Prepared by DigitalTrade4.EU

Linking the EU New Legislative Framework (NLF) Revision with Peer Review of National Cybersecurity Certification

Feedback to the EU Commission

August 2025

Cover Letter

The DigitalTrade4.EU consortium is pleased to submit the attached package, which was originally prepared as feedback to the European Commission's ongoing revision of the **New Legislative Framework (NLF)**. While the main focus of this document lies in the NLF context, we believe that its findings and recommendations are of **direct relevance to the work on peer review of National Cybersecurity Certification Authorities (NCCAs)** under the draft Implementing Regulation.

Our motivation to share this document with the NCCA Working Group is threefold:

1. **Horizontal Integration** – The proposed **European Union Trade Indexes Registry (EUTIR)** is designed as a digital trust anchor across compliance and certification data. The same principles of immutability, interoperability, and liability allocation can strengthen the peer review methodology foreseen in the Cybersecurity Act.
2. **Cross-Pillar Consistency** – The European Commission has emphasised the need for consistency between product legislation, cybersecurity certification, and digital trust services under **eIDAS 2.0 (Regulation (EU) 2024/1183)**. Aligning NCCA peer review processes with EUTIR's trust and verification model would deliver a structured, machine-readable, and interoperable approach.
3. **Strategic Added Value** – Both the NLF revision and the NCCA peer review framework pursue similar objectives: **transparency, proportionality for SMEs, integration of sustainability, and mutual recognition across borders**. By linking the two processes, duplication can be reduced, innovation encouraged, and the EU's global leadership in digital trust frameworks strengthened.

For this reason, we are sharing our NLF input with the NCCA Working Group in the form of a consolidated package, which includes:

- A cross-mapping table between NCCA peer review and the EUTIR framework,
- Suggested changes to the draft Implementing Regulation, and
- The full NLF feedback document of DigitalTrade4.EU (August 2025).

We look forward to further cooperation with the Working Group and stand ready to discuss possible **synergies between the NLF reforms and the implementation of the Cybersecurity Act**.

Riho Vedler

DigitalTrade4.EU Consortium

NCCA Peer Reviews vs. EUTIR Framework

	Dimension	NCCA Peer Reviews	EUTIR (NLF Feedback Proposal)	Synergy / Added Value
1	**Governance & Oversight**	Commission organises peer reviews every 5 years; review teams formed from Member State experts (Art. 2–3).	Hybrid model: decentralised nodes (EBSI/DLT) + central supervision (ESMA, DGs, accreditation bodies).	Peer review governance could benefit from EUTIR's hybrid model to ensure transparency, independence, and balance of authority.
2	**Transparency & Reporting**	Summary reports published; details of methodology not always disclosed (Art. 5).	Immutable and auditable lifecycle of records, with structured metadata, machine-readable summaries, and public verification services.	Peer review reports could adopt EUTIR-style metadata publication (hashes, statuses), ensuring wider transparency and verifiability.
3	**Conflict of Interest & Integrity**	General obligation to avoid conflicts of interest (Art. 3).	Explicit liability allocation and role-based rights (CSPs, Competent Authorities, Financial Institutions).	EUTIR's liability clarity model can enhance NCCA integrity rules with enforceable declarations and traceability of decisions.
4	**Data Management & Security**	Confidential documents handled securely; no specific digital trust requirement (Art. 6).	Reliance on **qualified trust services under eIDAS 2.0** (signatures, seals, timestamps, logs).	NCCA peer reviews could align with eIDAS 2.0 trust layer, increasing authenticity, secure exchange, and cross-border recognition.
5	**Methodology / Assessment Criteria**	Annex II: covers separation of certification & supervision, monitoring, enforcement of obligations, conformity assessment body oversight.	Annex II & III: structured submission rules, immutable records, role-based functional rights, audit logs.	EUTIR lifecycle model provides a more granular and tamper-proof system for documenting peer review findings and follow-up.

6	**SME & Proportionality**	Annex II: focus on procedures, but no SME-specific provisions.	Strong emphasis on SME support, tiered compliance thresholds, and simplified reporting.	Integration would reduce compliance burden on SMEs while keeping peer review rigorous but proportionate.
7	**Sustainability / ESG Integration**	No explicit mention of ESG or circular economy data in peer review scope.	Integrates ESG, CBAM, DPP, sustainability datasets into traceable records.	Peer review could expand scope to verify whether NCCAs consider ESG-linked compliance obligations, supporting Green Deal objectives.
8	**International Dimension**	Limited to EU/EEA NCCAs peer-reviewed on fixed cycles (Annex I).	Includes **Mutual Recognition Agreements (MRAs)** with third countries for global interoperability.	EUTIR's MRA model could inspire NCCA reviews to include benchmarking with third-country certification bodies, strengthening EU leadership.
9	**Digital Interoperability**	No requirement for machine-readable or interoperable reporting formats.	Built as a metadata-based interoperability layer, linked with DPP, eFTI, CBAM, Customs Data Hub.	Peer review results could be published in EUTIR-compatible format, allowing reuse by authorities, auditors, and market actors.
10	**Legal Certainty & Liability**	Reports provide recommendations; no binding legal liability allocation.	Explicit rules on liability by role (CSP, authority, financial institution, operator).	Adding liability allocation principles from EUTIR would make peer review outputs more enforceable and credible.

Amendment Proposals to the Draft Implementing Regulation on NCCA Peer Reviews

1. Transparency of Peer Review Reports

Proposed Legal Text, Article 5(3)**:**

> *The summary report to be made public shall include, in addition to the general findings, a non-confidential overview of methodologies, identified best practices, and recommendations relevant for other NCCAs and stakeholders, ensuring consistency and transparency across the Union.*

Justification: The current text foresees only the publication of a "summary" without clarity on what this entails. Without further details, there is a risk that reports may become overly generic and fail to deliver real value to other authorities or stakeholders. A requirement to include methodologies and best practices strengthens transparency and enables mutual learning across the Union. It also helps SMEs and conformity assessment bodies to better understand expectations, thereby lowering compliance costs and raising trust in the peer review process.

2. Digital Interoperability of Peer Review Documentation

Proposed Legal Text, Article 4(2) + Annex II, Section II.1**:**

> *All documentation, including self-assessment questionnaires, supporting documents, and peer review reports, shall be made available in a structured, machine-readable format, interoperable with Union-wide registries such as the Digital Product Passport (Regulation (EU) 2024/1781), the electronic Freight Transport Information system (Regulation (EU) 2020/1056), and the European Union Trade Indexes Registry (EUTIR).*

Justification: The draft only refers to "documents", which risks fragmentation if Member States use different formats. By requiring structured, machine-readable data, the Commission ensures that peer review results are reusable across EU digital infrastructures. This approach reduces administrative duplication and allows automated analysis, improving both efficiency and traceability. Interoperability with existing EU registries also ensures that cybersecurity peer reviews are not isolated but integrated into the EU's wider digital trust and compliance ecosystem.

3. Clearer Conflict of Interest Rules

Proposed Legal Text, Article 3(3)**:**

> *Members of the review team shall provide a signed declaration of impartiality and absence of conflicts of interest, including disclosure of any prior consultancy, certification, or supervisory activity within the peer-reviewed authority during the last five years.*

Justification: The current text requires "avoidance of conflicts of interest" but leaves too much discretion to interpretation. Without a concrete obligation, trust in the impartiality of reviews may be undermined. A mandatory declaration provides legal certainty and aligns with international conformity assessment standards (ISO/IEC 17040). Furthermore, introducing a five-year lookback ensures sufficient independence, helping avoid both perceived and actual conflicts that could discredit the review process.

4. Rotational Diversity in Review Teams

Proposed Legal Text, Article 2(2) + Annex I**:**

> *The Commission shall ensure that review teams include experts from at least three different peer review cycles, avoiding concentration of roles among the same Member States. Diversity in expertise shall include cybersecurity certification, conformity assessment, market surveillance, and digital trade compliance.*

Justification: While the draft includes a rotation principle, it does not prevent over-representation by certain Member States. This creates a risk that the peer review process will be dominated by a few actors, reducing objectivity and balance. By requiring diversity both in geographical and professional background, the Commission strengthens legitimacy and resilience of the system. The explicit inclusion of digital trade compliance experts also ensures alignment with broader EU policy objectives, including the integration of Digital Product Passports, CBAM, and electronic freight systems.

5. Link to Union Digital Trust Services (eIDAS 2.0)

Proposed Legal Text. Article 6(1), (Confidentiality & data handling)**:**

> *Confidential peer review documents shall be transmitted and stored using qualified trust services under Regulation (EU) 2024/1183 (eIDAS 2.0), ensuring authenticity, integrity, and secure access management.*

Justification: The current text only requires "secure handling" of data, which leaves room for inconsistent practices across Member States. By mandating the use of qualified trust services, the regulation ensures legally binding protection of authenticity and integrity. This harmonises procedures with other EU digital frameworks and reduces cybersecurity risks in the peer review process. Furthermore, it reinforces the EU's digital sovereignty by using its own established trust infrastructure rather than fragmented or ad hoc national solutions.

6. Integration of ESG and SME Proportionality Considerations

Proposed Legal Text, Annex II, Section II.3**:**

> *When assessing procedures for monitoring and enforcing obligations of manufacturers or providers, the peer review shall explicitly evaluate whether the NCCA has proportionate procedures adapted to SMEs and whether ESG-related compliance data (e.g., carbon footprint declarations, sustainability obligations) are integrated into supervisory activities.*

Justification: The current draft focuses narrowly on enforcement without reflecting the wider policy priorities of the Union. Integrating SME proportionality ensures that compliance obligations do not create disproportionate burdens, which is essential for maintaining competitiveness. Explicitly linking ESG compliance strengthens coherence with the Green Deal, CBAM, and circular economy objectives. It also encourages NCCAs to develop supervisory practices that are forward-looking, data-driven, and supportive of both sustainability and digital transition.

Prepared by DigitalTrade4.EU

Strengthening the EU's New Legislative Framework (NLF) through the European Trade Indexes Registry (EUTIR)

Feedback to the EU Commission

August 2025, v7

Executive Summary

The **European Trade Indexes Registry (EUTIR)** is **a proposed framework** designed as a strategic solution to support the ongoing revision of the **New Legislative Framework (NLF)**. Its central purpose is to provide a horizontal, **digital trust layer** for trade-related data, addressing weaknesses in fragmented digital integration, inconsistent compliance signals, and high administrative burdens identified in the Commission's 2022 evaluation. EUTIR ensures that product, trade, and sustainability data are **authentic**, **traceable**, and **machine-readable**, thereby reinforcing consumer trust, strengthening market surveillance, and supporting the EU's green and digital transitions.

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** could also include 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/vLEI)**. Importantly, EUTIR should be scoped in close alignment with the ongoing revision of the **EU Customs Code** 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 foresees a hybrid approach: **decentralised infrastructure nodes (EBSI)** combined with **centralised supervision** leaded by **European Securities and Markets Authority (ESMA)** and competent 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**.

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

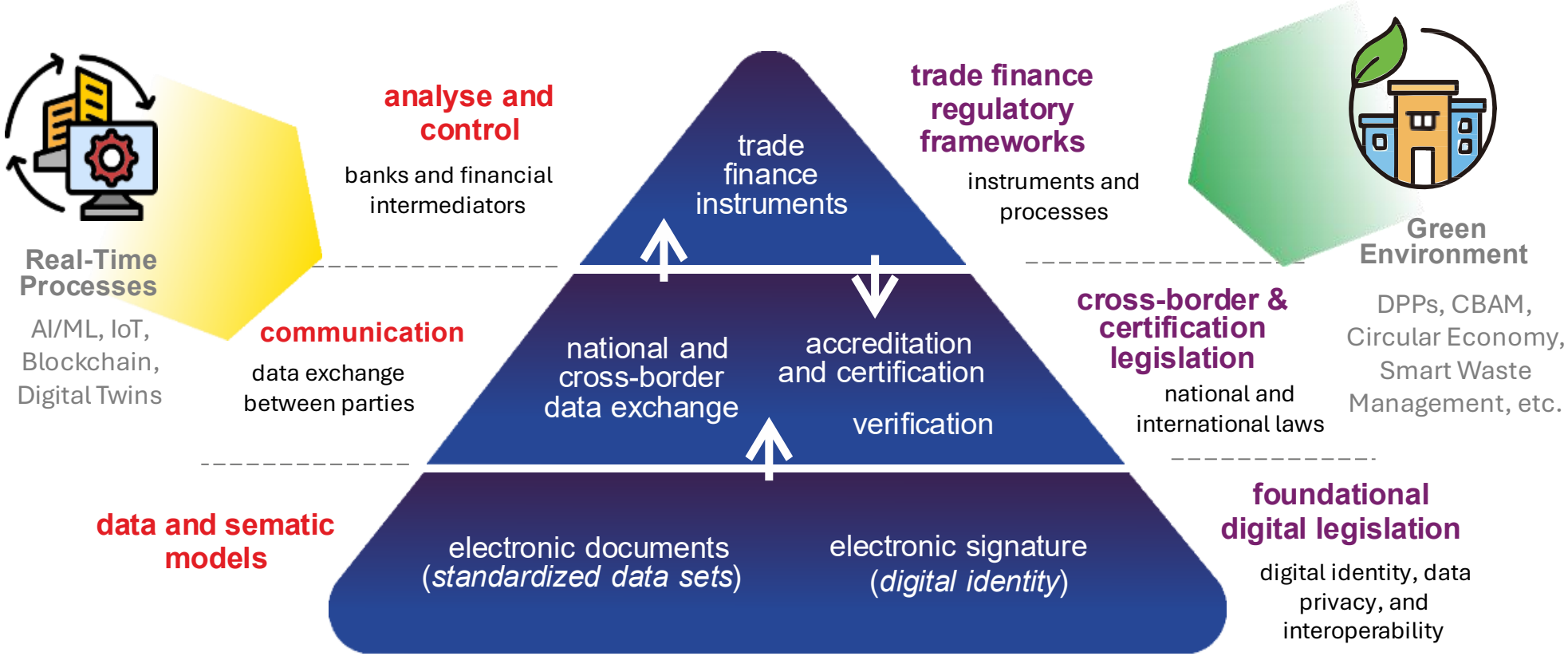


Figure 1. This visual model bridges the European Commission's strategic objectives with the proposed regulatory and operational solutions, illustrating how digital requirements and compliance mechanisms can be implemented in a technologically neutral and future-proof manner. Companies remain free to 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.

2.3. 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

#	Participant Role	Authorised Actions	Restrictions
1	**Certified Service Provider (CSP)**	Creation and amendment of new data records	Actions are limited to their authorised scope of activity.
2	**Competent Authority (CSP with extended rights)**	Status change of data records (e.g., flagged, locked, released, cancelled)	Cannot change the content data of the document, only its status.
3	**Financial Institution (CSP with extended rights)**	Creation and amendment of financial and payment-related metadata	Actions are limited to obligations related to AML/CFT legislation.

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 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 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 record may be deleted or overwritten."** Instead, all 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 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 record lifecycle statuses and legal implications

#	status	definition	legal effect
1	active (submitted)	Status assigned when a new record is created for a new document or initial dataset.	The record is legally valid and has full legal effect until it is amended, terminated, cancelled, or expires.
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	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.
4	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 original state.
5	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.
6	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.
7	terminated	Status applied when the underlying legal or contractual process has concluded (e.g., contract ended, shipment delivered).	The record ceases to have legal effect from the time of termination, but remains preserved in EUTIR.
8	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 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 IV)

The **use cases** presented in Annex IV 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 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 record, preventing **multiple pledges** of the same document.
- **Real-time data-driven supervision**: Use Case 6 shows how a **customs authority** can change a 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 records (e.g., customs declaration) without affecting the validity of the base document, ensuring **traceability** and **validity** across the chain.

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)**[1], 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)**[2], 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 data record is valid.
Use Case 4	Tracking the chain of custody of a shipment between carriers.	Illustrates the data record chain principle from Annex III, ensuring that each change in the chain of custody corresponds to a new, immutable data record.
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.
Use Case 6	A customs officer flagging and locking a data record.	Establishes the rules for flagging and locking in Annex III, Section 5, giving Competent Authorities the right to real-time intervention.

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

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

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 data record without affecting the base document's validity.

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**.

5.2. 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 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. 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 **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**.

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 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.

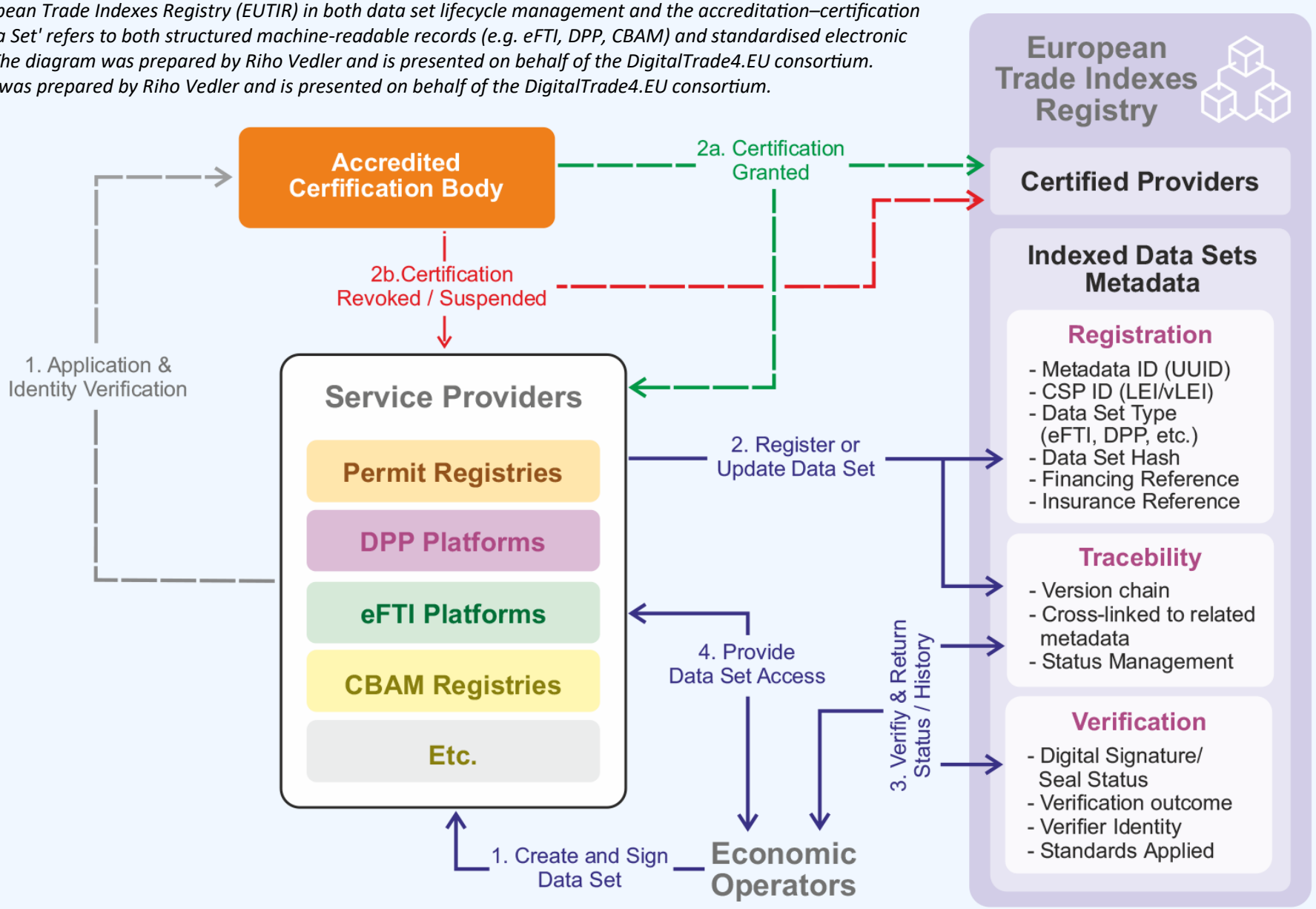
5. **Support for Digital Trust Infrastructure**: Full interoperability with **Global Legal Entity Identifier Foundation (GLEIF) LEI/vLEI** framework and EBSI-based DLT creates a trust environment that extends beyond the EU, enabling recognition in global supply chains and finance networks.

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

a) **"Cryptographic Hash (Hash)"** – 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.

b) **"Data Set"** – 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 within the meaning of this Regulation.

c) **"Electronic Document (eDocument)"** – any digital file or dataset, including but not limited to trade, transport, customs, financial, environmental, or compliance records, which is 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 this Regulation, no full electronic documents are stored or submitted to EUTIR. Only the metadata of structured electronic documents (Data Sets) is registered, ensuring authenticity, integrity, and traceability without storing the underlying content.

d) **"European Union Trade Index Registry (EUTIR)"** – 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. EUTIR is operated by Certified Service Providers (CSPs) and authorised stakeholders through national nodes, ensuring interoperability with other Union digital systems.

e) **"Legal Entity Identifier (LEI)"** – a globally unique legal entity identifier in accordance with ISO 17442, administered by an accredited global operational unit.

f) **“Metadata”** – 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.

g) **“Node”** – 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”).

h) **“Submission”** – the act of transmitting metadata into EUTIR by a Certified Service Provider (CSP).

i) **“Verification”** – the validation of metadata by uncertified parties or competent authorities.

j) **“Verifiable Legal Entity Identifier (vLEI)”** – in accordance with ISO 17442-3, a digitally signed credential interoperable with Regulation (EU) 2024/1183 (eIDAS 2.0), enabling secure and automated identification and authorisation of legal entities.

k) **“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.

l) **“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.

m) **"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.

n) **"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.

o) **"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.

p) **"Mutual Recognition Agreement (MRA)"** – an international agreement concluded between the Union and a third country or regional body, under which EUTIR records and nodes are recognised as legally valid and interoperable in both jurisdictions.

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 (CSPs)

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**.

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.

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. Record Lifecycle

4.1. Statuses include:

Status	Definition	Legal Effect
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.

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.
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.
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.
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.
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.
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.
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. Each has distinct legal effects but all records remain preserved and auditable. No record shall be deleted or overwritten. Default validity is **84 months** if not otherwise specified, in line with generally accepted accounting and transport documentation retention practices.

4.3. 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.

4.4. 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. Flagging and Locking Rules

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

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

5.3. All actions are logged immutably in EUTIR.

6. Content-Specific Rules

6.1. **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.

6.2. **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.

6.3. **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.

7. Transparency, Auditability and Traceability

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

7.2. 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.

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

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

8. Liability and Legal Certainty

8.1. 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.

8.2. 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.

8.2.1. **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.

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

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

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

8.3. In case of disputes or damages resulting from incorrect 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. This framework guarantees that **legal certainty extends beyond data authenticity to responsibility and redress**, thereby addressing critical liability issues within value chains and trade ecosystems.

8.4. 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).

9. Verification Services

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

9.2. 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.

9.3. **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**.

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

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

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

9.5. 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.

9.6. 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.

9.7. 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.

9.8. 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.

10. Interoperability and Data Submission Standards

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

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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 15.

11. Payments, Financial and ESG Metadata

11.1. 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).

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

11.3. 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.

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

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

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

11.7. 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.

11.8. 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.

11.9. 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.

12. AI/ML Integration

12.1. 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.

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

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

12.4. 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

13. SME Support and Proportionality

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

13.2. 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.

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

14. Service Availability

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

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

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

POLICY AND INTERNATIONAL LEVEL

15. Global Interoperability and Mutual Recognition

15.1. 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. [3]

15.2. 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.

15.3. 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.

15.4. 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).

[3] 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.

15.5. 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.

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

Annex IV. Use Cases for Legislative Input and Technical Implementation

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

Sample Data.

1. {hash:"ABC123", status:"active", signature:"QES"}
2. {record:"R1", hash:"ABC123", status:"active", ts:"2025-08-12T10:05:00+02:00"}

3. {hash:"XYZ987"}
4. {record:"R2", hash:"XYZ987", supersedes:"ABC123", 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. Record 2 valid; 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 → Record 1 (*active*).
3. Verification shows status *active*.

Sample Data.

1. {hash:"DEC456", status:"active", signature:"QES"}
2. {record:"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. 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 → Record 2 (*terminated*).

Sample Data.

1. {hash:"LOG123", status:"active", signature:"QES"}
2. {order:"terminate", authority:"EE-Customs"}
3. {record:"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. {record:"M1", hash:"SHIP001", status:"active", ts:"2025-08-12T08:00:00+02:00"}
2. {record:"T1", hash:"SHIP002", parent:"SHIP001", status:"active", ts:"2025-08-12T12:00:00+02:00"}
3. {record:"W1", hash:"SHIP003", parent:"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. {record:"E1", hash:"EBL001", status:"active", ts:"2025-08-12T07:30:00+02:00"}
2. {record:"FIN1", hash:"FIN001", parent:"EBL001", amount:"€100000", status:"active", ts:"2025-08-12T09:00:00+02:00"}

3. {record:"FIN2", hash:"FIN002", parent:"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. {record:"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.

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. {record:"S1", hash:"SHIP001", status:"active", ts:"2025-08-12T08:00:00+02:00"}
2. {record:"INS1", hash:"INS001", parent:"SHIP001", coverage:"€200000", status:"active", ts:"2025-08-12T09:15:00+02:00"}
3. {record:"INS2", hash:"INS002", parent:"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. {record:"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.

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. {record:"CMR1", hash:"CMR123", status:"active", ts:"2025-09-02T08:00:00+02:00"}
2. {record:"DEC1", hash:"DEC456", parent:"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.

Annex IV. Interoperability Ecosystem for EU Digital Trade and Customs Integration

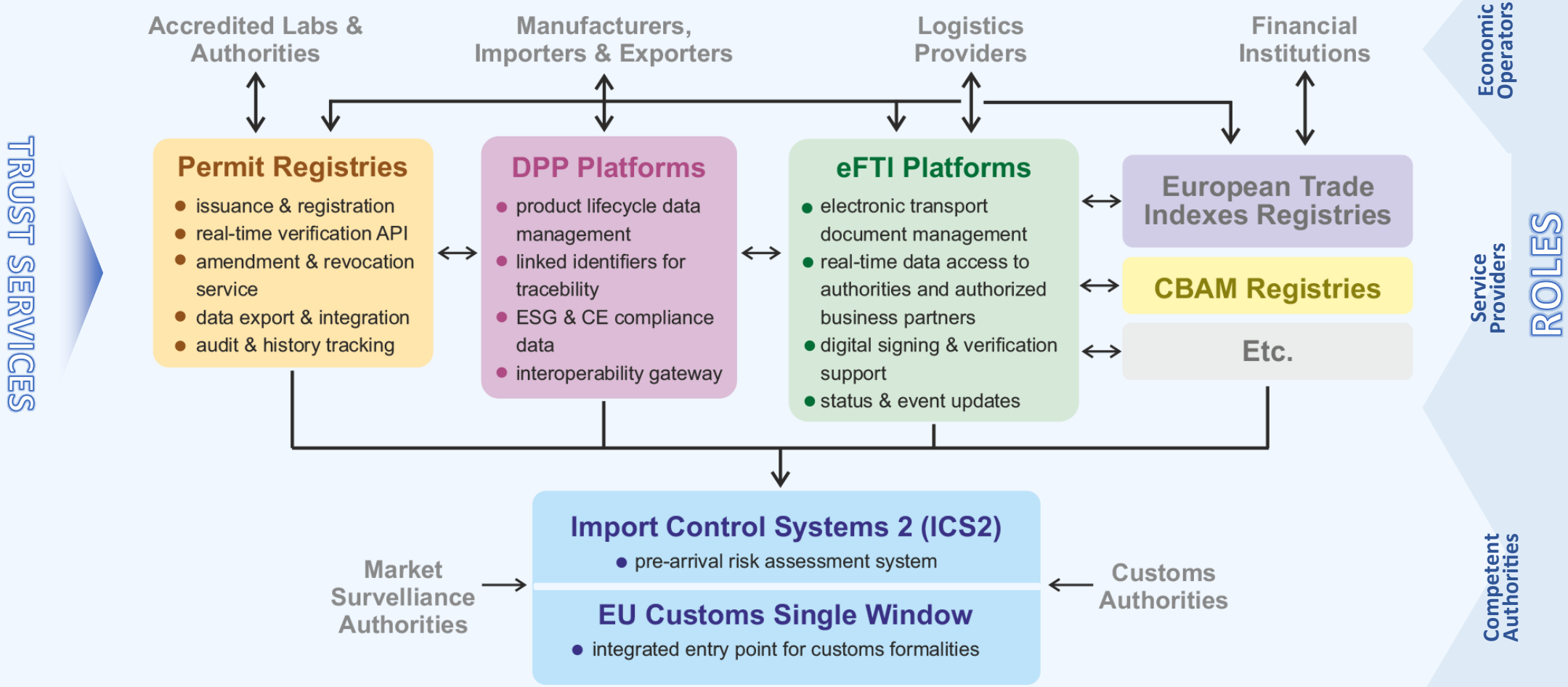


Figure 4. This diagram illustrates the key platforms, data flows, and stakeholder interactions across the EU's digital trade and customs ecosystem. It shows how manufacturers, logistics providers, and regulatory systems connect through structured data platforms—such as eFTI, the Digital Product Passport, and EU Customs systems—while integrating with trusted external sources including TRACES, REACH-IT, and EUDAMED. ***Trust Services*** *supporting this interoperability include LEI/vLEI, Qualified Electronic Signature, Qualified Electronic Seal, Qualified Timestamp, etc. All data exchanges comply with the* ***General Data Protection Regulation (GDPR)****. The diagram was prepared by Riho Vedler and is presented on behalf of the DigitalTrade4.EU consortium.*

Annex V. 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 VI. Digital Trade & Capital Markets Integration Roadmap (DigitalTrade4.EU 2025)

#	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