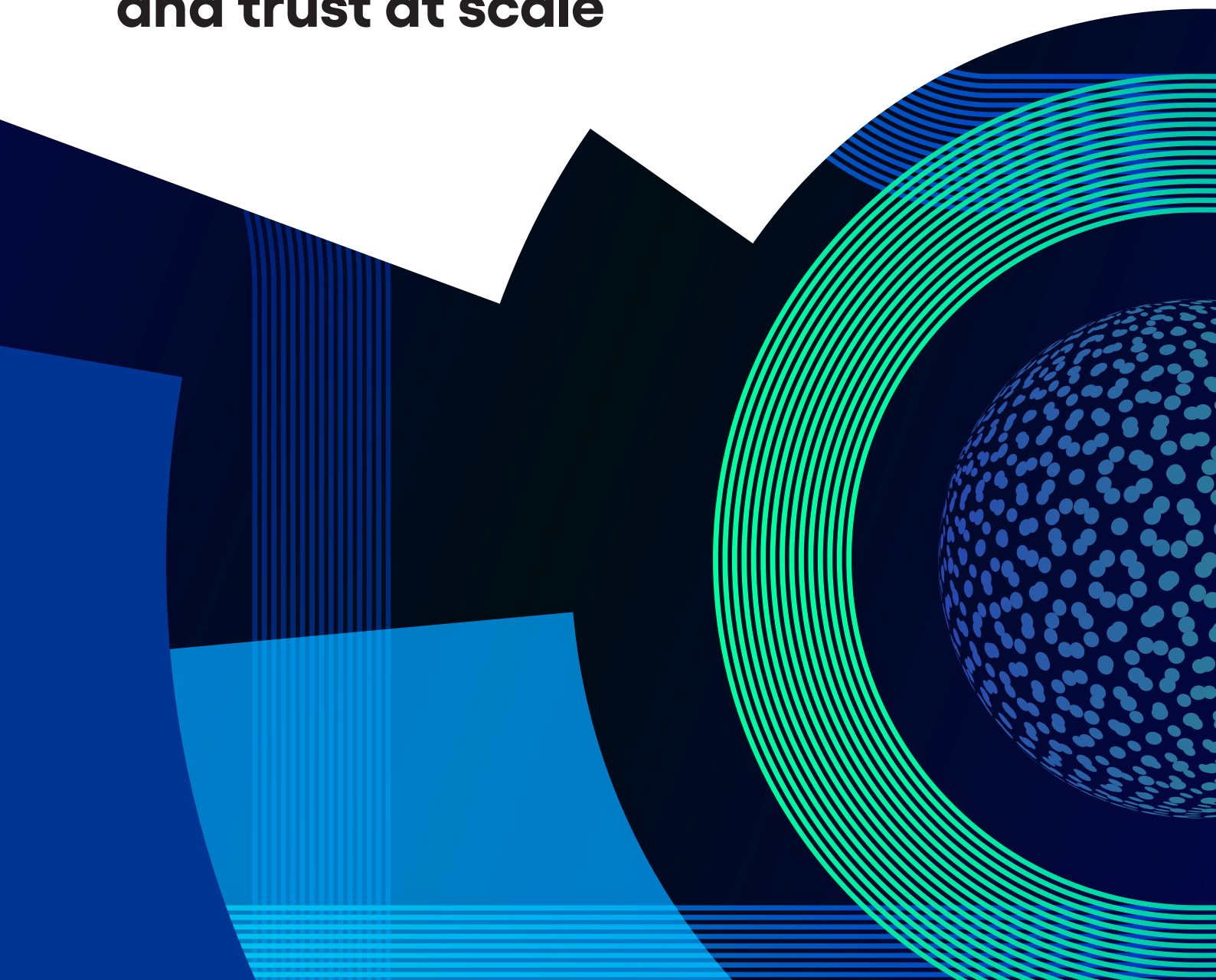
ICC Digital Standards Initiative

Digitalising Global Trade

A roadmap to interoperability and trust at scale



Contents

Foreword **3**

Executive summary **4**

Abbreviations **5**

Figures **7**

1. Introduction: A new chapter in trade digitalisation **8**

2. Understanding today's supply chains **9**

2.1 Why semantics come first 10

2.2 Why digitised documents alone are not the prize 13

2.3 A practical data hierarchy—harmonise what matters first 13

3. Digitalisation trends: What's emerging **15**

4. From digital documents to a truly digital trade fabric **18**

4.1 An "interoperability layer" could ensure the trade ecosystem evolves rationally and in the public interest 18

4.2 An integrated, stakeholder-driven roadmap to an interoperability layer 19

4.3 Why this can start now 20

5. Towards an integrated digital-trade ecosystem—From scattered digitisation to continuous, trusted data flow **20**

5.1 Three interoperable routes— context determines choice 20

5.2 Bridging tactics—what can be done in the next 12 months 21

6. Digital trust at scale—turning assurance into an ordinary feature of every transaction **22**

6.1 What a "trust supply chain" covers 22

6.2 From principles to practice—applying MLIT and MLETR 24

6.3 Recommended next steps for market participants 25

7. Governing digital trade for the long term—keeping the system coherent as it scales **25**

7.1 Four core functions of stewardship 25

8. Conclusion: A call to action **27**

8.1 Governments, trade policymakers and multilateral development banks 27

8.2 Standards development organisations 28

8.3 Financial institutions, credit insurers and trade finance innovation 28

8.4 Marine insurers and P&I clubs 30

8.5 IT infrastructure and corporate ERP providers 30

8.6 Industry associations and chambers of commerce 30

8.7 Key sectors and geographies in need of capacity building 31

Foreword

The ICC Digital Standards Initiative was founded to address critical challenges blocking the digitalisation of global trade and its many supply chains. We focus on four key challenges:

1. **Legal and regulatory reform** to enable and promote the use of digital and electronic forms and data in trade processes;
2. **Standards alignment and interoperability** to enable seamless data sharing and connectivity at scale across supply chains and borders;
3. **Digital trust** to enable trade data and documents to be verified, authenticated, and securely shared or transferred;
4. **Capacity building** to enable all enterprises and governments, regardless of their stage of development or size, to participate in and take full advantage of the future trade ecosystem.

The focus of this paper is the technical infrastructure required to operationalise digital trade, or in other words, the second and third pillars above. This is not to play down the importance of the legal infrastructure; indeed there is much good work being done by multilateral fora, development banks, and national governments on legal reform. We support these efforts wholeheartedly and hope to see a fully "green" MLETR tracker quite soon.

On the other hand, there is an increasing amount of attention, and many different views on how to achieve standards interoperability and digital trust at scale. It is an issue that is at once unifying—because many would like to see interoperability and agreed trust frameworks—and yet divergent because there is so little consensus on how to engender it on a global level.

We cannot assume that digitalising trade processes and increasing the flow of data across supply chains and borders will automatically produce the inclusive, interoperable trade system that we are aiming for. Rather we must map and stride towards this future with deliberate, coordinated steps, where connectivity and collaborative action become the default.

Hence this paper. Please take this as an initial articulation of how we might build the technical infrastructure needed for an interoperable, inclusive digital trade ecosystem. We have aimed to map out the vision, as well as how different stakeholders might contribute through their actions.

This work is the result of many rounds of discussion, reflection and input—and we would like to thank all those who contributed their time and insights to the successive drafts of this paper.

We see this as a continuing discussion, grounded in action, learning and shared purpose—as we create the future together. Thank you for your partnership and collaboration.

Pamela Mar
Managing Director
For and on behalf of the ICC Digital Standards Initiative

Executive summary

Digitalising global trade and supply chains promises vast benefits—greater efficiency and speed, resilience, traceability, and inclusion—but until recently, the transition from paper to digital has lagged the rapid pace at which technology has advanced. Many parties have made genuine efforts at digitalisation but instead of advancing in concert, progress has been fragmented and somewhat disjointed.

At least in 2023 and 2024, there was palpable momentum notably in legal reform, growing recognition of the importance of digital trade standards for data and its exchange, and high-profile pilots that have demonstrated interoperability. But there is more work to be done, to develop and advance a common language for data, trust mechanisms that work across platforms, and governance that holds the system together as it scales.

This paper sets out a pragmatic, stakeholder-led roadmap to advance our collective work. It shows how to:

- **Align semantics** by applying the Key Trade Documents & Data Elements (KTDDE) framework and the KTDDE Implementation Guides (KIGs) to the 36 documents that drive most supply chain processes.
- **Embed portable trust** using "verify once, use many" framework using globally recognised identifiers and accredited trust services.
- **Pilot, measure and scale** through an interoperability layer that separates common protocols and standards from commercial applications.
- **Govern for inclusivity** with a light-touch stewardship model that keeps standards, platforms and capacity building in sync, especially for SMEs and emerging markets.

If governments, standards bodies, financiers and industry leaders act on this common plan, the payoff is immediate and measurable: faster clearance times, lower capital charges on financed shipments, and transparent supply chain data that unlock new ESG and risk insights.

The legal frameworks, technical tools and economic incentives are already in place. What remains is concerted execution. This paper provides the sequence, roles and milestones to realise cross-border digital trade.

Abbreviations

3PLs	Third Party Logistics Providers
AI	Artificial Intelligence
AML	Anti Money Laundering
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
ASEAN	Association of Southeast Asian Nations
B2B	Business-to-Business
B2G	Business-to-Government
BIMCO	The Baltic and International Maritime Council
BIS	Bank for International Settlements
CEO	Chief Executive Officer
CODEX	Generic Model Official Certificate
CSV	Comma Separated Values
DAP	Delivered at Place
DCSA	Digital Container Shipping Association
DLT	Distributed ledger technology
DNI	Digital Negotiable Instruments
Docs	Document
DSI	Digital Standards Initiative
EBL	Electronic Bill of Lading
ERP	Enterprise Resource Planning
ESG	Environmental, Social and Governance
ETDA	Electronic Trade Documents Act
EPHYTO	Electronic Phytosanitary Certificates
ETR	Electronic Transferable Records
FI	Financial Institutions
FIATA	International Federation of Freight Forwarders Associations
FOB	Free on Board
G2B	Government-to-Business
GLEIF	Global Legal Entity Identifier Foundation
GNC	Globally Networked Customs
GS1	Global Standards One
GTIN	Global Trade Item Number
HS	Harmonized System
ICC	International Chamber of Commerce

ID	Identification
IOT	Internet of Things
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
JSON	JavaScript Object Notation
KIG	KTTDE Implementation Guidelines
KTDDE	Key Trade Documents & Data Elements
KYC	Know Your Customer
LC	Letters of Credit
LEI	Legal Entity Identifier
MDB	Multilateral Development Bank
MLETR	Model Law on Electronic Transferable Records
MLIT	Model Law on Identity Management and Trust Services
MOU	Memorandum of Understanding
NIST	U.S. National Institute of Standards and Technology
OCR	Optical Character Recognition
P&I	Protection and Indemnity
PDF	Portable Document Format
PKD	Public Key Directory
PO	Purchase Order
SCF	Supply Chain Finance
SDO	Standards Development Organizations
SKU	Stock Keeping Unit
SLA	Service Level Agreement
SME	Small- and Medium-sized Enterprise
TCP	Transmission Control Protocol
UBL	Universal Business Language
UK	United Kingdom
UNESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UN/LOCODE	United Nations Code for Trade and Transport Locations
vLEI	Verifiable Legal Entity Identifier
WCO	World Customs Organization
WTO	World Trade Organization
XML	Extensible Markup Language

Figures

Figure 1: Key trade documents in the end-to-end supply chain 10
Figure 2: Mapping the standardisation journey of key trade documents 11
Figure 3: Understanding data sharing within the supply chain 12
Figure 4: Data hierarchy for digitalising global trade. 13
Figure 5: Trade document data hierarchy. 14
Figure 6: Unpacking interdependent layers of the global supply chain 22
Figure 7: Four core functions of stewardship 26

1. Introduction: A new chapter in trade digitalisation

2023 and 2024 marked a turning point for global trade digitalisation, with significant progress in legal reform, articulation and alignment of digital standards, and active piloting across public and private sectors. Cross-border trade—long burdened by paper-based processes, fragmented standards, and siloed platforms—turned towards a new era of digital transformation.

To date, 10 jurisdictions—including the UK and most recently, France—have enacted laws based on UNCITRAL's MLETR, which enable the digitalisation of documents of title within supply chains globally. Economies accounting for **37% of global GDP are now aligned to MLETR with another 34% actively working on legislative and capacity building needed for alignment**[1]. This progress at the national level follows on broad multilateral support in global and regional forums such as the G7, G20, APEC, the E-Commerce Joint Statement Initiative, the Digital Economy Partnership Agreement, the ASEAN Digital Economy Framework Agreement, and others.

Momentum on legal reform is clear. But legal infrastructure is just one building block needed to realise digital trade at scale. This paper thus focuses on the technical infrastructure required for digital trade, in its interoperable and trusted form, to become a reality. Many initiatives are already underway among diverse stakeholders, and joining these up into a collective journey will accelerate progress towards a future-ready trade system.

Key questions include:

Question that must now be answered	Why it matters
How freely can verifiable trade data cross borders, and where must states retain control?	Determines the scope of "data free flow" and "trusted corridors."
Will distributed-ledger and token-based platforms reach mainstream trust?	Impacts scalability and cost of digital instruments.
Do current legal reforms guarantee interoperability between *systems*, not just *documents*?	Prevents new digital silos.
Will proprietary platforms open their APIs and data models?	Critical for SME inclusion.

1 Digital Standards Initiative, Year In Review (ICC DSI, 2024) Available at https://www.dsi.iccwbo.org/_files/ugd/8e49a6_f1114437bef14b4eac7ffa857a741abb.pdf

2. Understanding today's supply chains

Modern supply chains are complex, involving multiple parties, tiers, and nations, and are often digitally fragmented. Upstream suppliers may still use spreadsheets to track orders, while downstream 3PLs manage cargo with advanced IoT dashboards. Banks and insurers, positioned in the middle, re-key or ingest data from PDFs into legacy systems or receive data through various proprietary customer-facing apps. This results in a patchwork of formats, identifiers, and trust levels that slow commerce and increase costs. Fragmented visibility not only creates inefficiencies but also heightens risks related to fraud, compliance, and contract enforcement.

Trade documentation binds these actors together. Key trade documents—such as commercial invoices, certificates of origin, bills of lading, and customs declarations—are essential for international trade. However, their formats, legal standing, and systems for implementation vary widely. Many of these documents are still generated, shared, and processed in inconsistent formats, often paper-based or PDF, with varying legal standing and interoperability. Even today, a cross-border transaction involves multiple actors and on average requires the exchange of 36 documents and 240 copies.[2]

A common semantic foundation is needed to unlock interoperability. The WTO, UNCITRAL, and UNESCAP have identified 36 key trade documents central to trade transactions and suitable for digitalisation.[3] Digitising these documents and turning them into structured, connectable datasets is crucial for resilient, traceable, and scalable trade processes. With this data, trade can also address issues like sustainability, inclusivity, and access to financial services.

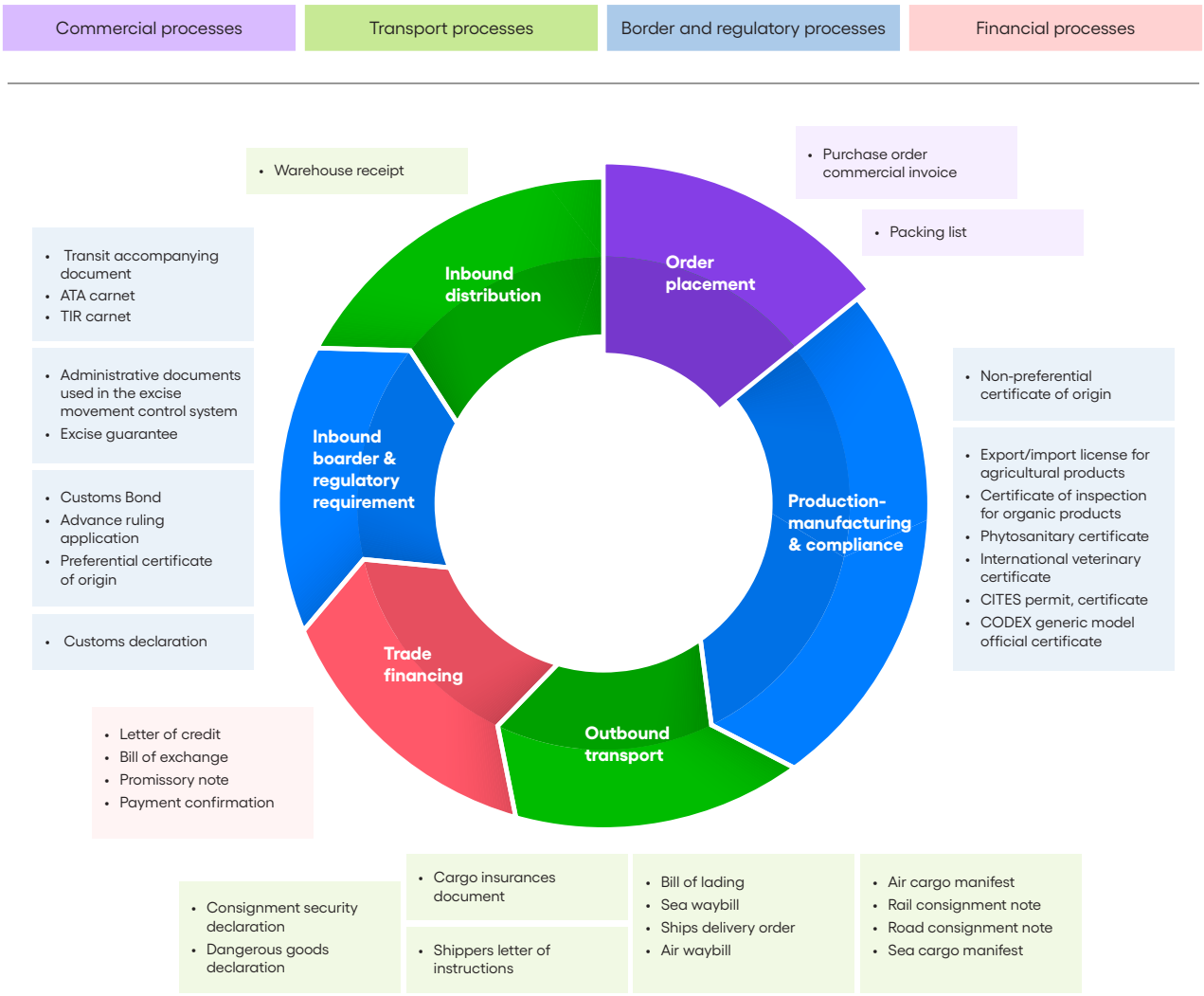
ICC DSI addresses the fragmentation by breaking down documents into their core data elements and mapping the flow of these data across the end-to-end supply chain.[4] The KTDDE framework aims to align digital versions of the 36 key trade documents (see next page) —whether commercial, transport, financial, or compliance—via their core data elements, connecting public and private sector users into one common data framework.

2 Standards Toolkit for Cross-border Paperless Trade (ICC, 2022). Available at https://iccwbo.org/news-publications/policies-reports/standards-toolkit-for-cross-border-paperless-trade/

3 Cross-border Paperless Trade Toolkit (World Trade Organization, 2022). Available at https://www.wto.org/english/res_e/publications_e/paperlesstrade2022_e.htm

4 End-to-end supply chain refers to the complete flow of goods, services and information across borders, from initial suppliers to final buyers, throughout the entire international trade system.

Figure 1: Key trade documents in the end-to-end supply chain



Source: Digitalising global trade: A roadmap for achieving interoperable, inclusive, and trusted trade (ICC, 2025)

2.1 Why semantics come first

Digitising the 36 documents is only step one; turning them into *structured, connectable datasets* unlocks benefits from automation, finance and risk analytics. The KTDDE analysis shows that 189 core data elements recur across 33 documents, proving that a common semantic layer is feasible.[5]

Digital standards development for the international supply chain has been ongoing for over three decades, led by organisations such as UN/CEFACT, GS1, OASIS, Swift, and others. There may already be a number of electronic versions for key trade documents; indeed, there is an overabundance as parties developed different electronic versions trade documents without aiming for interoperability. Different key trade documents might use the same data element differently, referencing different data models.

5 Key Trade Documents and Data Elements: Digital standards analysis and recommendations— An integrated framework for digitalising the entire supply chain (ICC DSI, 2024). Available at https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf

This approach acknowledges a few key realities:

- Of the 36 key trade documents, 21 are already digitalised and, in some cases, there are multiple digital versions of a given document that might be used differently. Fortunately, different standardised digital versions of a document contain data that can be interoperated with guidelines bridging semantic and technical differences.

Figure 2: Mapping the standardisation journey of key trade documents

Adopt	Align	Develop
Standardised	**Standards exist, but without interoperability**	**Early stage standardisation**
1. Commercial Invoice 2. Bill of Lading 3. Sea Waybill 4. Ship's Delivery Order 5. Air Waybill 6. Sea Cargo Manifest 7. Air Cargo Manifest 8. Rail Consignment Note 9. Consignment Security Declaration 10. Non-preferential Certificates of Origin 11. Customs Declaration 12. CODEX Generic Model Official Certificate 13. Phytosanitary certificate 14. CITES permit/certificate 15. ATA Carnet 16. TIR Carnet 17. Transit Accompanying Document 18. Administrative Documents used in the Excise Movement Control System 19. Payment Confirmation 20. Bill of Exchange 21. Promissory Note	1. Purchase Order 2. Shipper's Letter of Instruction 3. Packing List 4. Certificate of Inspection for Organic Products 5. Advanced Ruling Application 6. Letter of Credit	1. Road Consignment Note 2. Cargo Insurance Document 3. Warehouse Receipt 4. International Veterinary Certificate 5. Dangerous Goods Declaration 6. Customs Bond 7. Export/Import License for agricultural products 8. Excise Guarantee 9. Preferential Certificates of Origin

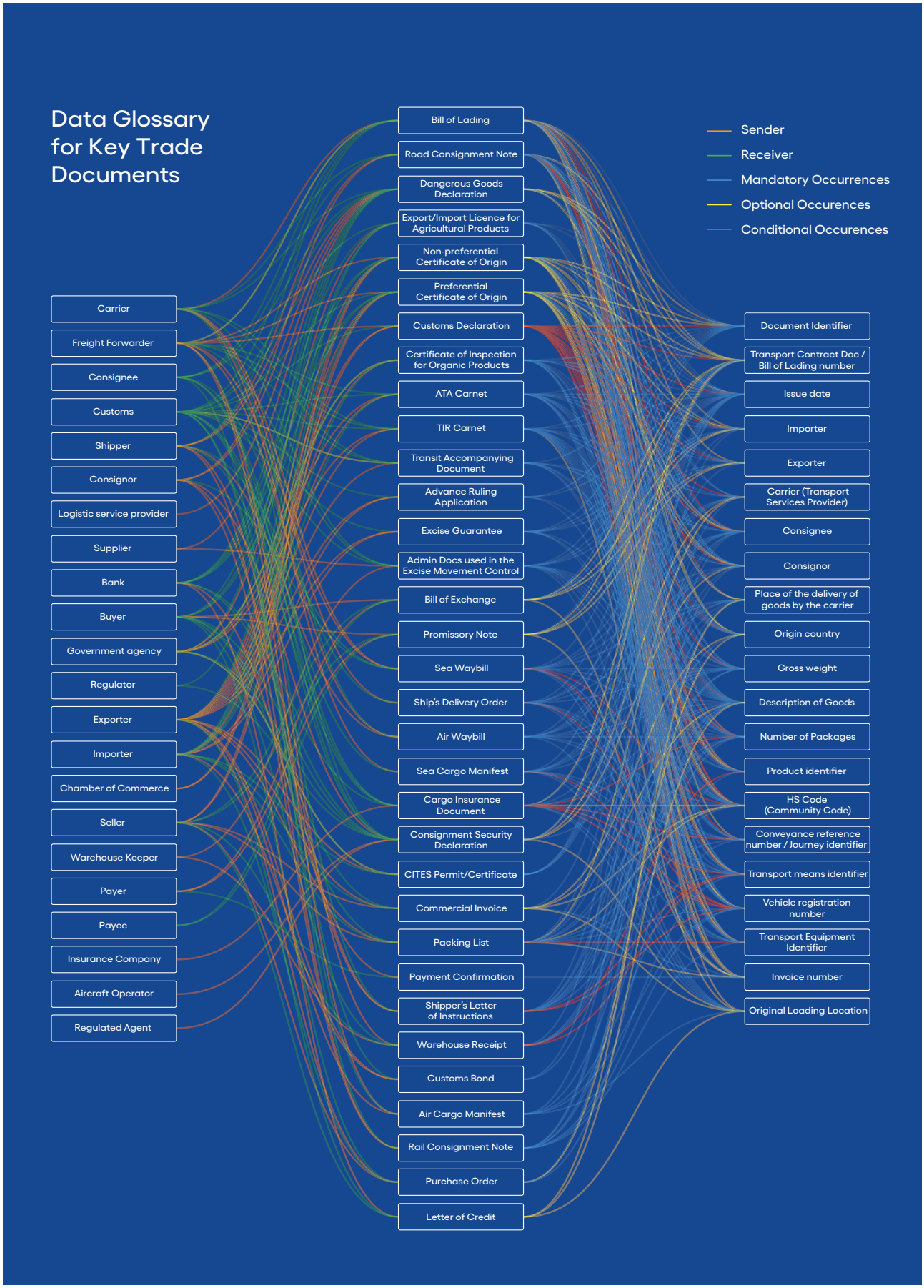
Source: Key Trade Documents and Data Elements: Digital standards analysis and recommendations— An integrated framework for digitalising the entire supply chain (ICC DSI, 2024)

- Across 33 key trade documents covered by the Key Trade Data Glossary,[6] 189 data elements are considered core, as they are shared by more than two parties or across multiple documents. 53 data elements are shared across more than five documents, and 21 are shared across more than 10 documents. Understanding that interoperability is possible at the data level makes data mapping essential across the entire 36-document dataset.[7]

6 The DSI KTDDE working group analysed 36 trade documents. The data glossary is based on the analysis of these trade documents, except three of them: CODEX Generic Model Official Certificate, Phytosanitary certificate, International Veterinary Certificates. See details at https://www.digitalizetrade.org/ktdde

7 Key Trade Documents and Data Elements: Digital standards analysis and recommendations—An integrated framework for digitalising the entire supply chain (ICC DSI, 2024). Available at https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf

Figure 3: Understanding data sharing within the supply chain



Source: Guide to Digital Trade Finance (Deutsche Bank, 2024)

The core dataset is critical to facilitate interoperability between different documents, given their differences; identifying the core dataset will also enable subsequent digital tagging of data as it travels across the supply chain.

Paper's last advantage—and how to move beyond

Paper is still the *de facto* interoperable medium not because technology is absent, but because digital systems have yet to share **common semantics and portable trust anchors.** Intelligent document-processing tools, OCR engines and AI models already convert PDFs into neatly structured CSVs or JSON. These solutions are valuable **on-ramps**—they free data from static images—but they do **not** guarantee interoperability: if every platform maps extracted fields to its own schema, the industry merely swaps one set of silos for another.

2.2 Why digitised documents alone are not the prize

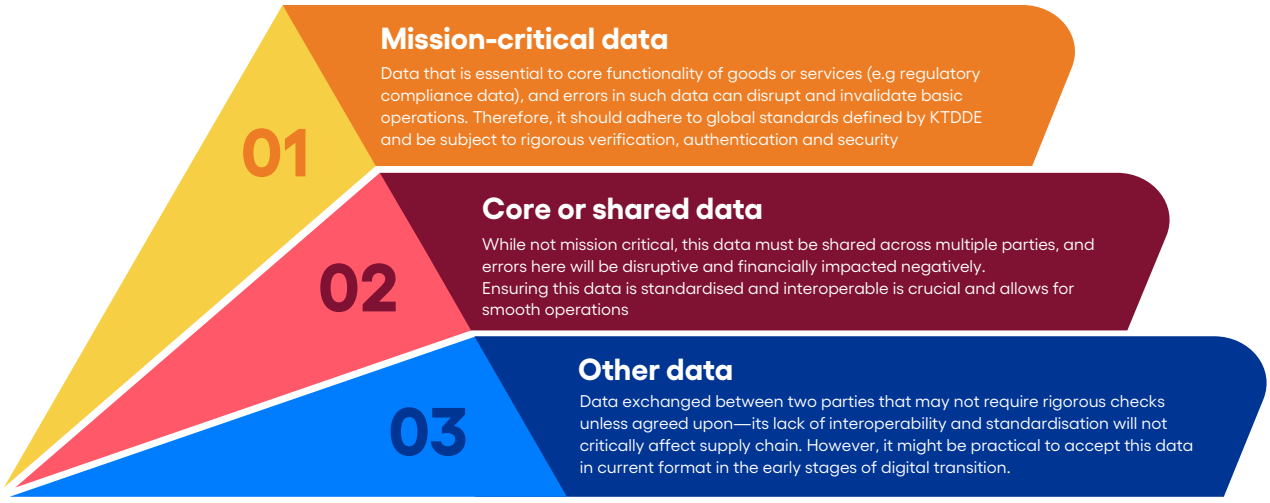
Converting a paper bill of lading into a PDF may cut courier fees, but it still obliges a document checker to re-key data and perform compliance checks. The real efficiency gain occurs when data—not files—flow between systems in a form that is machine-readable, verified and traceable. In a data-first operating model, core data remain in their source environments (ERP platforms, customs portals, IoT gateways). Authorised parties retrieve only the fields they require, assemble a document on demand, apply a digital signature, and attach a time stamp. Documents therefore become momentary views of already-trusted data, rather than static objects that circulate indefinitely.

Digitising individual forms is only the first step; those forms must also be harmonised through shared semantics and identifiers. When this alignment is in place—using tools such as the KTDDE data catalogue and its implementation guides—efficiency analysis, risk detection and process automation become commercially relevant and possible.

2.3 A practical data hierarchy—harmonise what matters first

To build on this concept, a structured data hierarchy can be developed to prioritise different types of data:

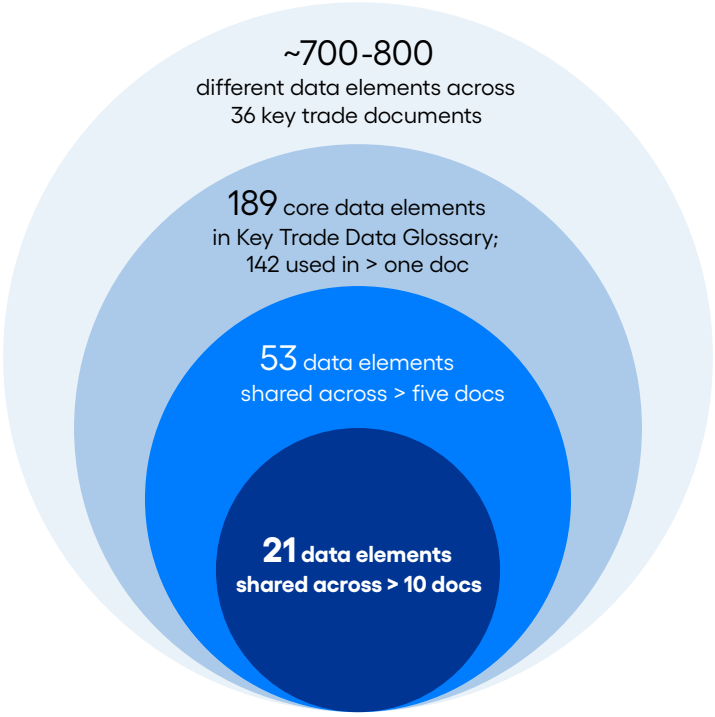
Figure 4: Data hierarchy for digitalising global trade



Source: Digitalising global trade: A roadmap for achieving interoperable, inclusive, and trusted trade (ICC, 2025)

The data hierarchy acknowledges that not all data within a document is crucial for interoperability and therefore does not need to be standardised. Most documents contain more data than necessary for their primary function, as various elements may have been added over time to meet the specific needs of different parties. When multiple versions of a document exist, they may share some data but often include different elements. While some of these data points are standardised, many are not.

Figure 5: Trade document data hierarchy



Source: Digitalising global trade: A roadmap for achieving interoperable, inclusive, and trusted trade (ICC DSI, 2025)

Take the commercial invoice as an example. Multiple versions of a commercial invoice may exist depending on the exporter, importer, or platform used. Core data points like the invoice total, date, and buyer and seller details are often standardised. However, other elements such as payment terms, tax identification numbers, or detailed shipping instructions can vary. These non-standardised data points can create inconsistencies and complicate information sharing across different systems or platforms.

Table 1: Illustrative tiering for a commercial invoice

Tier	Example fields on a commercial invoice	Why it sits in this tier	Standardisation recommendation
Mission-critical	• HS code (6-digit minimum) • Seller and buyer LEI/vLEI • Net weight/quantity • Invoice total (amount + ISO-4217 currency) • Country of origin	Errors here can block customs clearance, tax assessment, or bank compliance checks.	Must follow global code lists (HS, ISO 4217, ISO 3166), party identification must follow global standards and be cryptographically signed or otherwise strongly verified.

Core/ shared	• Purchase-order reference • Incoterms® (e.g., DAP, FOB) • Contract / sales agreement number • Container or package ID • Port of loading & discharge (UN/LOCODE)	Used by multiple parties (buyer, forwarder, bank) but a mistake usually causes delay, not legal invalidation.	Structured, unique, and consistent within the transaction; moderate verification (e.g., cross-checking against PO database).
Other/ bilateral	• Seller's internal SKU or ERP line ID • Marketing or campaign code • Optional remarks/handling notes • Buyer's internal project code	Relevant mainly to the contracting parties; does not affect regulatory or financial processing.	Free-text or proprietary codes are acceptable; may remain unstandardised until a clear business case emerges.

By segmenting the data elements within documents and identifying those that are repeated and potentially shared across multiple stages of the supply chain, we can focus alignment efforts on a smaller, more manageable set of data elements. Establishing a shared data foundation with KTDDE and developing a practical data hierarchy allows us to harmonise what matters most, ensuring a seamless flow of information across the supply chain. This approach not only enhances efficiency but also mitigates risks, paving the way for a resilient and scalable digital trade ecosystem.

3. Digitalisation trends: What's emerging

Four key trends are influencing the shift from document-driven to data-driven trade. Each trend is real, but none will reach scale without shared semantics and open trust rails.

Table 2: Digital trade infrastructure: Trends, momentum and systemic challenges

Trend	Momentum	Fault-lines
1. Trade-data platforms and networks	• Over 200 private or public platforms now handle shipping, compliance, finance or ESG data, with many using DLT or secure APIs[8].	• Most remain *closed systems*. The shutdown of TradeLens in 2023 showed that scale eludes platforms seen as proprietary and lacking open APIs.
2. Next-generation Single Windows	• UN ESCAP's 2023 global survey finds 69% average implementation of domestic paperless-trade measures[9].	• But only **47%** of *cross-border* paperless-trade measures are even partially implemented, reflecting significant challenges in the electronic exchange and legal recognition of trade-related data and documents across borders[10].

8 Blockchain & DLT in Trade: Where do we stand? (World Trade Organization, 2020). Available at https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf

9 Digital and Sustainable Trade Facilitation: Global Report 2023, (UNESCAP, 2023). Available at https://repository-uat.unescap.org/server/api/core/bitstreams/fbffab6f-223b-447a-a6ff-8f4bea16d6e7/content

10 Digital and Sustainable Trade Facilitation: Global Report 2023 (UNESCAP 2023). Available at https://repository-uat.unescap.org/server/api/core/bitstreams/fbffab6f-223b-447a-a6ff-8f4bea16d6e7/content

3. Digital trade-finance and payment rails	• Adoption of ISO 20022[11] surged to 1.4 million cross-border messages a day in December 2024, spanning 150 sending and 220 receiving countries. • Legal reform is catalysing new DNIs[12]	• In a 2024 Surecomp survey[13] of nearly 100 trade-finance professionals, 46% of corporate respondents manage their processes manually, while 44% of banks depend on hybrid (manual and digital) workflows—evidence of the prevalence of manual processes among corporates, which also means most financial institutions cannot yet automatically ingest structured supply-chain data end-to-end.
4. Portable digital identity and trust services	• The LEI system surpassed 2.6 million active identifiers[14] in 2024, with an annual growth rate of 11.5%.	• The Financial Stability Board's 2024 cross-border-payments review[15] described the use of the LEI in payment messages as "very limited" and urged regulators to make its inclusion best practice. Until the LEI (or equivalent) travels with every transaction, automated KYC, sanctions screening, and document, authentication will remain patchy.

Why alignment matters now

Industry momentum is tangible, yet the four digitalisation trends still advance largely in silos. Divergent data fields, inconsistent use of legal-entity identifiers, and uneven deployment of trust services limit straight-through automation.

A *trust service* is any electronic service that reliably guarantees a property of a data message—who signed it (e-signature/seal), when it was created (timestamp), whether it reached the intended party intact (registered delivery), or whether a website genuinely belongs to a stated entity (website authentication).

When a service can demonstrate reliability—consistent with UNCITRAL's MLIT—its legal effects can be recognised across borders without renegotiating bilateral rules. Critically, organisations can apply these reliability principles through contracts and independent audits today; they do not have to wait for formal MLIT transposition in their jurisdiction.

Shared assurance mechanisms are beginning to emerge. The Reliability Assessment Framework, launched by ICC DSI and Canada's Digital Governance Council in 2024, lets platform providers complete a single self-assessment aligned with MLETR reliability criteria and share the results with multiple regulators and clients—clarifying for all users the capacity of systems to handle ETRs in line with the technical and legal requirements. This is especially important for SME users, given that they are the ones without the resources to perform individualised due diligence on every trade service

11 ISO 20022 in bytes for payments: Maintaining the momentum in 2025 (Swift, 2025). Available at https://www.swift.com/news-events/news/iso-20022-bytes-payments-maintaining-momentum-2025#:~:text=As%20we%20kick%20off%202025,global%20nature%20of%20this%20adoption.

12 Creating a modern digital trade ecosystem: The economic case to reform UK law and align to the UNCITRAL Model Law on Electronic Transferrable Records (MLETR) (ICC, 2021). Available at https://www.dsi.iccwbo.org/_files/ugd/0b6be5_e6bef2857560420793110fa0bea642d8.pdf

13 Survey reveals trends in trade finance: digitalisation's growing impact (Surecomp, 2025). Available at https://surecomp.com/blog/survey-reveals-trends-in-trade-finance-digitalisations-growing-impact/

14 The LEI in Numbers: 2024—A Landmark Year (GLIEF, 2025). Available at https://www.gleif.org/en/newsroom/blog/the-lei-in-numbers-2024-a-landmark-year

15 Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments (FSSB, 2024). Available at https://www.fsb.org/uploads/P121224-1.pdf

provider; in the industry of the future such diligence processes should be carried out by objective, transparent certification processes, rather than by each user individually.

Absent common semantics and portable proofs of reliability, digital documents and payments remain trapped in bilateral corridors and trade data continues to circulate as PDFs or bespoke APIs.

Table 3: Implications for key stakeholder groups

Stakeholder	Priority actions (technology-neutral & vendor-agnostic)	Why it matters
Governments & regulators	• Embed internationally recognised data standards (UN/CEFACT core components, KTDDE mappings) when upgrading National Single Windows or negotiating digital-corridor MOUs. • Issue technical guidance that links domestic legal reforms (e.g., MLETR) to shared assurance mechanisms where available, using the DSI Reliability Assessment Framework as a reference point.	Standards alignment plus trustworthy services enables cross-border B2G and G2B data exchange; legislation alone does not create interoperability.
Platform & solution providers	• Publish open APIs and full data-model documentation. • Support portable identifiers (e.g., LEI/vLEI) and adopt trust services—e-signatures, timestamps, electronic registered delivery—whose reliability can be independently evidenced via methods such as DSI Reliability Assessment Framework.	Open interfaces and recognised credentials lower onboarding costs, reduce vendor lock-in, and future-proof platforms for global use.
Financial institutions & fintechs	• Leverage ISO 20022 migration to ingest structured supply-chain data. • Map internal data schemas to KTDDE core elements and use verifiable trust services for DNIs.	A shared data backbone and reliable trust services enable automated, scalable financing decisions and streamline compliance checks.
Standards bodies & industry associations	• Treat every new or revised standard as a bridge, not an island: publish *crosswalks*[16] that map each data element to existing schemas (e.g., KTDDE), enabling translation rather than re-keying. • Coordinate and maintain neutral reliability frameworks—building on models like the DSI Reliability Assessment—to translate principles into testable criteria, checklists, and optional certification schemes recognised across markets.	Crosswalks maximise semantic interoperability, while common reliability frameworks provide a "verify once, use many" pathway that reduces duplication and scales trust globally.

16 A common practice in the standards community is to publish a cross-walk (or mapping table) with new or revised schemas. This tool lists each data element in the 'source' standard and shows its correspondence to elements in another standard or earlier version. The U.S. National Institute of Standards and Technology (NIST) defines a cross-walk as a tool to understand how diverse standards relate to each other and avoid redundant requirements. Publishing a cross-walk signals the goal of interoperability, helping users move data across ecosystems.

Bottom line: The technical capability is largely in place; what is missing is a common language—shared semantics—and universally recognised proofs of reliability for the trust services that move data. With those two foundations, today's isolated pilots can merge into an integrated digital-trade fabric.

4. From digital documents to a truly digital trade fabric

Every trade transaction confronts users with the same question: "Can I trust data enough to directly act on it (without checks)?". Paper once answered that question because the physical document itself was (i) perceived to be relatively hard to forge, (ii) easy to hand over and (iii) accepted by courts everywhere. A digital equivalent must therefore combine three attributes but do so at near-zero marginal cost:

1. **Universality**—readable by any counterparty, border agency or bank.
2. **Reliability**—tamper-evident provenance and timestamps that stand up in court.
3. **Openness**—an architecture that welcomes new use cases rather than locking users into one platform.

4.1 An "interoperability layer" could ensure the trade ecosystem evolves rationally and in the public interest

Most digital-trade projects to date have focused on delivering the above attributes within the *applications* (eBL platforms, single windows, fintech portals). Each works well inside its own perimeter, yet exchanging data across perimeters requires bilateral mapping and negotiation. Friction scales with every additional participant.

An **interoperability layer**—a virtual umbrella of shared assets (schemas, code lists, APIs, conformance tests)—breaks that pattern.

Table 4: The three layers of a trusted and interoperable digital trade ecosystem

Layer	What it contains	Why it matters
Applications	Shipping portals, LC processing tools, ESG dashboards, etc.	Compete and innovate freely.
Interoperability layer	• Common data definitions (e.g., KTDDE). • Globally portable identifiers (e.g., LEI/vLEI). • Reliability criteria and conformance tests (e.g., DSI Reliability Assessment).	Allows any two applications to exchange and verify data without bilateral customisation.
Legal & policy layer	MLETR, MLIT, data-protection rules, trade agreements.	Provides legal certainty and market signals.

It separates public interest standards and practices from *applications*, allowing innovation at the edge while keeping the core predictable, much as TCP/IP does for the Internet.

What TCP/IP does for the Internet

TCP/IP does two main things:

1. **IP:** IP breaks information into small packets, gives each packet a unique address, and sends them across various types of networks (like local, satellite, fibre-optic, or wireless) to their destination.
2. **TCP:** Once the packets arrive, TCP puts them back together and makes sure everything is in order. It checks for errors and resends any missing packets, so the information is complete and reliable.

By separating these tasks—sending packets (IP) and ensuring reliability (TCP)—and keeping them independent of the hardware used, TCP/IP allows any application to communicate with any other, no matter the vendor or network type.

The KTDDE catalogue maps each element to global data models such as UN/CEFACT, UBL, GS1, SWIFT MT and the WCO Data Model. Building on that foundation, each KIG converts the mappings into *executable artefacts* so developers can integrate once and interoperate everywhere. **In effect, KTDDE catalogues the common vocabulary and KIGs supply the phrase book, allowing solutions to keep their own schemas yet speak a language every other solution understands.**

Why KIGs matter: Without them, every implementer must decode multiple standards and build their own mapping tables. KIGs provide an "off-the-shelf" blueprint, cutting weeks of analysis and ensuring that even incremental upgrades remain KTDDE-consistent.

4.2 An integrated, stakeholder-driven roadmap to an interoperability layer

Table 5: Sequenced workstreams for building an interoperable digital trade layer

Sequenced workstream	Core question	Immediate deliverables	Content owners
a. Supply-chain mapping	Which documents and data flows matter most?	Prioritised list of high-impact documents (title, regulatory, finance).	Traders, logistics providers, regulators.
b. Interoperability by design	How do we align data models **before** new projects launch?	**KIGs**—one per priority document. Each KIG maps existing standards (UN/CEFACT, UBL, etc.) and prevailing market practices to KTDDE data elements, shows field-by-field "crosswalks," and provides JSON/XML examples that developers can drop into code bases.	Standards bodies, platform providers, ERP vendors.
c. Trust infrastructure	How do parties prove "who, what, when" across systems?	Wider adoption of digital identity; a common certificate profile for e-signatures; assessment frameworks and maturity models that platforms and end-users can pass once and reuse globally to signal readiness to trade digitally.	Certification entities, tech vendors, regulators.
d. Outcome-driven collaboration	How do we scale what works?	Cross-jurisdiction pilots using KIG templates and shared KPIs; feedback loop into KIG revisions and national single-window upgrades.	Public-private consortia, MDBs.

In short:

- **Supply-chain mapping** pinpoints *where* to focus.
- **KIG-enabled interoperability** design shows *how* to align data from day one.
- **Trust infrastructure** lets every system verify *who*, *what*, *when* without bilateral audits and due diligence.
- **Outcome-driven collaboration** turns guidance into scale, ensuring each new pilot validates and strengthens—rather than fragments—the global interoperability layer.

4.3 Why this can start now

- Legal foundations (MLETR, MLIT) cover the "can we?" question.
- KTDDE + KIGs answer "what and how do we align?"
- The "verify once, use many" path is being articulated through open assessments such as the Reliability Assessment Framework and its corollary, the Digital Trade Readiness Assessment framework in development.

If sectoral bodies, governments and solution providers adopt the four workstreams as a shared plan of record, a fully interoperable trade network is achievable in the near term.

5. Towards an integrated digital-trade ecosystem—From scattered digitisation to continuous, trusted data flow

5.1 Three interoperable routes— context determines choice

The heterogeneity of the current trade digitalisation landscape—marked by divergent development and adoption rates—calls for three basic approaches to interoperability.

Table 6: Interoperability in practice: Three KIG-enabled routes for data exchange

Route	When to use it & how it works (KIG-enabled)
1. Converge on a single e-document standard	**When to use:** This route is best when the user community is fairly uniform and there are strong incentives to use the same standard, such as in eBLs under organisations like BIMCO, DCSA, and FIATA. **How it works:** Stakeholders agree on one "reference" schema, publish guides for transitioning to the new standard, set timelines for phasing out old versions, and validate data against KIG where needed to ensure every system retrieves the same authoritative data set.
2. Align shared data fields across co-existing standards	**When to use:** This route is suitable when multiple standards continue to exist, but the important data fields overlap, such as in UBL invoice and ERP-system generated invoices. **How it works:** Each message keeps its original format, but common fields (like HS code, quantity, currency) are standardised according to KTDDE definitions. KIG cross-walk tables and sample data sets help developers map these fields once and reuse them, allowing systems to convert only the format, not the data itself.

3. Bridge semantically through a canonical layer	**When to use:** This route is practical when different standards are legally required or deeply embedded, such as insurance certificates or customs bonds that vary by jurisdiction. **How it works:** A canonical model, documented in the relevant KIG, acts as a "pivot language." Source data is mapped into this canonical form, checked for accuracy, and then converted into the target format as needed.

Choosing a route is context-specific: **converge** where momentum exists, **align shared fields** where quick wins are available, and **bridge** where convergence is impractical. All three options rely on the same KTDDE semantics and KIG implementation guidance, ensuring that each project strengthens the overall interoperability layer rather than fragmenting it.

5.2 Bridging tactics—what can be done in the next 12 months

Advancing digital trade does not require waiting for every system and process to be fully overhauled. Practical, phased actions can begin immediately, unlocking value while building toward long-term interoperability and trust. Over the next year, market participants can drive meaningful progress through four bridging tactics:

- **Digitise priority documents:** Leverage existing platforms to digitise high-impact trade documents, guided by their respective KIGs. Focus first on documents that unlock efficiencies across multiple parties, such as commercial invoices, certificates of origin, and transport documents.
- **Pilot DNIs:** Test the creation, exchange, and settlement of DNIs within defined contractual guardrails. Early pilots help validate reliability and legal enforceability under frameworks like MLETR, while building organizational confidence.
- **Expose KTDDE-aligned APIs:** Encourage ERP systems, port community systems, and logistics platforms to expose APIs aligned to KTDDE standards. KIGs provide ready-to-use code samples that can accelerate development and reduce custom mapping.
- **Use AI/OCR as a transitional bridge:** Employ AI and OCR technologies to extract structured data from PDFs and scanned documents as an interim step. While not a substitute for native digital workflows, these tools can free trapped data and support incremental migration toward fully structured exchanges.

Digitalisation is not an all-or-nothing proposition. Legal frameworks such as MLETR explicitly recognises the possibility of switching between digital and paper formats for negotiable instruments. This flexibility means organisations can start by partially digitalising their processes, such as creating a bill of exchange digitally, while retaining the option to produce a paper version for specific stakeholders or workflows if needed. Building hybrid readiness ensures immediate operational benefits while laying the groundwork for full digital maturity over time.

Parallel to harmonising data structures through the KTDDE framework and its implementation guides, the next critical requirement is embedding trust at the data level. In the physical world, possession of an original paper document provided assurance of authenticity. In the digital world, we need mechanisms that ensure authenticity, integrity, and exclusive control across networks, technologies, and jurisdictions. Trust must be embedded as an attribute of the data itself, not left to depend on the characteristics of the network transporting it.

6. Digital trust at scale—turning assurance into an ordinary feature of every transaction

In the digital trade ecosystem, ensuring trust and authenticity is crucial. One way this is achieved is through the use of digital signatures linked to LEI or vLEI. These signatures are timestamped and logged, allowing any supply chain partner or regulator to independently verify the content without needing to contact the issuing platform directly. This process ensures that the data remains secure and unaltered throughout its lifecycle.

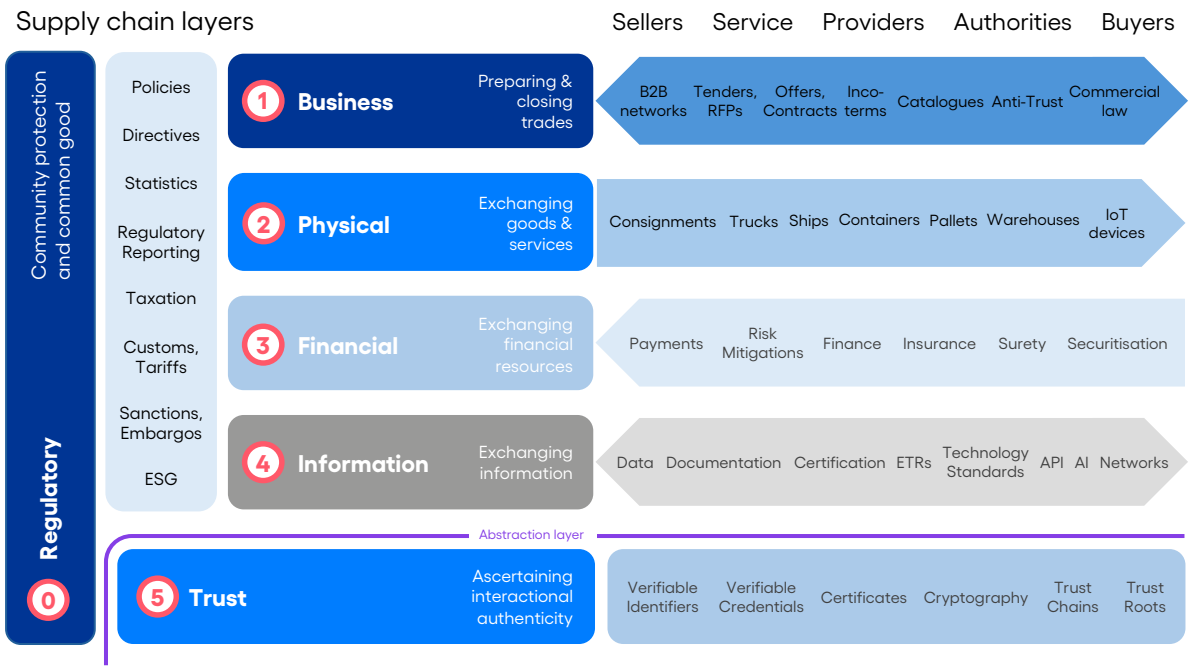
Another important enabler of digital trust at scale is the DSI Reliability Assessment, which provides a standardised framework for electronic trade document platforms to demonstrate their reliability. Unlike digital signatures, which authenticate individual documents, this assessment focuses on platform-level assurance, ensuring that ETRs are managed with integrity, singularity, and exclusive control.

If platforms and ETR services evidence their technical and legal compliance through the Reliability Assessment Framework, any users of these platforms can also evidence their readiness to trade digitally through the Digital Trade Readiness framework under development (expected completion December 2025). The framework allows users to demonstrate their ability to manage digital trade documentation, data, and related processes.

Application of these frameworks work towards a trust supply chain, where trust is embedded in every transaction, minimising costs and complexity for all participants. By building out this trust infrastructure, we can ensure that digital assurance becomes a standard feature of every transaction, fostering a more secure and efficient global trade environment.

6.1 What a "trust supply chain" covers

Figure 6: Unpacking interdependent layers of the global supply chain



Source: Principles for Digital Trust (ICC DSI, 2023)

The graphic above unpacks several interconnected layers of the supply chain, which include:

1. **Regulatory layer:** This layer involves policies, directives, standards, taxation, customs tariffs, environmental, social, and governance (ESG) principles, and community protection. It sets the rules and guidelines that govern trade and ensures compliance with legal and regulatory requirements.
2. **Business layer:** This layer focuses on preparing and closing trades. It includes B2B networks for sellers, tenders/RFPs for service providers, and commercial law. It ensures that business transactions are conducted efficiently and legally.
3. **Physical layer:** This layer deals with the physical movement of goods across the supply chain. It involves consignments, trucks, ships, containers, pallets, warehouses, and IoT devices. It ensures that goods are transported and handled properly.
4. **Financial layer:** This layer concerns the exchange of payments and risk mitigation measures. It includes credit assessment, loans, risk management, factoring, and securitisation. It ensures that financial transactions are secure and reliable.
5. **Information layer:** This layer pertains to the exchange of information. It involves data, documentation, certification, and APIs. It ensures that information flows seamlessly and accurately across the supply chain.
6. **Trust layer:** This bottom layer is about ensuring the authenticity of interactions. It includes verifiable identifiers, credentials, certificates, cryptography, and trust anchors. It ensures that all interactions within the supply chain are secure, authentic, and trustworthy.

Digital identity is a fundamental element in the trust layer of the supply chain. It identifies counterparties, organisations, objects, processes, and algorithms in a cryptographically secure, timeless, and unambiguous way.

In addition to proving identity, digital identity can secure any digital content—called payload—by placing it into a digital container and signing it with the originator's digital credentials. The receiver of such digitally signed content can be certain that both the origin and the content are authentic and have not been altered. This is similar to placing a document in an envelope and sealing it in the traditional world. This concept is foundational for digitalising trade, securing content, and preventing fraud.

Digital identity can be conferred by governments or private organisations. Examples include digital credentials, such as ID cards issued to citizens. Governance is ensured by law, and government-conferred credentials can be used as legal proof in disputes. Private organisations issue credentials tailored to specific use cases or platforms, such as access cards with embedded chips or public-private key pairs for blockchain use.

While digital identity systems may raise market concerns such as hacking and data breaches, these risks are well understood and can be effectively mitigated. With the implementation of widely adopted safeguards—such as cryptographic encryption, role-based access control and multi-factor authentication—digital tools can be deployed securely. These measures ensure that only verified users can access or act on digital trade documents, strengthening security and building trust in the overall system.

Both public and private sector digital identity schemes have a key limitation: they only work within the boundaries of the respective issuer. For example, a Japanese e-Seal cannot be used for signing trade documents abroad without a bilateral trade treaty, and most national digital identities cannot be used as international credentials.

There is a need for interoperable, global identity schemes in trade.[17] Examples include GS1's product credentials based on the GTIN and GLEIF's digital credentials based on the LEI. Both are globally available and interoperable.

GLEIF's vLEI enables clear identification of business organisations and individuals acting on behalf of a legal entity. It supports digital delegation of authority, allowing roles like CEO or Head of Accounting to be verified digitally. The vLEI system also allows for multi-signature verification, providing a complete and trustworthy representation of organisational interactions.

6.2 From principles to practice—applying MLIT and MLETR

- UNCITRAL's **MLIT** defines "reliable" trust services in functional terms, avoiding technology mandates.
- UNCITRAL's **MLETR** states that systems handling ETRs must guarantee singularity, integrity and exclusive control.

Neither model tells providers *how* to achieve those outcomes. To close that gap, the ICC Digital Standards Initiative and Canada's Digital Governance Council published the **Reliability Assessment Framework**—a checklist of technical and organisational controls (e.g., key-management, auditability, change management) against which a platform can be assessed once and then reference the result in multiple markets.

Why these matters:

- **Regulators** gain a common yardstick without prescribing vendors or algorithms.
- **Service providers** avoid duplicating evidence packages country-by-country.
- **SMEs** can trust that a platform certified under the framework meets baseline expectations without commissioning legal opinions.

Table 7: Technology-neutral mechanisms to operationalise legal trust requirements in digital trade

Need	Digital mechanism (technology-neutral)	Why it matters to trade
Prove identity—*Who is acting?*	Globally portable organisation identifiers (e.g., LEI) and role-based credentials issued by a recognised authority.	Removes ambiguity, automates KYC/AML screening, supports cross-border recognition.
Prove integrity & authenticity—*What exactly was sent?*	Electronic signatures or seals generated with public-key cryptography; hash values included in the message.	Makes tampering detectable; provides legal evidence equivalent to a wet signature.
Prove timing & sequence—*When did it happen?*	Trusted timestamps and tamper-evident audit logs.	Supports performance SLAs, limitation periods and customs deadlines.
Prove exclusive control of ETRs	Transfer tokens or registry logic that ensures only one party controls the original at any moment.	Satisfies **MLETR** requirements of singularity, integrity and control—the digital equivalent of holding the paper original.

17 The new UN/CEFACT project called "Global Trust Registry" (GTR) takes a different approach. It defines a way for existing identity registers to issue digital credentials that other nations can trust, similar to passports and the ICAO Public Key Directory (PKD). Each country issues its own credentials in a standard format, and GTR maintains a list of trusted schemes, allowing businesses to leverage existing registrations.

6.3 Recommended next steps for market participants

Three coordinated steps will bring us closer to digital trust at scale.

1. **Clarity on the components of "interoperability-ready":** (i) KIG-conformant data structures, (ii) identity markers that are globally interoperable (e.g., LEI/vLEI) and (iii) connectivity to a trust service that meets legal and technical requirements as set out in an open standard (e.g. Reliability Assessment).
2. **Staged maturity pathways** (e.g., "bronze/silver/gold") so organisations can adopt trust services incrementally—for instance starting with signed PDFs, moving to structured KIG payloads, and finally to tokenised ETRs.
3. **Official recognition**—through customs circulars, central-bank notices, or trade-agreement annexes—that data exchanged via a credentialled system enjoys legal effect comparable to paper.

Taken together, these steps allow trust to become an *attribute of the data itself*, not a privilege granted only to parties inside a closed network.

What follows is not just more reliable data, but smarter liquidity. Next-generation SCF platforms will do more than exchange documents. They will extract structured invoice data, generate DNIs, and link that data to real-time settlement status.

This is transactional intelligence in action. It enables liquidity to flow automatically from verified trade events. Banks and financiers can fund, monitor, and reconcile transactions as they happen—finally bridging the historic disconnect between goods, documents, and capital.

7. Governing digital trade for the long term—keeping the system coherent as it scales

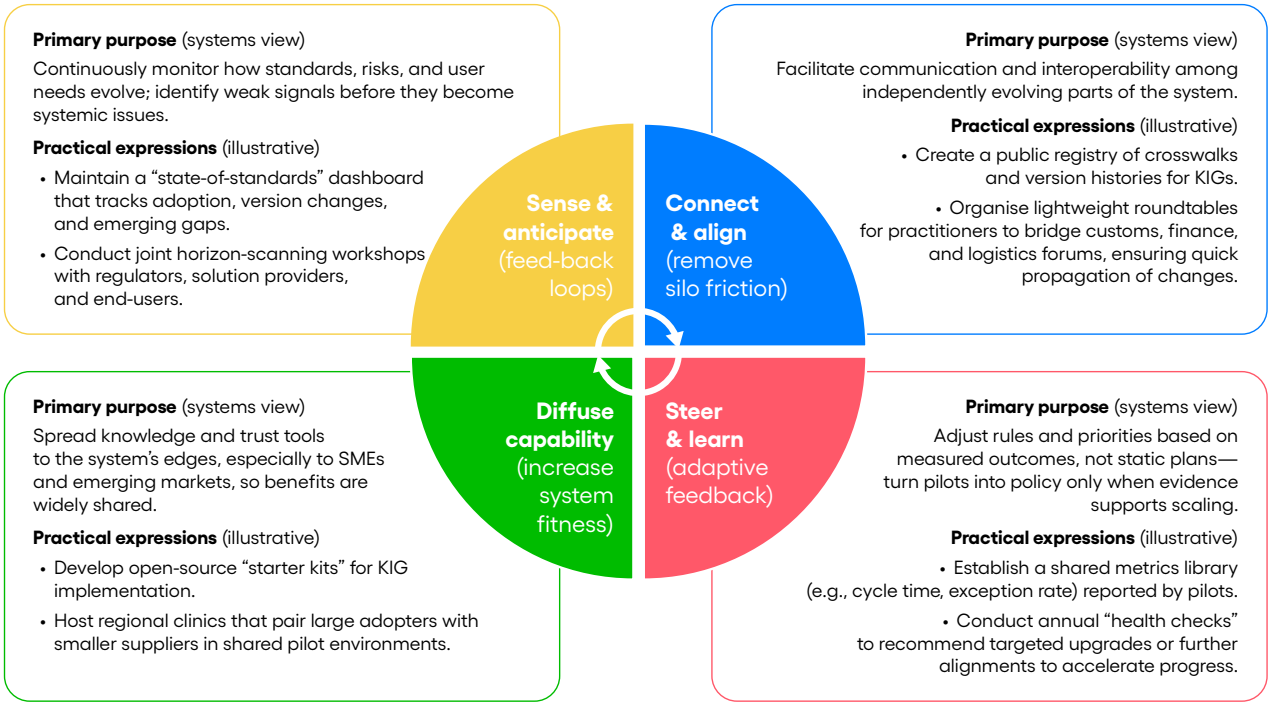
Digital trade is a complex, adaptive system: thousands of actors, multiple feedback loops and continuous technological change. Effective governance therefore resembles *gardening more than engineering*—creating the conditions for healthy growth rather than dictating every branch.
To succeed, governance must be:

- **Inclusive:** It should bring in SMEs and emerging markets, ensuring that all participants have a voice and can benefit from digital trade.
- **Adaptive:** It must update protocols as technology evolves, allowing the system to remain relevant and effective in the face of rapid change.
- **Coordinated:** It should avoid duplicative or competing efforts, ensuring that all initiatives work together in a coherent and complimentary manner.

7.1 Four core functions of stewardship

Borrowing from systems-thinking practice, we frame governance around four **functions of stewardship**, each aimed at reinforcing virtuous cycles and dampening fragmentation.

Figure 7: Four core functions of stewardship



Source: Digitalising global trade: A roadmap for achieving interoperable, inclusive, and trusted trade (ICC, 2025)

Why these matters:

- Systems thinking shifts governance from *command-and-control* to *coordination-and-adaptation*, recognising that leverage often lies in feedback loops (e.g., transparent metrics) and connectors (e.g., crosswalk registries).
- By sensing, connecting, diffusing capability and steering adaptively, the governance layer keeps the data and trust layers—outlined in Sections 4-6—coherent without stifling innovation.

This approach does **not** prescribe a single lead agency or rigid roadmap. Instead, it provides a set of stewardship roles that any coalition—public, private or mixed—can adopt and adjust as the digital-trade ecosystem matures.

Just as the Internet relies on TCP/IP, digital trade will rely on **light-touch but continuous governance**: version control for data models, dispute-resolution rules for trust-service reliability, and living *crosswalks* so new versions never break old integrations.

Table 8: Horizon view: Key milestones and transformational outcomes in digital trade

Horizon	Milestones	Visible change
0-2 years	Priority documents digitised with KIGs; +20 platforms pass Reliability Assessment.	Operational costs fall; processing times shorten; trade volumes increase.
2-5 years	ERPs embed KIG APIs; 50% of payments carry LEI/vLEI.	Data pre-populates customs and financing screens.
>5 years	Machine-readable data flows end-to-end; trust verified automatically.	"No-touch" trade: goods clear and funds settle based on data, not files.

With legal scaffolding, a common data layer, and a "verify once" trust framework in place, the ecosystem already has 80% of the puzzle. The remaining 20% is coordinated adoption—work that begins, not ends, with the roadmap outlined above.

8. Conclusion: A call to action

The building blocks of digital trade are falling into place. What is needed now is **alignment in execution**. This paper has presented a roadmap for:

- Mapping key documents and shared data
- Embedding trust and interoperability into systems
- Piloting real-world use cases and scaling success
- Governing the ecosystem to ensure sustained, inclusive progress

What remains is **coordinated execution**. Because trade is a **system of systems**, progress depends on many actors reinforcing one another rather than working in isolation. The sections below translate that systems view into near-term priorities for each stakeholder group. These suggestions build on the roadmap laid out earlier and span both individual actions and collaborative initiatives. They are neither exhaustive nor strictly prioritised, but intended as a menu for engagement tailored to each stakeholder's capabilities, incentives, and influence.

8.1 Governments, trade policymakers and multilateral development banks

Legal certainty and modern public infrastructure are the platform on which private investment is built. National authorities and MDBs therefore carry the system-level responsibility for turning global principles into enforceable, day-to-day rules:

- **Anchor domestic law to recognised international models:** Align statutes with the UNCITRAL MLETR and prepare to incorporate the forthcoming Convention on Negotiable Cargo Documents so rail and road shipments gain the same legal clarity as maritime trade.
- **Treat digital trade as a whole-of-government programme:** Because data moves across customs, finance, transport and innovation silos, a cross-agency task-force—Australia's Simplified Trade System offers a template—should own policy coherence, allocate budgets and track progress against a single roadmap.
- **Upgrade border systems for data, not documents:** When modernising a National or Regional Single Window, embed KTDDE mission-critical fields and publish an API that accepts KIG-conformant payloads. The WCO Digital Customs Maturity Model, Single Window Interactive Map (SWIM) country dashboards and the GNC framework all provide diagnostics and reference implementations.
- **Prove concepts via corridor pilots before scaling nationwide:** Digital chapters in bilateral or regional agreements allow two administrations to test the full stack—KIG data structures, reliability-assessed platforms, mutual recognition of trust services—then extend what works. Singapore's network of digital economy agreements shows the acceleration possible when pilots and policy travel together.
- **Enable globally portable business identity:** National business registration and digital identity systems should align with international standards, such as the Global LEI System, to facilitate the unique identification of businesses across borders. Making such digital identities genuinely portable means embedding them in key trade processes like customs declarations, licensing

portals and trade-finance messages, or working towards interoperability between nationally bound digital ID systems and global frameworks.

- **Pair legal reform with funding for capability building:** Grants for training, sandbox licences and SME onboarding—be they under WTO's Third Country Training Programme, bilateral trade corridor development programmes, or sector-specific training resources —ensure smaller traders can comply with the same standards as multinationals.
- **Use multilateral development banks as catalysts, not just financiers:** MDBs can embed digital-trade milestones in policy loans, co-fund national interoperability roadmaps and back neutral, open-standards platforms. Their convening power helps keep reforms transparent, balanced and adaptable as technology evolves.

8.2 Standards development organisations

To effectively support digital trade, SDOs must position standards as a single, navigable ecosystem rather than a catalogue of separate artefacts. Global trade relies on horizontal foundations (ISO, UN/CEFACT), sector-specific extensions (DCSA, BIMCO, FIATA), and cross-cutting identifiers (GLEIF, GS1). Senior SDO leaders should present this landscape to markets as one coherent "map," making it clear which specification to use and how each relates to the others. Visibility, not additional documents, is the first accelerant of adoption:

- **Provide decision-makers with confidence in predictable evolution:** Company boards and ministries invest in digital trade only when they know today's choices will remain valid tomorrow. SDOs can create that confidence by committing publicly to clear, principle-based change management: advance notice of significant updates, explicit rationales for any discontinuity, and transitional guidance that protects past investments.
- **Anchor coordination in outcome-driven alliances:** Initiatives such as the FIT Alliance and the UNECE-ICC Joint Call to Action already convene the right actors; what executives now need is a concise, shared roadmap that lists the next synchronisation milestones— for example, completing a common data spine for transport and finance documents—so resources and political capital can be deployed against a visible timetable.
- **Focus alignment efforts on high-impact commonalities:** Perfect convergence across every data field is unrealistic and unnecessary. By concentrating first on elements that unlock the greatest network effect—entity identifiers, product codes, location references and core trade dates—SDOs deliver immediate systemic value while preserving room for sector-specific innovation.
- **Underwrite adoption with clear, non-technical guidance:** Executive teams and regulators require short, concept-level briefs—why a standard matters, where it fits, what benefits it secures—rather than schema diagrams. Issuing such guidance alongside technical releases ensures that strategic decisions keep pace with technical progress, closing the last mile between standard setters and market uptake.

8.3 Financial institutions, credit insurers and trade finance innovation

Banks, fintechs, and FIs are crucial for building digital trust, funding innovation, and bridging the trade finance gap. When banks and fintech platforms accept digital bills of lading or electronic invoices, the rest of the market follows; when they reject them, paper persists. Their strategic importance in any digital trade agenda cannot be overstated:

- **Adopt a common data language:** This is the most immediate lever to unlock liquidity and efficiency gains available to the sector. Banks have historically relied on proprietary data formats and closed systems. The KTDDE shows that just seven key trade documents provide 50–70% of the data needed for LCs, collections, and supply chain finance.[18] The ICC Banking Commission's *Bank-Defined Dataset* initiative translates those KTDDE elements into an operational "minimum viable payload" that satisfies bank requirements. Mapping internal schemas once to this shared dataset is far cheaper—and far more future-proof—than maintaining a patchwork of bilateral formats that must be rebuilt every time a new counterpart enters the picture.
- **Leverage global digital identity:** Global digital identity is now an asset for market access, not merely a reporting requirement. Embedding LEI or forthcoming vLEI codes in every trade message allows KYC and sanctions checks to run in near-real time, reducing onboarding friction and freeing compliance budgets for higher-value tasks. Jurisdictions that explicitly recognise LEI-tagged transactions will give their domestic banks a measurable speed advantage.
- **Embrace embedded finance:** The next competitive frontier is embedded finance delivered at the moment operational data are created. Pilots like the UK ETDA workflow, the BIS "Project Dynamo," and Hong Kong's Commercial Data Interchange demonstrate a future in which financing decisions are triggered inside a logistics or ERP system, not through a manual upload portal. For banks, this shifts the primary constraint on growth from balance-sheet capacity to data-processing capability.
- **Utilise richer operating data for broader, safer credit:** Richer operating data open the door to broader, safer credit—if risk models evolve to use them. Aggregated performance data—on-time shipment records, verified ESG metrics, chain-of-custody proofs—can serve as new proxies for creditworthiness, bringing deep-tier suppliers into the formal finance net. Institutions that treat these signals as first-class inputs, rather than exotic exceptions, will set the benchmark for inclusive trade finance.

By embracing shared semantics, portable identity and event-driven workflows, financial institutions can convert the technical assets described in this paper into the economic incentive that finally tips global trade from paper to digital.

Credit insurers, historically focused on protecting sellers against buyer default, are now positioned to become major enablers of digital trade. In a world of DNIs and structured supply-chain data, credit insurance can move from paper-based indemnity to real-time credit enhancement.

By digitally wrapping a bill of exchange or similar instrument with a guarantee (aval), credit insurers can transform a seller's receivable into a financeable, liquid asset—accessible even to small exporters and emerging-market suppliers. This lowers the credit risk faced by banks and alternative financiers, expands funding availability, and accelerates working-capital cycles.

Beyond individual guarantees, credit insurers could offer portfolio solutions that bundle trade receivables and digitally track risk exposure in real time—creating entirely new risk-transfer products for digital trade corridors. Together with MDBs, credit insurers can thus play a transformative role: not just mitigating risk but actively creating new liquidity for digital supply chains.

---

18 How can the trade finance industry create a digital ecosystem? Pamela Mar, Managing Director, Digital Standards Initiative, International Chamber of Commerce (ICC) explores how bridging trade and financial flows could be the key (Deutsche Bank, 2024). Available at https://flow.db.com/trade-finance/data-as-a-building-block-for-digital-trade-finance

8.4 Marine insurers and P&I clubs

Marine-risk insurers have a unique ability to normalise fully digital trade, but only if cargo underwriters and P&I clubs advance in tandem. Cargo insurers safeguard the value of the goods; P&I clubs cover the shipowner's third-party liabilities. These risk guarantees oil the logistics chain, and both must recognise electronic evidence with the same confidence they once reserved for paper:

- **Rally around a harmonised data core:** Cargo underwriters should rally around one concise, industry-endorsed data core for the insurance certificate and make it digitally verifiable. A harmonised field set—e.g. voyage particulars, insured value, commodity description, digital ID tagged parties—would let underwriters issue cover in hours rather than days, embed proof of insurance directly into shippers' digital workflows, and tap richer operational data for more accurate pricing. For clients, that means faster confirmations and simplified compliance; for insurers, it frees capacity now lost to manual checks and could expand addressable markets to include smaller and niche shipments.
- **Embrace electronic bill of lading platforms:** P&I clubs have already signalled a breakthrough by granting deemed approval to eBL platforms that meet recognised reliability tests. Doing so shifts the discussion from legal uncertainty to operational readiness and gives shipowners, charterers and banks a predictable basis for adoption.

Together, these moves would align risk cover with the digital documents and data flows now emerging across trade finance, customs and logistics. The result is systemic: lower documentation risk premia, faster policy issuance, and a trade environment where emerging-market shippers gain the same friction-free access to insurance and finance as their established counterparts—precisely the inclusiveness digital trade is meant to deliver.

8.5 IT infrastructure and corporate ERP providers

IT infrastructure and ERP service providers have the ability to ensure interoperability and connectivity of the "first mile" and "last mile" of any supply chain transaction. By enabling any company—especially those SMEs without the capacity to bilaterally configure every supply chain undergoing digitalisation—to generate globally interoperable data, IT infrastructure providers can enable scale, automation, and access to every company.

The key is to use system upgrades as opportunities to standardise any of the 189 core data elements which are either sourced or must be read by corporate ERP systems, thereby allowing them to be automatically connected to the trade process in a globally interoperable format.

8.6 Industry associations and chambers of commerce

Industry associations and chambers of commerce are uniquely positioned to convene, educate, and represent. They are often the connective tissue between governments, standards bodies, and the business community—particularly in sectors where large enterprises rely on extended networks of SMEs.

- **Set clear, sector-wide roadmaps grounded in commercial priorities:** By aggregating members' goals—cycle-time targets, regulatory deadlines, ESG metrics—associations can signal to solution providers and authorities which digital-trade capabilities matter most, reducing the risk of fragmented rollouts.

- **Convert pilot results into concise, reusable playbooks:** Whenever a digital-trade trial proves its worth—be it a cross-border eBL flow or a digitally signed inspection certificate—associations should capture the essentials in plain language: *who did what, under which legal basis, using which standards or tools*. Disseminating that knowledge lets peers replicate success without starting from scratch.
- **Scale capability across the entire supply chain pyramid:** Large brands already profit from digital efficiencies; the value multiplies when their SME suppliers and logistics partners join in. Sector bodies can broker group training, pool sandbox licences and coordinate vendor support so smaller firms clear the same digital-readiness bar as their larger customers.
- **Channel frontline evidence back into the standards and policy cycle:** Rather than advocating abstract positions, associations can feed concrete "what worked/what stalled" insights into standards meetings and regulatory consultations. This feedback keeps updates grounded in operational reality and guards against rules that inadvertently exclude newer or smaller market entrants.

By focusing on road-mapping, knowledge transfer, capacity building and evidence-driven feedback, industry associations can turn scattered initiatives into coherent, scalable progress—advancing digital trade for every firm that depends on global supply chains.

8.7 Key sectors and geographies in need of capacity building

A persistent digital divide keeps entire value chains on the margins of global commerce. The WTO estimates that one-third of the world's population still lacks meaningful internet access, and least-developed countries generate only 0.2% of global digital-services exports.[19] For labour-intensive sectors—agriculture, textiles, resource commodities—this gap translates into slower cycle times, lower margins and limited access to finance. Capacity—not technology—is now the binding constraint.

Yet these same sectors stand to gain disproportionately from digital trade. e-Phyto can shave days off perishable-food shipments; machine-readable rules of origin reduce compliance costs in garment supply chains; verifiable sustainability data raises the value of responsibly mined minerals. DSI's collection of 22 case studies[20]—ranging from the India-UAE fruits and vegetable exports corridor, Latin America's multimodal transport networks and the ASEAN Single Window's live exchange of e-Phyto certificates—demonstrates how replacing data with structured, verifiable data can reduce processing time by 80-90% and cut costs by up to 70%.[21]

The binding constraints tend to be organisational. Emerging-market traders report three recurring hurdles: 1) overlapping donor or vendor initiatives that pull in different directions; 2) limited pools of legal and data-governance expertise; and 3) regulatory patchwork (e.g., divergent rules across government agencies and processes, conflicting data localisation rules) that forces exporters to manage multiple playbooks and restrict cross-border data flows.

---

19 Digitally delivered services trade dataset (World Trade Organisation, 2025). Available at https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

20 ICC Digital Standards Initiative (DSI), Key Trade Documents and Data Elements on the Frontlines: Tracking the digitalisation of trade through 22 case studies, (ICC, 2024). Available at https://www.dsi.iccwbo.org.

21 ICC Digital Standards Initiative (DSI), Key Trade Documents and Data Elements on the Frontlines: Tracking the digitalisation of trade through 22 case studies, (ICC, 2024). Available at https://www.dsi.iccwbo.org.

Five capacity levers can unlock rapid, scalable progress:

- **Legal alignment with MLETR and related UNCITRAL Model Laws** gives traders confidence that an electronic transferable record will be recognised from origin to destination.
- **Standardised core data inside supply-chain systems, using KTDDE/KIG templates,** removes the need for small firms to interpret multiple formats.
- **Digital public infrastructure—identity registries, trust-service providers, cross-border data gateways—creates a level playing field** so SMEs can plug into global networks without prohibitive up-front cost.
- **Mainstreaming portable digital identities such as the LEI** enables automatic KYC/AML checks and lowers the documentation burden that keeps small suppliers out of formal finance.
- **Targeted training, sandbox pilots and peer-to-peer exchanges** convert abstract standards into workable routines, reinforcing technical adoption with human capability.

Multi-stakeholder engagement is the proven accelerator. Projects linking key players across public and private sector reach implementation stage much quicker than had each side tried to go it alone—because industry engagement, technology transformation and policy calibration need to happen in the same room.

Digital trade is expanding, but it must be inclusive and systemic to succeed. Focusing investment on the five levers above—while aligning them with the legal, data and trust architecture detailed in this paper—will turn isolated pilots into inclusive, system-wide gains in resilience, transparency and growth.

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

ICC Digital Standards Initiative

The Digital Standards Initiative (DSI) aims to accelerate the development of a globally harmonised, digitised trade environment, as a key enabler of dynamic, sustainable, inclusive growth. We engage the public sector to progress regulatory and institutional reform, and mobilise the private sector on adoption, implementation and capacity building.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo