Prepared by DigitalTrade4.EU

Feedback on the Future of Digital Trade, eFTI Regulation, and European Strategy

June 2025, v3.1

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 **107 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

Executive Summary

DigitalTrade4.EU **welcomes and strongly supports** the European Commission's ambitious initiatives to create a **simple, seamless, and strong** Single Market, bolster the EU's defence capabilities, and lead the global green-digital transition. This document presents our consolidated feedback, drawing upon our expertise in digital trade and logistics. We believe that a **truly interconnected and interoperable** digital framework is the cornerstone of Europe's future competitiveness, resilience, and strategic autonomy.

Our core assertion is that the principles of **interoperability, decentralisation, and harmonised international legal frameworks and standards**—such as the **UNCITRAL Model Law on Electronic Transferable Records (MLETR)**[1] **legal framework** and the new **eIDAS Regulation (eIDAS 2.0)**[2]—are **not just beneficial for commercial trade but are critical enablers** for the Commission's wider strategic objectives, including defence readiness and a robust industrial base. These principles offer **dual-use potential**, seamlessly bridging commercial logistics and defence supply chains—ensuring that innovations in trade digitalisation directly enhance Europe's **military mobility** and **defence resilience**.

Establishing a **globally interoperable system** for identifying **legal entities** is essential to building **trust** in digital freight and logistics. The **Legal Entity Identifier (LEI)** and its **verifiable counterpart (vLEI)**, governed by the **Global Legal Entity Identifier Foundation (GLEIF)**[3], provide **secure**, **standardised**, and **globally recognised** identification mechanisms. The **2025** UNECE ***White Paper on Globally Unique Identifiers in Supply Chains***[4] recognizes the **LEIs** as a **key enabler** for **transparency** and **risk reduction** across global supply chains. Furthermore, the ***UNNExT Working Paper***[5] demonstrates how the **UNCITRAL Model Law** on the Use and

[1] UNCITRAL. Model Law on Electronic Transferable Records
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
[2] European Commission. Discover eIDAS
https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
[3] GLEIF – Global Legal Entity Identifier Foundation
https://www.gleif.org/en
[4] UNECE. White Paper on Globally Unique Identifiers in Supply Chains (June 2025)
https://unece.org/trade/documents/2025/06/standards/white-paper-globally-unique-identifiers-supply-chains
[5] Organizational Identity for Cross-border Digital Trade: Achieving Technical and Legal Interoperability Within the Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT)

Cross-border Recognition of **Identity Management and Trust Services (MLIT)**[6] and the **vLEI** may interact to provide **legal and operational certainty** to identification needs, thus fostering **global economic growth.**

This approach not only addresses the immediate needs of **streamlining freight transport information** but also establishes a **foundational digital infrastructure**. Such an infrastructure is crucial for the **European Union's long-term strategic goals**, including the successful implementation of the **Digital Product Passport**, the achievement of the **Green Deal objectives**, and the strengthening of the **Single Market** against **future disruptions**.

We propose specific, actionable recommendations to **integrate these principles** into the EU's legislative and strategic frameworks, particularly the Electronic Freight Transport Information (eFTI) Regulation. By **leveraging proven, market-driven digital solutions**, the EU can significantly **reduce administrative burdens, enhance security, foster innovation**, and ensure that both its economic and security frameworks are **fit for a complex, uncertain world**. We propose concrete amendments to the draft eFTI implementing regulation to ensure it is future-proof, technologically neutral, and aligned with globally recognised legal frameworks **like the MLETR**, thereby creating a truly unified and efficient data-based Single Market.

Using the vLEI (June 2025)
https://repository.unescap.org/items/7d0c96ab-b108-4d75-b74d-5471ca6696fd

[6] UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022)
https://uncitral.un.org/en/mlit

Introduction

DigitalTrade4.EU is a **broad consortium**, dedicated to fostering a seamlessly interconnected Europe powered by **harmonised standards for the digitalisation of trade**. Our mission aligns directly with the Commission's vision for a more competitive and resilient Union. The current geopolitical and economic landscape demands **bold and decisive action**, and we believe that the strategic adoption of digital technologies is the **most potent tool** at the EU's disposal.

This feedback is submitted to contribute constructively to the ongoing legislative and strategic discussions. We have carefully analysed the Commission's strategy for the Single Market, the objectives for European Defence Readiness, and the detailed draft regulations concerning eFTI. Our goal is to **bridge the gap between policy ambitions and practical implementation**, offering a clear pathway to **leverage digital trade solutions** for broader European goals.

We aim to align our deep expertise in digital standards, secure data exchange, and supply chain digitalisation with the Commission's objectives, ensuring that the resulting framework is **not only compliant but also competitive and innovative**.

Note: *In this document, the terms* ***Small and Medium-sized Enterprises (SMEs)*** *and* ***Micro, Small and Medium-sized Enterprises (MSMEs)*** *are used interchangeably and carry the same meaning and weight. This clarification is important because different sources and contexts may refer to these groups using either acronym, but both encompass the full range of smaller business categories critical for economic development.*

Expectations from the Commission's Side: The Objectives

We have thoroughly reviewed the Commission's strategic documents, including the ***Strategy for making the Single Market simple, seamless and strong (COM(2025) 500 final)***[7]***,*** the ***Joint White Paper for European Defence Readiness 2030 (JOIN(2025) 120 final)***[8] and the draft eFTI implementing regulation. In order of criticality to achieving a data-driven Single Market, the Commission's objectives are:

- **Simplification and Burden Reduction:** A core goal is to **reduce red tape and make things simple** for businesses, especially SMEs, by moving from a document-based to a **data-based Single Market**.
- **Seamless Interoperability:** The Commission expects eFTI platforms to **ensure interoperability and seamless communication** with the systems used by competent authorities, creating a unified digital environment.
- **Security and Trust:** There is a strong emphasis on **secure and authenticated connections**, ensuring the confidentiality and integrity of commercially sensitive data. This includes robust access management and adherence to high cybersecurity standards.
- **Technological Flexibility:** The regulations aim to allow economic operators to **flexibly re-use existing ICT solutions**, avoiding significant new technological investments and facilitating a wider and faster uptake of eFTI.

[7] European Commission, Internal Market, Industry, Entrepreneurship and SMEs. The Single Market: our European home market in an uncertain world (May 2025) https://single-market-economy.ec.europa.eu/publications/single-market-our-european-home-market-uncertain-world_en

[8] European Commission. Joint White Paper for European Defence Readiness 2030 (March 2025) https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

- **Effective Enforcement and Compliance:** The framework must enable competent authorities to **efficiently access and process regulatory information**, ensuring uniform enforcement of rules across all Member States.
- **Strategic Autonomy and Resilience:** Broader strategies underscore the need to **strengthen European value chains**, reduce external dependencies, and build a resilient European Defence Technology Industrial Base (EDTIB), where secure logistics and data exchange are paramount.

DigitalTrade4.EU fully supports these objectives and believes our recommendations provide the **most effective means** to achieve them.

Approach and Recommendations

DigitalTrade4.EU advocates for an approach rooted in **three core principles**: **global interoperability, decentralisation, and the adoption of harmonised international digital legal frameworks and standards**. These principles offer significant dual-use potential, supporting both commercial competitiveness and the EU's defence and security goals.

Our Key Recommendations:

1. **Champion EU-wide Adoption of the MLETR Legal Framework:** We strongly recommend that the Commission **champion the adoption of the UNCITRAL MLETR legal framework** across all Member States. This model law provides a **globally recognised legal basis** for electronic transferable records (like e-bills of lading and other Negotiable Cargo Documents[9]) to be treated as functionally equivalent to their paper counterparts. Adopting this framework is the **essential first step** to creating a legally certain, paperless, and efficient trade environment that aligns with the practices of key global trading partners. For example, Singapore's adoption of MLETR in 2023 reduced maritime trade document processing time by 40%, demonstrating its scalability for cross-border trade[10].
2. **Embrace Decentralised Architectures:** Rather than mandating a single, centralised system or gate, the EU should **foster an environment that supports technologically neutral,** decentralised and resilient architectures (e.g., based on DLT, peer-to-peer networks). Decentralisation enhances security by **eliminating single points of failure**, increases resilience against cyberattacks, and gives economic operators greater control over their data. For instance, blockchain-based systems used in cross-border logistics (e.g., TradeLens) have demonstrated reduced fraud risks and faster dispute resolution by distributing data across multiple trusted nodes.

[9] United Nations. Working Group VI: Negotiable Cargo Documents
https://uncitral.un.org/en/working_groups/6/negotiablecargodocuments
[10] UK Government, British Chambers of Commerce Singapore, LogChain. The UK - Southeast Asia Trade Digitalisation Pilots (December 2024)
https://www.wto.org/english/tratop_e/msmes_e/uksea_10dec24.pdf

3. **Digital Product Passports (DPPs)[11] and Extend for Dual-Use:** We **fully support** the EU's vision for **DPPs** as a **fundamental enabler** of **supply chain transparency** and **sustainability**, directly aligned with initiatives such as **UNECE Recommendation No. 49 ("Transparency at Scale")**[12].

   DPPs provide **verifiable, machine-readable data** on a product's **composition, origin, lifecycle, and environmental footprint**—critical for supporting the following initiatives (some examples):

   - **Regulation (EU) 2024/573 on Fluorinated Greenhouse Gases (F-gases):** DPPs enable tracking and reporting of F-gas types, quantities, and containment measures within products throughout the supply chain. This supports compliance with phase-down targets, leak prevention requirements, and documentation for safe disposal/recovery at end-of-life, crucial for mitigating these potent greenhouse gases.
   - **Regulation (EU) 2019/1148 on the Marketing and Use of Explosives Precursors:** Through detailed documentation of chemical composition and distribution, DPPs strengthen oversight of explosive precursors and other high-risk chemicals, mitigating risks of misuse or unauthorized access.
   - **Regulation (EU) 2023/955 on the Carbon Border Adjustment Mechanism (CBAM):** DPPs help exporters demonstrate compliance by recording embodied carbon emissions across a product's lifecycle, aligning with CBAM's goal to reduce carbon leakage and incentivize low-carbon manufacturing.
   - **Regulation (EU) 2017/821 (Conflict Minerals Regulation):** DPPs ensure compliance by tracing the provenance of minerals like tin, tantalum, tungsten, and gold, preventing conflict-linked materials from entering supply chains and upholding ethical sourcing standards.

[11] European Union. EU's Digital Product Passport: Advancing transparency and sustainability (September 2024) https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability

[12] United Nations Economic and Social Council. Recommendation No. 49: Transparency at Scale – Fostering Sustainable Value Chains (March 2025) https://unece.org/sites/default/files/2025-05/ECE-TRADE-C-CEFACT-2025-03E.pdf

- **Regulations (EU) 2021/2115 & 2021/2116 (Common Agricultural Policy - CAP Simplification):** DPPs support CAP objectives by providing traceable data on agricultural inputs, product origin, and sustainability practices. This enhances transparency for conditionality checks, eco-scheme verification, and market access under the simplified CAP framework.
- **Circular Economy, e.g. Regulation (EU) 2024/1110 on Ecodesign for Sustainable Products (ESPR), Regulation (EU) 2023/1542 (Battery Passport):** By enabling transparency into material sourcing and end-of-life management, DPPs facilitate resource recovery, reduce waste, and promote sustainable reuse. This directly supports circular economy principles central to the ESPR and Battery Passport requirements.
- **Regulation (EC) No 1223/2009 (Cosmetic Products Regulation):** DPPs centralize access to safety-critical information including full ingredient disclosure (INCI names), product formulation details, manufacturing compliance records, and safety assessment reports (PIF). This enables real-time verification of regulatory requirements for banned substances, allergen labelling, and claims substantiation.
- **AI-Driven Resilience Strategies:** DPPs serve as critical data infrastructure for AI systems predicting and mitigating catastrophic events. By providing real-time, granular supply chain visibility, DPPs enable AI models to anticipate climate-induced disruptions (e.g., floods, droughts) and prevent cascading supply chain failures through dynamic rerouting and resource allocation.

From a **logistics perspective**, DPPs are **critically important** because they enable **seamless, trusted information exchange** among diverse actors across the supply chain — from **manufacturers and transporters** to **customs authorities** and **end-users**. This comprehensive **visibility** facilitates **efficient handling**, better **risk management**, **streamlined customs clearance**, and **compliance with regulatory requirements**. Moreover, DPPs help reduce **operational delays** by providing **real-time, accessible product data** that supports **decision-making** and **traceability** at every stage of **transport and storage**.

We also recommend that the DPP framework be **extended beyond commercial applications** to cover **critical components, equipment, and materials** within the **defence supply chain**. This would enable real-time tracking of military assets, such as semiconductors, ensuring compliance with NATO Standardization Agreements (STANAGs) and EU Defence Directives. For these **defence-related applications**, **DPPs** shall operate under a **strictly controlled**, **conditioned-based data access model**, ensuring that **information access is limited** to **authorized entities** with **appropriate security clearances**, diverging from **open data principles** that may apply to certain commercial DPP functionalities.

To accommodate the **diverse sensitivities** of product information, particularly for **dual-use applications**, a **multi-tiered access and security model** shall be implemented for **Digital Product Passports**. This model will **delineate data access** based on **predefined security classifications** and **roles**.

- **Tier 1 (Public/General Access):** This tier will encompass basic, non-sensitive product information intended for broad public access or general commercial visibility, such as generic sustainability metrics or basic product identification that does not compromise intellectual property or security.
- **Tier 2 (Restricted Commercial Access):** This tier will include commercially sensitive data, such as detailed material composition, specific manufacturing process data, or supply chain specifics, accessible only to authorized entities within the commercial supply chain with legitimate business needs and appropriate digital credentials.
- **Tier 3 (Classified/Defence Access):** This highest tier will be reserved for highly sensitive or classified data pertaining to critical defence components and military assets. Access to this information will be restricted exclusively to duly authorized defence entities with verifiable security clearances and subject to stringent protocols for data encryption, access logging, and audit trails in compliance with national and EU defence security regulations.

This dual-use application significantly strengthens traceability and verification of authenticity, combats counterfeiting, and ensures compliance with stringent security and ethical sourcing standards. For example, embedding DPPs into military supply

chains could verify the provenance of critical components like semiconductors, preventing tampering and ensuring adherence to NATO's STANAG 4755 standards for defence materiel *(NATO Standardization Recommendation (STANREC) 4755: "NATO Guidance on Life Cycle Costs". May 23, 2018).*

Such enhanced traceability directly supports the **European Defence Technology and Industrial Base (EDTIB)** and **military mobility objectives** by improving **supply chain resilience**, securing **sensitive materials**, and facilitating **rapid deployment and maintenance of military assets**.

Digital Product Passports (**DPPs**) are also strongly supported by the **European Union's overarching strategy** to make the Single Market **simple, seamless, and strong**. As outlined in the **EU Strategy COM(2025) 500 final**, the primary goal of this strategy is to enhance the **competitiveness, resilience, and strategic autonomy** of the European Market by **removing barriers, simplifying rules, and accelerating digitalisation**. By leveraging **DPPs**, the EU aims to **reduce administrative burdens**, promote **sustainability through traceable product lifecycles**, and strengthen **security**—thereby supporting both **commercial and dual-use applications** critical to the Single Market's future **prosperity and stability**.

4. **Interlinking Digital Compliance Portals and Platforms.** To maximize the efficiency and impact of digital trade and regulatory frameworks, the European Commission should **prioritize the seamless interoperability of various digital compliance portals and platforms**, including but not limited to the eFTI platforms, DPP platforms, and sector-specific portals such as the F-gas Portal[13]. This interoperability is critical to **avoid data duplication, reduce administrative burdens, and streamline regulatory reporting and enforcement** across Member States.

   A **harmonized infrastructure shared among Member States at multiple levels**—including platform technology, accreditation procedures, and certification bodies—would substantially simplify the digital ecosystem. By **enabling Member States to use the same technical infrastructure and align accreditation and certification processes**,

[13] European Commission, Climate Actions. F-gas Portal — Explore the F-gas Portal for HFC quota management, import/export licensing, and compliance with Regulation (EU) 2024/573 https://climate.ec.europa.eu/eu-action/fluorinated-greenhouse-gases/f-gas-portal_en

the Commission can create a more efficient, cost-effective, and secure digital environment for logistics, trade and compliance management.

5. **Leverage eIDAS 2.0 for a Secure and User-Controlled Digital Identity:** The **European Digital Identity (EUDI) Wallet**, established under the new **eIDAS 2.0 Regulation**, should serve as the **cornerstone** of **trusted digital identity** in the EU. Complemented by the **EU Business Wallet** (a **key priority** for **2025**), these frameworks **empower citizens and businesses** by granting them **full control over their data**. Users can **securely store and share identity information**, **verifiable credentials** (e.g., **licenses**, **qualifications**), and **business-related attestations** across borders for both **public and private services**.

   To support **seamless logistics, trade** and **cross-border interoperability**, the **EUDI** and **EU Business Wallets** should also prioritize **compatibility with international unique identity (UID) systems and registries**, **such as the Legal Entity Identifier (LEI)**, to ensure **alignment with global standards** while maintaining the **security** and **user-centric principles** central to **eIDAS 2.0**. By fostering **connectivity with external ecosystems**, the EU can strengthen its **Digital Single Market** as a **globally interoperable**, **harmonized hub** for **trusted digital interactions**.

6. **Fostering Supply Chain Security and Transparency through Globally Unique Identifiers:** A truly **secure** and **transparent supply chain** requires not only the **authentication of data** but also the **unambiguous verification** of the **legal entities** that handle goods at every stage. The current **eFTI framework** focuses on the **secure exchange** of freight information, but it can be significantly strengthened by integrating a mechanism for verifying the **legal and operational status** of the **economic operators** themselves. By embedding a **verifiable legal identity** within the **eFTI data structure**, the EU can create a powerful, **real-time assurance layer** that goes far beyond simple **data validation**. This goes beyond mere data validation, addressing the fundamental identity crisis in digital interactions where a lack of cryptographic assurance about real-world entities behind digital activities has led to significant security vulnerabilities and fraud in other sectors.

   This is achievable by mandating the use of a **globally recognized legal entity identifier**—specifically, the **Legal Entity Identifier (LEI)**, defined under the **ISO 17442**

standard[14]—for every **economic operator** involved in a transaction. When a **competent authority** inspects a **digital transport document**, they could not only validate the data but also instantly verify the **legitimacy** and **status** of the **consignor**, **carrier**, and **consignee**. The **LEI** enables **real-time cross-checks** with **official registries**, such as **business registers** or **insolvency databases**, ensuring that a company is **legally registered**, **solvent**, and **not subject to legal restrictions** that could undermine its reliability.

The use of **ISO 17442-compliant LEIs** is already **mandated** in several **EU financial regulations**, including Regulation (EU) 600/2014 (**MiFID II**), Regulation (EU) 648/2012 (**EMIR**), Regulation (EU) 2015/2365 (**SFTR**), and should be extended to the **eFTI ecosystem** to ensure **regulatory consistency** and **interoperability**. This capability would dramatically **reduce fraud**, **prevent illicit trade**, and **enhance compliance** by ensuring that all parties are **who they claim to be** and are in **good legal standing**. For instance, just as vLEI prevents fraudulent token impersonation in decentralized finance by cryptographically linking tokens to legitimate issuers, it can similarly secure digital transport documents against counterfeit or spoofed entities.

It would transform the **eFTI platform** from a **static information-sharing system** into a **dynamic, standards-based risk management tool**—aligning with the EU's goals for a **trusted and secure Digital Single Market**.

7. **Enable Trusted Legal Entity Identification via LEI and vLEI**: The **LEI**, based on **ISO 17442** and overseen by **GLEIF** under the auspices of **70+ regulators** including the **European Commission**, serves as a **global, public good identifier** for legal entities. The vLEI, built on the Key Event Receipt Infrastructure (KERI) protocol and compatible with **eIDAS 2.0**, offers not only secure, role-based digital identification and delegation but also capabilities like **quantum-secure identifiers** and robust compromise recovery, ensuring enduring trust even in evolving threat landscapes. We recommend integrating **LEI and vLEI** into the **eFTI and DPP frameworks** to:
   - **Ensure reliable identification** of all legal entities

[14] GLEIF. Identifying Organizations – the Legal Entity Identifier (LEI)
https://www.gleif.org/en/organizational-identity/introducing-the-legal-entity-identifier-lei

- **Reduce fragmentation** by harmonising identity frameworks across Member States
- **Improve regulatory compliance**, including know your customer (KYC), instant payments, Markets in Crypto-Assets Regulation (MiCA), and European Single Access Point (ESAP)
- **Bridge EU and third-country identifiers** for cross-border interoperability
- Leverage **GLEIF's foundational role** as the **global root of trust** for **organizational identity**, thereby providing **unparalleled assurance** in **digital transactions**

8. **Invest in Dual-Use Digital Infrastructure:** We recommend allocating a significant portion of the Connecting Europe Facility (CEF) Digital budget to **dual-use digital infrastructure**, such as quantum-secure networks along military mobility corridors. This ensures that the **physical and digital infrastructure are co-developed** to support secure and rapid military and commercial operations. **At the same time, it is essential to develop and maintain robust EU digital infrastructure—including hardware, software, and skills—while ensuring flexibility in technology choices and minimizing implementation burdens** for **public and private stakeholders**.

Specific Changes to the Legislation

To translate our recommendations into concrete legislative action, we propose the following amendments to the **DRAFT COMMISSION IMPLEMENTING REGULATION (EU) .../... laying down detailed specifications regarding the functional requirements for eFTI platforms**[15].

Proposed Changes:

1. **Article 1 (Add Definitions):**
    - ***'Decentralised Network Node'*** *means an ICT component within a decentralised eFTI platform network responsible for managing secure communication with the eFTI Gate, ensuring compliance with authentication and security requirements;*
    - ***'MLETR-compliant system'*** *means a system enabling the creation, management, and transfer of electronic transferable records in accordance with the UNCITRAL Model Law on Electronic Transferable Records, ensuring legal equivalence to paper documents;*
    - ***'Digital Product Passport (DPP)'*** *means a digital record providing verifiable data on a product's composition, origin, lifecycle, and environmental footprint, as defined in (EU) Regulation 2024/1781 (Ecodesign for Sustainable Products Regulation).*
    - ***'Legal Entity Identifier (LEI)':*** *a globally unique, ISO 17442-compliant identifier for legal entities, governed by a global, accredited operating entity.*
    - ***'Verifiable Legal Entity Identifier (vLEI)':*** *ISO 17442-3, is a digitally signed credential compatible with eIDAS 2.0, enabling secure and automated entity identification and authorisation, issued by an authorized global operating entity within the LEI ecosystem.*

[15] European Commission. Electronic freight transport information (eFTI) platforms – specifications on the functional requirements, Draft act
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14373-Electronic-freight-transport-information-eFTI-platforms-specifications-on-the-functional-requirements_en

- **Justification:** These definitions provide clear, internationally recognised legal and technical benchmarks for systems that manage negotiable documents **and product data**, fostering legal certainty, technological neutrality, and global interoperability.

2. **Article 2 (eFTI platforms system architecture):**
   - **Current Text:** "*The system architecture of eFTI platforms shall consist of any combination of ICT components or systems that comply with the requirements laid down in this Regulation.*"
   - **Proposed Amendment:** "*The system architecture of eFTI platforms shall consist of any combination of **decentralised or centralised** ICT components or systems that comply with the requirements laid down in this Regulation, and **shall recognise and interoperate with MLETR-compliant systems** for the management of transferable records.*"
   - **Justification:** This change explicitly allows for **technological neutrality** by supporting both decentralised and centralised models, which enhances security and user control, and ensures the eFTI ecosystem is compatible with the global legal framework for digital trade documents.
3. **Article 3 (Access to eFTI platforms by competent authorities):**
   - **Current Text:** Specifies access "*solely by means of machine-to-machine communication, via a secure connection between the eFTI platform and an eFTI Gate.*"
   - **Proposed Addition (New Paragraphs):**

     *"**1a.** Where an eFTI platform operates as part of a decentralised network architecture, the connection to the eFTI Gate may be managed by a certified **Decentralised Network Node Operator**, provided that the node meets all applicable security, authentication, and audit trail requirements as laid down in this Regulation and Implementing Regulation (EU) 2024/1942. The Node Operator shall be certified by a conformity assessment body in accordance with Article 12 of Regulation (EU) 2020/1056. The decentralised architecture shall prevent single points of failure, support interoperability with centralised*

components, and ensure operational resilience.

***1b.** Where relevant, Decentralised Network Node Operators and eFTI platforms may retrieve and integrate **Digital Product Passport (DPP)** data in accordance with Regulation (EU) 2024/1781. The use of DPPs shall support the provision of regulatory transport information, enable lifecycle data sharing with competent authorities, and reinforce compliance with sustainability and circular economy obligations under Union law."*

- **Justification:** This future-proofs the regulation by accommodating decentralised architectures, which are inherently more resilient and secure than centralised gate models. It prevents vendor lock-in and promotes innovation.

4. **Article 9 (Processing operations):**
   - **Proposal:** *Add a new processing operation: **"(j) Transfer of control of an electronic transferable record"**.*
   - **Associated Action in Annex:** "*The eFTI platform, or interconnected MLETR-compliant system, shall enable a user with control of an electronic transferable record (e.g., an electronic bill of lading) to **securely and verifiably transfer control** to another authenticated user, creating an **immutable and auditable log of the transfer** in line with the principles of the MLETR legal framework.*"
   - **Justification:** This is the **single most critical function** for enabling true digital trade finance and logistics. Without the ability to legally transfer control of documents of title, as enabled by the **MLETR legal framework**, the system remains a mere information portal, failing to unlock massive efficiencies and cost savings.

5. **Interoperability with Digital Product Passports (DPPs)**
   - **Proposed Addition (Article 10 or Annex):** *"eFTI platforms shall ensure interoperability with Digital Product Passports (DPPs) as defined in Regulation(EU) 2024/XXX, enabling seamless exchange of product lifecycle data (e.g., origin, environmental footprint, and security-critical components) between freight transport systems and DPP platforms. For defence-related*

consignments, platforms shall support extended DPP functionalities for traceability of critical components and compliance with security sourcing standards. Crucially, all data operations involving defence-related DPPs must adhere to the highest standards of cybersecurity and data protection, including end-to-end encryption, multi-factor authentication, and strict access controls based on security clearances. The underlying infrastructure for such defence-sensitive DPPs shall be subject to regular, independent security audits and comply with relevant national and international military security protocols, in addition to general EU data protection regulations."

- **Justification:** Enhances supply chain transparency, sustainability, and security, aligning with **EU Green Deal objectives** and **strengthening the European Defence Technology Industrial Base (EDTIB)**.

6. Interlinking Compliance Platforms

- **Proposed Addition (Article 11):** *"eFTI platforms shall interoperate with other Union digital compliance platforms (e.g., DPP platforms, F-gas Portal) through common technical standards and data exchange protocols. Member States shall use harmonised accreditation procedures and certification bodies to ensure seamless cross-platform communication."*
- **Justification:** Reduces administrative burdens, avoids data duplication, and creates a unified digital ecosystem.

7. Globally Recognized Legal Entity Identifiers and ISO 17442

- **Proposed Addition (to Article 4 or 8): "***To further enhance the reliability and traceability of economic operators in the eFTI environment, the use of a globally recognized legal entity identifier, such as the Legal Entity Identifier (LEI) defined under ISO 17442, should be supported. This would enable competent authorities to cross-reference the identity and legal status of each actor in a consignment movement with official registries, in real time. Such integration complements existing electronic identification measures and aligns with EU financial regulations requiring LEIs under MiFID II, EMIR, and SFTR. "*

- **Justification:** Supporting the use of the Legal Entity Identifier (LEI), defined under ISO 17442, further enables real-time verification of legal entities, ensures interoperability with trade and transport documents.

8. **Amend Article 4 (Access to eFTI platforms by business users) and Article 5 (Authorisation mechanism):**
    - **Proposed Amendment (to Article 4 or 5, as a new sub-point or expansion):** *"The European Digital Identity (EUDI) Wallet and the EU Business Wallet, implemented through Regulation (EU) 2024/1183, shall serve as primary mechanisms for business users to securely provide their identity credentials, including the presentation of Verifiable Legal Entity Identifiers (vLEIs) for the authenticated and verifiable identification of legal entities involved in freight transport operations. The eFTI platform shall support the automated verification of such vLEIs. Legal entities may authenticate using a vLEI credential in compliance with Regulation (EU) 2024/1183 and ISO 17442, providing a trusted, cross-border mechanism for access and digital delegation."*
    - **Justification:** This integration leverages the vLEI's inherent cryptographic security and its unique capabilities for perpetual recovery and real-time verification of organizational identity, creating an unbreakable and highly resilient digital link between legal entities and their freight transport operations, thereby ensuring a consistent and secure method for identifying legal entities.

The Case for Aligning the eFTI Regulation with eIDAS 2.0 Regulation

While the draft **eFTI Implementing Regulation** correctly identifies the need **for secure and reliable electronic identification** as a cornerstone of trust in digital freight transport, its current approach is fundamentally flawed. However, its reliance on the original 2014 eIDAS Regulation (EU) No 910/2014 is a **significant flaw** that risks making the eFTI framework **obsolete** before it is even fully implemented. The new **eIDAS 2.0 framework (Regulation (EU) 2024/1183)**, which entered into force in May 2024, represents the **definitive future** of digital identity in the Union.

The full application of the eFTI Regulation is mandated for **July 2027**. By this date, **Member States** will also be deep into the implementation of **eIDAS 2.0**, which requires **national authorities** to offer **EUDI Wallets** to **citizens** and **businesses** by **December 2026**. **Delaying eFTI's alignment** with eIDAS 2.0 risks creating **parallel systems** that **cannot interoperate**, undermining both regulations' **objectives**.

This **misalignment** would create a **fragmented digital landscape** where businesses in the **logistics sector** are forced to navigate a **complex** and **outdated identity verification system**, while other sectors advance with the more **secure** and **user-friendly EUDI Wallet**. Such a scenario directly contradicts the Commission's stated goal of creating a **simple** and **seamless Single Market**.

Aligning the eFTI Regulation with eIDAS 2.0 is not merely a technical update; it is a **strategic imperative** that offers three fundamental benefits:

- **Future-Proofing and Preventing Fragmentation:** Referencing the outdated eIDAS 1.0 framework will lead to the creation of **parallel, incompatible identity systems**. Businesses and authorities would be forced to support both the legacy eID schemes and the new EUDI Wallets, creating confusion, increasing costs, and **undermining the core objective** of a **seamless Digital Single Market**. By adopting **eIDAS 2.0 now**, the eFTI framework aligns with the **harmonised, future-proof standard** that will govern all other sectors.
- **Enhancing Efficiency and Reducing Burden:** Forcing economic operators and platform developers to build solutions based on a 2014 standard, only to have to re-engineer them for the 2024 standard, is **inefficient** and imposes a **dual compliance burden**. A **single, harmonised framework** based on eIDAS 2.0 allows for investment in **one modern, streamlined, and interoperable system**, reducing administrative overhead and costs for all stakeholders.
- **Strengthening Security and User Control:** eIDAS 2.0 introduces the **EUDI Wallet**, a paradigm shift towards a more **secure and user-centric** identity model. The Wallet **empowers businesses and individuals** by giving them **direct control** over their own data and credentials, allowing them to share only what is necessary for a given transaction. This model **significantly reduces the risks** of **data breaches and identity**

fraud compared to older systems and is **essential for building the trust** needed for widespread adoption of eFTI platforms.

In conclusion, updating the eFTI Implementing Regulation to be **fully compliant with eIDAS 2.0** is the only logical path forward. It ensures the eFTI ecosystem is **secure, efficient, and seamlessly integrated** into the EU's wider digital architecture, thereby delivering a truly **simple and strong data-based Single Market**. Proposed Changes:

To align the draft eFTI Implementing Regulation with the new European Digital Identity framework, the following amendments are proposed. All references to Regulation (EU) 910/2014 should be updated to Regulation (EU) 2024/1183 (eIDAS 2.0).

1. Recital (6)

- **Current Text:** "*At the same time, authorisations should be granted only to users that have been reliably identified and authenticated, using electronic identification means compliant with the requirements laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council.*"
- **Proposed Amendment:** "*At the same time, authorisations should be granted only to users that have been reliably identified and authenticated, using electronic identification means compliant with the requirements laid down in* ***Regulation (EU) 2024/1183*** *of the European Parliament and of the Council."*

2. Article 1 (Definitions)

- **Article 1(15) 'advanced electronic signature'**
  - **Current Text:** "'*advanced electronic signature' means an electronic signature that meets the requirements laid down in Article 26 of Regulation (EU) No 910/2014;"*
  - **Proposed Amendment:** "'*advanced electronic signature' means an electronic signature that meets the requirements laid down in* ***Regulation (EU) 2024/1183****;*"
- **Article 1(16) 'advanced electronic seal'**
  - **Current Text:** "'*advanced electronic seal' means an electronic seal that meets the requirements laid down in Article 36 of Regulation (EU) No 910/2014;*"

- **Proposed Amendment:** "'*advanced electronic seal' means an electronic seal that meets the requirements laid down in* ***Regulation (EU) 2024/1183****;*"

3. Article 4 (Access to eFTI platforms by business users)

- **Article 4(3)**
  - **Current Text:** "*The electronic identification scheme referred to in paragraph 2, point (a)(i), shall comply, as a minimum, with the requirements laid down in Article 8(2), point (b), of Regulation (EU) No 910/2014."*
  - **Proposed Amendment:** "*The electronic identification scheme referred to in paragraph 2, point (a)(i), shall comply with* ***Regulation (EU) 2024/1183 (eIDAS 2.0)*** *and its subsequent revisions. It shall be implemented through the* ***European Digital Identity (EUDI) Wallet****, once available, to provide a* ***user-controlled, secure, and harmonised means*** *of authentication and sharing of verifiable credentials across the Union."*

4. Article 5 (Authorisation mechanism)

- **Article 5(5)(c)(i)**
  - **Current Text:** "*enable the non-onboarded user to provide identification credentials in one of the following formats: email address, phone number, or by electronic identification means issued under an electronic identification scheme notified in accordance with Regulation (EU) No 910/2014;*"
  - **Proposed Amendment:** "*enable the non-onboarded user to provide identification credentials in one of the following formats: email address, phone number, or by electronic identification means issued under an electronic identification scheme compliant with* ***Regulation (EU) 2024/1183****;*"

5. Article 9 (Processing operations)

- **Article 9(5)**
  - **Current Text:** "*When the processing operations referred to in paragraphs 1 and 2 involve signing by the business user by means of electronic signature, the eFTI platform shall enable users to sign either with an electronic signature or with an*

electronic seal that is compliant, as a minimum, with the requirements for an advanced electronic signature laid down in Regulation (EU) No 910/2014."

- **Proposed Amendment:** "*When the processing operations referred to in paragraphs 1 and 2 involve signing by the business user by means of electronic signature, the eFTI platform shall enable users to sign either with an electronic signature or with an electronic seal that is compliant, as a minimum, with the requirements for an advanced electronic signature or seal laid down in* ***Regulation (EU) 2024/1183***."

Key Differences Between eIDAS (2014) and eIDAS 2 (2024)

Aspect	eIDAS (910/2014)	eIDAS 2.0 (2024/1183)
Objective	Enable cross-border recognition of electronic IDs and trust services within the EU.	Expand digital identity with the European Digital Identity (EUDI) framework for all citizens and businesses.
Digital Identity	Recognition of national eID schemes voluntarily notified by Member States.	Mandatory EUDI Wallets provided by all Member States to citizens and businesses.
EUDI Wallet	Not included.	A secure app enabling users to store and share personal identity data and credentials securely.
EU Business Wallet	Not included.	A secure framework enabling businesses to store and share organizational credentials (e.g., vLEIs) for cross-border transactions, ensuring alignment with global standards like ISO 17442.
Scope of Use	Mainly for accessing public sector services.	Extended to both public and private sectors, including banks, telecoms, transport, and online platforms.
Private Sector Adoption	Voluntary or limited.	Mandatory for large online platforms (e.g., social media, marketplaces) and critical infrastructure providers (e.g., banks, transport services) to accept EUDI Wallets for authentication.
Control over Data	Limited; dependent on national systems.	User-centric: Full control over which data is shared, with selective disclosure mechanisms.
Trust Services	Covers electronic signatures, seals, timestamps, eDelivery, and website authentication.	Strengthened existing trust services + introduces electronic ledgers (e.g., blockchain-based systems) for decentralized data integrity, improved website authentication, and enhanced electronic archiving with quantum-secure identifiers.
Interoperability	Based on mutual recognition of national schemes.	Fully harmonized across the EU via EUDI Wallets with common technical standards.
Legal Obligations	Member States can choose whether to notify national eID schemes.	Obligatory: All Member States must issue EUDI Wallets and ensure cross-border functionality.
Privacy & Security	General requirements for security and data protection.	Enhanced: Privacy by design, strong encryption, decentralized identity principles, and interoperability.
Governance & Oversight	National supervisory bodies.	Stronger EU-level governance, with a significant role for ENISA, the European Commission, and cross-border supervisory cooperation.
Implementation Deadline	Ongoing since 2014; slow adoption in some areas.	Clear deadline: By mid-2026, all Member States must implement EUDI Wallets.

Table 1. These adaptations increase clarity and precision to highlight eIDAS 2.0 improvements compared to the 2014 framework.

Conclusion and Next Steps

DigitalTrade4.EU is **firmly committed** to supporting the European Commission in building a **more secure, resilient, and competitive Union**. The strategic implementation of digital transformation, centred on **interoperability, decentralisation, and harmonised legal frameworks and standards**, is the most fundamental enabler for achieving this vision. The principles revolutionising global trade offer **profound dual-use opportunities** to enhance the EU's economic and defence capabilities simultaneously.

This approach aligns with the core **ethos of self-sovereignty and decentralization**, enabling participants to **manage their own cryptographic infrastructure** while benefiting from a **globally trusted network**, thus avoiding **centralized points of failure** inherent in many existing digital identity solutions.

We are convinced that by **embracing these future-proof digital solutions**, the EU can unlock significant synergies, improve operational efficiency, and bolster security across all sectors. We propose the following next steps:

1. **Engage in a structured dialogue** with DG MOVE, DG DEFIS, and DG CNECT to elaborate on the practical implementation of these recommendations. This task force should be co-chaired by **DG MOVE** and **DG DEFIS** to ensure dual-use alignment.
2. **Establish a joint task force,** including industry experts from DigitalTrade4.EU, to refine the technical specifications for the eFTI framework, ensuring they are aligned with global legal frameworks like MLETR.
3. **Collaborate on pilot projects** that test and showcase the application of decentralised and interoperable digital solutions in dual-use contexts, such as secure defence logistics and critical component traceability using DPPs.

We are confident that by working together, we can build a digital future for Europe that is **innovative, secure, and prosperous**.

In conclusion, **DigitalTrade4.EU's recommendations** provide a **comprehensive blueprint** for transforming **Europe's trade** and **defence ecosystems** through **digital innovation**. By adopting **MLETR**, **decentralised architectures**, and **dual-use DPPs**, and by aligning **eFTI with eIDAS 2.0**, the

EU can secure its position as a **global leader** in **green-digital trade**. These steps will not only **simplify regulatory compliance** and **reduce costs** but also **fortify Europe's strategic autonomy** in an era of **geopolitical uncertainty**. We urge the **Commission** to **act swiftly** to implement these changes and collaborate with **industry stakeholders** to ensure a **seamless transition**.

The integration of **vLEI**, underpinned by **KERI's advanced cryptographic features**, signifies a **fundamental paradigm shift** in **digital trade**, elevating **security**, **trustworthiness**, and **compliance** to **unprecedented levels**.

EU Green-Digital Trade Leadership Roadmap (DigitalTrade4.EU, 2025)

activity	objective	indicative metrics	tools/enablers
1. EU-Singapore DTA & Expand DEPA Partnerships	Strengthen digital trade diplomacy in Asia through high-standard agreements.	- 5+ new digital trade agreements with key Asian partners (e.g., Japan, India, ASEAN) by 2030 - 15% increase in EU-Asia digital services trade by 2028	DEPA framework, EU-Singapore DTA, Global Gateway Initiative, eIDAS 2.0
2. Implement Digital Product Passports (DPPs)	Ensure traceable, sustainable supply chains aligned with EU Green Deal.	- 50% adoption of DPPs by 2030 - 20% reduction in supply-chain carbon intensity by 2030	EU Sustainable Products Initiative, CBAM incentives, UNECE Recommendation 49
3. Fund Secure Digital Corridors in Asia	Build interoperable digital infrastructure for EU-Asia trade.	- ~€2B allocated via NDICI-Global Europe - 10+ blockchain-based traceability pilots by 2027	NDICI-Global Europe, ASEAN digital customs systems, EU Customs Data Hub
4. Harmonize Digital Standards (MLETR/eIDAS 2.0)	Enable cross-border recognition of e-documents and digital identities.	- 90% mutual recognition of e-signatures by 2028 - 70% SME adoption of eIDAS wallets	MLETR framework, eIDAS 2.0, EU Transport Law updates, UN/UNECE protocols
5. Implement LEI and vLEI for Supply Chain Trust	Harmonise and simplify legal entity identification across borders	- 90% entity coverage with LEI by 2030; 50% vLEI use in customs and eFTI transactions	ISO 17442, vLEI, eIDAS 2.0, UNECE UID
6. Launch Green-Digital Trade Academy	Upskill SMEs and officials on DPPs and carbon accounting.	- 40% increase in SME participation by 2027 - 60% cost savings for SMEs	Erasmus+ grants, COSME programme, tiered compliance thresholds
7. Integrate ESG into Trade Finance	Link trade finance to sustainability metrics for cheaper capital access.	- €10B/year unlocked for green trade finance - 30% lower Scope 3 emissions by 2030	InvestEU guarantees, CSRD-aligned reporting, FinTech platforms
8. Enforce Platform Interoperability	Prevent vendor lock-in and empower SMEs.	- 100% compliance with CJEU rulings by 2026 - 50% reduction in platform dominance	Court of Justice of the European Union (CJEU) Case C-233/23, DEPA, eIDAS 2.0, Digital Markets Act (DMA)
9. Global Digitalisation Projects with EU Standards	Extend EU digital infrastructure and norms globally.	- 20+ co-funded projects by 2030 - 80% interoperability with EU systems	Digital Europe Programme, CEF funding, EU-Asia Digital Standards Taskforce
10. Advance UNECE Transparency Protocols	Globalize EU sustainability standards for supply chains.	- 100% alignment with UNECE Rec. 49 by 2028 - 30% reduction in greenwashing claims	UNECE CEFACT, W3C Verifiable Credentials, EU CBAM registry
11. Pilot CBAM-DPP Corridors	Link trade finance to verifiable ESG metrics for tariff incentives.	- 20% CBAM compliance cost reduction - 50% DPP adoption by 2030	IoT carbon trackers, CBAM rebate schemes, EU Customs Single Window

Table 2. The roadmap above, DigitalTrade4.EU's input to the European Commission's "International Digital Strategy" operationalises the recommendations outlined in this document. For instance, Activity 1 (EU-Singapore DTA & Expand DEPA Partnerships) directly supports the harmonisation of international digital standards, while Activity 8 (Global Digitalisation Projects with EU Standards) aligns with efforts to promote dual-use infrastructure globally. These activities collectively reinforce the EU's ability to leverage digital trade diplomacy as a tool for both economic growth and strategic security.

Comparison of eIDAS 2.0 and UNCITRAL MLIT

Aspect	eIDAS 2.0	UNCITRAL MLIT
Legal Nature	EU regulation (legally binding across EU Member States)	Model law (non-binding template for national adoption)
Geographic Scope	European Union (27 Member States + EEA countries)	Global (for adoption by any country)
Purpose	Enable interoperable, secure, and trusted digital identity and trust services across the EU	Harmonize laws to support legal recognition of digital identity and trust services across borders
Core Components	- European Digital Identity Wallets- Qualified and non-qualified trust services - Mutual recognition of notified eID schemes	- Identity Management (IdM) frameworks - Trust services (electronic signatures, seals, timestamps, etc.) - Cross-border recognition principles
Cross-border Recognition	Mandatory mutual recognition of notified eID schemes and qualified trust services	Recognition based on functional equivalence and non-discrimination principles
Trust Services Covered	Same as MLIT plus new services (electronic ledgers, electronic archiving, remote signing, digital wallets)	Electronic signatures, seals, timestamps, electronic registered delivery, and website authentication
Digital Identity Requirements	Prescriptive: introduces **European Digital Identity Wallet** and minimum technical/UX standards	Technology-neutral and principle-based (does not prescribe specific implementation models)
Technology Neutrality	Partially – allows innovation but includes detailed technical specs for interoperability	Strongly emphasized
Governance Model	EU-level governance (European Commission, ENISA, national competent authorities)	National authorities choose implementation and recognition procedures
Implementation Flexibility	Medium (Member States must comply but can choose providers and local context for rollout)	High (jurisdictions tailor to local needs)
Interoperability Focus	Strict technical and legal interoperability within EU Digital Single Market	General cross-border legal acceptance
Private Sector Role	Both public and private sector can issue and operate EUDI Wallets and trust services	Encouraged, but implementation is state-led
Adoption Status (as of 2025)	In force in the EU since 2024, rollout of EUDI Wallets ongoing	Adopted or under review in several countries globally

Table 3. As the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) does not belong to a single country or region, it provides an excellent foundation to extend similar principles globally. Its adoption reduces political influence over technological development, promotes legal interoperability, and fosters innovation in digital identity and trust services.