2.2. Accreditation bodies shall be responsible for the accreditation of Certified Service Providers (CSPs) within the EUTIR framework, in accordance with applicable Union legislation and internationally recognised standards.

2.3. Accreditation decisions issued by a national accreditation body shall be **mutually recognised across all Member States**, ensuring that CSPs accredited in one Member State may operate Union-wide without additional national requirements.

2.4. Accreditation bodies may delegate testing and technical evaluation to accredited Conformity Assessment Bodies (CABs) in line with ISO/IEC 17065, ensuring consistency with established Union conformity assessment practices.

2.5. Accreditation bodies shall maintain appropriate technical competence, resources, and procedures to ensure the integrity and reliability of the accreditation process, including regular monitoring and reassessment of accredited entities.

2.6. Accreditation bodies shall cooperate at Union level, ensuring effective peer evaluation and preventing duplication of assessments, in order to promote uniform application of accreditation rules across all Member States.

3. Certified Service Providers: Requirements, Roles and Scope

3.1. **General requirements**. Only Certified Service Providers (CSPs) are authorised to perform submissions into EUTIR. Each CSP shall be uniquely identifiable via a valid **LEI or vLEI**, and, where applicable, an **EORI**. Certification shall be valid for **five years** and may be renewed following reassessment. Every submission shall include the CSP

identifier linked to its LEI/vLEI. Certification shall always include designation of the certified role (Certified Service Provider, Competent Authority, or Financial Institution), which determines the functional rights applicable under Annex III.

3.2. **Certification validity and scope.** Certification granted in one Member State shall be valid across all Member States without additional requirements. All CSPs must use **qualified trust services under eIDAS 2.0** (Regulation (EU) 2024/1183), ensuring authenticity, non-repudiation, and interoperability.

3.3. **Role model**. All certified organisations automatically hold the role of **Certified Service Provider (CSP)**. During certification, organisations may additionally be marked as:

a) **Competent Authority**, if they are legally mandated to enforce compliance under Union or national legislation (limited to status-related updates such as flagged, locked, released).

b) **Financial Institution**, if they hold a valid license or registration under Union or national financial supervision law (limited to financial and payment-related metadata).

These designations are recorded in the Union CSP Register and form part of the organisation's certification status in EUTIR.

3.4. **Scope limitation.** Certification under this Annex establishes the right of a Service Provider to act within the EUTIR framework under its designated role. The legal validity of submissions, as well as all processes of validation, verification, amendment, and termination, are governed exclusively by Annex III.

4. Technical and Organisational Requirements for CSPs

4.1. CSPs shall comply with the following requirements:

4.2. **Data integrity and security** – all submitted metadata must be complete, accurate, and protected against unauthorised access.

4.3. **GDPR and data protection** – personal data processing must comply with Regulation (EU) 2016/679.

4.4. **Cybersecurity** – CSPs must comply with the security requirements of the NIS2 Directive.

4.5. **Audit trail** – all activities in EUTIR must be logged; logs shall be immutable and accessible to competent authorities.

4.6. **Use of trust services** – CSPs must use qualified trust services in accordance with eIDAS 2.0 (Regulation (EU) 2024/1183).

4.7. **Standardised data sets** – all metadata submissions must comply with the Union's standardised data set frameworks.

4.8. **Interoperability obligation** – all submissions shall be machine-readable and interoperable with Union digital infrastructures, including but not limited to:

- **Digital Product Passport (DPP)** (under ESPR),
- **Carbon Border Adjustment Mechanism (CBAM)** (Regulation (EU) 2023/956),
- **electronic Freight Transport Information (eFTI)** (Regulation (EU) 2020/1056),
- **Union licensing and permitting registers** (e.g., F-Gas Regulation, chemicals, waste shipments),
- **Union electronic invoicing and VAT reporting frameworks**,
- **other Union-wide registries** relevant to trade, environment, and compliance as defined by delegated acts of the Commission.

4.9. **Compliance with data standards** –CSPs shall ensure that all submissions comply with the Data Submission Standard set out in Annex III and the detailed technical requirements defined in the Common Technical Specifications (CTS, Annex IV).

5. Certification Process

5.1. CSPs shall undergo independent assessment covering technical capacity, security measures, and compliance with Union law, including GDPR.

5.2. Certification shall be granted by the national accreditation body in cooperation with ESMA.

5.3. Certification shall be revoked if the CSP breaches the obligations set out in this Regulation.

6. Supervision and Reporting

6.1. ESMA shall act as the Union-level supervisory authority responsible for the accreditation, certification, and Union-wide register of Certified Service Providers (CSPs) under EUTIR. ESMA's mandate shall cover horizontal oversight of certification integrity, cybersecurity standards, and compliance with this Regulation.

6.2. Sector-specific supervision shall remain within the competence of the respective Union and national supervisory authorities. This includes, inter alia, the European Banking Authority (EBA) and national financial supervisors for financial services, the European Insurance and Occupational Pensions Authority (EIOPA) for insurance-related records, customs authorities and OLAF for customs and trade data, and competent environmental authorities for environmental and climate-related submissions.

6.3. Where sector-specific supervision falls under the competence of Commission Directorates-General, the respective Directorate-General shall retain supervisory responsibility in its domain. This includes, inter alia, DG MOVE for logistics and electronic Freight Transport Information (eFTI) service providers, DG GROW for Digital Product Passport (DPP) providers, DG TAXUD for customs and related trade processes, and DG CLIMA and DG ENV for climate- and environment-related records. In the case of licences and permits, which fall under diverse Union and national regimes, the competent licensing authority shall retain full responsibility for the legal validity and enforcement of such records.

6.4. Each Commission Directorate-General responsible for sectoral legislation integrated into EUTIR shall designate a specialised supervisory unit. These units shall coordinate with ESMA and participate in the Joint Supervisory Coordination Platform. Their role shall be to ensure that sector-specific records and licensing regimes (including eFTI, Digital Product Passports, customs and environmental declarations, and permits) are properly integrated into EUTIR, without duplicating the certification and accreditation functions assigned to ESMA.

6.5. In order to avoid duplication of competences, ESMA shall establish and coordinate a **Joint Supervisory Coordination Platform**, bringing together the relevant Union

agencies, Commission Directorates-General, and national competent authorities. The Platform shall ensure coherent supervision across all domains of EUTIR, promote mutual recognition of supervisory actions, and facilitate the exchange of incident reports. The Joint Supervisory Coordination Platform shall operate as a permanent inter-institutional working group, ensuring consistency of EUTIR implementation across all Union policy domains, including financial stability, trade, consumer protection, and environmental objectives.

6.6. Accreditation bodies shall submit annual reports to the Commission, ESMA, and DG JUST, covering certification processes, breaches, and systemic incidents.

6.7. The Commission shall review the framework every three years and may adopt additional implementing measures.

6.8. CSPs shall ensure that their services are **globally interoperable** and aligned with international standards (e.g., ISO metadata models).

7. Rules on Termination, Cancellation, and Suspension for CSPs

7.1. CSPs shall establish procedures for **suspending, cancelling, or terminating submissions** under the following conditions:

a) the submission is incomplete or inconsistent with required data standards

b) the economic operator withdraws the declaration before validation;

c) a competent authority issues an order for cancellation or invalidation;

d) a cybersecurity incident or system failure requires temporary suspension.

7.2. Cancelled or terminated submissions shall not be erased. Instead, they shall be preserved in EUTIR with a status label **“cancelled”** or **“terminated”**, ensuring full auditability.

7.3. CSPs must notify both the economic operator and the competent authority of any suspension, cancellation, or termination, including justification and timestamp.

7.4. Suspended submissions may only be reactivated once the root cause has been resolved and, where applicable, with competent authority approval.

7.5. All suspension, cancellation, and termination events shall be recorded in the **audit logs**, accessible to ESMA and competent authorities.

7.6. In the event of the bankruptcy, insolvency, or compulsory liquidation of a Certified Service Provider, its certification shall be automatically revoked. The CSP shall be removed without delay from the Union CSP Register, and all pending submissions shall either be transferred to another authorised CSP designated by the competent authority or preserved in EUTIR with the status label "terminated".

7.7. In the event of suspension of a CSP, all records already submitted shall remain valid in EUTIR with their original status. The CSP shall not be permitted to make new submissions or amendments during the suspension period. Any pending processes (e.g., flagged records awaiting lock) shall be managed directly by the competent authority or transferred to another authorised CSP as designated.

8. CSP Register

8.1. The Commission shall maintain and publish, on a **dedicated webpage**, a **Union-wide register of Certified Service Providers (CSPs)** authorised to operate within the EUTIR framework.

8.2. The register shall be kept up to date and include at minimum:

a) the name and LEI/vLEI of the CSP,

b) the Member State of accreditation,

c) the date of certification and expiry,

d) the status (active, suspended, withdrawn).

8.3. The register shall be made available:

a) via a **public webpage**, and

b) via a **public API service**, enabling real-time verification of CSP status.

8.4. The register shall be **machine-readable and interoperable** with other Union registers (e.g., **EU Trusted List (EUTL)**, **NANDO**) and provided in open data formats (JSON, XML, XBRL).

8.5. CSPs not listed in the register shall **not be recognised** as authorised submitters to EUTIR.

9. Future Categorisation

9.1. CSPs shall be certified under a single Union-wide framework, based on the functional rights defined in this Annex.

9.2. The Commission may, by delegated acts, establish **sector-specific categories or sub-categories of Certified Service Providers**, and define differentiated requirements and rights where justified by:

a) the nature of the service,

b) the risk profile, or

c) sectoral legislation.

9.3. Any such categorisation shall remain consistent with the general rights-based framework of EUTIR and ensure interoperability across all Member States.

10. International Nodes

10.1. Subject to international agreements or adequacy decisions, third countries may connect their own blockchain node to the EUTIR distributed ledger infrastructure. Such connection shall be based on a **Mutual Recognition Agreement (MRA)** between the Union and the respective third country, and shall ensure that:

a) the node fully complies with the Union's interoperability, cybersecurity and governance standards for EUTIR;

b) the node is subject to joint supervision, monitoring, and auditability in cooperation with the competent Union authority;

c) the legal and technical validity of the node and its operations are mutually recognised.

10.2. Procedural rules:

a) A third country requesting connection of a node shall submit a formal request to the European Commission.

b) The Commission, in consultation with ESMA and the relevant Union bodies, shall assess the technical readiness and legal framework of the requesting country.

c) Where the assessment is positive, a mutual recognition agreement shall be negotiated, defining rights, obligations, governance arrangements, and dispute resolution.

d) Upon entry into force of the agreement, the third-country node may be connected to the EUTIR infrastructure and shall be listed in the official EU register as an "international node".

e) The operation and compliance of international nodes shall be reviewed at least every three years.

10.3. International nodes may also be operated as part of equivalent regional trade index registries, provided that a **Mutual Recognition Agreement (MRA)** between the Union and the respective regional body ensures interoperability, compliance with common standards, and reciprocal supervision mechanisms.

10.4. The detailed rules on data protection and the handling of personal data in relation to international nodes shall be defined in the respective **Mutual Recognition Agreement (MRA)**, ensuring full compliance with Union law, including the GDPR.

Annex III. Rules on Metadata Submission, Status and Verification Rules

DRAFT

OPERATIVE LEVEL

1. General Principles

1.1. **EUTIR** shall serve as a **Union-wide trusted registry** for the **submission**, **amendment**, **verification**, **flagging**, **locking**, and **availability** of trade-related metadata.

1.2. All operations in EUTIR shall be performed in accordance with the **accreditation and certification framework** defined in Annex II and the **functional rights** defined in this Annex.

1.3. The EUTIR framework is designed to be **language-neutral**, verifying metadata and machine-readable formats (such as XML, JSON, or XBRL) rather than the human-readable content of documents. This ensures that documents are validly registered in EUTIR regardless of language. The acceptance of such documents for customs, regulatory, or judicial purposes remains subject to **domestic rules and the applicable provisions of Union law**.

2. Functional Rights of Actors in EUTIR

2.1. **Certified Service Providers (CSPs):** May create and amend Metadata Records within their authorised scope (e.g., logistics, product, insurance, customs). All CSP actions are logged in immutable audit trails.

2.2. **Competent Authorities:** May update the status of records (flagged, locked, released, cancelled) but cannot alter substantive business content. Their authority to impose restrictive statuses derives exclusively from Union or national legislation applicable to their domain.

2.3. **Financial Institutions:** May create and amend only financial and payment-related metadata under obligations linked to AML/CTF legislation. These entries must be linked to parent trade records and verified through EUTIR.

2.4. **Universal rights:** Verification of records is open to all via EUTIR APIs and the public web-based service, which confirms authenticity, current status, and legal validity without modifying the record.

2.5. **Sector-specific rules:** Each Union policy domain (customs, transport, environment, climate/CBAM, product compliance) shall define detailed submission and amendment rules in implementing or delegated acts, consistent with Annex II and this Annex.

2.6. A Joint Supervisory Coordination Platform shall be established, composed of the European Commission (DG FISMA, DG TRADE, DG TAXUD), ESMA, and national accreditation authorities, to ensure coherent supervision of EUTIR. This platform shall coordinate policy, technical standards, and compliance monitoring.

3. Submission and Amendment Rules

3.1. **Metadata records** in EUTIR may be created only by **CSPs** within the scope of their certified role.

3.2. Each initial submission shall constitute the creation of a base record for a new digital document or dataset, and must include: timestamp, LEI/vLEI, a qualified trust service seal (eIDAS 2.0), a cryptographic hash, and initial status “submitted”.

3.3. **Amendments** shall take one of three forms:

a) **new version** (previous record becomes “superseded”),

b) **supplementary record** referencing a **parent record**,

c) **status update** (flagged, locked, released, cancelled, terminated, expired).

3.4. Each new record must include a new **cryptographic hash**, ensuring **traceability** via **version chains** or **document trees**.

3.5. Only the most recent record in a version chain is legally valid; earlier versions are preserved for audit purposes.

4. Metadata Record Lifecycle

4.1. Statuses include:

	Status	Definition	Legal Effect
1	**active (submitted)**	Status assigned when a new record is created for a new document or initial data set.	The record is legally valid and has full effect until it is amended, terminated, cancelled, or expired.
2	**superseded**	Status assigned to a record when a new version has been registered referencing it.	The record remains preserved for audit and traceability but no longer has legal validity. Only the most recent version is legally valid.
3	**transferred (controlled)**	A status indicating that exclusive control over a Metadata Record has been lawfully transferred to a new party. This status confirms that the transfer is completed and that the record is now associated with the new controller.	Upon application of this status, the previous holder permanently loses all rights associated with the Metadata Record. The new controller obtains exclusive and enforceable rights to the record, with the same legal certainty as if the record had been originally issued to them.
4	**flagged**	Status applied when a record is marked for irregularities, pending review by a Competent Authority.	The record remains legally valid but is subject to regulatory review. Its use may be restricted depending on applicable Union or national law.
5	**locked**	Status imposed by a Competent Authority to prevent further amendments or supplements.	No new linked records may be created until the lock is released. The locked record itself remains preserved in its prior state.
6	**released**	Status update applied by a Competent Authority lifting a previous lock or flag.	The record regains the status it held before being locked or flagged (typically active), unless it has since been superseded, terminated, or cancelled.
7	**cancelled**	Status applied when a record is invalidated due to error, withdrawal, or regulatory order before it takes legal effect.	The record remains preserved for audit but has no legal validity.
8	**terminated**	Status applied when the underlying legal or contractual process has concluded (e.g., contract ended, shipment completed).	The record ceases to have legal effect from the time of termination, but remains preserved in EUTIR.
9	**expired**	Status automatically applied when a predefined validity period lapses.	The record ceases to have legal effect after the expiry time but remains preserved for audit purposes.

4.2. Liability attaches from the moment a record is submitted to the EUTIR registry. Where a later actor submits more accurate or updated information, liability for that correction begins from the moment of its registration in EUTIR. Earlier records remain immutable and auditable, but legal reliance rests exclusively on the most recent verified version. Later corrections do not release the original actor from liability for incidents or damages that occurred prior to the correction. Where an error is corrected by the same actor who submitted the original record, liability remains with that actor for both the initial error and the correction. Where a correction is submitted by a different actor, liability for the accuracy of the correction attaches to the correcting actor, while the original actor remains liable for any damage or legal effect caused before the correction was registered.

4.3. All access to EUTIR records shall be fully logged. Logs shall be preserved as metadata for auditability and legal certainty for at least the same retention period as the underlying records, and in any case no shorter than the applicable statutory limitation periods for liability or claims. Logs must remain in their original, unaltered form throughout this period and shall be subject to secure archiving practices.

5. Retention and Preservation Rules

5.1. **Metadata Records.** Each Metadata Record has distinct legal effects but all Metadata Records remain preserved and auditable. No Metadata Record shall be deleted or overwritten. If no explicit expiry date is added at the time of creating the Metadata Record, the Metadata Record shall remain in active status for 24 months from the date of its creation and thereafter automatically transition to terminated (archived) status. All Metadata Records must be preserved and auditable for a minimum of 84 months (7 years), unless longer periods are required by Union or national law. The validity and retention period of a Metadata Record shall always align with the legal retention period of its associated Electronic Document or Data Set.

5.2. **Logs of Metadata Records.** All logs associated with Metadata Records shall be preserved and auditable for at least the same retention period as the Metadata Record itself. No log may be deleted, overwritten, or expired before the

corresponding Metadata Record, and logs must follow any extended retention period resulting from parent–child relationships.

5.3. **Versioning and Parent–Child Rules.** The rules governing versioning chains (supersede relationships) and parent–child inheritance, including dependent and independent descendants, shall be specified in the Common Technical Specifications (CTS). These CTS rules shall ensure compliance with internationally recognised standards (UN/CEFACT, ISO 15000/20022, WCO Data Model) and guarantee that all relationships remain auditable, machine-readable, and legally reliable.

5.4. **Orphan Metadata Records.** Where a Metadata Record is preserved in EUTIR but the associated Electronic Document or Data Set is no longer available, the Metadata Record shall continue to prove that such a document once existed and was validly registered. The evidentiary value of an orphan Metadata Record shall be limited to authenticity and timestamp verification, while full evidentiary value requires the associated Electronic Document or Data Set to remain preserved.

6. Flagging and Locking Rules

6.1. Records may be flagged or locked only by authorised Competent Authorities.

6.2. Locked records cannot be amended until released by the authority that imposed the lock.

6.3. All actions are logged immutably in EUTIR.

7. Content-Specific Rules

7.1. **Product and Sustainability Data.** EUTIR records shall integrate product- and sustainability-related metadata, including Digital Product Passport (DPP) identifiers, carbon footprint declarations, and compliance with the Carbon Border Adjustment Mechanism (CBAM) and due diligence frameworks such as the Corporate Sustainability Reporting Directive (CSRD) and the Corporate Sustainability Due Diligence Directive (CSDDD). These data fields ensure traceability from production and manufacturing to reporting obligations, providing verifiable links between product-level and corporate-level compliance.

7.2. **Contract and Order Metadata.** EUTIR records shall allow for integration of order and contract-related metadata, including purchase orders, delivery contracts, and financial guarantees linked to contractual obligations. This enables transparent monitoring of contractual performance and facilitates compliance audits across the supply chain.

7.3. **Logistics and Trade Documentation.** EUTIR records shall allow for integration of logistics- and customs-related metadata, such as electronic freight transport information (eFTI), consignment notes, import and export declarations, and electronic Bills of Lading (eBL) or other negotiable cargo documents. This provides a continuous custody chain and ensures that regulatory, transport, and commercial records are synchronised and auditable.

8. Transparency, Auditability and Traceability

8.1. All actions (submission, amendment, verification, flagging, locking, release) are logged in immutable audit trails, including actor's LEI/vLEI, timestamp, action, and digital signature.

8.2. An Audit Log shall mean the complete, immutable record of all such actions within EUTIR, covering submissions, amendments, linkages, status changes, verification queries, and authority interventions.

8.3. Version history must be fully traceable, enabling competent authorities to reconstruct document lifecycles.

8.4. Audit logs shall be accessible to ESMA and competent authorities.

9. Liability and Legal Certainty

9.1. **General principle.** EUTIR shall ensure not only authenticity and traceability of metadata but also a clear allocation of liability among actors. Liability follows the principle that each participant is responsible for the data they submit or the actions they take. Liability attaches from the moment a record is submitted to the EUTIR registry, ensuring that legal responsibility is clear and enforceable. This strengthens legal certainty across value chains and trade ecosystems and provides a basis for dispute resolution.

9.2. **Role-based liability.**

9.2.1. **Certified Service Providers (CSPs):** liable for the technical correctness, authenticity, and timely submission of metadata, including proper use of qualified trust services under eIDAS 2.0.

9.2.2. **Competent Authorities:** liable for restrictive actions (flagged, locked, cancelled, released), ensuring these are based on valid legal mandates and respecting due process.

9.2.3. **Financial Institutions:** liable for the accuracy and lawfulness of financial and AML/CTF-related metadata they submit.

9.2.4. **Economic Operators:** liable for the substantive accuracy of the underlying business, customs, or product data linked to EUTIR records.

9.3. **Damages and corrections.** In case of disputes or damages resulting from incorrect, misleading, or unlawful records, liability shall be attributed according to these roles. Where a later actor submits a correction, liability for that correction attaches to the correcting actor, while the original actor remains liable for any damages or legal consequences that occurred prior to the correction. Any material damage caused to third parties or Competent Authorities as a result of false or fraudulent information shall be borne by the submitting actor, in accordance with Union and national law.

9.4. **Sanctions.** Repeated or deliberate submission of false or misleading information by a Certified Service Provider, Financial Institution, or Economic Operator may result in suspension or revocation of certification under this Regulation, without prejudice to further administrative, civil, or criminal sanctions provided under Union or national law.

9.5. **SME access to finance.** EUTIR shall support SME access to finance by enabling financial institutions to rely on EUTIR-verified records for credit risk assessment. Records validated through EUTIR may be used by banks to reduce risk weights in line with prudential rules, subject to guidance from the European Central Bank (ECB) and the European Banking Authority (EBA).

10. Verification Services

10.1. Verification services enable non-certified parties to confirm authenticity, integrity, legal validity, and status of records.

10.2. Verification is based solely on the registered hash and lifecycle status, not on the identity of the submitter. The EUTIR register itself constitutes legal proof of authenticity and validity of electronic documents and datasets.

10.3. **Verification results** include:

a) **unique record identifier**,

b) **current status**,

c) **submitting CSP**,

d) **timestamp** of last change,

e) **competent authority identifier** (restricted layer only),

f) **legal validity** at reference time,

g) and **role-specific metadata visibility**.

10.4. **Verification** services operate in two layers:

a) **public** (basic confirmation),

b) **restricted** (authenticated access to detailed metadata).

10.5. CSPs must provide verification services as part of their certification. All queries are logged and retained for at least 7 years, or longer if required by Union or national legislation.

10.6. The right of Competent Authorities to impose restrictive statuses, including locking, releasing, or cancelling of records, shall derive exclusively from Union or national legislation applicable to their domain.

10.7. Each restrictive action must be explicitly linked to a specific legal mandate under Union law, ensuring legal certainty for economic operators and guaranteeing due process.

10.8. Member States may introduce additional or extended verification options under

their national legislation. In such cases, verification must be performed by a CSP, and EUTIR shall provide metadata confirming that the CSP performing the verification is duly certified and listed in the Union CSP Register.

11. Data Exchange and Access

11.1. **General Principle.** EUTIR registers Metadata Records as legally valid references to Electronic Documents or Data Sets. The registry does not replace the actual transmission of such data between parties, but ensures authenticity, integrity, and traceability of the exchanges. Electronic Documents or Data Sets that are verified through EUTIR and submitted in accordance with Union or national law shall have full legal effect equivalent to their paper-based counterparts.

11.2. **Business-to-Business (B2B) Exchange.** In B2B contexts, parties may exchange Electronic Documents or Data Sets directly, either bilaterally or through trusted platforms. Each exchange shall include a reference to the corresponding Metadata Record in EUTIR. The Metadata Record provides legal proof of authenticity, status, and versioning of the exchanged data.

11.3. **Business-to-Government (B2G) Exchange.** In B2G contexts, Economic Operators shall provide to Competent Authorities the Electronic Documents or Data Sets required by Union or national legislation. Each submission shall include a reference to the corresponding Metadata Record in EUTIR, which serves as proof of authenticity and immutability.

11.4. **Verification and Control.** Competent Authorities shall use EUTIR to verify authenticity, integrity, and legal status of Metadata Records. Automatic checks, risk assessment, and decision-making processes shall be performed by national or Union IT systems in accordance with sectoral legislation.

11.5. **Interoperability of Data Models.** Data exchange under this Article shall ensure interoperability with recognised international and Union standards. The specific standards applicable to metadata formats, data models, and secure transmission protocols are defined in the Common Technical Specifications (CTS, Annex IV).

11.6. **Transmission Methods.** Transmission of Electronic Documents or Data Sets

between parties shall take place through secure communication channels in compliance with Union trust service and security requirements. The applicable transmission methods, including short-range communication, network-based delivery, or registered electronic delivery, are defined in the Common Technical Specifications (CTS, Annex IV).

11.7. **Submission to Competent Authorities.** Economic Operators shall ensure that all Electronic Documents or Data Sets required by Union or national law are submitted or made available to the relevant Competent Authorities. Such submissions shall always reference the corresponding EUTIR Metadata Record, enabling verification of authenticity, integrity, and legal status. The obligation to provide data shall be exercised strictly in accordance with the applicable Union or national legislation governing the mandate of each Competent Authority.

12. Interoperability and Data Submission Standards

12.1. Submissions must be machine-readable and interoperable with Union infrastructures (DPP, CBAM, eFTI, licensing registers, e-invoicing, etc.).

12.2. The Commission shall adopt **Common Technical Specifications (CTS)** defining metadata structures, hash algorithms, APIs, timestamp formats, logging requirements, financial/ESG metadata, and AI/ML safeguards.

12.3. Implementing acts shall further specify technical interoperability and submission standards, preventing fragmentation among Member States and ensuring AI/ML systems can process metadata in line with GDPR.

12.4. Compliance with CTS is mandatory for CSP certification under Annex II. The Commission shall regularly review CTS with ESMA, CEN/CENELEC, and relevant Union agencies.

12.5. Federated interoperability shall allow verification across regional or international registries, based on harmonised standards, ensuring authenticity and traceability across jurisdictions. The legal and international framework for such interoperability is further specified in **Chapter 17.**

13. Payments, Financial and ESG Metadata

13.1. Processing of financial and payment metadata under EUTIR shall be based on a lawful ground under Article 6 of the GDPR (public interest, legal obligation, contractual necessity, or consent, as applicable).

13.2. Financial Institutions may submit supplementary records including guarantees, payments, collateral, or insurance. Each has its own hash and is linked to parent trade records.

13.3. ESG and Circular Economy compliance metadata may include sustainability declarations, carbon footprint data, DPP identifiers, or CBAM compliance. Such metadata, once linked, constitutes verifiable legal evidence.

13.4. Verification queries may enable financial institutions to apply preferential financing terms based on ESG/CE compliance metadata.

13.5. These provisions shall enable financial institutions to apply innovative financing models, such as preferential rates for companies operating sustainable supply chains.

13.6. Disclosure of sensitive financial and ESG data is restricted to authenticated users, ensuring compliance with GDPR and eIDAS 2.0.

13.7. EUTIR shall ensure interoperability with the VAT in the Digital Age (ViDA) initiative, including structured eInvoicing and VAT reporting, so that tax-related metadata can be directly verified and used for compliance purposes.

13.8. EUTIR shall align with the forthcoming Payment Services Regulation (PSR) and PSD3 Directive, ensuring that payment references and financial transaction data can be integrated and applied uniformly across Member States. This alignment shall prevent divergent national implementations observed under PSD2.

13.9. EUTIR shall also ensure consistency with the proposed **Financial Data Access (FiDA) framework**, enabling interoperability between trade-related financial

metadata in EUTIR and broader financial data-sharing infrastructures once adopted. This ensures synergies between trade compliance, financing, and risk assessment.

14. AI/ML Integration

14.1. Metadata may be used in AI/ML systems for risk assessment, fraud detection, compliance, and supply chain analytics, provided systems comply with EU AI Act, GDPR, and eIDAS 2.0.

14.2. AI/ML applications may not alter records but may rely on standardised metadata and pseudonymised logs for anomaly detection.

14.3. The Commission may adopt delegated acts to establish additional technical standards for AI/ML.

14.4. EUTIR may provide AI- and machine learning-based risk dashboards for Competent Authorities and financial supervisors, enabling predictive monitoring of fraud, money laundering, and customs risks. Such tools shall only use providers that are subject to regulatory oversight in accordance with the AI Act and GDPR requirements. Providers established in the Union shall be supervised under Union law, while providers from third countries shall only be eligible where equivalent regulatory frameworks and supervisory mechanisms are in place.

IMPLEMENTATION LEVEL

15. SME Support and Proportionality

15.1. To reduce compliance burdens, the Commission shall provide support programmes for SMEs (training, guidance, financial aid).

15.2. The Commission shall establish targeted SME support programmes including training on DPP and carbon accounting, as well as phased compliance thresholds to avoid disproportionate burden.

15.3. Simplified reporting or phased compliance thresholds may be introduced to maintain proportionality.

16. Service Availability

16.1. EUTIR verification services (API and web) must ensure minimum annual availability of 99.9% (excluding notified maintenance).

16.2. CSPs must guarantee equivalent standards for their services. Fallback procedures must be available to ensure continuity of critical compliance operations.

16.3. ESMA shall continuously monitor and report service availability to the Commission.

POLICY AND INTERNATIONAL LEVEL

17. Global Interoperability and Mutual Recognition

17.1. EUTIR shall align with UNECE recommendations, UNCITRAL model laws (such as the Model Law on Electronic Transferable Records), and other relevant international standards to ensure interoperability, legal certainty, and wide acceptance of digital trade practices at the global level.[5]

17.2. For third countries and regional registries to join and cooperate, a **Mutual Recognition Agreement (MRA)** must be concluded, ensuring interoperability and supervision. Such MRAs are international agreements between jurisdictions and cannot be substituted by private or bilateral commercial contracts. MRAs shall act as **bridging instruments**, similar to international transport conventions, to guarantee that EUTIR records obtain equivalent recognition across different legal regimes.

17.3. Recognition of EUTIR records outside the Union shall be subject to the applicable **national law** of the jurisdiction concerned, interpreted in light of relevant international conventions (such as CMR, Hague-Visby, or Montreal) and customary trade practice. Where no MRA exists, EUTIR records may serve as **evidence of authenticity**, but do not constitute binding legal validity unless explicitly recognised in the applicable jurisdiction.

[5] This approach follows established international practice, comparable to the way **INCOTERMS** become binding when incorporated into contracts, or how transport conventions such as **CMR** recognise documents as evidence unless explicitly granted binding legal effect by national law or international agreement.

17.4. Contractual clauses may provide that EUTIR records constitute binding proof of authenticity and validity for transactions between the contracting parties. Such contractual recognition simplifies cross-border processes, reduces disputes, and strengthens the evidentiary role of EUTIR in arbitration and litigation. **This contractual effect binds only the parties to such agreements and does not extend to public authorities (such as customs, police, or courts) unless recognised by law or international agreement.** This principle reflects established international practice, where private contracts may regulate rights and obligations between parties but cannot replace compliance with mandatory public law (e.g., customs or safety requirements).

17.5. The Union shall prioritise the negotiation and conclusion of **Mutual Recognition Agreements (MRAs)** with third countries and regional registries in areas such as transport documentation, customs data, financial information, and sustainability-related compliance. These MRAs shall ensure that EUTIR records obtain the same legal effect as equivalent paper-based documents, guarantee reciprocal supervision mechanisms, and provide a legally certain basis for seamless cross-border data exchange.

17.6. Regular reporting on international alignment shall be conducted by the Commission with Member States and international partners.

Illustrative Digital Trade Flow with eBL and EUTIR

1. Shipper issues eBL

– The shipowner/operator issues an **electronic Bill of Lading (eBL)** with a digital signature.
– An **eBL Metadata Record** is created in the EUTIR database, legal confirming its existence and validity.

2. Bank verifies and links eBL to financing

– The bank conducts due diligence: verifying the shipper, consignee, and the validity of the eBL to mitigate risks.
– Once conditions are met, the bank finances the cargo.
– The eBL Metadata Record added update in EUTIR, marking the eBL as pledged (collateral).

3. Consignee pays the bank

– The consignee pays the bank for the goods, either as a lump sum or according to a payment schedule.
– The bank acts as intermediary, ensuring the seller receives payment and the cargo is ready for release.

4. Bank releases the cargo

– After the payment has been made, the bank adds the removal of the pledge to the EUTIR eBL metadata record.
– The supplier/port operator checks in EUTIR that the pledge has been lifted.
– Based on this, the consignee receives the cargo at the port or terminal.

Figures 3. Illustrative images generated with AI.

Annex IV. EUTIR Common Technical Specifications (CTS)

DRAFT

This Annex presents a **draft version** of the Common Technical Specifications (CTS) for the European Union Trusted Issuance Registry (EUTIR). The objective of this draft is not to provide a final, legally binding standard, but rather to **illustrate how different pieces of EU legislation can be connected in a coherent technical framework**. The draft CTS demonstrates how **interoperability, security, and accountability** can be achieved across regulatory domains such as eFTI, DPP, CBAM, CSRD, and customs.

The draft CTS therefore serves as a **reference model** to guide further discussion and refinement. It highlights the points of convergence between multiple legislative acts, while leaving space for adjustment as the European Commission and Member States continue developing implementing acts.

1. Scope and Objectives

a) **Purpose:** Ensure interoperability, security, legal validity, liability certainty, and cross-border recognition of metadata submissions and verification within EUTIR.

b) **Applicability**: Binding for all Certified Service Providers (CSPs), Competent Authorities, Financial Institutions, and Economic Operators interacting with EUTIR.

2. Normative References

a) Regulation (EU) 2024/1183 (**eIDAS 2.0**)

b) Regulation (EU) 2016/679 (**GDPR**)

c) Regulation (EU) 2025/XXX (**AI Act**)

d) **ISO/IEC 27001** (Information Security)

e) **ISO 20022** (Financial Messaging Metadata)

f) **XBRL** (Extensible Business Reporting Language – ESEF, IFRS, ESRS, CBAM, PEPPOL-UBL taxonomies)

g) **JSON-LD / RDF / Ontologies** (for semantic data under DPP)

h) **WCO Data Model**

- Customs & Trade
- Previous / Supporting Document Reference

i) **UN/CEFACT Core Components Library (CCL)**

j) **ETSI EN 319 400-series** (Trust Services)

k) Regulation (EC) No 765/2008 (**Accreditation**)

3. Data Structures and Formats

a) **Metadata Schema**

Format: **JSON, XML Schema, XBRL, or JSON-LD/RDF** (machine-readable).

- **JSON/XML** preferred for operational metadata.
- **XBRL mandatory** for structured financial, tax, and sustainability reports (ESEF, CBAM, ESRS).
- **JSON-LD/RDF required** for semantic interoperability under **DPP**.

b) **Document Types and Profiles**

1. Predefined profiles for:
   - **eFTI** (Regulation (EU) 2020/1056)
   - **DPP** (ESPR Regulation (EU) 2024/1781)
   - **CBAM reports** (Regulation (EU) 2023/956)
   - **Customs declarations** (EU Customs Code reform)
   - **Financial guarantees**
   - **Insurance certificates**
   - **E-invoices and VAT reporting** (ViDA, PEPPOL-UBL/XBRL)
   - **Corporate ESG/CSRD reporting** (XBRL ESRS taxonomy)

c) **Financial and Regulatory Metadata Formats (ISO 20022 + XBRL + JSON-LD/RDF)**

1. **ISO 20022** defines financial messaging semantics (pacs, tsrv, camt).
2. **XBRL** ensures structured sustainability and supervisory reporting (ESEF, PEPPOL, CBAM, ESRS).
3. **JSON-LD / RDF** required for semantic interoperability of product and lifecycle data under **DPP**.

All financial submissions must reference both the **ISO 20022 message type** and the relevant **XBRL or RDF taxonomy**.

Example: a **guarantee record** = ISO 20022 tsrv.001 message + XBRL tags for supervisory reporting.

Example (DPP): a **product passport entry** = JSON-LD file linking to RDF ontology with sustainability attributes.

d) **Legal Entity Identification (LEI/vLEI)**

1. All actors interacting with EUTIR must be uniquely identified by a **Legal Entity Identifier (LEI)** issued under **ISO 17442**
2. **Certified Service Providers (CSPs)** must also be identified by **LEI**.
3. Where verifiable credentials are used, the **verifiable LEI (vLEI)** framework issued under the **GLEIF governance model** shall apply.
4. **vLEI credentials** allow binding of a **person's role** (e.g. CEO, customs representative, CSP officer) to the organisation's **LEI**, in compliance with **W3C Verifiable Credentials standards**.
5. **All audit log entries** must include **actor LEI or vLEI**, together with a **QSeal signature**, to ensure **legal accountability** and **evidentiary value**.
6. For **SMEs** lacking direct LEI registration, **proxy issuance of vLEI** by accredited CSPs may be permitted under Commission guidance.

4. Cryptographic Requirements

a) Hashing

- **Algorithm:** minimum **SHA-256**; higher algorithms (e.g. **SHA-3**) are permitted.
- **Input:** full content of the electronic document or dataset.
- **Output: Base64-encoded hash value**.

a) Digital Signatures and Seals

1. Each Metadata Record must include a qualified electronic signature (QES) or qualified electronic seal (QSeal) in accordance with **Regulation (EU) 2024/1183 (eIDAS 2.0)**. QES shall be used where a natural person

signs, while QSeal shall be used for legal entities and Certified Service Providers.

2. Digital seals and signatures ensure **authenticity, integrity, and non-repudiation** of Metadata Records throughout their lifecycle.
3. Implementations must follow relevant standards, including **X.509v3 with QSeal extension**, ETSI EN 319 102-1/2 (qualified signature profiles for XAdES, CAdES, PAdES), and **ISO 14533** (long-term validation and business process signatures).
4. The preservation and retention rules for Metadata Records and logs are defined in **Annex III, Article 5**, and apply equally to signed and sealed records.
5. All audit log entries must include actor LEI/vLEI, a timestamp, and the QSeal signature cryptographically bound to the Metadata Record ID.

5. APIs and Interfaces

a) **Submission API**: POST /eutir/submit, supports JSON/XML/XBRL.

b) **Verification API**:

1. **Public Layer**: GET /eutir/verify/{metadataRecordId}.
2. **Restricted Layer**: GET /eutir/verify/{metadataRecordId}/detail (requires authentication).

c) **Audit Log API**: restricted to **Competent Authorities** and **ESMA**, format **NDJSON**.

6. SME Financing Support

a) Verification API must allow **authorized Financial Institutions** to access structured **financial/ESG metadata (ISO 20022/XBRL)** for **credit risk assessment**.

b) This supports **SME financing** and **preferential risk treatment** under EU financial legislation.

7. DLT Integration (EBSI-based)

a) **Off-chain storage:** original documents stored by CSPs in compliance with **GDPR**.

b) **Interoperability:** EBSI DIDs, alignment with EBSI Trusted Issuance Registry.

c) **International Nodes:** allowed only via **Mutual Recognition Agreements (MRAs)**, reviewed every 3 years.

d) **Outside the Union**, metadata validity is interpreted in light of **local law and international conventions** (e.g. CMR, Hague-Visby, Montreal).

8. Security and Compliance

a) Compliance with **NIS2 Directive**.

b) **Encryption in transit:** TLS 1.3+

c) **Encryption at rest:** AES-256

d) **Immutable audit logs:** retained ≥84 months.

e) **Audit logs** must include **actor LEI/vLEI, action, timestamp, QSeal signature**.

f) **Monitoring:** real-time anomaly detection (ML-based).

g) **Data protection:** Privacy by Design, no personal data stored in EUTIR.

h) **AI/ML safeguards:** metadata usable for risk analysis only under **AI Act** & **GDPR**.

9. Conformity Assessment

a) CSPs undergo **annual audits** against CTS.

b) Certification bodies accredited under Regulation (EC) No 765/2008.

c) **Liability rules:**

- **CSPs**: technical correctness & trust services.
- **Competent Authorities**: restrictive actions (flag/lock/release/cancel).
- **Financial Institutions**: financial & AML/CFT metadata.
- **Economic Operators**: substantive trade/customs/product data.
- **Corrections:** if made by another actor, the original actor retains liability for the original submission; the correcting actor assumes liability only for the amended part.

10. Data Exchange Models and Transmission Methods

a) **Data Exchange Models.** Data exchange within EUTIR must support interoperability across recognised international and Union frameworks

1. **Single Window systems** (WTO TFA, EU Customs SW, ASEAN SW) for centralised submissions.
2. **Verifiable Credential model** (W3C, eIDAS 2.0, vLEI, DIDs) for decentralised B2B/B2G document proofs.

3. **KERI (Key Event Receipt Infrastructure)** for event-based validation of identity and document lineage.
4. **UN/CEFACT Core Components Library** and **WCO Data Model** as the baseline for trade, customs, and transport data exchange.
5. **ISO 20022**, **XBRL**, and **JSON-LD/RDF ontologies** for financial, tax, ESG, and product lifecycle data.

b) **Transmission Methods.** Transmission of Electronic Documents or Data Sets shall rely on secure communication channels aligned with Union legislation (eIDAS 2.0, NIS2, GDPR)

1. **NFC-based short-range communication** – recommended for physical border checkpoints (truck drivers, customs terminals).
2. **Wi-Fi / Bluetooth local communication** – applicable in controlled environments (ports, airports, warehouses).
3. **CEF eDelivery / AS4** – mandatory in maritime, customs, and financial supervisory reporting.
4. **Registered Electronic Delivery Services (REDS)** under Regulation (EU) 2024/1183 – mandatory where legal proof of sending/receiving is required.
5. **API-based secure transfer** (REST/GraphQL with TLS 1.3+) – allowed for B2B operational integration.

11. Service Quality and Availability

a) **Minimum uptime per node:** 99.9% annually.

b) **Network availability target:** 99.95% annually, ensured through multi-node redundancy across Member States and CSPs.

c) **Fallback continuity procedures:** mandatory for all nodes, including automatic rerouting of queries and submissions to other available nodes.

d) **Node redundancy and backup:** each Member State or CSP node functions as a **backup** for others. In case of downtime, maintenance, or **cyberattack** on one node, operations continue seamlessly via other nodes without loss of data integrity.

e) **Logs:** retained in original form for ≥84 months, accessible to Competent Authorities under audit and investigation right

12. Versioning and Maintenance

a) CTS reviewed every **24 months**.

b) Backward compatibility ensured for at least **36 months**.

c) Changes notified via **EU Official Journal**.

13. SME Proportionality

a) Tiered compliance thresholds.

b) SME training and financial support programmes.

c) Simplified reporting / phased roll-out allowed.

Annex V. Use Cases for Legislative Input and Technical Implementation

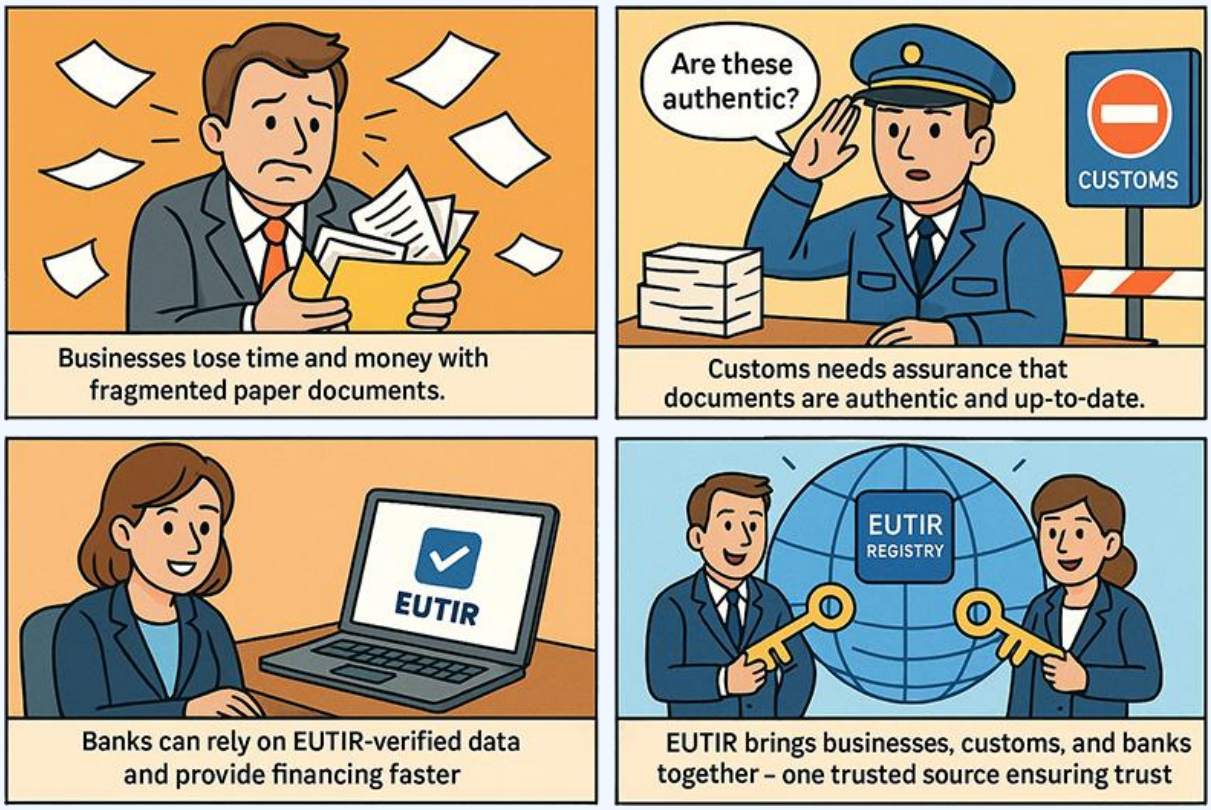


Figure 4. Illustration of how EUTIR ensures legal certainty, transparency, and efficiency for all trade actors. (Illustrative image generated with AI.)

This Annex provides harmonised, real-world use cases that demonstrate how the European Union Trade Index Registry (EUTIR) operates across sectors. The objective is twofold:

1. **Legislative input** – to show how the rules in **Annex II** (Accreditation and Certification) and **Annex III** (Submission, Status and Verification) apply in practice.
2. **Technical design guidance** – to give software architects end-to-end flows with version chains, linkages, access layers, and status transitions.

Use Case 1 – New Version (Hash Superseded)

Scenario. A company renegotiates a long-term supply contract to reflect updated delivery conditions and pricing. The original contract is still stored and auditable, but a newer version must take precedence to avoid confusion. The EUTIR ensures that the most recent version is

clearly identified as the only valid one, while still preserving the historic version for audit purposes.

Actors. CSP (Annex II).

Process.

1. CSP creates Contract v1 and applies **signature**.
2. Metadata submitted → Metadata Record 1 (*active*).
3. Contract v2 created and signed.
4. Metadata submitted → Metadata Record 2 (*active*, supersedes Metadata Record 1).
5. Verification shows Metadata Record 2 valid.

Sample Data.

1. {hash:"ABC123", status:"active", signature:"QES"}
2. {metadataRecordId:"R1", hash:"ABC123", status:"active", ts:"2025-08-12T10:05:00+02:00"}
3. {hash:"XYZ987"}
4. { metadataRecordId:"R2", hash:"XYZ987", supersedesMetadataRecordId:"R1", status:"active", ts:"2025-08-15T14:00:00+02:00"}
5. verify:{current_hash:"XYZ987", chain:["ABC123"→"XYZ987"], checked_at:"2025-08-15T14:05:00+02:00"}

Outcome. Metadata Record 2 valid; Metadata Record 1 superseded (new contract replaces old)

Benefits: Companies – clarity; Authorities – audit trail; Architects – versioning logic.

Use Case 2 – Continuing Validity (No Termination)

Scenario. A customs declaration is filed without an expiry date, as many declarations are valid until the goods reach their destination or are formally cancelled. Businesses and customs

authorities need to rely on its ongoing validity until an explicit change occurs. The EUTIR ensures that such records remain visible and legally binding until an official update is made.

Actors. CSP (Annex II).

Process.

1. CSP creates Declaration v1 and signs it.
2. Metadata submitted → Metadata Record 1 (*active*).
3. Verification shows status *active*.

Sample Data.

1. {hash:"DEC456", status:"active", signature:"QES"}
2. {metadataRecordId:"R1", hash:"DEC456", status:"active", ts:"2025-08-12T12:05:00+02:00"}
3. verify:{current_hash:"DEC456", status:"active", checked_at:"2025-08-13T09:00:00+02:00"}

Outcome. Metadata Record continues indefinitely (open-ended contract).

Benefits: Companies – stability; Authorities – certainty; Banks – enforceability.

Use Case 3 – Termination of Record

Scenario. A logistics company enters into a transport agreement that later becomes unnecessary when the shipment is cancelled. Authorities must ensure that the terminated record cannot be reused for fraud or misrepresentation. The EUTIR provides a transparent termination entry, preserving the history but clearly marking the record as no longer valid.

Actors. CSP, Competent Authority.

Process.

1. CSP creates Contract v1 and signs it.
2. Authority issues termination order.
3. Termination submitted → Metadata Record 2 (*terminated*).

Sample Data.

1. {hash:"LOG123", status:"active", signature:"QES"}
2. {order:"terminate", authority:"EE-Customs"}
3. {metadataRecordId:"R2", hash:"LOG123", status:"terminated", ts:"2025-08-15T15:00:00+02:00"}

Outcome. Contract ended (cancellation).

Benefits: Companies – obligations end; Authorities – certainty; Banks – avoid invalid reliance.

Use Case 4 – Chain of Custody for Goods

Scenario. Manufactured goods often pass through several hands – manufacturer, carrier, warehouse – before reaching the customer. Each handover must be provable, ensuring no tampering or substitution of goods has occurred. The EUTIR allows every custody event to be registered, creating a verifiable and immutable chain of responsibility.

Actors. Manufacturer CSP, Carrier CSP, Warehouse CSP, Customs.

Process.

1. Manufacturer submits Shipment M1.
2. Carrier submits Handover T1 (parent=M1).
3. Warehouse submits Receipt W1 (parent=T1).
4. Customs flags W1.

Sample Data.

1. {metadataRecordId:"M1", hash:"SHIP001", status:"active", ts:"2025-08-12T08:00:00+02:00"}
2. {metadataRecordId:"T1", hash:"SHIP002", parentMetadataRecordId:"SHIP001", status:"active", ts:"2025-08-12T12:00:00+02:00"}
3. {metadataRecordId:"W1", hash:"SHIP003", parentMetadataRecordId:"SHIP002", status:"active", ts:"2025-08-12T18:00:00+02:00"}
4. {action:"flag", target:"SHIP003", authority:"EE-Customs"}

Outcome. Custody chain traceable (obligation transfer).

Benefits: Logistics – proof; Authorities – integrity; Banks – assurance.

Use Case 5 – Financial Amendment (Guarantee on eBL)

Scenario. A bank issues a financial guarantee based on an electronic bill of lading (eBL) that secures the payment obligations of a buyer. Later, the buyer requests a higher credit line and the bank adjusts the guarantee amount. The EUTIR ensures all versions of the guarantee are visible, so that the final financing terms are always enforceable.

Actors. Logistics CSP, Bank CSP.

Process.

1. Logistics CSP submits eBL.
2. Bank submits Guarantee FIN1 (parent=eBL).
3. Bank amends → FIN2 (parent=FIN1).

Sample Data.

1. {metadataRecordId:"E1", hash:"EBL001", status:"active", ts:"2025-08-12T07:30:00+02:00"}
2. {metadataRecordId:"FIN1", hash:"FIN001", parentMetadataRecordId:"E1", amount:"€100000", status:"active", ts:"2025-08-12T09:00:00+02:00"}
3. {metadataRecordId:"FIN2", hash:"FIN002", parentMetadataRecordId:"FIN1", amount:"€120000", status:"active", ts:"2025-08-14T11:15:00+02:00"}

Outcome. Financing traceable.

Benefits: Banks – visibility; Companies – secure; Authorities – fraud reduced.

Use Case 6 – Flagging and Locking by Authorities

Scenario. Customs authorities often encounter declarations with anomalies or risk factors. To prevent fraud, they must temporarily freeze such records while an investigation is underway. The EUTIR supports this by allowing flagging and locking, preventing any further actions until the authority resolves the case.

Actors. CSP, Competent Authority.

Process.

1. CSP submits declaration D1.
2. Authority flags D1.
3. Authority locks D1.
4. Authority releases or terminates.

Sample Data.

1. {metadataRecordId:"D1", hash:"SHIPX", status:"active", ts:"2025-08-12T09:10:00+02:00"}
2. {action:"flag", target:"SHIPX"}
3. {action:"lock", target:"SHIPX"}
4. {action:"release", target:"SHIPX"}

Outcome. Record frozen, then resolved (suspension)

Benefits: Authorities – control; Companies – clarity; Banks – protection.

Use Case 7 – Public Verification (Two-Layer Model)

Scenario. Importers often need only to confirm that a record exists and is authentic, while banks require full legal and status details. A two-layer verification model balances transparency with privacy by allowing different levels of access. The EUTIR logs all queries, ensuring accountability.

Actors. Importer, Bank.

Process.

1. Importer queries public layer.
2. Bank queries restricted layer.
3. Both queries logged.

Sample Data.

1. public_verify:{hash:"SHIPY", exists:true, checked_at:"2025-08-13T15:00:00+02:00"}
2. restricted_verify:{hash:"SHIPY", status:"terminated – delivered", checked_at:"2025-08-13T15:05:00+02:00"}
3. audit_log:{caller:"BANK-LEI-777", ts:"2025-08-13T15:06:00+02:00"}

Outcome. Two-tier access (public vs private clauses).

Benefits: Importers – confirmation; Banks – detail; Authorities – privacy.

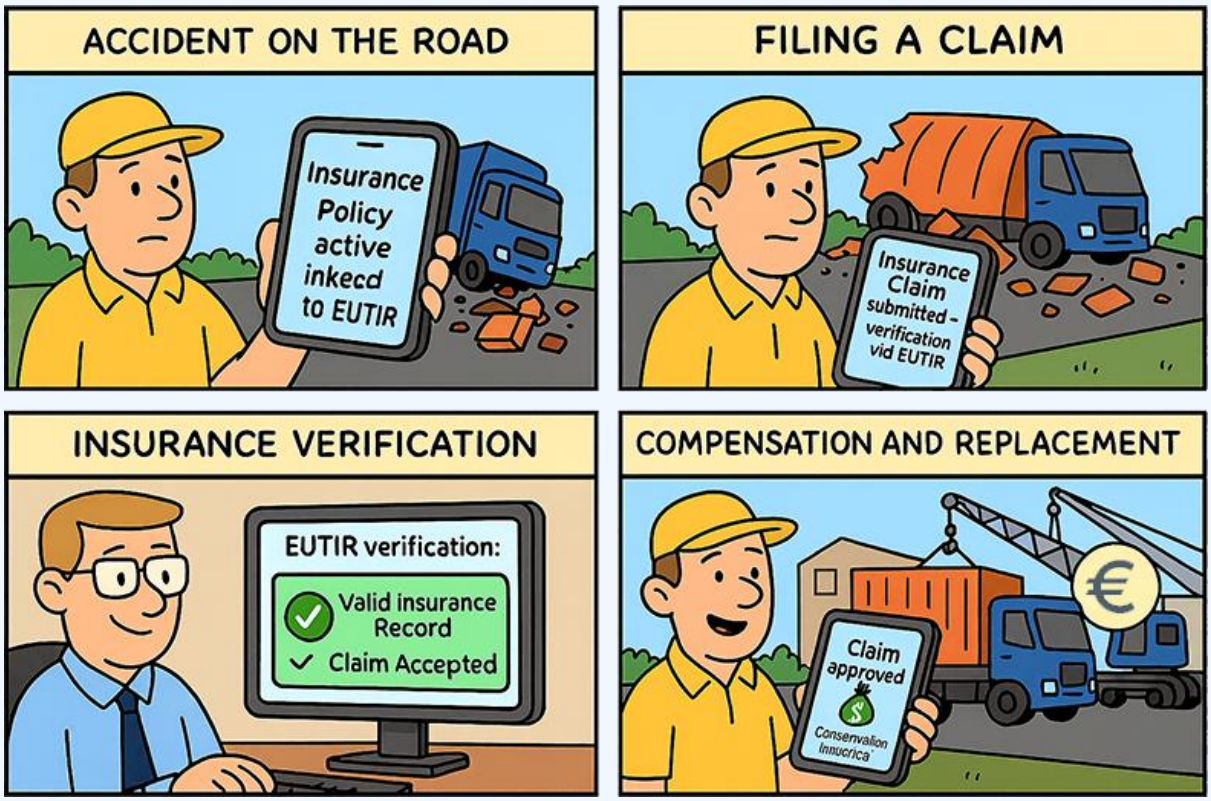


Figure 5. Electronic cargo documents and the related electronic cargo insurance certificate verified via EUTIR. (Illustrative image generated with AI.)

Use Case 8 – Insurance Linkage

Scenario. A shipment is insured against risks such as loss or damage. Later, the insured company decides to extend the coverage amount. The EUTIR links the insurance record to the shipment, ensuring that the relationship and updates are visible to both authorities and financial institutions.

Actors. Logistics CSP, Insurer CSP.

Process.

1. Logistics CSP submits Shipment S1.
2. Insurer submits Policy INS1 (parent=S1).
3. Insurer extends Policy INS2 (parent=INS1).

Sample Data.

1. {metadataRecordId:"S1", hash:"SHIP001", status:"active", ts:"2025-08-12T08:00:00+02:00"}
2. {metadataRecordId:"INS1", hash:"INS001", parentMetadataRecordId:"SHIP001", coverage:"€200000", status:"active", ts:"2025-08-12T09:15:00+02:00"}
3. {metadataRecordId:"INS2", hash:"INS002", parentMetadataRecordId:"INS1", coverage:"€300000", status:"active", ts:"2025-08-14T10:30:00+02:00"}

Outcome. Insurance traceable.

Benefits: Insurers – linkage; Companies – certainty; Authorities – fewer disputes.

Use Case 9 – AML Suspicion and Investigation

Scenario. Banks are obliged to monitor transactions and guarantees for signs of money laundering. When suspicious patterns appear, a Financial Intelligence Unit (FIU) must be involved. The EUTIR allows banks to flag, and FIUs to lock, ensuring immediate containment of risky records.

Actors. Bank CSP, FIU.

Process.

1. Bank submits Guarantee G1.
2. Bank flags record.
3. FIU locks record.
4. FIU resolves case.

Sample Data.

1. {metadataRecordId:"G1", hash:"FINAML001", status:"active", ts:"2025-08-12T11:00:00+02:00"}
2. {action:"flag", target:"FINAML001"}
3. {action:"lock", target:"FINAML001", authority:"EE-FIU"}
4. {action:"resolve", target:"FINAML001", outcome:"cleared", ts:"2025-08-16T11:20:00+02:00"}

Outcome. Risk contained (suspension due to suspicion).

Benefits: Banks – early warning; Authorities – control; Companies – reputational safety.

Figure 6. Illustrative process flow for submission of truck digital documents: Digital Business Wallet → data upload at the border sensor via NFC technology → electronic documents verified through the EUTIR system → automated control performed by the customs system → the driver proceeds without direct interaction with customs officers. (Illustrative image generated with AI.)

Use Case 10 – Supplementary Record (Declaration + Consignment Note)

Scenario. A trucking company uploads a consignment note (e.g. CMR for international movements) for a shipment, and later the exporter attaches a customs declaration to the same record. This ensures that all documentation is linked in one place, providing transparency for cross-border checks. Authorities and financial institutions can easily verify both the base transport record and the supplementary customs declaration.

Actors. Trucking CSP, Exporter CSP.

Process.

1. Trucking CSP submits CMR1.
2. Exporter submits Declaration DEC1 linked to CMR1.

Sample Data.

1. {metadataRecordId:"CMR1", hash:"CMR123", status:"active", ts:"2025-09-02T08:00:00+02:00"}
2. {metadataRecordId:"DEC1", hash:"DEC456", parentMetadataRecordId:"CMR123", status:"active", ts:"2025-09-02T08:30:00+02:00"}

Outcome. Both valid (annex to contract)

Benefits: Exporters – extend docs; Authorities – oversight; Banks – certainty.

Use Case 11 – Digital Product Passport (DPP) Submission

Scenario. A manufacturer of electronic appliances must issue a **Digital Product Passport (DPP)** to comply with ESPR Regulation (EU) 2024/1781. The passport contains sustainability, reparability, and recycling information. The EUTIR ensures that the passport is submitted in a **semantically interoperable format (JSON-LD/RDF)** and remains valid for the product lifecycle (up to 15 years), while still enabling auditability and version control.

Actors. Manufacturer CSP, Competent Authority (CA), Financial Institution (FI).

Process.

1. Manufacturer generates a DPP in **JSON-LD** format, referencing RDF ontology and sustainability data.
2. CSP applies **QSeal**, computes **cryptographicHash**, and assigns **metadataRecordId**.
3. Metadata submitted → metadata Record 1 (active, expiryDate = 2038-12-31).
4. CA verifies the digitalSeal, LEI/vLEI, and ontology compliance.
5. FI queries restricted API to check product sustainability classification.

Sample Data.

1. {hash:"DPP123", productId:"GTIN:4006381333931", status:"active", signature:"QSeal"}

2. {metadataRecordId:"R1001", hash:"DPP123", status:"active", ts:"2025-09-10T09:30:00Z", expiry:"2038-12-31"}
3. {actorLei:"5493001KJTIIGC8Y1R12", actorVlei:"vc-12345", cspId:"529900T8BM49AURSDO55"}
4. {ESGmetadata:"XBRL-ESRS:E1-1", ontology:"RDF:repairabilityIndex"}
5. verify:{current_hash:"DPP123", valid:true, chain:["R1001"], checked_at:"2025-09-10T09:35:00Z"}

Outcome. DPP record accepted and preserved; expiry aligned with product lifecycle.

Benefits. Manufacturers – compliance with ESPR; Authorities – ontology validation; Financial Institutions – ESG-linked financing; Consumers – trusted repair/recycling data.

Figure 7 & 8. LEI and vLEI verification reduces confusion with similarly named companies, eliminates the use of "shell firms" or bankrupt entities, and provides a solid basis to ensure that the trading partner is real and legally registered. By combining company identification (LEI) with representative authorization (vLEI), customs and public authorities can achieve faster, safer, and more trustworthy clearance processes. (Illustrative image generated with AI.)

Use Case 12 – CBAM Report Submission

Scenario. An EU importer submits a **CBAM report** under Regulation (EU) 2023/956, detailing embedded CO_2 emissions in imported steel. The report is structured in **XBRL CBAM taxonomy** and verified by an accredited body. The EUTIR ensures authenticity, traceability to the verifier, and long-term retention (84 months).

Actors. Importer CSP (Verifier), Competent Authority (CA), European Commission (EC).

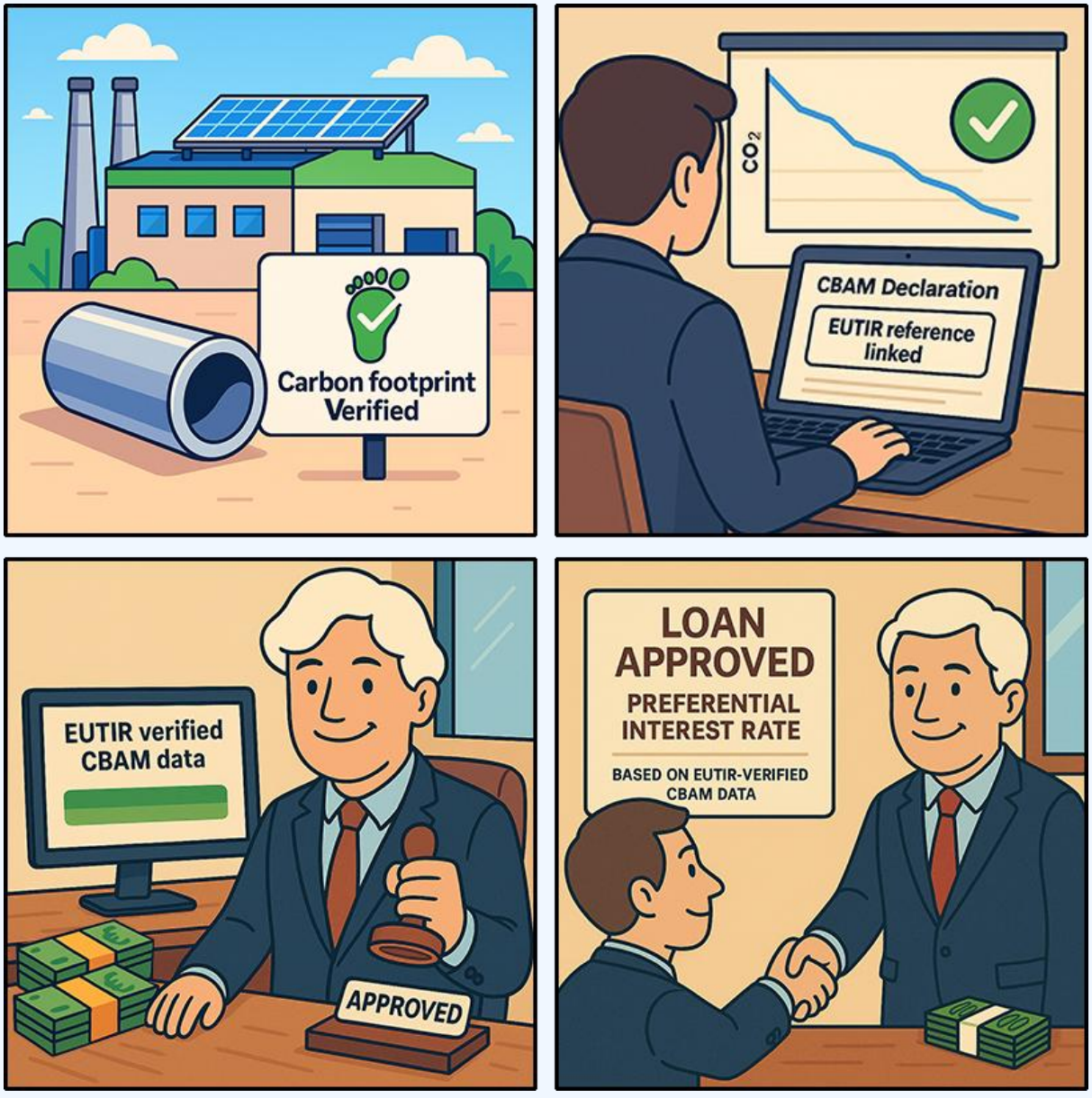


Figure 9. Illustrative process flow: low-carbon products certified through EUTIR-verified CBAM data enable financial institutions to assess sustainability performance and grant preferential financing with lower interest rates, in line with the EU Framework for Financial Data Access (FiDA). (Illustrative image generated with AI.)

Process.

1. Importer prepares CBAM report in XBRL format.
2. Verifier validates emissions data and provides certificate.
3. CSP applies **QSeal**, computes **cryptographicHash**, and assigns **metadataRecordId**.
4. Metadata submitted → metadata Record 2001 (active).
5. CA retrieves record and verifies verifier linkage (liabilityReference).
6. EC consolidates reports via restricted API.

Sample Data.

1. {hash:"CBAM789", status:"active", signature:"QSeal"}
2. {metadataRecordId:"R2001", hash:"CBAM789", actorLei:"529900T8BM49AURSDO55", ts:"2025-07-15T16:00:00Z"}
3. {liabilityReference:"VerifierID:V-2025-11", ESGmetadata:"XBRL-CBAM:CO2e"}
4. verify:{current_hash:"CBAM789", valid:true, checked_at:"2025-07-15T16:05:00Z"}
5. reportStatus:{submitted:true, expiry:"2032-07-15"}

Outcome. CBAM report accepted; linked to accredited verifier; preserved for audit for 84 months.

Benefits. Importers – simplified compliance; Authorities – traceable verification; Commission – EU-wide consolidation; Auditors – long-term audit trail.

Use Case 13 – Customs Declarations & Supporting Documents

Scenario. An economic operator submits a customs declaration together with supporting documents (invoice, packing list, certificates). The declaration (parent record) is later amended and superseded. Authorities must ensure that supporting records linked to the old declaration lose their legal validity once the parent is superseded, while still remaining preserved and auditable.

Actors. Economic Operator, CSP, Customs Authority (Competent Authority).

Process.

1. EO submits Customs Declaration v1 → Metadata Record P1 (status: active).
2. EO/CSP submit supporting docs (invoice, packing list, origin certificate) → Metadata Records C1, C2, C3 with parentMetadataRecordId:P1 and validityInheritance:dependent.
3. EO submits amended Declaration v2 → Metadata Record P2 with supersedesMetadataRecordId:P1.
4. P1 becomes superseded. C1–C3 remain preserved but lose legal validity as of supersede date. New supporting docs may be linked to P2.

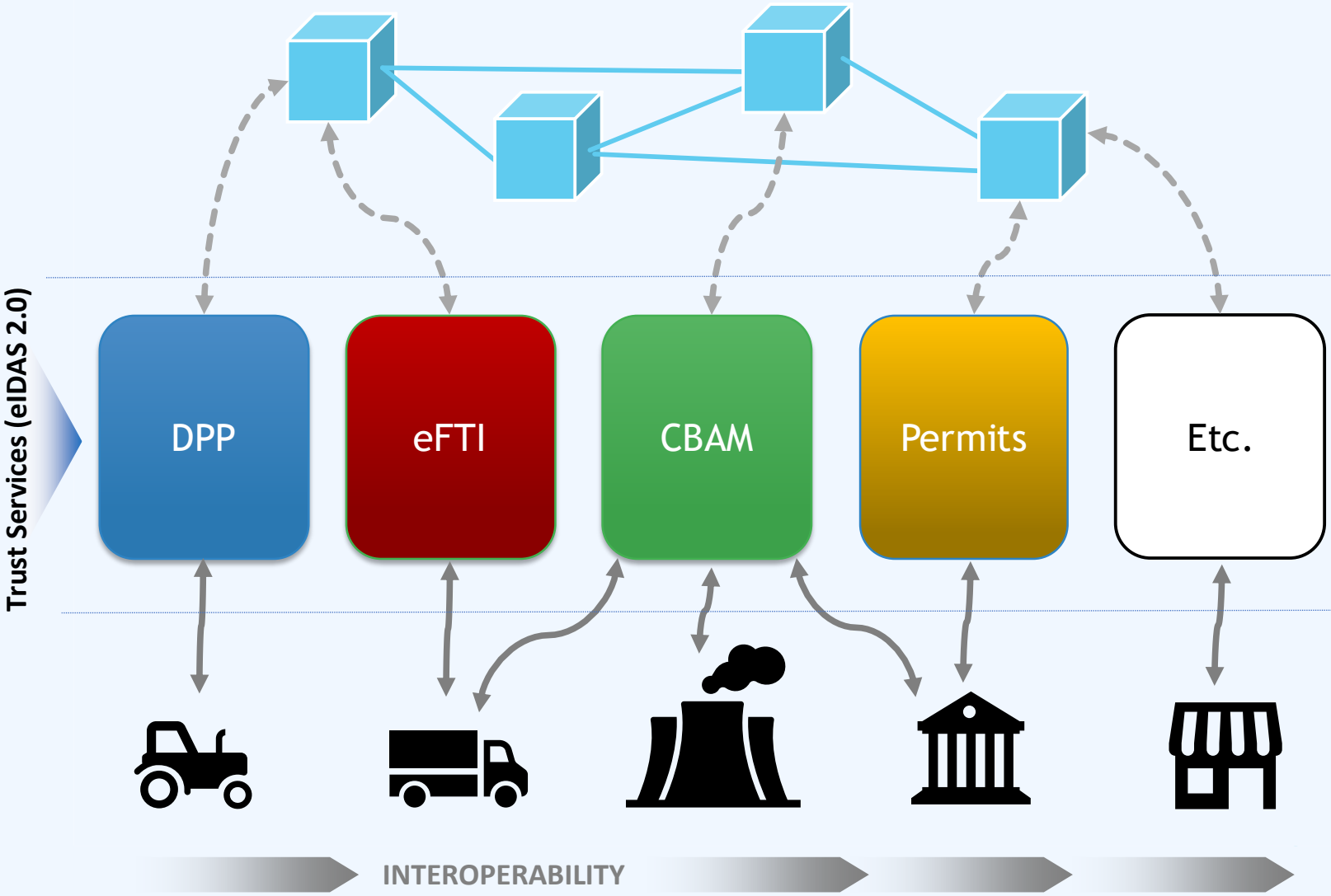
Sample Data.

1. {metadataRecordId:"P1", type:"CustomsDeclaration", status:"active"}
2. {metadataRecordId:"C1", parentMetadataRecordId:"P1", type:"Invoice", validityInheritance:"dependent", status:"active"}
3. {metadataRecordId:"P2", type:"CustomsDeclaration", supersedesMetadataRecordId:"P1", status:"active"}
4. {metadataRecordId:"P1", status:"superseded"}
5. {metadataRecordId:"C1", parentMetadataRecordId:"P1", status:"active", legalValidity:"invalid"}

Outcome. Declaration v2 replaces v1; supporting records tied to v1 lose legal effect but remain preserved for audit. New declaration has its own valid children.

Benefits. EO – clear audit trail, reduced risk of double filing; Authorities – legal certainty, prevention of fraud; Banks – clarity which documents remain valid for trade finance.

Annex VI. EUTIR Technical Infrastructure



Layer 3 – EUTIR Trust Layer

- Based on EBSI (European Block-chain Services Infrastructure)
- Ensures authenticity, integrity, traceability
- Provides audit trail, certification, metadata registry
- Oversight: EU institutions (e.g. ESMA, Commission)

Layer 2 – Accredited Service Providers

- Customs brokers, banks, platforms, auditors
- Provide validation, transmission, and storage services
- Operate under accreditation & certification rules

Layer 1 – Economic Operators

- Companies (SMEs, corporates)
- Importers, exporters, manufacturers, distributors, retailers
- Generate, use and exchange electronic trade documents

Figure 10. The diagram was prepared by Riho Vedler on behalf of the DigitalTrade4.EU consortium.

Annex VII. Platform Functions and Trust Roles in the EU Digital Trade Ecosystem

#	Platform	Core Function	Key Actors	Interoperability Role	Trust Features
1	**eFTI Platform**	Structures and exchanges electronic freight transport information in accordance with EU regulation. Supports Digital Business Wallet submissions to third parties (e.g., warehouses) without granting direct platform access.	Logistics providers, freight forwarders, customs brokers, software vendors, cargo owners	Connected to ICS2, Customs SW, DPP; can interact with TDR for version verification before release to third parties.	Signing-enabled, eIDAS/vLEI, traceable submission logs, TDR-assisted latest-version checks
2	**DPP Platform**	Digitally represents product lifecycle data, ESG/CE compliance, and traceability information.	Manufacturers, importers/exporters, ESG auditors, platform providers	Linked to eFTI, permit registries, eInvoicing, CBAM Registries, customs declarations; interoperable via linked identifiers.	Verifiable ESG/CE data, linked traceability to other platforms
3	**EU Customs Single Window**	Single EU-wide gateway for customs and regulatory documentation (incl. permits).	National customs authorities, inspection agencies	Receives data from eFTI, DPP, ICS2, CBAM Registries and directly from importers; pushes to national systems.	Integrated with risk analysis
4	**ICS2**	Performs pre-arrival cargo risk assessments using Entry Summary Declarations (ENS).	EU customs administrations, transport carriers, EU security agencies	Pulls eFTI/DPP/ permit info	Real-time validation
5	**Permit Registries**	Hosts and validates official permits and certificates (e.g., veterinary, phytosanitary, chemical). Real-Time Verification API checks legal validity, current status, and conditions — even when TDR provides technical authenticity verification.	National competent authorities (e.g., TRACES, ECHA), EU agencies	Linked from DPP & eFTI; accessible to TDR for live status lookups.	Real-time legal verifiability, amendment and revocation logs
6	**EU Trade Indexes Registry (EUTIR)**	Anchors and registers metadata (e.g., hashes, signatures, timestamps) of trade documents (e.g., eFTI, eBL, invoices), enabling full document traceability across platforms. Tracks document origin, versioning, Certified Provider ID (LEI/vLEI), and custody history without exposing content.	Registry operators (EU or delegated), customs, logistics integrators, financial institutions	Reference point for document verification and linking across eFTI, DPP, CBAM, and Customs SW.	Tamper-proof identifiers, issuer verification, Certified Provider registry, MLETR compliance, traceable audit trails with DocumentCustodyHistory
7	**CBAM Registries**	Record and manage embedded carbon emissions data for imported goods under the EU Carbon Border Adjustment Mechanism.	Importers, customs authorities, national CBAM authorities, accredited CO_2 verifiers, ESG auditors	Linked with DPP for product-level emission data, Customs SW for compliance validation, trade finance systems for tariff adjustments.	Verified emission declarations, EU-accredited verifier network, secure transmission to customs
–	**Business Wallet**	Decentralised environment for securely holding and sharing credentials and electronic documents under user control.	Traders, SMEs, logistics operators, authorised representatives, identity providers	Interacts with all above	vLEI identity, eIDAS 2.0

Annex VIII. Digital Trade & Capital Markets Integration Roadmap

#	activity	objective	indicative metrics	tools/enablers
1	**Establish European Trade Indexes Registry (EUTIR)**	Decentralize and secure cross-border trade/ESG data for supervision using a distributed architecture, enabling trusted and interoperable access to regulatory and ESG information across the EU.	- 30% reduction in duplicate filings by 2027 - 100% fraud detection rate	Zero Trust Architecture & cross-border verification (e.g., blockchain-based systems like EBSI), MLETR-compliant systems, PSD3-PSR/FiDA APIs, vLEI
2	**Digitalise Tax & Customs Interfaces**	Integrate trade, tax, and customs data flows to reduce friction and fraud	- 50% faster customs clearance (full cycle) - 30% reduction in VAT fraud (detected cases) - Full EU Single Window uptake by 2028 (MS + procedures)	EU Customs Data Hub, Single Window for Customs, VAT in the Digital Age (ViDA), vLEI for trader authentication, eFTI/eCMR linkages
3	**Adopt MLETR + eIDAS 2.0**	Enable seamless digital negotiable instruments and cross-border recognition	- 70% faster transaction times - 95% SME adoption of e-signatures	MLETR framework, eIDAS 2.0 digital identity wallets, EU legal harmonization tools
4	**Develop RegTech supervision tools**	Enhance real-time oversight of capital markets and ESG compliance	- 50% reduction in supervisory costs - 80% automated ESG data collection	AI/ML dashboards, Legal Sandboxes, ETDR-linked reporting systems
5	**Digital Bonds & Convertibles**	Enable automated, ESG-linked debt instruments	- 30% reduction in issuance costs - 20% lower interest rates for ESG-compliant bonds - 100% real-time conversion execution	ETDR registry, smart contracts, DPP/ESG data integration, eIDAS 2.0 authentication
6	**SME-friendly compliance frameworks**	Ensure SMEs benefit from digital reforms without disproportionate burden	- 40% increase in SME participation - 60% cost savings for SMEs	Tiered compliance thresholds, Green-Digital Trade Academy, Erasmus+ grants
7	**Pilot CBAM-DPP Corridors**	Link trade finance to verifiable ESG metrics for tariff incentives	- 20% CBAM compliance cost reduction - 50% adoption of DPPs by 2030	Digital Product Passports (DPPs), IoT carbon trackers, CBAM rebate schemes, CBAM certificate registry integration, EU Customs Single Window
8	**Harmonize e-document laws**	Eliminate legal fragmentation for digital trade documents	- 90% mutual recognition of e-Bills of Lading - 0 paper-based processes	EU Transport Law updates (e.g. eFTI, eCMR), UN/UNECE protocols, Legal Harmonization Sandboxes
9	**ESG-linked finance incentives**	Reward sustainable supply chains with cheaper capital	- €10B/year green trade finance unlocked - 30% lower Scope 3 emissions	InvestEU guarantees, FinTech platforms, CSRD-aligned reporting templates

About Us

The **DigitalTrade4.EU consortium** envisions a **seamlessly interconnected Europe** and **neighbouring regions** powered by harmonized standards for the digitalisation of trade documents and processes. By fostering the digital transformation of trade, we aim to promote economic integration, enhance cooperation, and ensure long-term trade facilitation across borders.

Our consortium is made up of **experts in their field**, including **108 full partners**—trade associations, logistics providers, shipping lines, banks and insurances, technology innovators, etc.—**from 17 European Union countries** (*France, Belgium, Netherlands, Austria, Estonia, Finland, Italy, Latvia, Spain, Germany, Sweden, Poland, Luxembourg, Lithuania, Slovenia, Denmark, Bulgaria*) and **22 non-EU countries** (*United Kingdom, Switzerland, Montenegro, Japan, Singapore, Hong Kong, Australia, New Zealand, India, Nepal, Canada, United States of America, Cameroon, Morocco, Egypt, Kenya, Pakistan, Nigeria, Brazil, Uzbekistan, Turkey, Ukraine*).

Our consortium is already **aligned with the fundamentals** of the **EU Competitiveness Compass**. Learn more:

- How DigitalTrade4.EU Can Help Achieve the Objectives of the EU Competitiveness Compass (February 2025) https://www.digitaltrade4.eu/how-digitaltrade4-eu-can-help-achieve-the-objectives-of-the-eu-competitiveness-compass/

Web page: www.digitaltrade4.eu

EU Transparency Register: 355266197389-94

Contact person: Riho Vedler

Email: riho.vedler@ramena.ee