Verifiable.Trade

Proposal for an Open-Source, Globally Interoperable Protocol for Trade and Supply Chains

ISTTP (International Secure Trade Transfer Protocol)

Verifiable.Trade Foundation – in formation
Basel, Switzerland, November 2024

Authors:

Hans J. Huber
Verifiable.Trade Foundation

www.linkedin.com/in/hansjhuber

Stephan Wolf
Verifiable.Trade Foundation

https://www.linkedin.com/in/stephan-wolf-9229b8105/

Contributors and Reviewers:

Shawn Butterfield	https://www.linkedin.com/in/shawn-butters-butterfield-63a47aa/
Stephane Canon	https://www.linkedin.com/in/stephanecanon/
Eva Chan	https://www.linkedin.com/in/eva-chan-a318aa110/
Daniel Cotti	https://www.linkedin.com/in/danielcotti/
Pascal Gottret	https://www.linkedin.com/in/pascal-gottret-207487195/
Felix Greve	https://www.linkedin.com/in/felix-greve-2a163544/
Georg Greve	https://www.linkedin.com/in/georggreve/
Gerard Hartsink	https://www.linkedin.com/in/gerard-hartsink-7340b920/
Oswald Kuyler	https://www.linkedin.com/in/oswaldkuyler/
Pamela Mar	https://www.linkedin.com/in/pamela-mar-874189/
Ivan Mortimer-Schutts	https://www.linkedin.com/in/ivan-mortimer-schutts-6b5b6/
Chad Pasha	https://www.linkedin.com/in/chadpasha/
Drummond Reed	https://www.linkedin.com/in/drummondreed/
Gianluca Riccio	https://www.linkedin.com/in/gianluca-riccio-cfa-749461a5/
Timothy Ruff	https://www.linkedin.com/in/rufftim/
Daniel Säuberli	https://www.linkedin.com/in/danielsaeuberli/
Chris Taggert	https://www.linkedin.com/in/countculture/
Randy Warsaw	https://www.linkedin.com/in/randywarshaw/

Table of content

Building the Future of Global Trade Digitalization

Management Summary

Global trade drives wealth creation and prosperity, enabling businesses worldwide to connect and collaborate. Yet, much of the essential documentation remains paper-based—the only universal protocol currently accepted by all parties.

Digitalizing trade and supply chains boosts efficiency, transparency, and resilience while reducing cost, operational risks, errors, fraud, and environmental impact. It enables real-time data access, global scalability, and integration with technologies like AI and IoT to meet modern market demands and drive competitive advantage. To unlock this business value from paperless supply chains, a modern, robust protocol is essential that is:

- Open, barrier-free, and inclusive, accessible to everyone without IP, copyright restrictions or asking for fees.
- Legally compliant, secure, and business-secret-focused, ensuring seamless collaboration between businesses and governments.
- Designed with organizational identity and authority delegation at its core, ensuring authenticity, end-to-end verifiability and the resulting automation capabilities between sellers, buyers, their respective service providers and governments
- Tamper-proof and auditable, providing reliable, court-admissible records.
- Entirely decentral with no central registries, ledgers or data bases.

We call this protocol ISTTP (International Secure Trade Transfer Protocol).

The Verifiable.Trade Foundation, a Swiss non-profit organization, is dedicated to advancing this vision. Through its support for open-source protocol implementation and libraries, the foundation invites global contributors to join its mission of creating a unified, digital framework for trade.

Introduction

Trade, both domestic and international, is the foundation of the world's economic systems. Global trade is entertained by countless participants[1], but even after more than four decades[2] in pursuit of paperless trade, interoperable solutions are still elusive. Today's trade still relies on a multitude of physical documents and electronic PDFs. This is slow, expensive, insecure, fragile and provides opportunities to fraudsters on multiple fronts. However, paper and paper substitutes like PDF have one major advantage: they provide interoperability and great flexibility. The paper processing protocol operates in the brains of the many involved, enabling everyone to trade with anyone else, peer-to-peer. However, all at the prices described above.

The political, legal, organizational, and technical challenges posed by going to machine-readable, digital solutions are significant. To achieve interoperability, changes are required on a multitude of layers; decades old practices require change and harmonization. Many believe that universal platforms, APIs, blockchains and centralized solutions are the way going forward. Monopolistic and oligopolistic platforms attempting the exchange of electronic bills-of-lading globally, global trade-finance platforms, and single-window solutions for customs are just a few examples of the trials to go digital. They all face very similar challenges, e.g.:

1. Will all market participants agree to use the same platforms?
2. If so, would this foster or impede healthy competition in the trade ecosystems (horizontal view)?
3. How can the risk be mitigated, that a central monopolistic platform provider is raising the prices later on (vertical view)?
4. Can these platforms achieve global, large-scale semantic interoperability?
5. Will the use of platforms further discriminate against small and medium sized businesses, especially in emerging economies?
6. Are market participants willing to share their trade data (and trade secrets) with platforms operated under foreign governance rules?
7. Who bears the costs and/or risks? Who has the benefits? Who has control?

---

1 The International Chamber Commerce claims to voice the interests of around 45 million businesses involved in global trade around the world.

2 In UNECE Recommendation 14 ("Authentication of Trade Documents") UN/CEFACT refers to its predecessor, the "Working Party on Facilitation of International Trade Procedures" and its ninth session in March 1979. In this session discussions were held about "Authentication of Trade Documents By Means Other Than a Signature" (document TRADE/WP.4/INF.63, TD/B/FAL/INF.63).
See: https://unece.org/sites/default/files/2023-09/Rec14-ECE_TRADE_C_CEFACT_2014_6E.pdf

8. Are the platforms' underlying technologies future-proof. Are they using data standards of international standard development organizations?
9. How are changes made to these platforms and agreed upon by their users?
10. How is the market addressing the significant surge in fraud and scams today? Will platforms help to break this trend or contribute to further escalation, fueled by the proliferation of fake documents and messages generated by artificial intelligence?
11. How are acting parties in digital trade being identified, be it organizations or people? Are these mechanisms legally valid in all jurisdictions? Are these mechanisms conductively standardized to allow for low-threshold integration?
12. Can natural persons be reliably identified and verifiably attributed to parties that they are representing and acting on behalf of?

Looking back to the dawn of the Internet teaches us some lessons. Invented as "Arpanet" by university researchers in 1969, the internet remained a niche for two decades. Inspired by its progress, centralized platforms, such as AOL, Yahoo and CompuServe, tried to build one-size-fits-all solutions for communication and information exchange. Ultimately, they all failed.

The internet revolution took off in the nineties with the availability of public domain, open protocols such as TCP/IP, HTTP, FTP, telnet, IRC, SMTP, POP and IMAP, among many more. These protocols created a plateau of communality for software developers to build upon. From this moment on, everyone could participate in the exchange of emails, access to websites, file-sharing, chats and alike, as long as the applications adhered to the internet protocol stack. Cloud computing followed with APIs, streaming of music and movies, digital assets, etc. Remarkably, each single solution was developed individually, controlled and owned by its creators. Technical, legal, and organizational diversity allowing for peer-to-peer access is the norm today.

This suggests that today's platform attempts have a high probability to fail. Especially in the Blockchain/DLT space this can be witnessed already. Many of the recent platform approaches in trade have collapsed: TradeLens[3] tried to digitalize the maritime container business and was given up. Marcopolo[4] and

3 In 2018, shipping conglomerate Maersk partnered with IBM to create TradeLens, a platform for sharing and streamlining shipping information across shipping partners, businesses, and different authorities. By 2019, the platform covered nearly half of the world's shipments of cargo containers. It was shut down in 2022. https://en.wikipedia.org/wiki/Freight_technology

4 Blockchain trade finance network Marco Polo is insolvent https://www.ledgerinsights.com/marco-polo-blockchain-trade-finance-insolvency/

we.trade[5] attempted to establish new risk mitigation and finance products around supply chain finance, but were discontinued, since network effects did not materialize. Contour[6] tried to build a platform to concert the business processes between the parties to Letters of Credit. Even though each of these efforts enjoyed support from many reputable banks, they did not succeed. The onboarding process (centralized registry), the permissioned / closed / centralized DLT and the need to use the specific interface without strong APIs are some of the obvious problems. There are more and more disappointments to be expected in future, despite the markets asking for the functions that the solutions were trying to provide.

Coming back to the challenges in trade, the authors suggest developing an equally open, public domain protocol stack on top of existing internet standards: the **International Secure Trade Transfer Protocol (ISTTP)**. Let's delve into the evolution of new protocols, addressing the critical layers of information flow and security.

Supply Chain Layers

Verifiable.Trade recognizes the need for universal but decentralized solutions that strike a balance between accessibility and confidentiality. Information is the most valuable commodity in the digital age, and the challenge lies in creating protocols that ensure confidentiality, security, data sovereignty and good governance while facilitating trade interactions underpinned by digitally seamless business processes between the participating parties - all in peer-to-peer fashion, enabling participants to keep custody of their data and share selectively.

The seamless operations between interconnected applications necessitate real-time authentication ("Who are you)?" and authorization ("Are you entitled to do this?"). Through this process, applications can validate the legitimacy of the information presented at the transaction layer, including its source and data access permissions. A novel trust layer, ensuring verifiability, must be built and commonly accepted to underpin the current information supply chain. This will constitute the trust supply chain.

---

5 we.trade, a blockchain-based platform for open account trade, has closed its doors after being unable to secure further investment to continue as a going concern. https://www.gtreview.com/news/fintech/we-trade-calls-it-quits-after-running-out-of-cash/

6 Digital trade finance consortium Contour is terminating its services, after being unable to raise sufficient funds from its bank shareholders to continue to sustain itself. https://www.gtreview.com/news/fintech/exclusive-contour-to-shut-down-as-bank-shareholders-pull-funding/

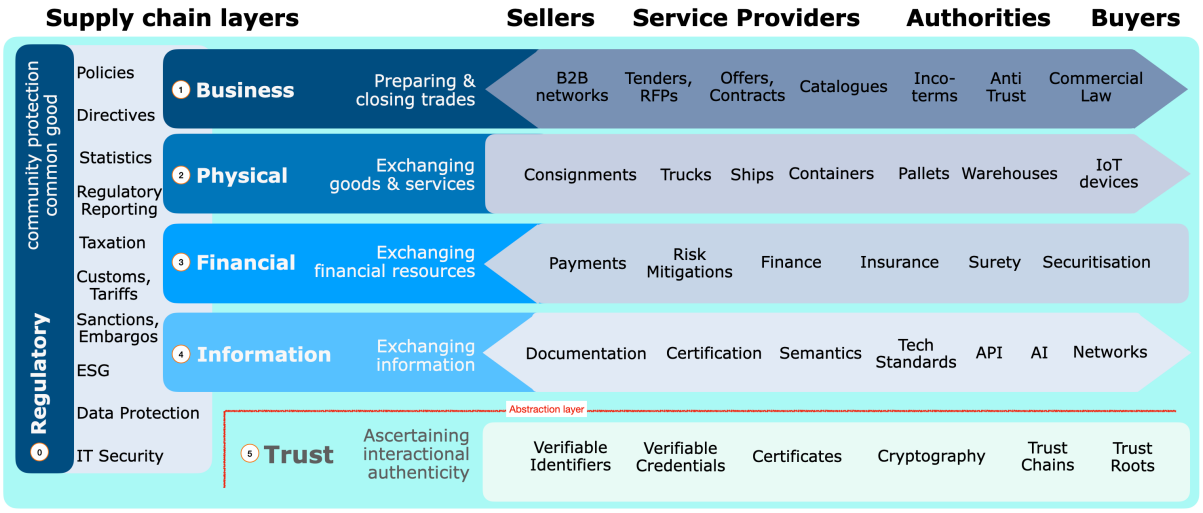


Figure 1: Supply Chain Layers (Source: ICC DSI)

When modeling supply chain logic, a layered concept is instrumental. According to ICC-DSI's Trust in Trade paper[7] supply chain layers are as follows:

- **Layer 0, the Regulatory Layer**, is focused on public administrative law and is emerging ever faster to serve all requirements that regulatory compliance brings about. A current rationale for the need for and the growth of this layer are customs single windows[8] and ESG requisitions. All authorities imposing laws, directives, rules, and policies, including customs, constitute layer 0. It spans all other layers as a vertical.

- **Layer 1, the Business Layer**, is where trade deals are prepared and closed. The fast-growing B2B networks offer space for product catalogues, allow for concerting of tenders, RFPs and Offers. This is where trade is increasingly prepared and executed. International contract law is located on layer 1. ICC offers solutions to these ends.[9]

- **Layer 2, the Physical Layer**, is concerned with the physical objects being handled while moving goods from origin to destination. From a distance and simplified, layer 2 could be seen as the logistics industry including inspections.

- **Layer 3, the Financial Layer**, deals with payments, risk mitigations and provision of financial elasticity, called trade finance. The flow direction of the financial layer is generally opposite to the physical layer. From a distance and

7 https://www.dsi.iccwbo.org/our-work
8 https://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/national-single-window/single-window.aspx
9 https://iccwbo.org/business-solutions/model-contracts-clauses/

simplified, layer 3 could be seen as the financial industry including insurance.

In response to the demand for interoperability without compromising security, Verifiable.Trade aims to establish open protocols for the fourth and fifth layer of the trading ecosystem.

- **Layer 4, called the Information Supply Chain**, represents the flow of information, and is a crucial aspect that traditionally relied on paper-based processes. Verifiable.Trade envisions a digital transformation where trade documentation can be exchanged in machine-readable form, maintaining the peer-to-peer nature of transactions while also addressing the needs of public sector authorities (B2B2G).

- **Layer 5, called the Trust Supply Chain**, focuses on the security and verification of authenticity. This applies to all data elements within a trade documentation as well as the organizations involved. The trust supply chain underpins and services all layers, 1 to 3 and especially layer 4, the information supply chain.

It appears imperative and conducive to abstract layer 5, trust, diligently from layer 4, information, to let data be and remain authentic, while traversing different applications in different networks.

Verifiable.Trade recognizes the importance of ensuring that digital objects are unique, and their data is current, meeting the legal requirements for digital transactions. By developing open protocols for security and verification following the Zero-Trust Architecture vision[10], Verifiable.Trade aims to foster trust and reliability in the digital trade landscape.

In its pursuit of developing open protocols – Zero Trust Protocols[11] - Verifiable.Trade aims to support existing standardization of public and private initiatives in the categories listed below.

A. **Policy standards of the public sector** such as the United Nations Sustainable Development Goals (SDG 9: Industry, Innovation and Infrastructure) or the Financial Action Task Force (FATF) Recommendations with International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

10 "Never trust – always verify" is the underlaying concept. Independent of the number of intermediaries or nodes, the data is always end2end verifiable.

11 Zero Trust security model: https://en.wikipedia.org/wiki/Zero_trust_security_model. See also: https://www.nist.gov/publications/zero-trust-architecture

B. **Public legislative standards (model laws)** such as the UNCITRAL Model Law on Electronic Transferrable Records, the UNCITRAL Model Law on Electronic Signatures, the UNCITRAL Model Law on Identity and Trust Management, the UNCITRAL Model Law on Electronic Commerce or the United Nations Convention on the Use of Electronic Communications in International Contracts.

C. **Private legal standards based on international private law** such as the ICC Incoterms 2020[12], the ICC Uniform Customs and Practice for Documentary Credits (UCP 600) and the Supplement for Electronic Presentation (eUCP) Version 2.0, the ICC Uniform Rules for Digital Trade Transactions (URDTT) and Industry Rulebooks and Master Agreements used for cross-border payments[13].

D. **Technical standards** from standards development organizations (SDOs such as ISO, GS1, OASIS, UN/CEFACT, VDA, IETF, etc.) covering identifier standards, data standards, message standards (like EDIFACT and ISO 20022) and/or security standards for the international supply chains.

The following chapters will delve further into the specifics of the ISTTP protocol stack being developed by Verifiable.Trade, exploring their features, benefits, and the impact they aim to have on the world of international trade. As we navigate the evolving landscape of digital trade, Verifiable.Trade strives to be at the forefront in providing open-source solutions that allow all trading partners, their trade service providers, and regulatory authorities to claim their interests by actively contributing. This should strengthen the overall security of the global trade ecosystem.

Sizing and scaling

Legal entities engaged in trade globally

Estimating accurate numbers of market participants or legal entities engaged in B2B trade and supply chains globally is complex due to the vast and dynamic nature of global markets. However, some statistics and estimates can provide a general sense of the scale:

12 Not yet machine-readable though
13 Ditto

1. **Small and Medium Enterprises (SMEs)**: According to the World Bank, there are around 400 million SMEs worldwide – from single farmers to mid-size corporations. A significant portion of these engage in B2B trade, either directly or as part of larger supply chains.
   This can be a carpenter in France, a small fishermen cooperative in Vietnam, or a family business canning peaches in Chile and employing 25 people, with a network of 15 farmers delivering fruit.

2. **Global Corporations**: There are several thousand large multinational corporations that dominate B2B trade in various sectors. The Forbes Global 2000 list includes the world's largest public companies, all of which are deeply involved in global supply chains. See also the OECD dataset of multinational corporates.[14]

   This can be a large multinational chemical cooperation (Du Pont, Dow Chemicals, BASF, Sekisui, ChemChina), large mining companies (BHP, Glencore, Anglo American, etc.), maritime carriers (Maersk, CGM CMA, Hapag Lloyd, etc.), food multis (Nestlé, Mondelez, Kraft etc.), traders (Lidl, Carrefour, Walmart, Seven Eleven, Tesco, etc.), or corporates from other industries.

3. **Registered Companies**: As of recent estimates, there are over 213 million registered companies worldwide. This figure includes all sizes and types of businesses, from sole proprietorships to large conglomerates, many of which participate in B2B trade. ICC assumes that around 160 million legal entities engage in international trade, either by selling or receiving goods and services. Exporters and importers use in general only a limited number of legal forms for their business operations. Typically, two or three legal forms per country are used.[15]

4. **Industry-Specific Participants**: Different industries have varying numbers of participants. For example, in manufacturing, retail, logistics, and technology sectors, millions of companies are involved globally. The industry building batteries for electric cars consists of a thread of specialized companies, starting from mining lithium ore, going to refineries, over to specialized chemical processing plants, cell manufacturers, and finally battery assemblers, before batteries are being built into vehicles in the car industry.

---

14 https://www.oecd.org/en/data/datasets/multinational-enterprises-and-global-value-chains.html

15 For a list of Entity Legal Forms see: https://www.gleif.org/en/about-lei/code-lists/iso-20275-entity-legal-forms-code-list

5. **Trade Networks and Platforms**: Numerous B2B platforms[16] and trade networks like Alibaba, Amazon Business, Temu, and the multitude of sector specific marketplaces have millions of registered businesses engaging in trade activities.

6. **Special purpose innovation consortia and foundations** pursuing goals like data sovereignty on data spaces, i.e. IDSA[17] on data sovereignty, data space endeavors in certain regions (GaiaX[18]) and sectors (CatenaX[19] in automotive).

To summarize, while exact figures are challenging to pinpoint due to the dynamic and broad nature of global trade, it is safe to estimate that there are over one hundred million market participants or legal entities involved in B2B trade and supply chains globally. Based on these figures, the assumption is that 120 – 160 million legal entities engage in cross-border trade. The amount of service providers, such as banks, logistic firm, shippers, etc. is estimated around 60.000 companies globally.

Documents in global trade

Global Trade is making use of paper and paper substitutes like PDF. How many documents are generated each year globally?

Estimating the total number of documents generated each year globally, especially in the context of global trade, involves considering various types of documents such as invoices, bills of lading, contracts, customs declarations, and more. While precise numbers are challenging to determine due to the vast and diverse nature of global trade, we can look at some key indicators and industry reports to get an idea.

Key Points to consider:

1. Volume of **Global** Trade:
   - The World Trade Organization (WTO) reported that the value of global merchandise trade was around $24 trillion in 2023[20].
   - The number of trade transactions can give an idea of the number of documents generated. Each transaction typically involves multiple documents.

16 Example Pharmaceutical: https://www.pipelinepharma.com, Example Metals: https://reibus.com, Example Ores and Alloys: https://www.metals-hub.com
17 https://internationaldataspaces.org/
18 https://gaia-x.eu/
19 https://catena-x.net/en/
20 https://www.wto.org/english/res_e/booksp_e/trade_outlook24_e.pdf

2. Digital **Transformation** in International Trade:
    - A significant portion of trade documentation is moving towards digital formats like PDFs, but paper documents are still widely used due to varying levels of digital adoption across countries and industries.

3. **Types** of Documents:
    - A single international trade transaction may involve dozens of documents, including invoices, packing lists, certificates of origin, customs declarations, and more.

Industry Estimates and Studies:

1. United Nations Conference on Trade and Development (UNCTAD):
    - Reports suggest that digitizing trade documents could **save billions of dollars** and significantly reduce the amount of paper used.

2. International Chamber of Commerce (ICC):
    - Studies indicate that the average trade transaction involves approximately **36 original documents** and **240 copies**, including regulatory filings and compliance documents.

Given these points, some rough estimates could be made:

- Suppose there are approximately 300 million international trade transactions annually (a conservative estimate based on various trade reports).
- If each transaction generates around 100 documents (considering both originals and copies), this will result in about 30 billion documents per year.

While exact numbers are challenging to pinpoint, a reasonable estimate is that global trade generates tens of billions of documents annually, encompassing both paper and digital formats. The shift towards digital documents like PDFs is growing, but paper documents still play a significant role in global trade documentation.

Trade Finance volume in global trade

Trade finance is a crucial component of global trade, facilitating the movement of goods and services across borders by providing necessary financial instruments and services. It bridges the finance with the supply-chain sectors. Trade finance is also requiring documentation, mostly on paper or PDF due to legal constraints

in many jurisdictions and the missing infrastructure and lack of standards to exchange the documents in a structured manner. The volume of trade finance can be examined through various lenses, including the value of trade transactions supported by trade finance instruments, the types of financial instruments used, and the institutions involved.

1. Types of trade finance instruments:
    - Letters of Credit (LCs)
    - Guarantees
    - Documentary Collections
    - Trade Credit Insurance
    - Export Credit Insurance
    - Supply Chain Finance
    - Factoring and Forfaiting

2. Institutions Involved:
    - Commercial Banks
    - Multilateral Development Banks (MDBs)
    - Export Credit Agencies (ECAs)
    - Insurance Companies
    - Funds, Private Equity

The World Trade Organization (WTO) estimates indicate that around 80-90% of global trade relies on some form of trade finance[21]. Given the global merchandise trade value was around $25 trillion in 2021, this implies that trade finance supports approximately $20-$22.5 trillion of global trade annually.

The ICC's annual trade finance surveys[22] provide detailed insights into the volume and trends in trade finance. For instance, the 2020 survey indicated a consistent demand for trade finance products, despite challenges posed by the COVID-19 pandemic. This trend continues.

Various market research reports, such as those by MarketsandMarkets[23] and Allied Market Research[24], estimate the trade finance market to be worth trillions of dollars. These reports often provide projections for market growth, influenced by factors like digital transformation and regulatory changes. The trade finance market is expected to grow due to increasing global trade volumes,

---

21 https://www.wto.org/english/thewto_e/coher_e/tr_finance_e.htm
22 https://iccwbo.org/news-publications/policies-reports/icc-trade-register-report/
23 https://www.researchandmarkets.com/
24 https://www.alliedmarketresearch.com/

advancements in financial technology (fintech), and the rising adoption of digital trade finance solutions.

It should be noted that Asian Development Bank (ADB) estimates a trade finance gap of 2,5 trillion annually[25]. It can be assumed that this is mostly a problem of SMEs. Further digitalization could widen that gap if technology doesn't make it easy and cheap to participate, especially for developing countries.
Trade finance encompasses a range of financial instruments and involves various financial institutions working together to facilitate international trade transactions. The market is poised for growth, driven by ongoing digitalization and evolving global trade dynamics.

The quantitative considerations enumerated above suggest that expected volumes having to be handled by Verifiable.Trade's ISTTP protocol must be

1. in the millions of trade data entry points,
2. capable to manage an overall throughput of billions of transactions on a yearly basis,
3. with probably a two-digit billion trade documentations issued and
4. up to a four-digit billion number of single interactions.

The decentralized architecture of the **ISTTP-Net** (International Secure Trade Transfer Protocol Network) allows for these volumes. All transactions occur peer-2-peer between so called Trade Data Gateways, which is explained below. There is no central repository, registry or load balancer necessary. The increase in Internet traffic is also manageable given modern network components. Some Trade Data Gateways will handle only a few transactions, while others may have to cope with millions a day.

[25] https://www.bloomberg.com/news/articles/2023-09-05/global-trade-finance-gap-at-record-2-5-trillion-says-adb

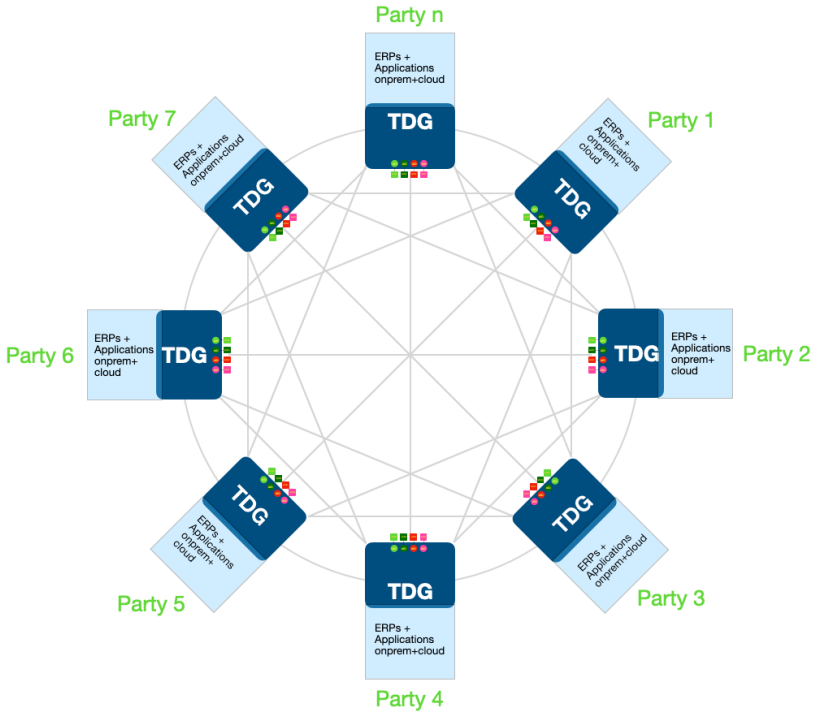


Figure 2: Peer-2-peer connectivity between Trade Data Gateways – the ISTTP-Net (International Secure Trade Transfer Protocol Network)

Verifiable.Trade protocols and architecture

The world is full of established technical solutions for a myriad of business requirements: Large ERP systems, accounting and management systems, dedicated software packages, cloud-based SaaS offerings, Blockchain, but also office software systems such as Word and Excel are a reality. This is not going to change soon and must be addressed by an innovative solution that can inject authenticatable security transparently between any business systems. The answer to these challenges is twofold:

1. Usage of protocols for the secure exchange of information,
2. Gateways bridging existing implementations

Verifiable.Trade suggests the development of open-source **Trade Data Gateways (TDGs)**. The TDGs entail the features below:

- Each counterparty to a trade has their own, open-source-based TDG, which they build or buy, operate themselves or have it operated by a service provider

- All TDGs speak the same standardized language to each other: Verifiable Credentials linked to Verifiable Identifiers.
- TDGs work globally: cross-cloud, cross-network, cross-vendor, cross-industry, cross-border.
- Trade instruments and the processes they support can be automated; and be spun across the limits of organizations to form a dynamic network for every trade, without having to onboard to a multitude of platforms. Connect once, connect to all[26]!
- Trade instruments of different providers can be programmatically interwoven. They form functional process networks based on protocols by being represented as configurable metadata. They get implemented through programmatic extension backed by a foundational, protocol-driven, framework.
- Identification of participants, be it legal entities, or natural persons on the Trade Data Gateways occurs following a global standard, so that authentication procedures enjoy legal validity in all jurisdictions. Like a wet ink signature today.
- Identification of objects, be it material or immaterial, occurs following suitable procedures, supporting full authenticity of data, even if further processed in a variety of downstream systems.
- Data that is exchanged between the trade peers remains predominantly in their own domains instead of being amassed in a variety of platforms.

The result: secure, universal verifiability[27] of trade instruments and their data elements and full data authenticity.

[26] Further considerations need to be done on permissioned sharing/data exposure implemented both in the protocol layer and down the stack within the network infrastructure layer. The TDG needs to be able to run in bastion mode. Externally accessible, untrusted by default, privileged escalation via federated authentication must be supported.

[27] Verifiability answers the question of who has produced data, it so makes data authentic. It does not ascertain the data being correct. In other words, if in a consignment of Paracetamol, the weight is specified as 4500kg and only 4200kg are being delivered, we only know who delivered wrong data.

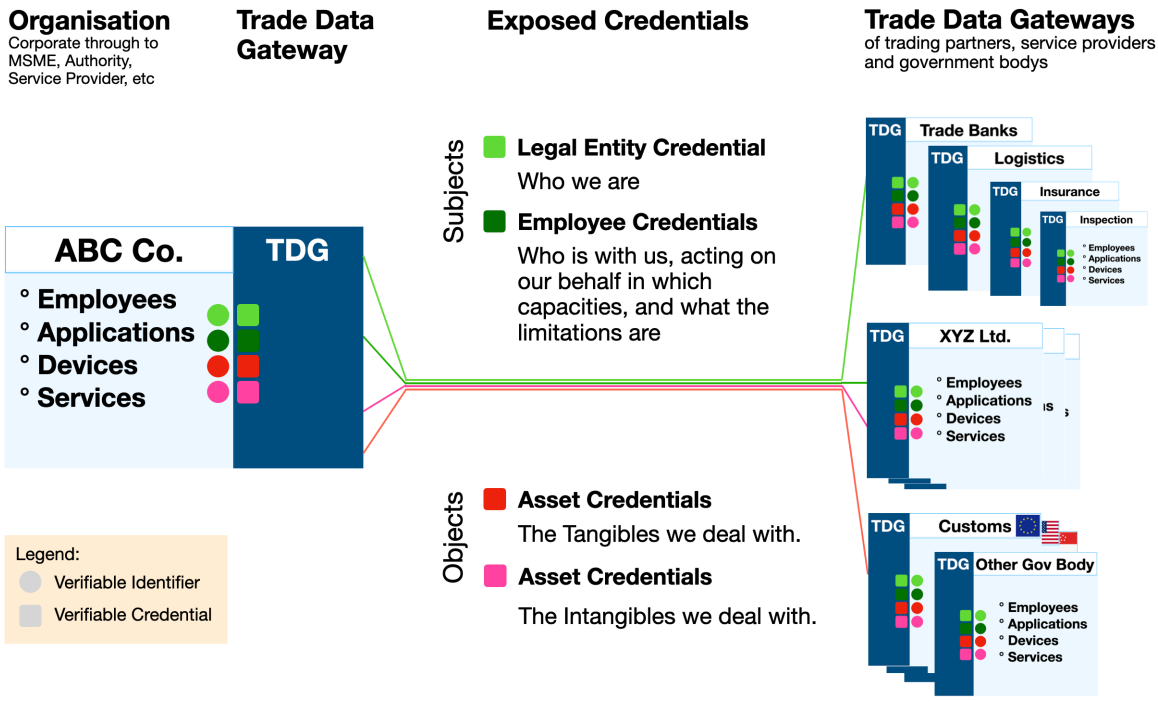


Figure 3: Schematic of an interwoven network of Trade Data Gateways for peer-to-peer credential exchange between a multitude of parties

At a very high-level, each TDG acts as a converter from internal systems installations to Verifiable.Trade protocols. First, TDGs understand the business language of existing trade applications, aka data models and external process flows. Second, the use of standards as recommended by the International Chamber of Commerce's Digital Standards Initiative (ICC DSI) will allow for the standardization of the payload in the message exchange protocol. As an example, an electronic bill-of lading (eB/L) will be converted to a verifiable bill-of-lading (vB/L) for the exchange between TDGs. The receiving TDG will receive and verify the data from the vB/L to store it in the existing systems. The same applies to all types of trade documentations, e.g. invoices to vInvoices, certificate-of-origin to vCoO, Letter-of-credit to vLoC, customs declarations (CD) to vC/D etc.

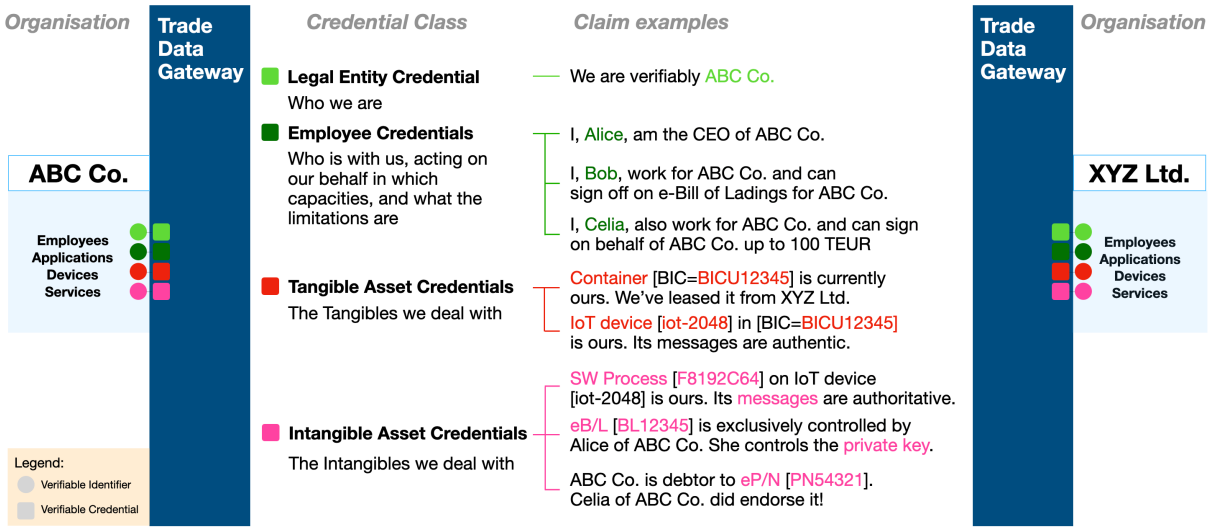


Figure 4: Credential Examples exchanged between Trade Data Gateways

It should be noted that the world has not agreed on one machine-readable standard per trade documentation type. Individual solutions differ in applying standards - often called competing standards. To the degree necessary, the TDGs will also convert messages between sender and receiver that follow different standards. The underlying protocol will act as a "universal translator", e.g. to map "e/BL" into "vB/L" without sacrificing legal constraints such as singularity of digital objects. This is why extensibility is pivotal to the TDG's basal functions. Without it, the open-source ecosystem is responsible for implementing every known translation and representation of eBL to/from vBL, including existing business system formats. That is not scalable or achievable. This extendibility is a challenging but doable task.

Amidst the myriads of trade documentations and instruments, another challenge hinders data exchange and the creation of cross-organizational process chains: the technical storage of data, particularly the notion of immutability. Blockchain has introduced a new set of protocols thereto, but often, in the pursuit of promoting certain projects, these blockchain initiatives are presented as "solutions" to minor issues, resulting in numerous separate data silos. This creates unnecessary complexity, becomes technically ever more expensive, and poses a detriment to all involved trade parties, service providers, platform operators, and regulators, who must navigate various blockchain protocols.

Trade would tremendously benefit from as few schemas as possible to store and transmit data in authentic and immutable fashion, aka within a single, well designed protocol stack. These protocols need to be conceived, developed, and maintained as open-source projects by those who have an interest in making trade less expensive and – as a result – more inclusive.

A digital peer-to-peer trade environment has the potential to evolve, that works similar to the current state of paper-based trade. This evolution would enable individuals to engage in transactions with anyone else, irrespective of the platform or legacy system in place. The adoption of suitable protocols would greatly enhance interoperability between current and future systems. As a consequence, many currently struggling platforms could experience substantial business volume increase and have the opportunity to finally leverage their investments in service functionalities.

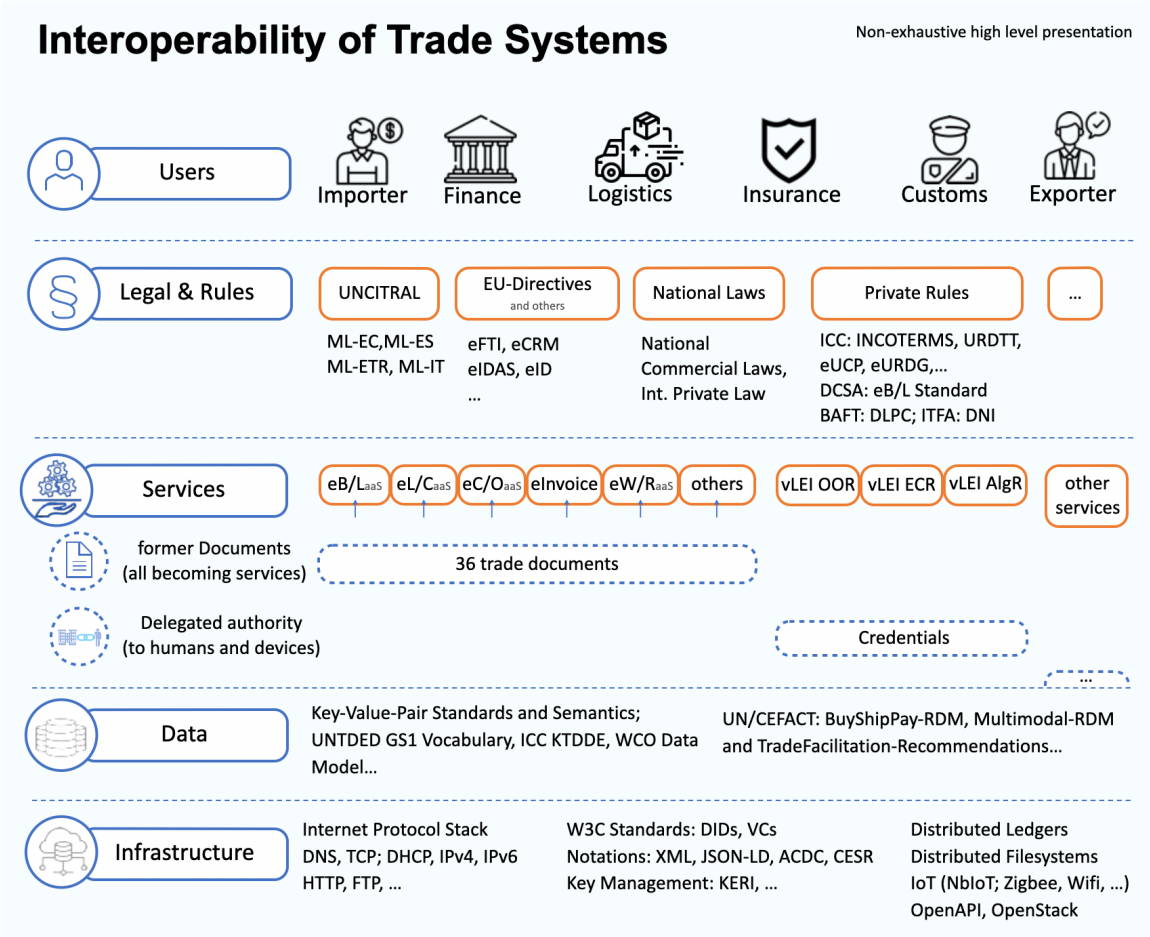


Figure 5: Simplified layered approach on potential interoperability of Trade Systems

Verifiable.Trade will extend the internet protocol stack upwards with protocols suitable for the common business processes in trade. This is called the "Trust Spanning Protocol"[28].

28 https://miro.medium.com/v2/resize:fit:2000/1*bk12Iykg8a25flQ1t12rVQ.png

Verifiable.Trade handling of message payload

Each documentation in trade consists of a set of related data elements. Standards for machine-readable representations are called taxonomies when strictly hierarchical or ontologies when multiple relations can be expressed. Both can be modeled as directed acyclic graphs. Nodes in the graph represent either autonomous scalar data elements (e.g. name of a product) or locally combined groups of data elements (e.g. product description, address information).

Data element assemblies as nodes in subgraphs

The Verifiable.Trade Trade Data Gateways will disassemble and in certain cases re-assemble trade documentations by using these nodes. The implementation will use digital data containers to store and secure each node separately. The entire documentation of a trade is then a compound of connected containers which are systematic, consistent, unique, unambiguous, singed, and secure. Trade documentations can then be exchanged and updated between the Trade Data Gateways peer-to-peer. Also changes to only parts of the documentation of a trade will be updated directly between TDGs, timestamped, historized, while ascertaining full data integrity. Relationships between the data element nodes will be maintained as part of the underlying technology for building those containers. Those relationships could manifest as part-of relationships as well as references. Referential integrity and consistency will be maintained on the protocol layer.

This architecture allows not only for the sending and receiving of digital trade data. It also allows for local memories at each side of the transaction. The sender knows exactly what has been sent while the receiver has a repository of all received data elements. This will allow audit trails for external or internal inspections. It can also be used for allowing 3rd party access with selective disclosure if and when the 3rd party also entertains an TDG or supports the protocols natively. Of course, if access to data is granted outside this protocol, consistency and security must be managed by both parties differently and under their own control.

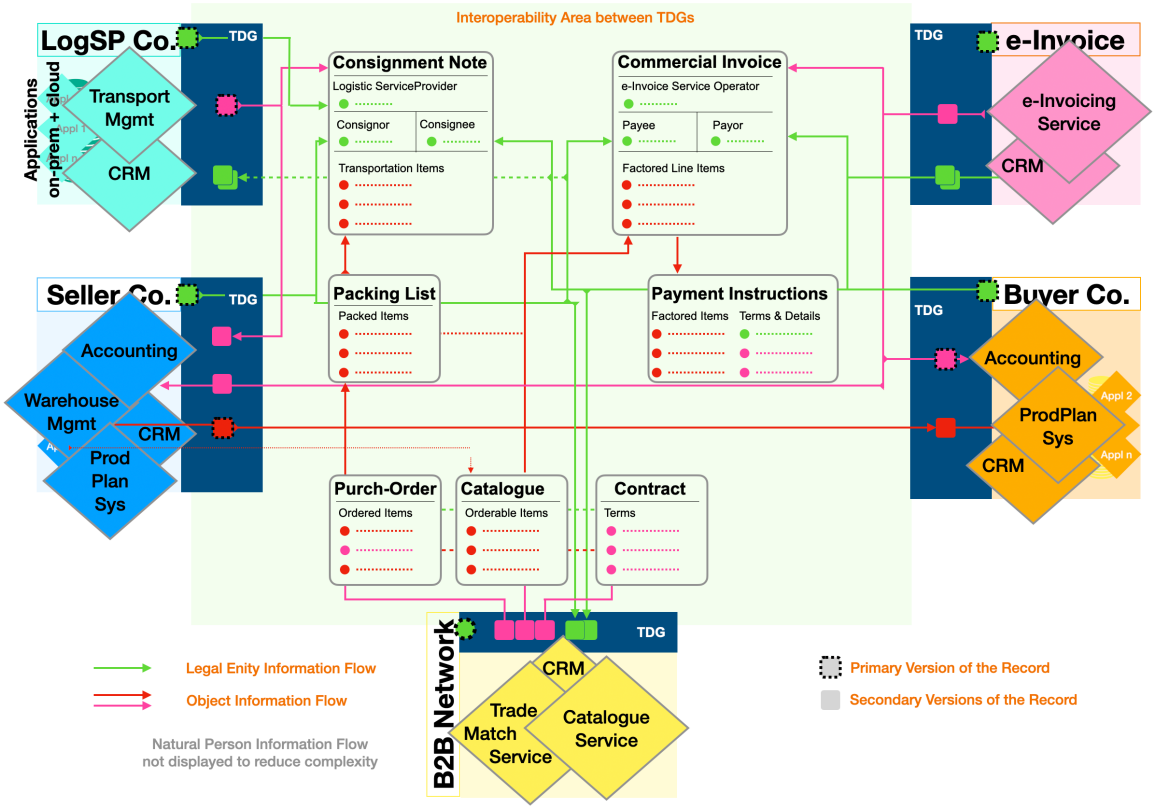


Figure 6: Composing payloads of authentic trade instruments in the Trade Data Gateway Peer-2-Peer-network

In its KTDDE[29] program ICC DSI has identified 200 core data elements, that are being used in the 36 most prevalent trade documentations or instruments (called “documents” in the KTDDE context).

Pull data access

In today’s paper-based world, prints and PDFs are sent from the originator to the receiver. This “pushes“ data element assemblies from party to party. Decomposing trade instrument payloads into subgraphs also supports the paradigm change of push to pull.

Instead of collecting the necessary data elements to compile a document and subsequently pushing it downstream, one could expose the data elements that need to be transferred to the Trade Data Gateway. Subsequently, a notification of data availability will be exchanged between the TDGs. All data consumers (i.e.,

29 The KTDDE program stands for "Key Trade Documents and Data Elements," a global initiative aimed at standardizing and digitizing key documents used in international trade. This effort, led by the International Chamber of Commerce (ICC) Digital Standards Initiative (DSI), focuses on harmonizing 36 essential trade documents and the data elements they contain and share.

today's document recipients) can then retrieve the data elements as needed. Access to the data elements will be granted based on proof of legitimate interest. This may depend on trading partners having admitted service providers into the circle of transaction stakeholders and the roles of those stakeholders. Individual agreements may also influence the extent and depth of trade data element accessibility.

For instance, a logistic service provider may require consignment data to file a consignment note. The consignment data has been exposed (and signed) to the TDG of the consignor (seller) as a data container and can be incorporated along with containers holding party information into a compilation of nodes, thereby forming a consignment note.

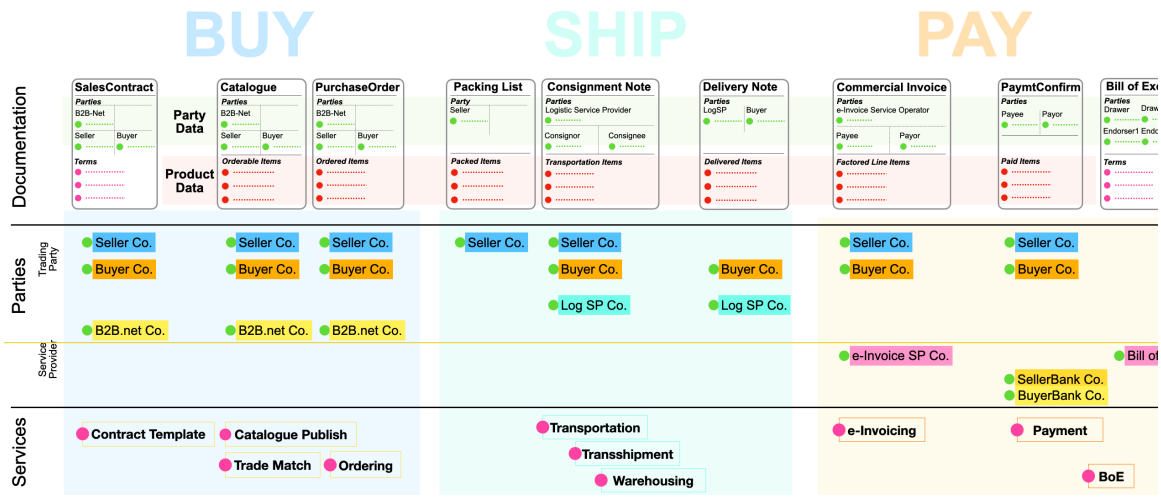


Figure 7: Database graph nodes of a trade with product-, service- and party information mapped to trade documentation instruments

The consignment note will so become a sub-graph of nodes that are the particles of the trade instrument. Each of it can be dynamically pulled as required for the purpose. And each particle will be signed by its data originator and so become verifiable. The same signed container payloads can again be pulled further downstream as particles for subsequent documentation types. Data elements that have been chosen in a catalogue while ordering, find their way on the Purchase Order, move on to the Packing List, are being used on the Consignment Note, ticked on the Delivery Note and listed up on a Commercial Invoice. Figure 7 shows for the consignment note the nodes 'transportation items' and the parties involved. And how these nodes propagate through the trade cycle.

A ‘meta layer messaging protocol’ is to evolve, which (1) notifies a party of data having been made available and (2) granting access rights to avail over the data on the remote TDG.

Pulling data can occur between neighboring tiers, but also between remote tiers[30]. Deep tier access can be facilitated and becomes a matter of the ability to prove legitimate interest. Which again depends on and is a function of authenticity. Deep tier access allows a party to retrieve data from the suppliers of their direct suppliers, despite only having an indirect relationship with these entities, established through their shared supply chain.

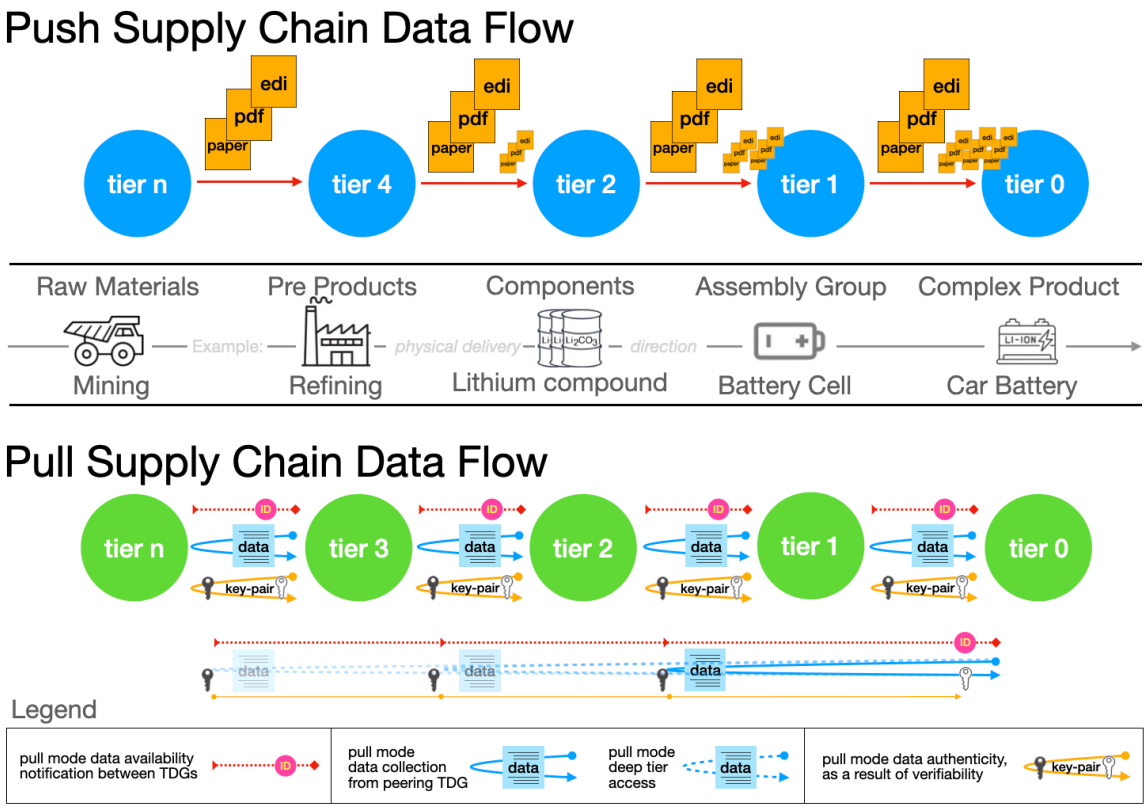


Figure 8: Supply chain information management pull approach enabled by peer-2-peer Trade Data Gateway

[30] An identifier is sent to inform the receiving node about the ability to pull the related data. The advantage is that this can happen asynchronously.

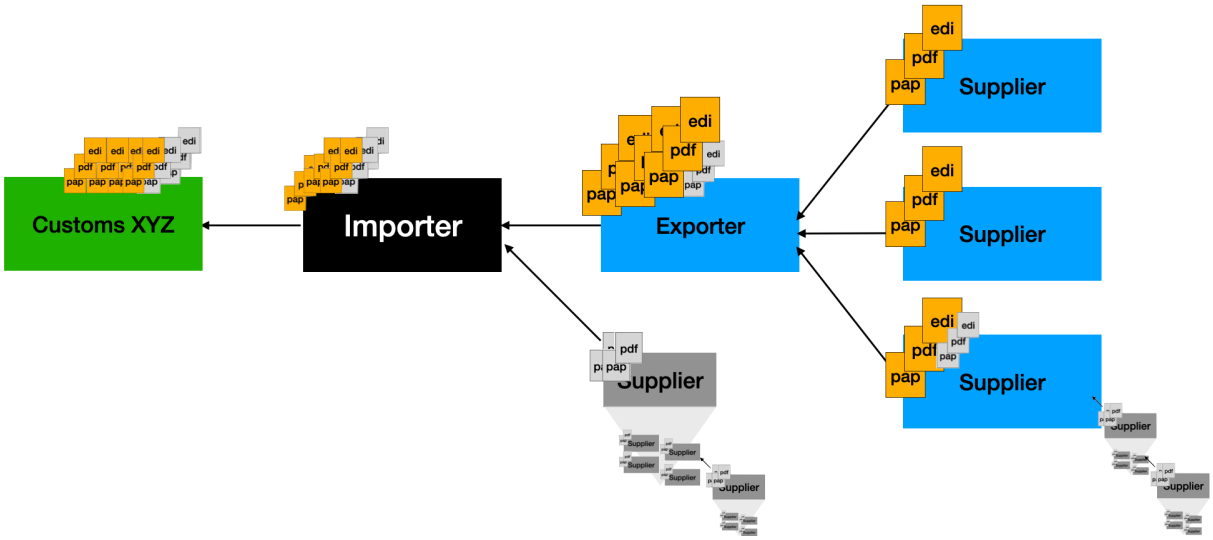


Figure 9: Paper pushed from leaves to root, consolidation required, SC deep tiers untraceable

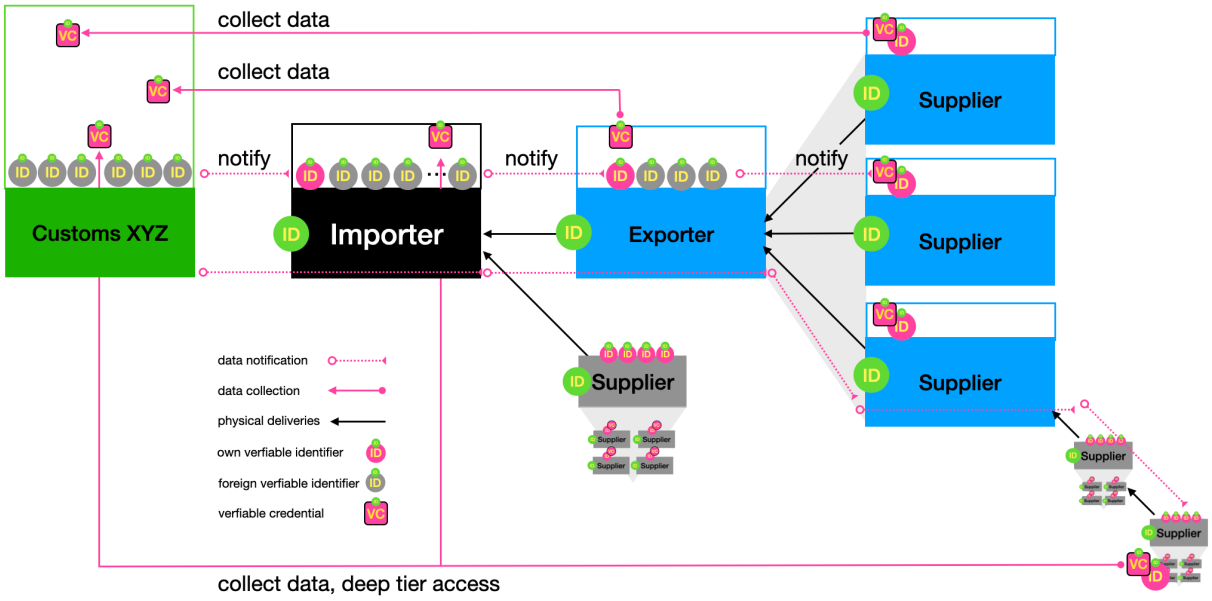


Figure 10: Data pulled from leaves by root. No depth limit for data consumers (i.e. customs authorities)

The role of identity

A supply chain can be described as a suite of trust relationships, starting from the contract and order and specifying all trustworthy interactions between the involved subjects, called the parties, and the objects, the physical matters and services involved.

As long as the identification of the subjects is fragmented between different platforms, and companies, interoperability between loosely coupled applications in trade will remain very limited, if not impossible, as a result of a lack of authenticity of process steps[31].

Subjects and Objects

Global trade is full of objects and subjects. The objects can be shipments, vessels, containers, pallets, bulk commodities, products, devices, services in the form of software instances, algorithms, and a lot more. The subjects are either legal entities[32] or natural persons. While subjects have rights and obligations, the objects are at all times controlled by the subjects.

Autonomously acting artificial intelligence algorithms, despite of seemingly acting like subjects, are objects. They are always under control of a subject, which is liable for their acting.

Any real world or virtual object comes with a set of attributes, attribute values and corresponding relationships with semantic constraints[33]. Is in other words, relationships with linked properties that are features of the relationship they are associated with. The identity of an object is expressed by the list of all its relevant attributes. The digital identity of an object is expressed by the digital signature attesting to its list of attributes.

Identifiers

Since it is easier to compute database requests using keys, these lists usually get a label assigned: an identifier. It is good database design practice to have these labels free of any semantic constraints. The set of attributes relevant for identification depends both on the type of object/subject to be identified and the purpose of the identification. If the set of attributes is supposed to be common to all users, they are often defined in standards.

Identification

Identification refers to the act of stating or otherwise indicating a claim purportedly attesting to a person, a legal entity, objects, and algorithms[34]. It

---

31 This is also a huge risk for SMEs. They easily could get bound to a dominating platform (lock-in). This contrasts with the overarching goal “inclusivity”.

32 More precisely: Legal Entities. This can be, next to companies, also be organizations of any sort, or a sovereign.

33 There has been a discussion in database modeling if relationships carry a meaning and are therefore objects in themselves, or if it is just a reference. We have chosen relationships to be objects with certain attributes, carrying the meaning of the relationship. That’s why they are called relationships with semantic constraints.

34 https://en.wikipedia.org/wiki/Authentication

comes with the requirement of verifying the claim against acceptable sources. Those sources include, but are not limited to, public registries, notaries, biometric signatures, testimonies by the origin, registries of goods and rights as well as other means.

Authentication

Authentication is the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity[35]. Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular[36]. These basic concepts apply to a wide array of objects (including products, rights, patents, avatars, artificial intelligences, devices or physical logistic containers) just as subjects (including individuals or legal entities, in particular companies or public bodies).

The LEI

One example for such an identifier is the Legal Entity Identifier (LEI)[37]. The LEI is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information and supporting processes that enables clear and unique identification of legal entities participating in financial and other transactions. As an example, the LEI contains as a mandatory field the company identifier of the authoritative source, the register the Legal Entity is listed in. Put simply, the publicly available LEI data pool is a global directory of market participants, which greatly enhances transparency in the global marketplace for any public or private purpose.

The LEI reference information is defined operationally in a standard called LEI-Common Data File format (LEI-CDF)[38]. The formats within this standard provide the specificity needed for the implementation of the ISO 17442 standard. External standards, e.g. the ISO 20275 standard for Entity Legal Forms (ELF), have been included in the LEI-CDF formats. In other words, the LEI can be seen as a reference or pointer to the data representing the real object in a semantically clear and structured way.

---

35 ditto

36 https://en.wikipedia.org/wiki/Authorization

37 A good overview on the LEI system and its characteristics can be found at:
Kennickell, Arthur B. (2016). “Identity, Identification and Identifiers: The Global Legal Entity Identifier System,” Finance and Economics Discussion Series 2016-103. Washington: Board of Governors of the Federal Reserve System,
https://doi.org/10.17016/FEDS.2016.103

38 https://www.gleif.org/en/about-lei/common-data-file-format/lei-cdf-format/lei-cdf-format-version-2-1

Similar examples can be found easily: a vessel-ID, a barcode for products, or a tax number among many more add to the complexity of today's data processing, especially when paper-based documents are in use. However, it is getting even worse.

The same object could have multiple labels[39]. Why is that? Because the selection of attributes is subject to both context and a purpose. Take, for example, the Business Identifier Code[40] (BIC) and the LEI. The same financial intermediary could have an LEI, and a BIC (sometimes even multiple BICs) assigned to it, each following different schemas and standards. The opposite is also true. The exact same alpha-numeric code could mean anything depending on the context. Take '41615087045' as an example. This string could be a telephone number or the social security number of a natural person in a certain jurisdiction.

Fragmented Subject Identity, heterogenous object identity

Today's applications and software solutions addressing trading partners are designed around documentation objects: A bill of lading, a certificate of origin, a packing list, a warehouse receipt, a customs declaration, a product passport, and many others[41]. On all of these documentation objects actors are specified, the parties, which are filing, and accessing these trade documentations. Or parties, which derive performance obligations from them.

This is where today's problems starts. Each application, platform, blockchain, industry sector or any other solution comes with different identifiers for the acting entities, be it organizations or people. This makes interoperability between the solutions almost impossible. Complicated APIs coming with rule sets require bilateral agreements and governance. This comes on top of missing or competing standards for the objects itself. The only universal interoperability solution still today, is using paper and text. However, this won't allow for digitalization across platforms, across countries, and across trading partners, including their intermediaries and service providers. This also prevents from seamlessly weaving business process chains across organization boundaries. The paper system very effectively foils all automation progress. This is also true

---

39 List of examples for legal entities: National business registry and tax numbers, international codes like OECD Tax Identification Number (TIN) and WCO Trader Identification Number (ITIN), ALEI, DUNS, GLN, BIC, proprietary codes form large data vendors, sector specific identifiers like the Odette-ID in automotive, etc.

40 ISO 9362 defines a standard format of Business Identifier Codes (also known as SWIFT-BIC, BIC code, SWIFT ID or SWIFT code) approved by the International Organization for Standardization (ISO). It is a unique identification code for both financial and non-financial institutions. https://en.wikipedia.org/wiki/ISO_9362

41 ICC DSI KTDDE, see page 11 of the KTDDE report, https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf

for seemingly verifiable PDFs. There is hardly any global verifiability, without globally valid identity.

Entities in trade, identity and authenticity centric supply chains

The authors therefore suggest an architecture where identity and authenticity are at the core. Subjects and objects are described by their identity and role in a certain context. The actors can only be subjects, so either a legal entity or an individual (Natural Person). Examples for the two entity types are:

1. Legal Entities (S/LE):
    - Companies of any size that produce and acquire goods and services
    - Service providing companies of any size, from a maritime carrier employing thousands of people through to a one-man veterinary inspection company.
    - Customs organizations and law enforcement bodies
    - Sovereigns and multinational organizations
    - Policy makers and regulators

2. Natural Persons (S/NP):
    - The CEO of a company
    - A manager in a procurement department
    - The captain of a vessel or aircraft
    - A bank clerk filing a letter of credit
    - A shipping clerk filing a vessels journey manifest
    - An employee educated in the handling and declaration of dangerous goods
    - A veterinary certifying the health status of livestock being prepared for a transport

These actors have multiple relationships:

- E.g., John Doe works for Producer Co. as a warehouse manager,
- Xue Wong works as a procurement manager for Buyer Ltd.
- Xue Wong of Buyer Ltd. asks Rekha Reckon, who is a trade finance clerk in Banking Inc. for risk mitigation and finance[42].

Transport Co. owns a container that Producer Co. becomes a temporary lessee to, when Transport Co. issues an electronic bill of lading to Producer Co., which Jon Doe signs and accepts. Xue Wong will require control over the bill of lading

---

42 The Peer-2-Peer approach guarantees data privacy. Names are not shared with 3rd parties. However, identities are persistent in TDGs to allow for being used in audits and legal disputes.

at a later stage to have her cargo released at the port of destination. Prior to this Producer Co.'s bank may want to control the bill of lading to mitigate their own risks, which result from mitigating Producer Co.'s risk in a letter of credit transaction.

References made to the entities 'Producer Co.', Buyer Ltd., 'Xue Wong', and 'Jon Doe' in a trade documentation answer the question of "Who" is interacting in a trade. These are the bearers of rights and obligations.

The question of "what" the interaction is about (what is traded or what helps to trade) is replied to with references to the two object types below.
Examples are:

3. Material Objects (O/Mat):
    - Consignments, a combination of merchandise and its package.
    - The merchandise itself (goods)
    - Planes, trucks, rail coaches, barges, vessels
    - Transport Unit Carriers (containers, palets)
    - Documents (i.e., a paper bill of lading, a paper delivery note, a paper invoice)
    - A tracking device for containers, any IoT or any computing device (like a smartphone used for signing electronically)

4. Immaterial Objects (O/Imt):
    - An identifier
    - Software instances like application containers running on a hypervisor instance or device. A software instance could as well be a process running authentically on behalf of a customer on an IoT device.
    - Datasets, i.e., a risk distribution database, storing a collection of trade risk, or the database graph of a trade.
    - Electronic trade documentation (i.e., an electronic bill of lading)
    - Algorithms, like an AI algorithm accepting orders
    - A defined geofence
    - Patents and trademarks

There is no limit to the variety of objects, neither material, nor immaterial. Objects have no rights or obligations. They are at all times controlled by subjects.

To repeat: as long as the identification of the subjects is fragmented between different platforms, companies, industry sectors, jurisdictions, and so on, interoperability between applications in trade will remain very limited, if not impossible, as a result of a lack of authenticity of the business process steps.

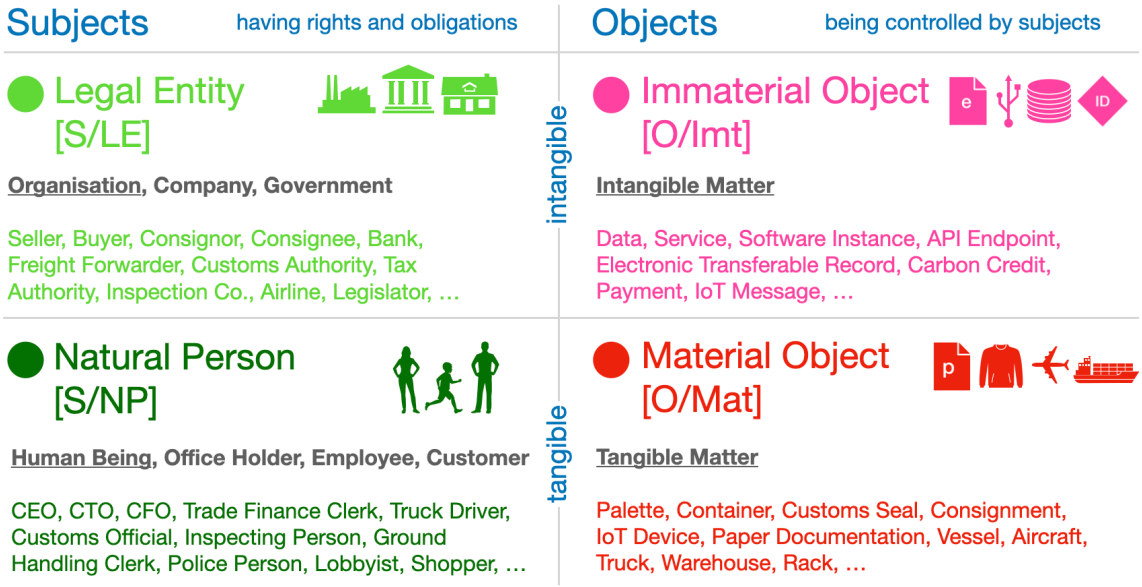


Figure 11: Identifiable entities in trade

Supply Chain event authenticity

A Supply Chain event refers to any occurrence within a supply chain in which other participants have a vested interest. Examples include the collection of merchandise for transportation, its stowage on a sea vessel, the transfer of exclusive control over a bill of lading or a transportation insurance certificate, the issuance of a letter of credit, or the delivery of a consignment.

With fragmented subject identity, it remains extremely challenging for an observing party to attribute supply chain events occurring upstream or downstream of a given point to the involved parties. Specifically, if a transfer of exclusive control to a trade instrument such as a bill of lading cannot be reliably attributed to the interacting parties (i.e., the old and new exclusive controllers of the B/L), then a third party (potentially a bank) observing the event cannot derive any authoritative action from it.

An authoritative action, in this example, could be the release of cargo or the granting of protection against payment default or the granting of credit. The release of cargo (at the port of destination in return for surrendering the B/L) is again a supply chain event, which, if observable and correctly attributable to interacting parties, can trigger new events, such as a payment.

Only supply chain event authenticity allows for comfort in deriving ‘subsequent action’. Subsequent action is the continuation of a business process chain. Hence, clear subject and object identification is a prerequisite to uninterrupted digitalized process chains across applications and platforms.

Supply chain events form a directed graph, in which all nodes need to be authentic to comply with the legal compliance requirements of all subjects participating in the supply chain.

Organizational Identity enabling authentic supply chain events

People, meaning mandated individuals, exert control over ETRs. People file and sign trade instruments. In doing so, they act on behalf of their principals, their employers, their companies. Any peer-2-peer architecture aiming to generate legally liable data exchange requires authenticity in the interactions between individuals as they act on behalf of the organizations they belong to.

Bob wants to verifiably act on behalf of ABC Co. and Rekha needs to act verifiably on behalf of XYZ Ltd. The individuals’ verifiable conduct translates into verifiable conduct of their respective employers helped by existing cryptographic bonds between employees and employers, individuals and organizations.

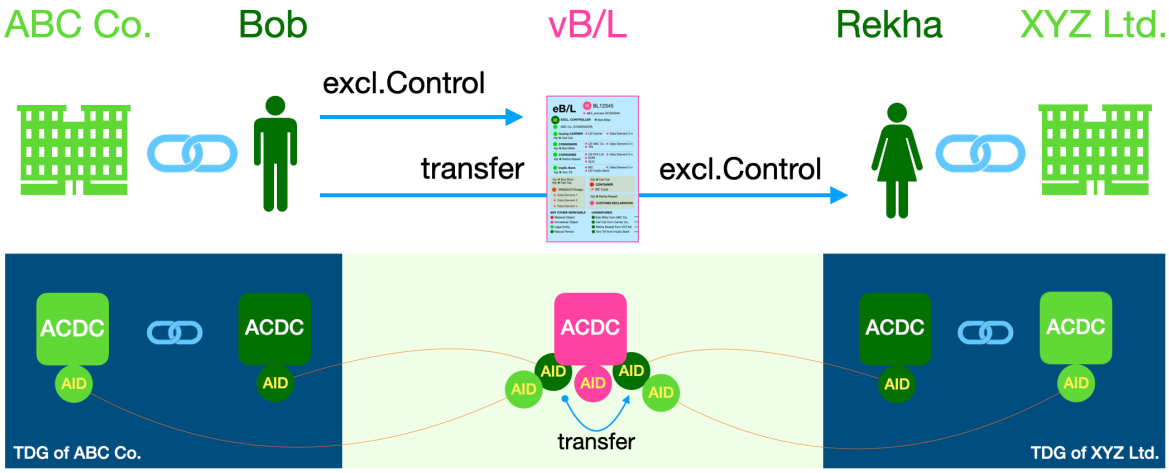


Figure 12: Organizational Identity assisted Transfer of Exclusive Control over an ETR

Also, machines or algorithms (both being objects) can act verifiably on behalf of an individual (being a subject), if both object and individual can be uniquely identified and the entities are cryptographically bonded.

If supply chain events become authentic and the authenticity of the events can be observed and reliably evaluated by authorized third parties, these third parties can derive their own actions from it.

Examples for supply-chain-events becoming authentic through organizational identity

Dispatching a consignment, filing a Bill of Lading

Alice Sold, who is employed by Seller Co. commissions Carl Cargo of Feedport Co. to have them collect a consignment to be destined for Buyer Co.

On collecting the consignment, Carl issues and signs a verifiable Bill of Lading, documenting the hand-over of the merchandise. Also, Alice signs the vB/L. The vB/L is an authentic dataset, including identifiers of the individuals involved and identifiers of their respective employers. It also includes a verifiable identifier of the consignment. One of the subject identifiers, identifying an individual, determines who the current exclusive controller of the Bill of Lading is.

Carl Car of Feedport, the company trucking the consignment to the seaport, is being given an identifier for the packing list prepared by Seller Co., which is stored on Seller Co.'s TDG. Carl uses this as an input for the Bill of Lading. Carl can also resolve all the data relevant for the service Feedport Ltd is about to provide, i.e. a pick-up location, and Carl can process this data in Feedport's systems.

The authentic vB/L-dataset is registered on Seller Co.'s TDG as an Authentic Chained Data Container (ACDC).[43], signed by Alice and Carl.

A reference to the vB/L is registered on Feedport's TDG and also onto the TDG of Buyer Co. Their responsible employee, Bob, is herewith being notified about these supply chain events ('dispatch occurred, vB/L issued'). Bob can now pre-notify his own logistic service provider, PortTruck Ltd., who will fetch the consignment from the port upon arrival. PortTruck Ltd. employs Pete, who has now access to all relevant data pertaining to the upcoming transport, including

[43] To simplify the illustration, we have refrained from displaying an "vB/L service" as an additional entity, where the entire instrument would originate and be processed. Feedport Ltd. could issue a House Bill of Lading for the pre-run to the seaport, which could automatically become part of a master B/L for the subsequent journey on the sea vessel. The information obtained by Feedport Ltd. through resolving into the packing list could be used to enquire into available sea transport service and, if booked, be directly routed into Shipping Co.'s systems.

verifiable delegated authority to collect the consignment on behalf of Bob of Buyer Co. Bob also notifies his bank, which is to issue a Letter of Credit with Seller Co. being the beneficiary. All this occurs in real-time.

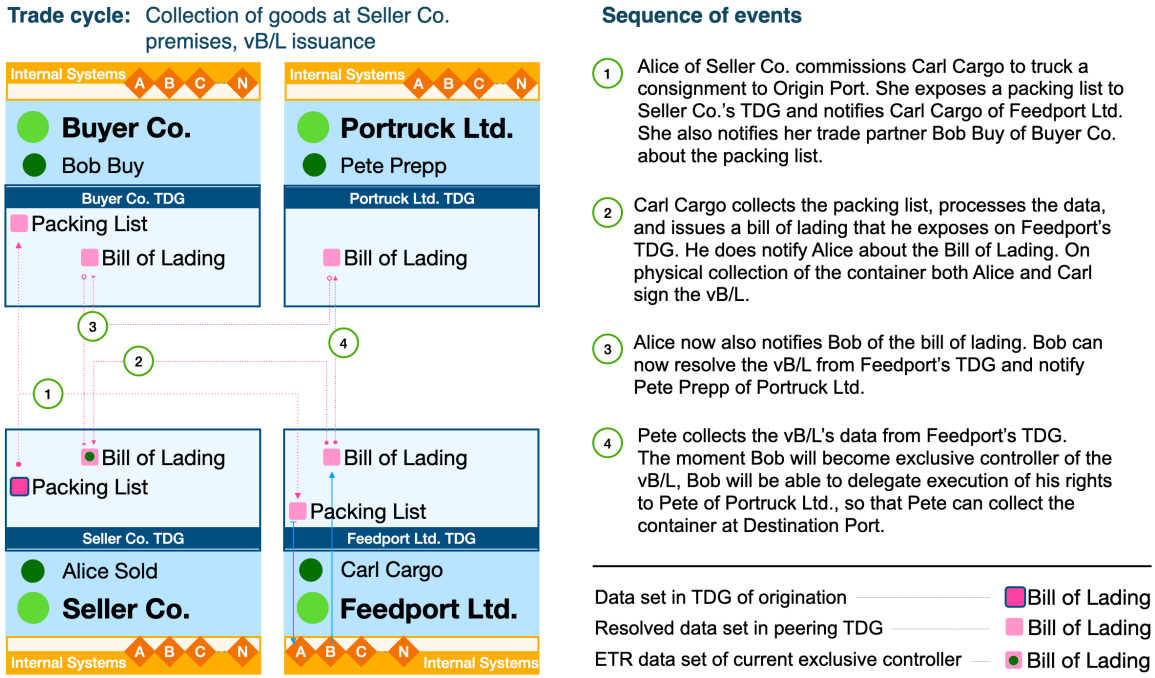


Figure 13: Dispatching a consignment, collection of goods, issuance of documentation, distribution of documentation

Issuing a Letter of Credit

Bob Buy of Buyer Co. applies for a Letter of Credit to be issued by Audrey Avaly of the negotiating bank Buyer Bank and with Seller Co. being the beneficiary and Seller Bank the advising bank. The two banks being involved (and a potential third as well) can see all agreed upon documentations at the very moments that they are being produced – in real time. The presentation phase of the L/C merges with the issuance phase.

Audrey Avaly of the issuing bank asks for transport insurance to be procured.

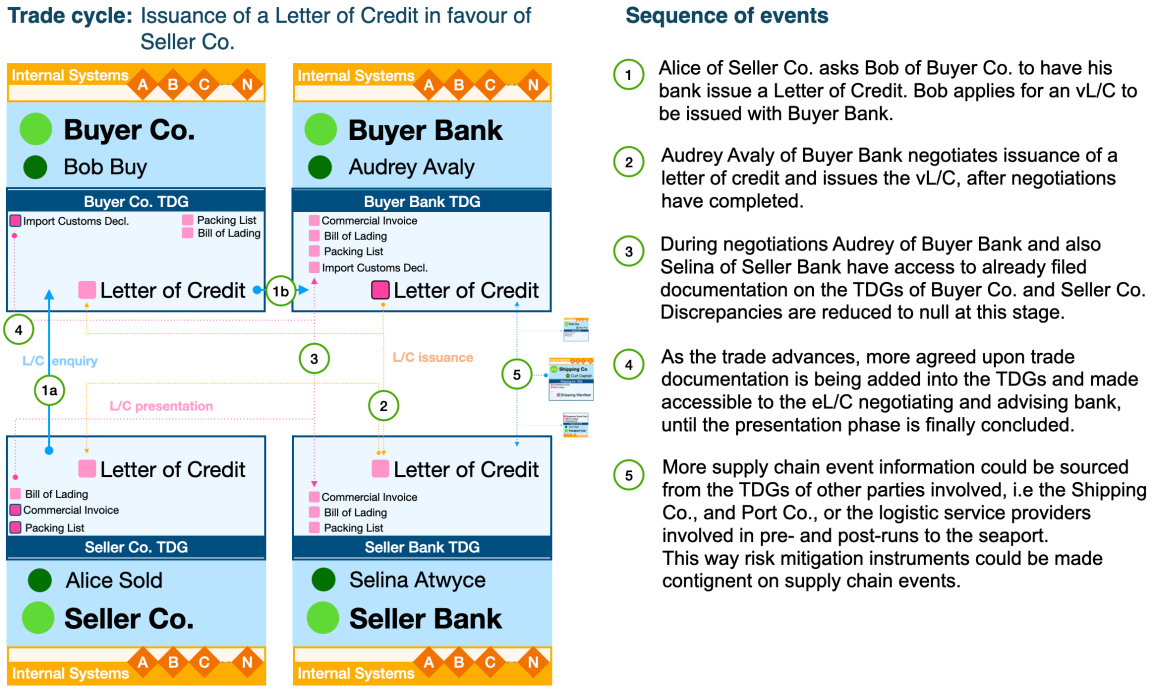


Figure 14: Issuing a Letter of Credit

Procuring transport insurance, passing of risk, transfer of exclusive control on an ETR

Alice of Seller Co. requests Celia of CoverTrans Co. to issue a transport insurance certificate. Celia issues the TIC, with Seller Co. being the beneficiary. The TIC is referenced on both Buyer Co.'s and Seller Co.'s TDGs., with Alice Sold becoming the exclusive controller.

By having granted Celia of CoverTrans Co. access to data on the TDG of Seller Co. pertaining to the trade, Celia also learns about the vessel the transport is booked on. As the agreed upon Incoterm for the trade is CIF[44], the transfer of risk for loss or damage occurs the moment the merchandise has been stowed on the ship. At exactly this time the claim for insurance shall transfer to Bob of Buyer Co.

Bob of Buyer Co. has been notified about the insurance cover before and found the TIC on his TDG. Now he sees having been made its exclusive controller.

---

44 CIF is an Incoterm and stands for "Cost, Insurance, and Freight". Under CIF, the seller delivers the goods and transfers the risk of loss or damage of the goods to the buyer once the goods are loaded on board the vessel at the named port of shipment. CIF also requires the seller to arrange and pay for the port-to-port carriage and insurance of the goods up to the port of destination. The risk of damage or loss then transfers to the buyer. An insurance claim for goods in transport often needs to transfer from seller to buyer at a certain point in time – in case of CIF after stowage on the vessel. See: https://icc.academy/incoterms-2020-cip-or-cif/

This supply chain event can also be observed by Audrey Avaly, who is responsible for the Letter of Credit, which Buyer Bank has issued.

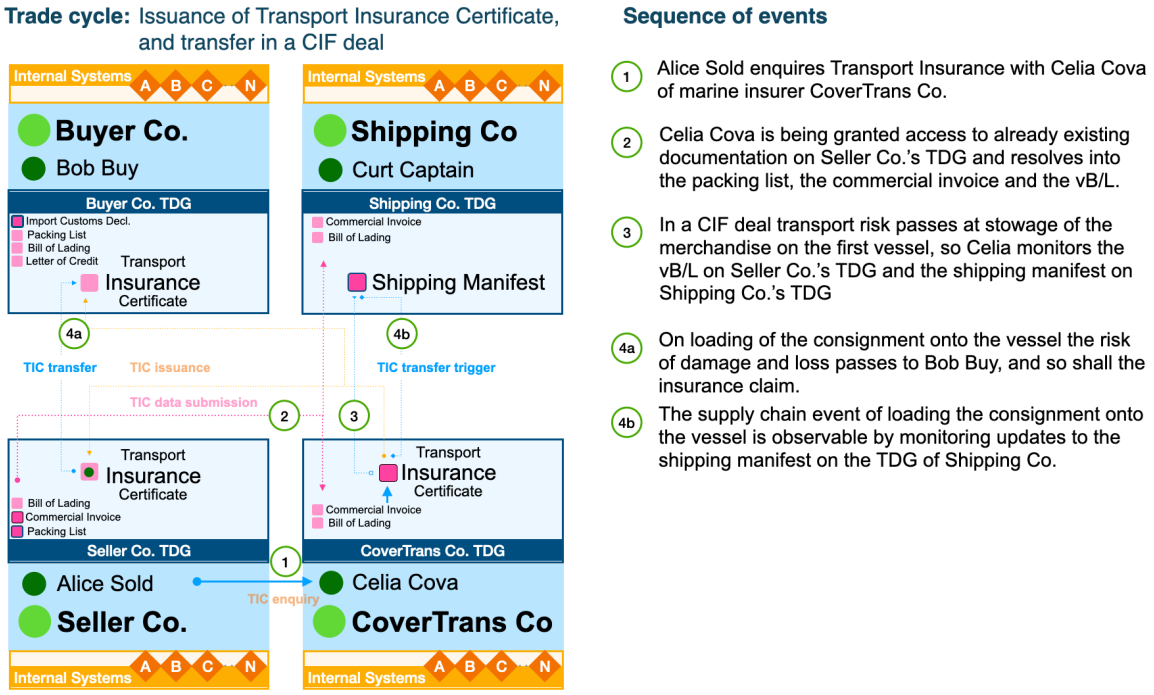


Figure 15: Procuring transport insurance, transfer of control on ETR (Transport Insurance Certificate) and time of risk passing

Cargo release on a seaport, surrendering a vB/L

The sea vessel has arrived at the port of destination. Portruck Ltd. has been delegated by Bob of Buyer Co. to collect the merchandise at the seaport. Portruck Co. has delegated this authority to Pete Prepp.

Destination Port Co., which is handling the consignment after unloading from the vessel wants sufficient comfort to hand it over to an authorized party, and not some fraudster or thief. Organizational identity allows for verifiable delegation of authority between a legal entity to an individual within that legal entity, which can be observed and verified by another party.

This case describes delegation of authority between a legal entity having authorized an individual to act on their behalf and using the authority to allow sub-delegation of his authorities to another legal entity, which then sub-delegates the authority to an individual of their choice.

This is just one simple case that will presumably occur in the millions of instances on a daily basis. There are far more complicated constellations of required sub-delegations thinkable.

Bob Buy has been made exclusive controller of the vB/L, which is verifiable on his TDG and can be confirmed by parties registered in the history of the vB/L, i.e. Alice Sold of Seller Co. or Audrey Avaly of Buyer Bank. Pete Prepp can avail over the vB/L, because Bob, as the exclusive controller of it, has delegated handling privileges to Pete.

By Pete requesting handover of the merchandise at the seaport, Dan Destiny of Destination Port Co. is being authorized to access the vB/L history on the TDGs of the involved parties. This way multiple parties confirm the status of the vB/L and also a trade relation to the legal entity Buyer Co., who verifiably claims to employ Bob. The same Bob did (indirectly) delegate authority to Pete to execute the rights of the vB/L. This Pete is now present at the port, and requests handover of a consignment destined for Bob.

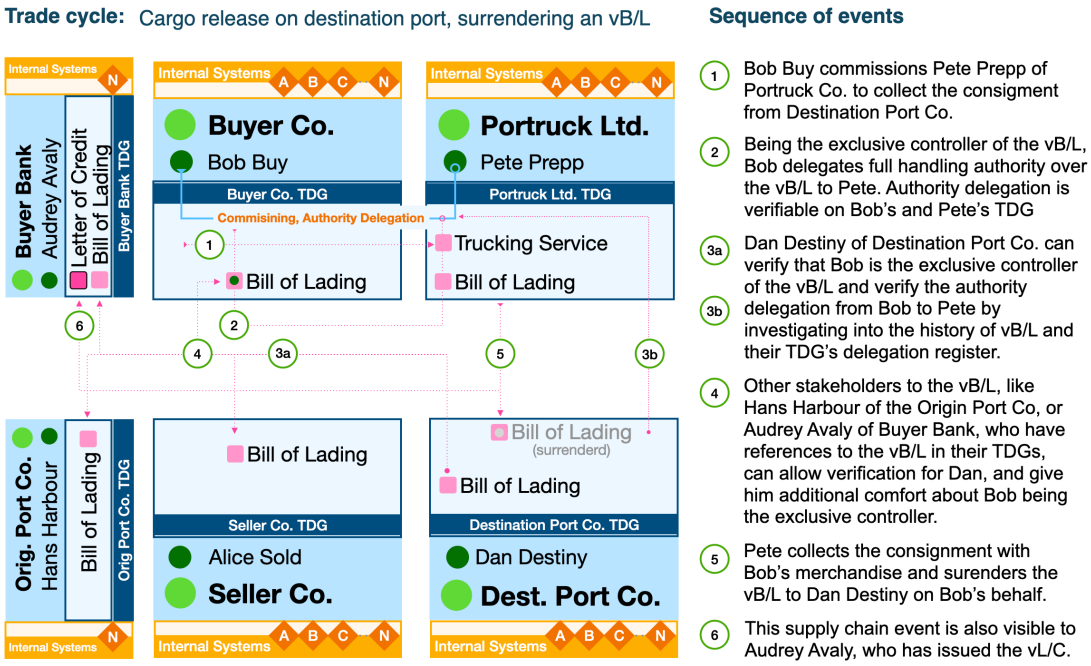


Figure 16: Cargo release, surrendering a vB/L under verifiable delegated authority

Delivery of a consignment, signing a delivery receipt

Pete of Portruck delivers the Container with Bob's goods to the premises of Buyer Co. Bob of Buyer Co. accepts the delivery and signs a delivery receipt without reservation.

Delivery of a consignment is an important supply chain event, which, if visible and verifiable in remote locations, and other networks of other trade domains,

can be used to trigger further business process steps. This is often referred to as “smart contracts”. What is rather concealed is the fact that “smart contracts” require event data authenticity.

To remain with this example: an observer of the event ‘goods delivery’ by consuming a delivery note needs certainty on the originator of the delivery note. Certainty in terms of legal bearing, legal compliance. Then subsequent action can be derived which again has can bear legal implications.

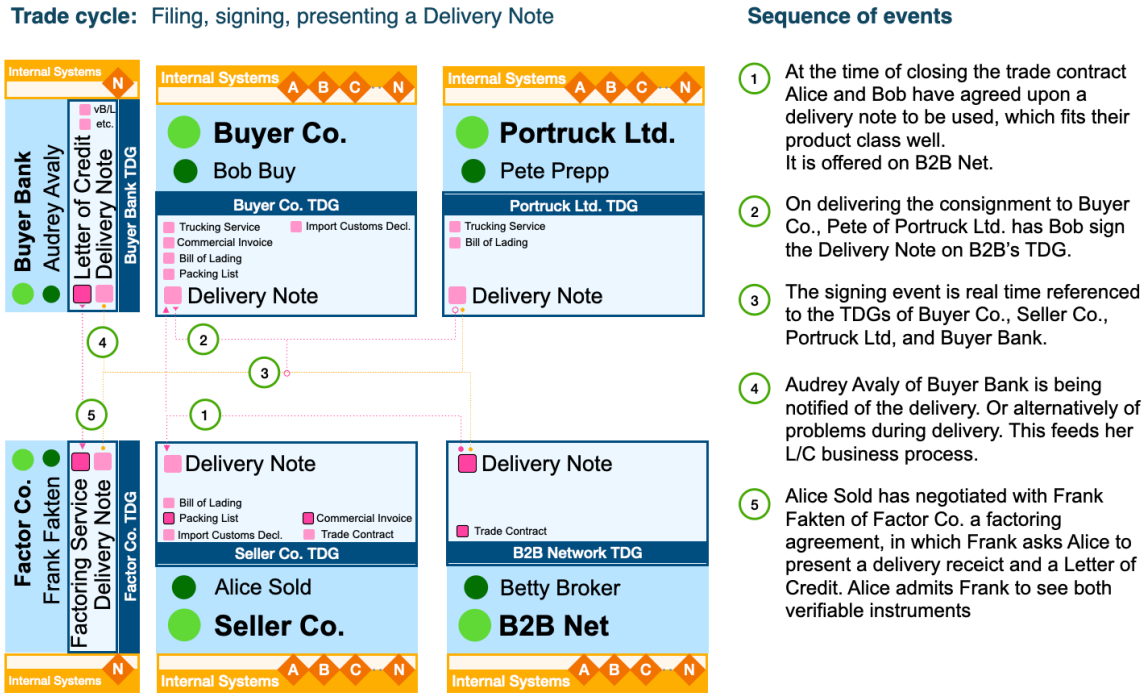


Figure 17: Delivery of a consignment, signing a delivery receipt, presenting it elsewhere

Issuing an invoice, factoring an invoice

The commercial invoice has been issued a while ago. It was auto-produced based on the data so far available. It is in status ‘issued’. In this status it can be used for many purposes, i.e. allowing the buyer to complete import customs formalities. Delivery of the goods to the buyer and signing of the delivery receipt triggers an invoice status to change from ‘issued’ to ‘released’. The invoice status change is performed in Seller Co.’s account receivables system, and real time registered on the TDG of Seller Co. From there, the information is propagated, also in real-time, to the Buyer’s TDG and further into his account payables system. Both the banks, Buyer Bank and Seller Bank, had been notified about the invoice issuance event as a pre-presentation for the Letter of Credit.

The banks can also be informed about the status change from ‘issued’ to ‘released’. More invoice meta-properties are imaginable: A factoring company may want to know about the financing status of the invoice (‘financed’, ‘not financed’). A partial payment may, if partial payments span over fiscal years, be interesting to evaluate automatically for taxation purposes by a tax advisor.

Invoices are not the only instruments requiring status characteristics. Also, an eB/L (or any other ETR) should have standardized status (pl). Think of characteristics like ‘in drafting’, ‘release candidate’, ‘released’, ‘amended’ ‘endorsed by’, ‘surrendered’. In a network protocol centric digital fabric these characteristics provide a multitude of support for new, better, and authentic business processes.

Seller Co. and Buyer Co. have agreed upon payment terms of 120 days after delivery. Alice of Seller Co. requires liquidity and has enquired for factoring services with Frank Fakten of Factor Co. Frank made an offer to acquire the invoice at very favorable rates, when Alice can present a clean delivery note, and a Letter of Credit has been issued. Both conditions are easily verifiable for Frank, since Alice elevated Frank to receive limited ‘trade scope internal’ access to the TDGs of Buyer Bank and Buyer Co. Frank can now see the status characteristics of the invoice. Frank can see that the invoice is in status ‘not financed’ and that the invoice has been accepted by Bob of Buyer Co.

Alice Sold accepts Frank Fakten’s offer and sets three instruments, Invoice, Delivery Note, and Letter of Credit visible for Frank.

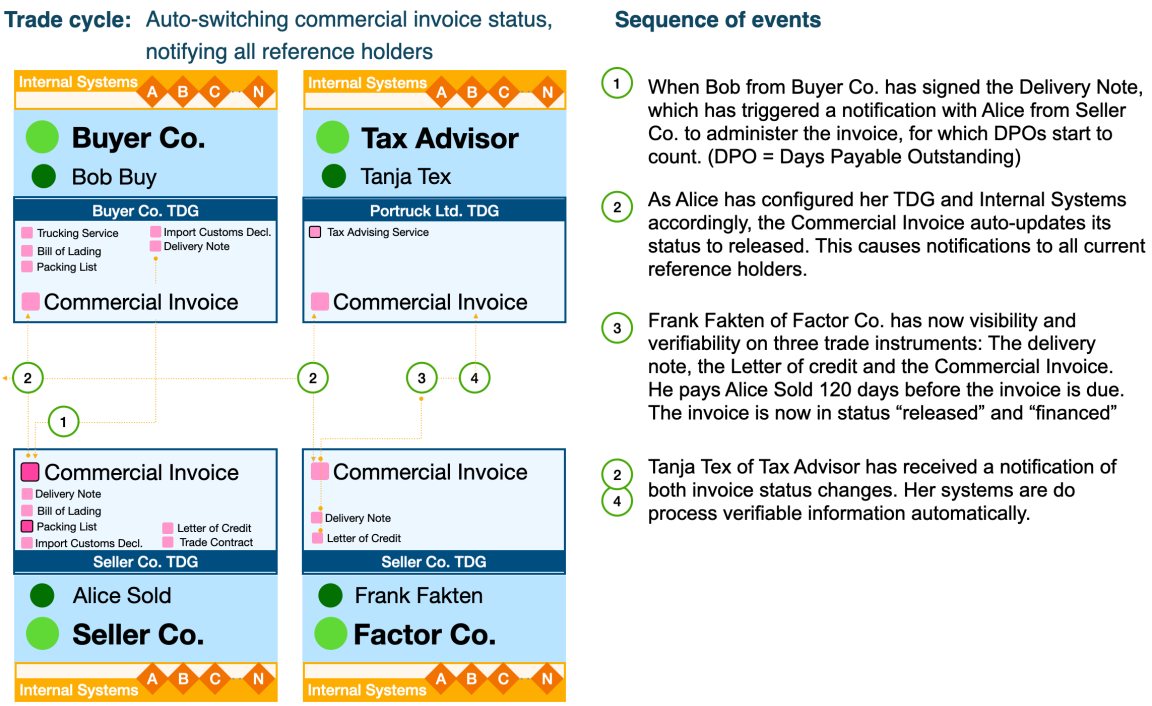
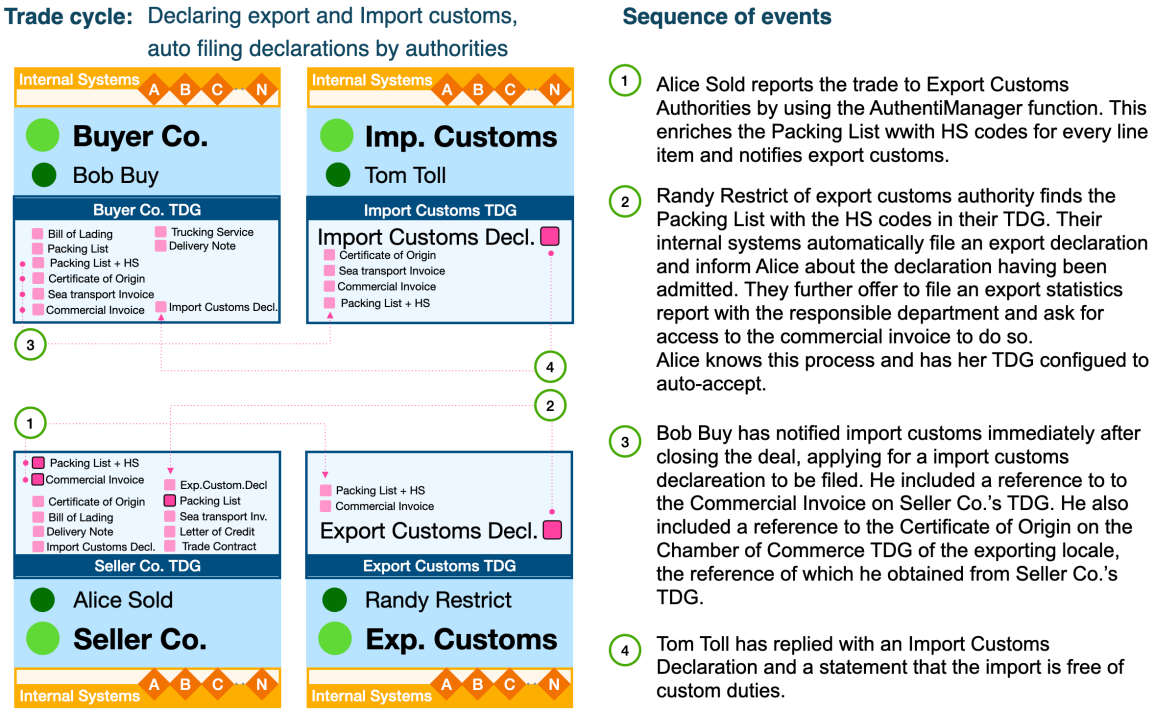


Figure 18: Commercial Invoice status change

Completing import customs formalities

Filing custom declarations could be entirely automated, were custom authorities operating their own TDGs (instead of so called ‘single windows’). The information submitted is almost always stored in internal systems already. In case governments were to adopt technology that they built in globally unique fashion and aligned with the exporting and importing industries, a lot of taxpayer money could be saved, and especially smaller participants could benefit from automation.



Sequence of events

1. Alice Sold reports the trade to Export Customs Authorities by using the AuthentiManager function. This enriches the Packing List wwith HS codes for every line item and notifies export customs.
2. Randy Restrict of export customs authority finds the Packing List with the HS codes in their TDG. Their internal systems automatically file an export declaration and inform Alice about the declaration having been admitted. They further offer to file an export statistics report with the responsible department and ask for access to the commercial invoice to do so.
   Alice knows this process and has her TDG configued to auto-accept.
3. Bob Buy has notified import customs immediately after closing the deal, applying for a import customs declareation to be filed. He included a reference to to the Commercial Invoice on Seller Co.'s TDG. He also included a reference to the Certificate of Origin on the Chamber of Commerce TDG of the exporting locale, the reference of which he obtained from Seller Co.'s TDG.
4. Tom Toll has replied with an Import Customs Declaration and a statement that the import is free of custom duties.

Figure 19: Issuance of export and import customs declaration

Verifiable Supply chain events in aviation

'Known Consignors' and 'Regulated Agents' are frequently being validated by their respective national aviation security authority for adherence to security protocols while packing air cargo containers or handling them.

A Known Consignor has educated staff pack ULDs (Unit Load Device) in an admitted location, according to a security protocol. A container packed by a Known Consignor requires reduced further security checks, before being loaded into an aircraft, if after packing only regulated agents have dealt with the container. A regulated agent can be any service provider or freight forwarder that is also validated frequently for adherence to prescribed protocols.

Any documentation filed and propagated by a KC or RA need to be authentic.

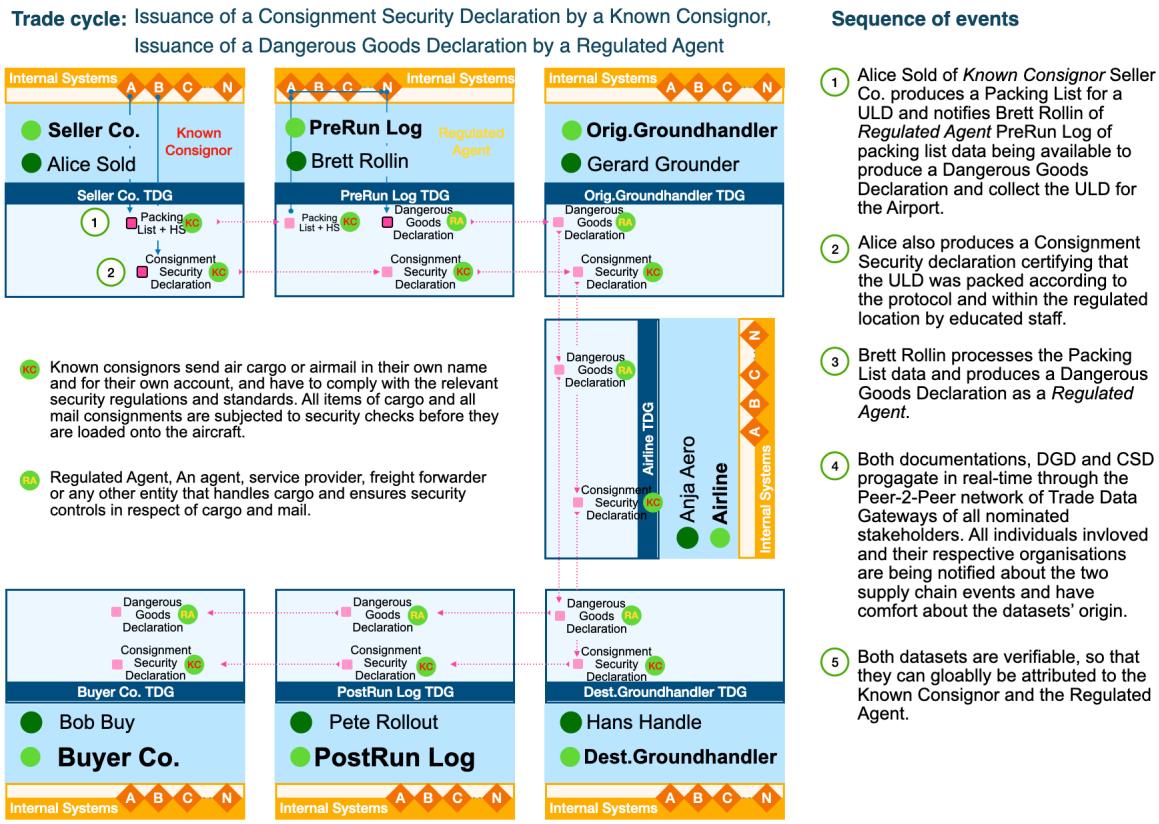


Figure 20: Globally verifiable documentation provided by Known Consignor and Regulated Agent in aviation

Supply chain event privacy

The supply chain events described above are visible to parties that have been included in the circle of stakeholders for a trade.

A party becomes "trade context internal" by either being a party to a trade (seller and buyer) or by being commissioned by the trading parties to provide services. A regulator or authority may have visibility on certain data of trades, likely in an aggregated manner.

Due to the peer-to-peer nature of the ISTTP-net, no other party can access the data of a trade. Not even the existence of a trade or a business relationship (trade metadata) can be seen by other parties except those that are "trade context internal."

Legal requirements placed on systems for ETRs

UNCITRAL's Model Law on Electronic Transferable Records (ML-ETR) is a legal framework developed by the United Nations Commission on International Trade Law (UNCITRAL) to facilitate the use of electronic transferable records in international trade. It aims to transfer the legal effects and legal treatment of traditional paper-based instruments to the digital world in a standardized way across all jurisdictions. The ML-ETR so became one of the principal sources for trade system's interoperability on the legal layer with a view to international harmonization of trade law. Find the other UNCTRAL sources listed below.

The ML-ETR suggests that law- and policy-makers shall strive for reforming their respective national commercial laws to make them assert that systems rendering and processing Electronic Transferable Records shall use 'Reliable Methods' to cater for 'Functional Equivalence' of an ETRs to the paper instrument that is replaced by the ETR.

Functional Equivalence involves implementing technological measures, such as digital signatures or other secure electronic means, to ensure that electronic transferable records can serve the same legal and practical purposes as their paper counterparts. It also takes into consideration that case law, collected over centuries, is an important source of law, especially in common law jurisdictions.

In general, Verifiable.Trade is not going to address ML-ETR or "Layer 0: Regulatory". However, among other things, that any protocol solution supporting Electronically Transferable Records[45] must reliably fulfill at least three legal requirements:

Integrity of the record

Imperceptible changes to an ETR must not be possible. Any protocol solution has to diligently create and maintain logs of all changes made to the ETRs it deals

45 Not all Electronically Transferable Trade Records have the same formal requirements. Most trade records do not require a paper bound signature / qualified signature. In such cases it is purely about the necessary evidential value. For example there are many cases where logistics providers conduct their "trade records" via WhatsApp or other messengers and deem the "time stamp" of such messengers sufficient for their documentation needs. This also applies to so called "seaway bills" which you could simply send via normal email and a pdf Attachment. On the other hand there are indeed documents with the special formal requirement of a paper bound signature, which may be substituted by qualified signature or similar technical means. For such cases the following bullet points are relevant.

with. These changes need to be reflected in the Trade Data Gateways of all current stakeholders around an ETR.

Exclusivity of control over the record

An ETR must at any time only have one clearly identifiable subject exercising control over it and this subject must be the only one able to assert the execution of the performance obligation that the ETR is securitizing. In simpler words and exemplified: At any time only one named person shall be able to ask for the merchandise to be handed over following the presentation of an vB/L or eW/R Prior controllers of the ETR must be reliably disenfranchised.

Singularity of the record

Digital objects like ETRs can be copied endlessly and unlike copies of paper, digital copies are not readily distinguishable. This means that documentation pertaining to an object and containing performance obligations thereto can exist numerous times. The singularity assertion asks for there being only one clearly distinguishable copy that effectively carries the performance obligation.

Singularity cannot be achieved offline in secure manner. To verify an ETR the Trade Data Gateway of its current exclusive controller must be online and reply to enquiries. However, being offline will soon have become a very rare condition for the exchange of ETRs.

Legal and Technological Framework

The ML-ETR provides guidelines for the standardized legal recognition of electronic transferable records, emphasizing the need for a reliable and secure framework to establish singularity. First implementations are in place. However, it is far away from being implemented globally.

Nevertheless, it provides valuable insights for some Verifiable.Trade related requirements. It outlines the criteria and conditions under which electronic records can be considered legally valid and enforceable, focusing on the integrity, reliability, and control of such records.

The implementation of ML-ETR comes with several challenges:

- **Technology and Infrastructure:**
  Implementing singularity in electronic transferable records requires robust technology and infrastructure. This includes data standards, secure storage, digital signing, encryption, and methods to track and control the record.

- **Legal Adaptation:**
  Jurisdictions need to adapt their legal frameworks to recognize and enforce the principles of reliability, integrity, exclusivity of control, and singularity in electronic records, ensuring consistency with international standards set by ML-ETR. Any solution must be consistent with any local legal framework to minimize the trade parties dependance on private rulebooks.

- **Interoperability**:
  Ensuring that electronic transferable records are interoperable across different systems and jurisdictions is crucial for their widespread adoption and effectiveness in international trade.

Integrity, Exclusivity of Control and Singularity in the Model Law on Electronic Transferable Records ensures that electronic records can be treated with the same level of trust and reliability as traditional paper documents.

The ML-ETR[46] should be seen in relation to further work of UNCITRAL:
- The Model Law on Electronic Commerce of 1998 (ML-EC)[47]
- The Model Law on Electronic Signatures of 2001 (ML-ES)[48]
- The Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services of 2022 (ML-IT)[49]

To address these requirements, Verifiable.Trade aims to implement strong authentication and authorization around any data object, making sure that copies can always be identified as such, by querying the Trade Data Gateway of the current exclusive controller. This will guarantee the verifiability of both “ownership” of and “control” over data.

- Ownership will be addressed by having access to the private key that was used for data signing. Only the owner/controller of the Autonomic Identifier (holding its private key) can create and maintain a data object.
- Control will be implemented by embedding the AID of the controlling entity.

This way any use of a data object will know for certain the authenticity of the origin as well as handling rights of other parties. All of this requires an efficient management of creating and revoking objects in related processes and protocols.

46 https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
47 https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
48 https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures
49 https://uncitral.un.org/en/mlit

Diligent means of authentication and authorization will also provide for high comfort levels on data sovereignty.

Virtual data containers and security

The Verifiable.Trade protocols take the data structure and content from documentations or messages and put them in virtual data containers. These data containers are then cryptographically secured or sealed with the private key of the owner. Or more precisely: the private key which controls the owners Autonomic Identifier[50].

This requires two main concepts:

Key management and signing of digital objects.
Key management addresses all functions for the creation, rotation and revocation of private/public key pairs which control a cryptographic identifier. The creation of the cryptographic identifier and the keys proving control over it is managed locally by the owner of the identifier. The propagation of keys and the identifiers these keys control, and the necessary validation and verification, uses the KERI protocol, the Key Event Receipt Infrastructure[51].

In effect, this implements a totally decentralized Public Key Infrastructure (PKI) with no need for a central instance or blockchain. These keys can then be used for signing and encryption. The payload of digital containers will be signed with the key of the respective owner. This owner must have the authority for signing. Authority can be delegated to legal or natural persons, devices or algorithms. The delegation requires that it is also cryptographically secured, and the respective roles can be verified.

Verifiable Credentials as containers
The containers used in TDGs are Authentic Chained Data Containers (ACDC)[52]. ACDCs can be chained and referenced. Chaining means that an ACDC can spawn off other containers that are then cryptographically bound to its predecessor. This is called “the chain of trust” with any top node being “the root of trust”. This mechanism can be used to create signed graphs that can be

50 Autonomic Identifier: A persistent identifier that does not rely on a verifiable data registry, but only a protocol for key management, which currently is KERI. See: https://medium.com/finema/the-hitchhikers-guide-to-keri-part-2-what-exactly-is-keri-e46a649ac54c
51 HTTP://KERI.ONE
52 ACDC specification https://github.com/trustoverip/tswg-acdc-specification

combined by delegation or reference to super graphs or graphs of graphs. Chained ACDCs form directed acyclic graph data structures.

To summarize the above[53]:

1. Trade documentations will be decomposed in data graphs
2. Each graph will be digitally signed with the key of the owner/controller.
3. Signed graphs can be assembled to define larger structures. This could be a documentation (part-of) or a reference view (which other graphs using the element).
4. Referential integrity will be assured by overlaying processes.
5. ACDC are the containers for signed graphs.

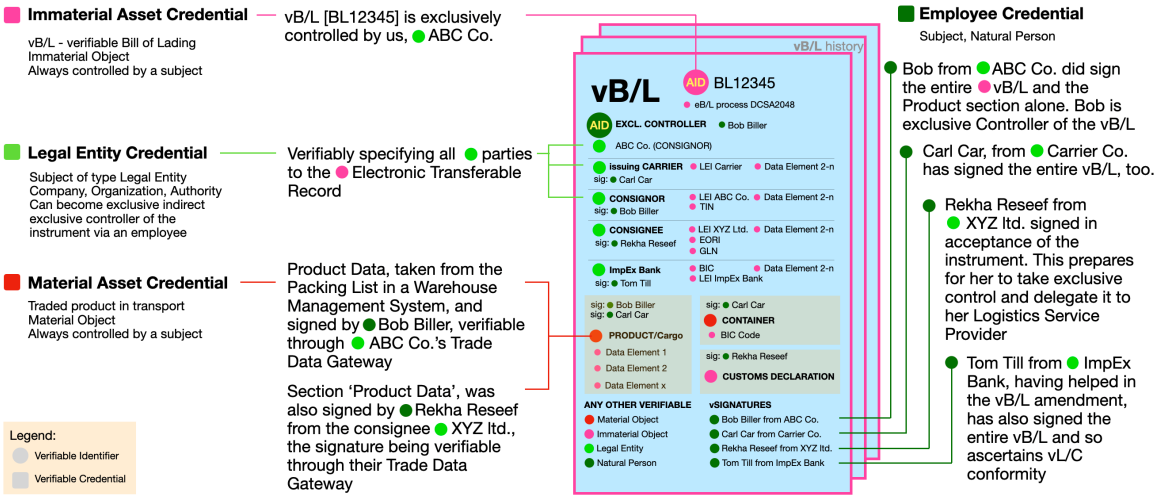


Figure 21: Verifiable bill of lading, all data elements are verifiable and feature flexible signing capabilities

Singularity of an ETR

The concept of singularity under the UN Model Law on Electronic Transferable Records (ETR) ensures that there is only one authoritative version of an electronic transferable record at any given time. This principle is vital to maintain the functional equivalence between electronic and paper-based transferable documents, such as bills of lading or promissory notes, which are as paper unique and singular in nature. Singularity ensures that the rights and obligations represented by the record are tied to one definitive version, preventing duplication or the creation of conflicting records.

53 Figures 21 and 22 show examples for verifiable ETRs

Any technical system governing ETRs needs to reliably only grant the rightful holder exclusive control over the record, ensuring that they are the only party able to exercise the rights the ETR represents. The principle is designed to be technology-neutral, meaning that it does not prescribe specific methods for achieving singularity but allows for various systems such as blockchain, cryptographic techniques, or centralized registries to ensure compliance.

Singularity plays a critical role in providing legal certainty, preventing fraud, and facilitating trust in electronic commerce. It ensures that when an electronic transferable record is transferred, the control over the singular record is seamlessly passed from one party to another, maintaining its integrity and unique status throughout its lifecycle.

The architecture that Verifiable Trade proposes guarantees full singularity within the peer-to-peer protocol network, without any central component.

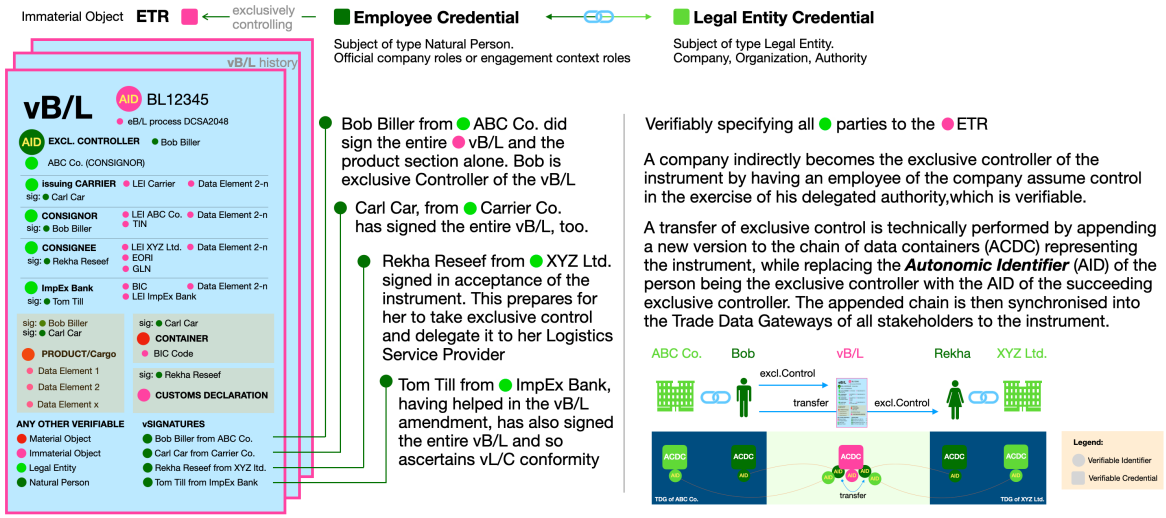


Figure 22: Transfer of exclusive control over an ETR occurring between employees using their verifiably delegated signing authority

Functionality of the Trade Data Gateway

Trade Data Gateway (TDG) is a synonym for several components. These components must implement all exchanges of data between legacy applications, the Verifiable.Trade protocol, and the provisioning of audit trails. An integral part of the TDG is the management of identity and role credentials in conjunction with primitives such as “create” and “revoke”.

The following components build the core functionality of TDGs:

1. **AuthentiGuard**
   Using 3rd party product interfaces for the management of user credentials, roles and authority
2. **AuthentiBridge**
   Import/Export handler library for content coming from legacy systems, implementation by commercial service providers at scale
3. **AuthentiGraph**
   Transforming legacy content into data graphs with the creation, signing and revocation of ACDC
4. **AuthentiVault**
   Local storage of all sent and received ACDCs including intelligent search functionality
5. **AuthentiXchange**
   Permissions based secure exchange of ACDCs between TDGs
6. **AuthentiAlert**
   Event notifications when creating and revoking ACDCs
7. **AuthentiPort**
   Allowing permissions-based remote pull requests
8. **AuthentiManager**
   Native Graphical User Interface (GUI) for managing TDGs and the related content access rights

AuthentiGuard

The AuthentiGuard module administrates all organizational identity and role credentials. It must ensure security, scalability, and ease of integration with various 3rd party systems such as Active Directory from Microsoft.

AuthentiGuard is supposed to manage user authentication, roles, and permissions using verifiable credentials. This system will leverage GLEIF's vLEI decentralized identity standards and technology to ensure a global root of trust and related transparency.

Components

1. Identity Provider (IdP)
   - Registration Service: Allows users to register by providing necessary details and generates an AID for each user.
   - Credential Issuer: Issues verifiable credentials to users after verifying their identities and roles.

- Credential Revocation: Manages the revocation of credentials in case they are compromised or no longer valid.

2. User Management
   - Profile Management: Allows users to view and update their profile information (local corporate wallet).
   - Credential Wallet: Secure storage for users' verifiable credentials. Can be a mobile or web-based wallet. Must be interoperable with common IAM systems.

3. Role Management
   - Role Definition: Allows to define roles with specific permissions.
   - Role Assignment: Assigns roles to users when vLEIs are created.

4. Authorization and Access Control
   - Access Policies: Defines policies for accessing resources based on roles represented by credentials.
   - Entitlement Engine: Evaluates access requests against defined policies and grants or denies access accordingly.

5. Audit and Compliance
   - Audit Logs: Records all actions and transactions for compliance and auditing purposes.
   - Compliance Checker: Ensures that all credentials and roles comply with relevant regulations and standards. Should be modular so users can plug in different compliance engines.

6. Integration Layer
   - APIs: Provides RESTful APIs for integrating with other systems and services.
   - Webhooks: Enables real-time notifications for events such as credential issuance, revocation, and role changes.

Workflows

1. User Registration and Credential Issuance
   - User registers through the IdP and provides necessary identity proofs.
   - IdP verifies the information and issues a verifiable credential, which is stored in the user's credential wallet and or hosted corporate wallets and IAM systems.
   - This includes onboarding of external subjects, i.e. "external employee in role R at company ABC is allowed to send in documentation type XYZ".

2. Role Assignment
   - Admin defines roles and assigns them to users based on their verifiable credentials.
   - Users receive role credentials that are stored in their credential wallet.

3. Authentication and Authorization
   - User requests access to a resource.
   - Access Control Engine checks the user's credentials and roles against access policies.
   - If the user meets the criteria, access is granted; otherwise, it is denied.

4. Credential Management
   - Users can update their profile and credentials through the profile management service.
   - Admins can revoke credentials if necessary, which is reflected in the wallet.

5. Audit and Compliance
   - All actions are logged for auditing purposes.
   - Compliance checker runs periodic checks to ensure all credentials and roles comply with regulatory requirements. Wallets should be modular so users can plug in different compliance engines.

AuthentiBridge

This module connects any TDG locally with the relevant outside legacy infrastructure. Designing a software module that acts as an import-export interface between supply-chain legacy applications requires careful consideration of interoperability, data consistency, and ease of integration. This should be done by software providers specialized in this area, e.g. CPI from SAP or Lobster, using the TDG API.

The AuthentiBridge module facilitates the seamless exchange of data between disparate legacy supply-chain systems and the TDG, enabling efficient import and export operations across different platforms.

Legacy Supply Chain Management (SCM) software and platforms play a vital role in optimizing processes, enhancing efficiency, and facilitating information exchange among stakeholders. This software comes in various forms, allowing businesses to select programs that meet their specific needs. For example, manufacturers, retailers, and e-commerce companies frequently use demand planning software to align production and inventory levels with customer demand.

Companies that manage the storage and movement of goods can utilize inventory management software to monitor product quantities and prevent overstocking or understocking. Likewise, transportation businesses can leverage transportation management systems to optimize shipping and delivery services. Many of these software programs are designed to seamlessly integrate with other systems, promoting collaboration and reducing silos. However, they lack a security layer for the exchange of cryptographically sealed information.

Technology is used in each stage of the supply chain, from planning and procurement to production and delivery. Some SCM software programs specialize in particular aspects of supply chain management, such as demand forecasting, product lifecycle management, or transportation, while others offer a comprehensive overview of supply chain logistics.

Legacy SCM featured software solutions comprise:

- Inventory Management
- Warehouse Management
- Transportation Management
- Supplier and Customer Relationship Management
- Demand and Production Planning
- Enterprise Resource Planning (ERP)
- And others …

For each category are numerous products and software packages available. Also new suppliers have entered the market with newly designed platforms based on distributed ledger technology.

AuthentiBridge is supposed to connect those legacy systems with TDGs via API and script language library. Wherever possible existing data standards must be used. Key Features of this module are:

1. Data Transformation and Mapping:
    - ETL (Extract, Transform, Load) Engine
      Extracts data from source systems, transforms it into a standard format, and loads it into the target TDG.
    - Mapping Templates: Pre-defined and customizable templates for data mapping to ensure compatibility between different data formats and ACDC structures.

2. Connectivity and Integration:
   - Adapters/Connectors: Provides connectors for various legacy systems (e.g.,).
   - APIs and Web Services: RESTful and SOAP APIs for real-time data exchange.
   - Batch Processing: Supports batch data transfers for high-volume transactions.

3. Data Validation and Error Handling:
   - Validation Rules: Ensures data integrity by applying business rules and validation checks during import/export operations.
   - Error Logging and Alerts: Logs errors and sends alerts for any issues encountered during data transfer, with detailed error messages for troubleshooting.

4. Security and Compliance:
   - Data Encryption: Encrypts data during transit to ensure security.
   - Access Control: Role-based access control to restrict access to sensitive data and operations. Access and data exchange is encrypted.
   - Compliance: Ensures compliance with relevant standards and regulations (e.g., GDPR, CCPA) on a technical level. For example: The solution should be designed “privacy first” and should document where which personal data may be stored and why. But this does in no way “ensure” compliance of the actual usage of the solution. It is rather following best practice while programming and offering the abstract software solution.
   - The logistic process itself is a business process of the user. Just as the terms and conditions of the trade is fully under control of the user. Trying to solve this complexity on behalf of the user- is a mission impossible.

5. User Interface:
   - Dashboard: Centralized dashboard for monitoring import/export activities, system health, and performance metrics.
   - Configuration Panel: UI for configuring connections, mapping rules, and scheduling jobs.

AuthentiBridge will need ability to mimic the endpoints that legacy systems are accustomed to send to. The following workflows will be supported:

1. Import Process:
   - A legacy application sends data to the AuthentiBridge module. Alternatively, TDG could pull data via API.

- The ETL engine extracts the data and calling the AuthentiGraph transforms it into a standard ACDC format.
- The Validation Engine checks the data for consistency and errors.
- Any errors are logged and alerts are sent to the relevant personnel.

2. TDG related Export Process:
   - Data is extracted from the source system by the ETL engine.
   - The Data Mapper transforms the data into the required format for the target system.
   - The transformed data is validated, and any errors are handled.
   - The data is then transmitted from a local TDG54 to the target legacy application or external partner system.

AuthentiGraph

AuthentiGraph is designed to transform legacy content into data graphs[55], ensuring the creation, signing, and revocation of Authentic Chained Data Containers (ACDC). This module enhances data integrity, traceability, and security, making legacy data more interoperable and reliable.

Key features of AuthentiGraph comprise:

1. Data Transformation:
   - Legacy Content Extraction: Extracts data from various legacy systems, databases, and file formats.
   - Graph Data Model Conversion: Converts extracted data into graph data models, enabling easier relationships and connections among data points.

2. ACDC Management:
   - Creation of ACDC: Generates Authentic Chained Data Containers from the transformed graph data, encapsulating data with a unique identifier.
   - Signing of ACDC: Digitally signs each ACDC to ensure authenticity and integrity, using cryptographic methods.
   - Revocation of ACDC: Provides mechanisms to revoke ACDCs when data is found to be outdated, incorrect, or compromised.

54 Local towards the owner. Technically it could be cloud based.

55 Structured data is key for more efficiency and verifiability. However, knowing from experience, onboarding business partners to exchange structured data is still problematic. Paper based exchange will not cease to exist the next 10 years. TDG also supports PDF documents from legacy systems, which can be included in ACDCs (e.g. the hash).

3. Interoperability and Integration:
   - Data Mapping and Standardization: Supports mapping legacy data to standard formats and ontologies, ensuring consistency and interoperability.

4. Security and Compliance:
   - Data Encryption: Ensures data is encrypted both in transit and at rest using KERI.
   - Access Control: Implements role-based access control (RBAC) to manage permissions and access to data.
   - Audit Trails: Maintains detailed logs of data transformations, ACDC creation, signing, and revocation for compliance and auditing purposes.

5. User Interface:
   - Dashboard: Provides a comprehensive view of data transformation processes, ACDC statuses, and system health.
   - Configuration Panel: User-friendly interface for setting up data sources, transformation rules, and managing ACDCs.

6. Performance and Scalability:
   - Scalable Architecture: Designed to handle large volumes of data and high transaction rates.
   - Optimized Processing: Utilizes advanced algorithms and caching mechanisms to ensure high performance and low latency.

7. Core Components:
   - Graph Converter: Converts legacy data into graph data models.
   - ACDC Engine: Manages the creation, signing, and revocation of ACDCs.

8. User Interface Layer:
   - Dashboard: Offers real-time insights and monitoring of the module's operations.
   - Configuration Panel: Allows for easy configuration and management of the module's features.

AuthentiVault

AuthentiVault is designed to provide local storage for all sent and received Authentic Chained Data Containers (ACDCs), incorporating intelligent search functionality to ensure efficient data retrieval. AuthentiVault will also provide audit trails for all data exchange between TDGs. Key Features of this module are:

1. Local Storage Management:
   - ACDC Repository: A centralized storage system for all sent and received ACDCs, ensuring data is securely and readily accessible.
   - Redundancy and Backup: Implements redundancy and backup mechanisms to protect against data loss and ensure data availability.

2. Intelligent Search Functionality:
   - Advanced Search Engine: Utilizes in-memory indexing and search algorithms to enable quick and accurate retrieval of ACDCs based on various criteria.
   - Filters and Facets: Supports filtering and faceting based on metadata, timestamps, sender/receiver information, and other relevant attributes.

3. Data Integrity and Security:
   - Digital Signatures: Ensures the authenticity and integrity of ACDCs through verifying digital signatures.
   - Access Control: Implements role-based access control (RBAC) to manage permissions and ensure that only authorized users can access sensitive data.

4. User Interface:
   - Dashboard: A centralized interface for managing and monitoring ACDCs, offering real-time updates and analytics.
   - Search Interface: A user-friendly interface for performing searches, with options for advanced search criteria and filters.
   - Configuration Panel: An intuitive panel for configuring storage settings, access controls, and search parameters.

5. Performance and Scalability:
   - Scalable Storage Solutions: Designed to handle large volumes of ACDCs and scale as needed to accommodate growing data needs.
   - Optimized Search Performance: Implements caching, indexing, and optimization techniques to ensure fast and efficient search results.

6. Architecture using distributed key value store databases
   - ACDC Repository: Securely stores all ACDCs for easy access and management.
   - Search Engine: Indexes ACDCs and provides intelligent search capabilities.
   - Security Module: Manages encryption, digital signatures, and access controls to ensure data integrity and security.

AuthentiXchange

AuthentiXchange is a robust protocol designed to facilitate the secure and permission-based exchange of Authentic Chained Data Containers (ACDCs) between Trade Data Gateways (TDGs). It is built to ensure the integrity, confidentiality, and authenticity of data transfers in a distributed environment. AuthentiXchange operates on top of the TCP/IP stack and the Issuance and Presentation Exchange Protocol (IPEX), leveraging these foundational protocols to provide a reliable and secure communication layer.

A major aspect of this module is that it will implement business logic across ACDCs. For instance, the revocation of a data container and the creation of a new one with the same content but different user credentials is a key requirement. Managing the rules for the business log is a vital part of AuthentiXchange.

Key Features of this module are:

1. Permission-Based Exchange
   - AuthentiXchange ensures that only authorized TDGs can request and receive specific ACDCs based on predefined permissions. It implements fine-grained access control policies to govern data exchange, ensuring that only those with the appropriate permissions can access sensitive information.

2. Secure Communication
   - The protocol utilizes KERI for encryption to protect data in transit, ensuring confidentiality and integrity. Digital signatures are employed to verify the authenticity of ACDCs, preventing tampering and ensuring that data has not been altered during transmission.

3. Interoperability
   - AuthentiXchange is designed to seamlessly integrate with existing TCP/IP networks and the IPEX protocol. It supports KERI and chained verifiable credentials for identity verification up to the root of trust.

4. Business Logic Integration
   - A major aspect of AuthentiXchange is its ability to implement business logic across ACDCs and TDGs. For instance, the protocol supports the revocation of a data container and the creation of a new one with the same content but different user credentials. AuthentiGraph has to be a part of this. Revocation (i.e. cancellation) information mostly come from the legacy system. Managing the rules for this business logic is a vital part

of AuthentiXchange, ensuring that data exchanges adhere to legal and organizational policies and requirements.[56]

5. Audit and Compliance:
   - Through AuthentiVault, AuthentiXchange maintains detailed logs of all exchanges, including timestamps, TDG identifiers, and ACDC details for auditing purposes. This ensures that all actions can be tracked and reviewed, providing transparency and compliance with relevant regulatory requirements as well as data protection and privacy regulations.

AuthentiXchange sits in the protocol stack as follows:

1. TCP/IP Layer:
   - Provides the basic transport and networking functionalities, ensuring reliable delivery of packets.

2. IPEX Layer:
   - Manages the exchange and presentation of credentials, establishing a secure framework for identity and credential management between TDGs.

3. AuthentiXchange Layer:
   - Adds an additional layer of security and permission management for the exchange of ACDCs.
   - Coordinates with the underlying IPEX layer to handle credential verification and presentation.

AuthentiXchange supports the following workflows:

1. Request Initialization:
   - A TDG discovers a trade peer's TDG using Verifiable.Trade's discovery protocols based on OOBI and IPEX57.
   - The TDG initiates a request to exchange an ACDC with another TDG.
   - The requesting TDG verifies its permissions to access the requested ACDC.

2. Authentication and Authorization:
   - AuthentiXchange verifies the identity of the requesting TDG using its AID and associated verifiable credentials.

---

56 This is likely based on a rule engine to address the challenges of allowing for business logic implementation, e.g. REGO, It can store its rule set in GIT to keep it versioned, author-controlled, and capable of evolving.

57 https://www.linkedin.com/posts/nuttawut-kongsuwan-682661169_keri-jargon-in-a-nutshell-part-3-oobi-and-activity-7088831643028770816-Dhdf

- Checks the access control policies to ensure the requesting TDG has the necessary permissions to access and exchange data in a certain trade context.

3. Data Exchange:
   - Upon successful authentication and authorization, the ACDC is securely transmitted over the network.
   - All further updates to previously exchanged ACDCs are being notified to all trade data gateways going further, unless subscription has been halted in pursuit of policies.
   - Data is encrypted during transit to ensure confidentiality and integrity.

4. Verification and Acknowledgment:
   - The receiving TDG verifies the integrity and authenticity of the received ACDC using digital signatures.
   - An acknowledgment is sent back to the requesting TDG, confirming successful receipt and verification.

5. Audit Logging:
   - All exchanges are logged with relevant details for auditing and compliance purposes.
   - Logs include information such as the identities of the TDGs involved, timestamps, and the nature of the exchanged ACDC.

AuthentiXchange provides a robust and secure mechanism for the exchange of linked ACDCs, ensuring that data transfers are performed with the highest levels of security and integrity while adhering to strict access control policies.

AuthentiAlert

AuthentiAlert is a notification system designed to provide real-time alerts for the creation and revocation of Authentic Chained Data Containers (ACDCs). This module ensures that all relevant stakeholders are promptly informed of critical changes, enhancing transparency, security, and operational efficiency in managing ACDCs. AuthentiAlert is built to respect the Data Sovereignty requirements of parties in trade.

Key Features of this module are:

1. Real-Time Notifications:
   - AuthentiAlert delivers instant notifications to remote TDGs whenever an ACDC is updated or revoked. This ensures immediate awareness of

changes, enabling quick and automated responses to any issues or updates.

2. Customizable Alerts:
   - Users can customize the types of notifications they receive. Options include email, push notifications, and in-app alerts, allowing users to be informed about changes to underlying ACDCs.

3. Event Logging:
   - Using AuthentiVault, every event, including ACDC creation and revocation, is logged with detailed information such as timestamps, involved entities, and the nature of the change. This provides a comprehensive audit trail for compliance and review purposes.

4. Integration with Existing Systems:
   - Using AuthentiBridge, AuthentiAlert can integrate with existing IT and security systems through APIs and webhooks. This ensures seamless incorporation into current workflows.

5. Role-Based Notification:
   - Notifications can be tailored based on user roles and permissions. For instance, administrators may receive detailed alerts about every change, while regular users might only be notified of events directly affecting their credentials.

6. Security and Compliance:
   - AuthentiAlert allows that all notifications and event logs are technically secure and comply with relevant technical regulations and standards. Data encryption and access controls are implemented to protect sensitive information.

AuthentiAlert supports the following workflows:

1. Event Detection:
   - Creation: When an ACDC is created, AuthentiAlert detects the event through integration with the ACDC management system.
   - Revocation: Similarly, when an ACDC is revoked, the system immediately recognizes the action.
   - Updates: When an ACDC is updated, i.e. undergoes a status change. (this may be a combined revocation and re-issuance

2. Notification Generation:
   - AuthentiAlert generates a notification message containing relevant details about the event. This includes information such as the type of event (creation or revocation), the affected ACDC, the entities involved, and the timestamp.

3. Delivery:
   - The notification is delivered to the appropriate stakeholders through the configured channels. This ensures that the right people are informed promptly.

4. Recovery:
   - Notifications can be used to recover from system outages of TDG nodes. The Alerts build the event queue necessary for a consistent and accurate state of each TDG.

5. Event Logging:
   - All events are logged in a secure database. Each log entry includes comprehensive details about the event, ensuring a robust audit trail.

6. User Actions:
   - Users and administrators can take appropriate actions based on the notifications received. For instance, they might need to update records, adjust access permissions, or investigate potential issues.

7. Security Considerations:
   - Encryption: All notification data is encrypted vias KERI both in transit and at rest to protect sensitive information.
   - Access Controls: Only authorized users can view and manage notifications and logs, ensuring that sensitive information is accessible only to those with appropriate permissions.
   - Compliance: AuthentiAlert complies with industry standards and regulations, such as GDPR, ensuring that all data handling practices are lawful and ethical.

AuthentiAlert enhances the management of ACDCs by providing timely and detailed notifications of creation and revocation events. This ensures that all stakeholders are aware of critical changes, enabling prompt action and maintaining the integrity and security of the decentralized data management system.

AuthentiPort

AuthentiPort is a secure API and protocol enabling permissions-based remote pull requests for Authentic Chained Data Containers (ACDCs). It ensures that only authorized organizations and user roles can request and retrieve specific data containers from remote locations, maintaining strict access controls and ensuring data integrity.

An example for a use case could be pull requests from customs single window applications

Key Features of this module are:

1. Permissions-Based Access:
   - Only authorized users can initiate pull requests, ensuring secure data retrieval.

2. Secure Communication:
   - Utilizes encryption to protect data during transmission.

3. Seamless Integration:
   - Integrates with existing systems and protocols for streamlined operations.

4. Audit Logging:
   - Tracks all pull requests for transparency and compliance.

5. Data Synchronization:
   - Securely syncs data containers across different systems or locations.

6. Remote Data Access:
   - Enables secure access to data for remote teams or partners.

7. Compliance:
   - Ensures that data retrieval processes meet regulatory standards.

AuthentiPort facilitates secure and efficient remote data retrieval, enhancing the flexibility and security of ACDC management.

AuthentiManager

AuthentiManager is the native Graphical User Interface (GUI) designed for the comprehensive management of Trade Data Gateway instances (TDGs).

AuthentiManager provides a centralized, intuitive platform for administrators to manage and optimize the use of their Authenti-Suite. Its graphical interface simplifies complex tasks, enhances user experience, and ensures that the system runs smoothly and securely.

The feature set derives from the GUI requirements of all Authenti-components.

Adoption

Managing the adoption of an open-source protocol for international trade and supply-chain involves multiple facets: technical, strategic, organizational, and collaborative. At the same time any new attempt for digital trade must demonstrate superior capabilities, lower costs and inclusion of all parties.

The following table shows how data is rendered today. For each option the suggested technology is shown. This table might help in assessing legacy applications as well as suggested new approaches:

Data Objects	Delivery Mechanism	Properties	Examples
Paper	Standard-Mail	100% globally interoperable, 0% programmable	ICC's certificate of origin
Simple PDF	e-Mail and API	Technical storage and access is easy at the endpoints, very limited programmability	e-Invoices, Docusign-solutions
Enhanced PDF with data elements allows for storage of data elements	Shared data platform with deliberate access rights, traditional or Blockchain	Invariably limited interoperability	Legacy applications, enigio trace:original, DNI Initiative
Machine readable data formats, e.g. XML, JSON	Shared hash codes on DLT, but decentralised data storage	Verifiablity of data element aggregates ("documents")	IOTA, TradeTrust
Authentic machine-readable data (ACDC)	Protocol based exchange of authentic, machine-readable data, peer-2-peer and without any central component	Verifiablity of single data elements Signing of arbitrary data element subsets	Verifiable.Trade

Figure 23: Current approaches for trade data exchange

Here is how to approach the adoption of Verifiable.Trade protocols:

1. Make it simple
   - Choose early adopters from top-tier international buyers (e.g. Nestle, Novartis),

- Work with them on choosing providers of commodities and intermediate goods,
- Choose logistic partners and also customs organizations,
- Define a small subset of trade documentation as test cases,
- Limit legacy interoperability in AuthentiBridge to a few key legacy systems, as a first step/test case,
- Setup a professional project organization,
- Develop Proof-of-Concepts,
- Publish success stories,
- Scale the approach with relevant stakeholders.

2. Stakeholder engagement and collaboration: Identify key stakeholders
   - Government Agencies: Customs, regulatory bodies, trade ministries,
   - Businesses: Importers, exporters, logistics companies, manufacturers,
   - Industry Associations: Chambers of commerce, industry-specific groups,
   - Technology Providers: Developers, software companies, blockchain experts,
   - Standards Organizations: ISO, GS1, WCO, UN/CEFACT.

3. Stakeholder engagement and collaboration: Establish collaborative frameworks:
   - Consortium Formation: Create a working group to oversee the adoption process,
   - Public Consultations: Engage with broader public and smaller stakeholders to gather diverse input.

4. Stakeholder engagement and collaboration: Fund raising
   - Determine funding needs,
   - Identify potential funding sources – Develop personas,
   - Develop a compelling value proposition,
   - Engage and persuade stakeholders,
   - Build and maintain trust,
   - Leverage partnerships.

5. Standards:
   - Use existing standards wherever possible,
   - Develop comprehensive technical documentation, including API specifications, data formats, and integration guidelines,
   - Ensure compliance with international standards and regulatory requirements.

6. Pilot Programs and Testing
    - Select pilot partners: Choose diverse partners across different regions and industry sectors,
    - Real-world scenarios: Test the protocol in real-world scenarios to challenges and gather data,
    - Implement pilot projects,
    - Establish a feedback loop for continuous improvement based on pilot results.

7. Education and Training
    - Conduct regular training sessions to educate stakeholders on the protocol.
    - Create detailed user guides and tutorials.
    - Establish support channels such as forums, help desks, and FAQ sections.

8. Marketing and Advocacy
    - Conduct outreach programs to raise awareness about the benefits of the protocol.
    - Publish case studies demonstrating successful implementations and benefits.

Glossary

ACDC	Authentic Chained Data Container
AID	Autonomic Identifier
API	Application Programming Interface
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
DPO	Days Payable Outstanding
eB/L	electronic Bill of Lading
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
ERP	Enterprise Resource Planning
ESG	Environmental, Social, Governance
ETR	Electronic Transferable Record
IP	Intellectual Property
IPEX	Issuance and Presentation Exchange Protocol
ISTTP	International Secure Trade Transfer Protocol
ISTTP-Net	International Secure Trade Transfer Protocol Network
KTDDE	Key Trade Document Data Elements
LEI	Legal Entity Identifier
Letter of Credit	Payment Risk Mitigation instrument in trade finance
ML-EC	Model Law on Electronic Commerce
ML-ES	Model Law on Electronic Signatures
ML-ETR	Model Law on Electronic Transferable Records
ML-IT	Model Law on Identity Management and Trust Services
P2P	Peer to Peer
PDF	Portable Document Format
PKI	Public Key Infrastructure
SAID	Self-Addressing Identifier
SDO	Standards Development Organization
SME	Small and Medium Enterprises
TDG	Trade Data Gateway
vB/L	verifiable Bill of Lading
S/LE	Subject of type Legal Entity
S/NP	Subject of type Natural Person
O/Mat	Material Object
O/Imt	Immaterial Object
eW/R	electronic Warehouse Receipt
vW/R	verifiable Warehouse Receipt

Table of figures

Prompt:
“Hey ChatGPT, can you please draw a picture of happy kids from all across the world arranging marbles into a world map, where the lighting and smiles capture a warm, friendly moment of teamwork and creativity?”
Iteration 2:
“Hey ChatGPT, the middle east seems not represented. Can you please try again? And please swap the slides in the background with tiny sea freight containers, which look like they have been miniaturized to serve as playground kit.”

This led to the picture on page one!