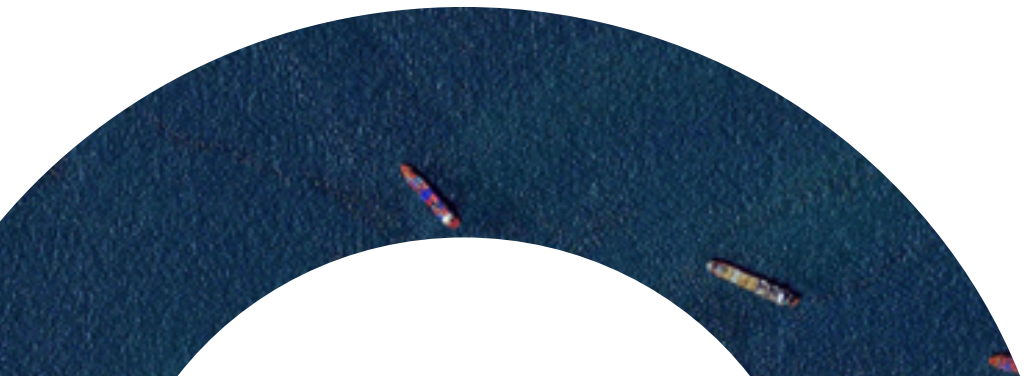
ICC Digital Standards Initiative

Trust in Trade

Verifiable Trust: A foundational digital layer underpinning the physical, financial, and information supply chain

March 2023

In this report



1 Executive summary

Digital trade, or the application of digital technologies to trade and supply chain processes, is an opportunity to drive efficiency, speed, and resilience for companies, industries and countries that rely on trade for growth. The pace of technological advancement, and the falling cost of computing power and storage, now make the benefits of digitally-enabled trade accessible to more parties than ever before.

However progress towards digital trade is slow - less than 5% of merchandise trade is digitalised by most estimates - with SMEs and the emerging markets relatively slower to adapt. Barriers to digital trade include the lack of an enabling policy environment, the proliferation of multiple digital trade practices and standards, as well as a lack of capacity and culture of data sharing. The ICC Digital Standards Initiative (DSI) was established to address these barriers.

Specifically this report is the outcome of the DSI's Industry Advisory Board's Trusted Technology Environment (TTE) working group, which was established in Spring 2022, to provide a perspective on how to create and maintain a technology environment that would facilitate trade digitalisation at scale. A particular focus was placed on issues of authentication, verification and security, with the caveat that the group would remain neutral with regard to the choice of technology and vendor/platform, and be inclusive of organisations regardless of their level of technological maturity.

In essence, transforming analogue supply chain and trade processes – represented by key trade documents – by the use of automated data transfer and sharing, the verification, authentication and protection of such data becomes paramount. Thus as DSI proposes alignment of digital standards for key trade documents (viz. the key trade documents and data environment working group), this report proposes to start the conversation about technology principles for the global digital trade ecosystem.

Trade transactions involve sometimes dozens of participants and roles along international supply chains. These parties undertake many interactions which frequently are documented in separate and security - encapsulated systems, resulting in digital islands, which often do not align to available data standards. Data transition between these 'islands' is mostly provided by using paper documentation or electronic paper substitutes. This makes end-to-end digitalising of all interactions between the participants in the execution of a trade transaction particularly challenging. It is aggravated by the often high number of parties involved in data exchange along trade processes.

Often, parties may invest in trade digitisation which retains conventional business processes but facilitated by electronic means. The goal of trade digitalisation is to reduce the friction or duplication of the information flow of data along the supply chain, by automating the data path in a secure way that crosses boundaries between entities and jurisdictions. Often called a digital twin, the data path in an international supply chain forms its own data-supply chain that modulates or facilitates the associated physical and financial supply chain. From a

secure data transmission perspective, the important data supply chain boundaries are those that define trust-domains. Information (data) that can cross trust-domain boundaries without losing its trustworthiness provides what we call transitive trust. Low friction transitive trust could be a primary enabler for automating secure international data supply chains and hence all supply chains that are reliant on information (data) as a facilitator.

To further the degree of automation, visibility, and manageability, among many other goals, business process chains should become interwoven between the systems of trading parties and their service providers. Breakpoints in the form of paper or paper-substitute 'interfaces' should be replaced by interfaces conveying data, preferably in real-time. However, this also requires replacing conventional trust mechanisms, like ink-signed paper. In other words, digitising supply chains by using electronic signing of paper substitutes (i.e. PDF) with a semi-digital equivalent (i.e. DocuSign or Adobe Sign) will produce efficiency gains or labor saving, but not the gains in terms of trust, traceability or anti-fraud.

In short, every digital interaction in an international trade transaction should become verifiable, non-repudiable, retro-traceable, accountable and auditable for any required retention period.

Trust, in its traded semantic, should be established through verifiability. The overall conception should be developed around the "never trust, always verify" mantra, embodied by the counterintuitively labelled "Zero Trust Architecture" movement, which is rapidly growing within the cybersecurity industry. A new, verifiable digital layer beneath the information supply chain, which itself underpins the physical and financial supply chains, is required: the "trust supply chain".

All interactions between two subjects of any country and a subject and an object (such as goods or containers) being part of a digital fabric would be supported by this trust layer, which would be abstracted and independent from any layer above. A trade asset created in system A and routed through system B and C, must be verifiable in system D to be reliably attributable to its original creator in system A.

A trust supply chain providing such "transitive trust" is a prerequisite for digitalising - as opposed to simply digitising - supply chains and will provide means for weaving trusted end-to-end supply chain processes across organisational boundaries. Strong cryptography deployed in Public Key Infrastructures (PKI) is instrumental to achieving this goal.

Zero Trust Architecture, an architecture proposal/paradigm for building organisation's future IT landscapes, will help lay further foundations, but also requires verifiable trust to provide for stringent and repetitive authentication and authorisation. Only the use of cryptographically produced verifiability will ensure that the multitude of parties in trade will be protected in a legally authoritative fashion along a chain of services.

An indispensable part of Zero Trust Architecture and the practice of cryptographically produced verifiability is the use of digital identity to secure, sign and authenticate data sets that document any transaction along the supply chain even as multiple borders are crossed. Basically, if parties rely on exchanged datasets in lieu of PDF and physical documents, these need to be signed and authenticated by the relevant parties, which can be achieved securely using digital ID.

Use of digital ID will also address the interoperability of authentication and authorisation as a key building block for the digital trade ecosystem. Digital identities will gradually replace conventional means of "signing off" on agreements and facts, which are exchanged in trade.

The Zero Trust Architecture[1] paradigm will change application landscapes widely over the coming decade. Network perimeters like firewalls are already losing their relevance to protect ringfenced resources, as the trend to cloudification moves enterprise resources into serviced data centres. Roaming resources, as "rolling stock" equipped with internet of things (IoT) devices, further blur the lines between internal and external networked resources, as "rolling stock" can be delivery trucks where the smartwatch of a driver becomes an instrument to sign off on a Delivery Note, or a ship moored in a port communicating with the port's infrastructure regarding its cargo.

Consequently, identity and access management functions in organisations will have to re-center their activity from role-based access to application functionality to resource-centric access admission in a more dynamic style. Cloud computing is already asking for this and supply chains partners which adapt earlier will position themselves for advantage in the future.

The foregoing principles – the application of Zero Trust Architecture to enable cryptographically produced verifiability and the use of digital identity – will enable data sharing that is key to efficiency, traceability and accuracy along the supply chain. However there is one caveat.

Interoperability between systems and software instances is critical to avoid investments in trade digitalisation turning into sunk investments in digital silos or islands. Interoperability is to be achieved by standardisation conducted on multiple layers, whereby standardisation efforts usually overarch single layers. It starts on the technical infrastructure layer, continues on the data layer, to reach up to the service layer and further up to the legal layer.

Digital identity for instance requires standardisation on all these layers to become fully interoperable.

Suffice to say that interoperability of data – and alignment of parties data infrastructure and practices to established standards for data sharing along the supply chain – will allow digital trade to become the de facto practice at scale. The present concerns of data security, particularly related to data flow across borders, can all be addressed by aligning to the technology principles established herein, namely the use or application of:

- Zero Trust Architecture, backed by cryptographically produced verifiability
- Digital ID for all parties transacting
- Interoperabilty for all data, implying alignment with global standards where they exist

The TTE working group has prepared this paper to build on the knowledge and work of others in the field, in order to contribute to the task of digitalising global trade in a secure, trusted manner taking advantage of the technologies available today. It goes without saying that as technologies advance, the technology principles proposed and described herein may evolve and improve our understanding of verifiable trust in the emerging digital fabric of international trade.

We invite feedback and contributions which might advance our collective thinking on how the concepts enshrined herein can enable trade digitalisation in the interests of efficiency, inclusion and sustainability worldwide.

[1] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

2 The Trusted Technology Environments (TTE) working group

The TTE is composed of the working group Co-chairs Stephan Wolf and Richard Morton† and the industry experts nominated by the ICC DSI members and the WG Chairs. The group consists of trade and standards experts from different fields and organisations who jointly contributed the recommendation paper for wider industry audience supporting the digitalisation of trade, including all parties in the supply chains and promoting existing and suitable standards and technical solutions supporting paperless trade.

The purpose of the TTE working group is to support the development and implementation of high-quality and informed recommendations for the International Chamber of Commerce (ICC) Industry Advisory Board (IAB) in line with the objectives of the Digital Standards Initiative (DSI) which this paper provides.

2.1. Members of the working group

Usman Aliyu	Dangote
Nico DeCauwer	Port of Antwerp
Ivano Disanto	Insiel S.p.A
Emmanuellue Ganne	WTO
Stephan Graber	FIATA
Sudha Gupta	BHP
Gerard van der Hoeven	iSHARE Foundation
Hans Huber	id4.trade GmbH
Amar Jandu	BHP
Aaron Kane	SWIFT
David Leung	BIS Innovation Hub
Derrick Loi	Ant Group
Hannah Nguyen	ICC Digital Standards Initiative
Benedicte Nolens	BIS Innovation Hub
Chris O'Neil	BHP
Phillipe Richaud	Finastra
Yefei Song	Ant Group
Louise Taylor Digby	SWIFT
Michael Vrontamitis	Finastra
Lucy Wong	BIS Innovation Hub
Stephan Wolf	GLEIF

3 Introduction

In international trade, many participants interact along a network of supply chains. Physical movements of goods are superimposed by the flow of financial resources. Both flows - the physical and the financial supply chain - are underpinned by many interwoven information flows - the information supply chain.

Almost all events in the information supply chain are subject to legal considerations, which vary in the perspectives that the individual participants assume. In the end, all actors in trade want to prove they have fulfilled their respective duties. In the pursuit of de-risking their activities, they all desire certainty on questions like:

"Will I be paid?"

"Are certified properties (like lead free circuitry) indeed facts or fake?"

"Has my consignment been delivered in good shape?"

"Does my labelling for hazardous goods meet the requirements in both Japan and Germany?"

"Will my cargo be released in time?"

"Can I perform my duties to supply required information at acceptable efforts?"

Be it certifying a good's origin as an input for customs clearance (Certificate of Origin), the fact of a consignment having been loaded on a ship as the point of risk passing (incoterm event), a case-by-case information of a buyer's credit status (Letter of Credit), information accompanying a transport of chemicals (Security Data Sheet), or a certification of the electronic circuits in a mobile phone being soldered lead-free (RoHS compliance certification), all legally meaningful information conveyed along the information supply chain must be relied upon as all this information can potentially become subject to later reference, scrutiny, and also litigation.

With the ever-increasing number of trade relations and rising quantities of goods traded, conventional means of information exchange on signed paper will lead to ever-growing efforts on rendering desired trust levels. Next to the rising quantities stands the need for an enhanced information density in supply chains, to improve steerability or fulfil intensified traceability assertions in pursuing ESG goals.

In an increasingly denser woven digital fabric of applications and networks, reliance on trust mechanisms provided by proprietary applications and protected networks appears too complicated and laborious to look through, and almost impossible to reliably register in a structured fashion for later reference, when using conventional, often paper-based means of administration.

The practice of imitating paper by digitising trade, which means retaining conventional processes, enhanced by sped-up dispatching of information in PDFs or spreadsheet files, neither yield the desired effects of acceleration and effort reduction, nor can it be considered secure or deliver processes of sufficient quality or in real-time fashion.

Digitalising trade must encompass holistic removal of process breakpoints in the form of paper or paper substitutes, like PDF, XLS, or XLS “printed” into PDF. Wet-ink signatures on paper further impede this case, and neither will electronic signatures placed on paper substitutes get us anywhere closer to end-to-end verifiable connectivity.

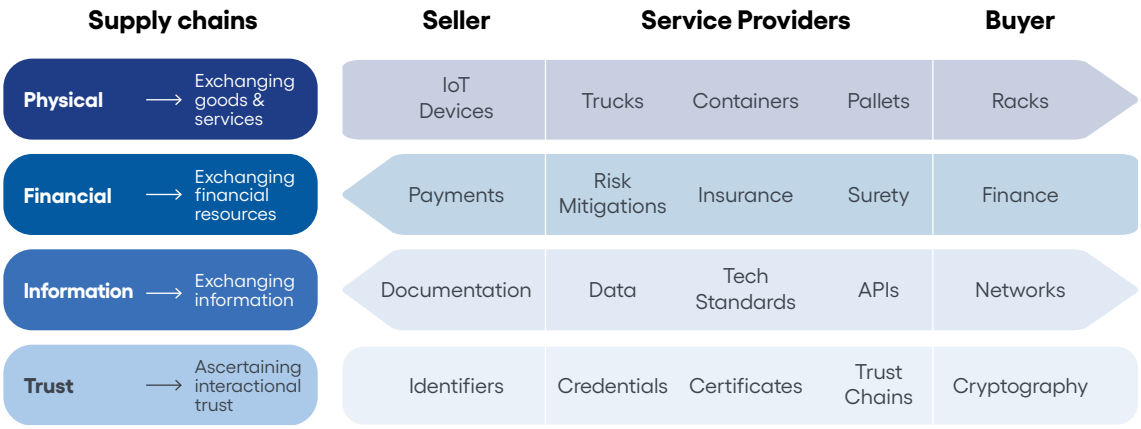
Bridging application islands through Application Programming Interface (API) - based connectivity is a means to that end.

The interactions performed between API-connected applications require authentication (“Who am I?”) and authorisation (“Am I entitled to do this?”) on-the-fly. With this, applications can verify the authenticity of presented information on the transaction layer, and its origin and data access permissions.

A new verifiable trust layer, underpinning the existing information supply chain, is needed.

This is the trust supply chain.

Fig. 1: Supply chain layers, subjects and objects (examples)



4 Layers of trust in trade

Trade is a risky business. Dispatching merchandise around the world exposes enterprises to all sorts of risks. Not only can outstanding payments become uncollectible, theft or arbitrary seizure of goods is also a constant threat. Fraud protection becomes imperative for reliable business transactions. The Merriam-Webster dictionary defines trust as “assured reliance on the character, ability, strength, or truth of someone or something.” Trust provides confidence in someone or something. There are three layers of trust building upon each other to make trade less risky for all participants, or allow smaller contributors to partake:

4.1. Trust in the legal layer

The sovereign of a jurisdiction can define trustworthiness by law. Examples are the legal truth about an individual or firm (birth certificate, business registration). Also important is the principle of legal certainty. It is at the heart of private law. Legal certainty is based on the requirement of clarity, stability, predictability and guarantee of legal norms as well as the specific legal obligations and entitlements linked to them. It is part of the elementary basis of a constitutional social order.

The legal systems underpinning trade are therefore a constant area to be further harmonised. Examples are rules and regulations around customs clearance or fixing incomplete, ambiguous and often hard to execute rules on data protection and digital signing.

4.2. Trust in the governance layer

Governance is the process of interactions through the laws, norms, power, or language of an organised society over a social system (family, tribe, formal or informal organisation, a territory or across territories). It is done by the government of a state, by a market, or by a network. In lay terms, it could be described as the political processes that exist in and between formal institutions.

A variety of entities (known generically as governing bodies) can govern. The most formal is a government, a body whose sole responsibility and authority is to make binding decisions in a given geopolitical system (such as a state) by establishing laws. Other types of governing include an organisation (such as a corporation recognised as a legal entity by a government), a socio-political group (chiefdom, tribe, gang, family, religious denomination, etc.), or another, informal group of people. In business and outsourcing relationships, governance frameworks are built into relational contracts that foster long-term collaboration and innovation.

Governance is often a matter for private actors to agree on standards. Examples are joint ventures or member organisations.

4.3. Trust in technology

On top of legislation and governance, the technology offered to enable digitally rendered interactions needs to provide sufficiently reliable trust levels using cryptographic (mathematical) verifiability. Information security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection. In InfoSec, trusted authorities or user trust are being generated using cryptography. For centralised systems, security is typically based on the authenticated identity of external parties (e.g., sign-in with Google, Apple, etc.). Rigid authentication mechanisms, such as public

key infrastructures (PKIs) have allowed this model to be extended to distributed systems within closely collaborating domains or within a single administrative domain. During recent years, the leading innovations in computer science have focused less on centralised systems and more on distributed computing. This evolution has several implications for security models, policies and mechanisms needed to protect users' information and resources in an increasingly interconnected computing infrastructure.

The need for verifiable trust doesn't stop at borders. There is no global legislature and no global government. Usually this is solved by bilateral treaties, e.g., trade agreements between countries or mutually granting of access to networks by private firms. But the need for an enormous variety of bilateral or multilateral agreements prevents the global trading community from efficiently administering trade. Paperless trade could become just as convoluted with disparate laws, governance structures, standards, etc. as we see in global supply chain today.

Technical standards on verifiable trust can help to prevent this. Standards are worked on at the W3C[2], ToIP[3], IETF[4], ISO/EIC[5], ITU[6], among others.

This paper will exemplify what role verifiable trust plays in digitalising international trade and will allow for business processes to be interwoven between the participants in trade in a trustable manner. This opens leeway for traditional processes to change and for new products and services to be invented.

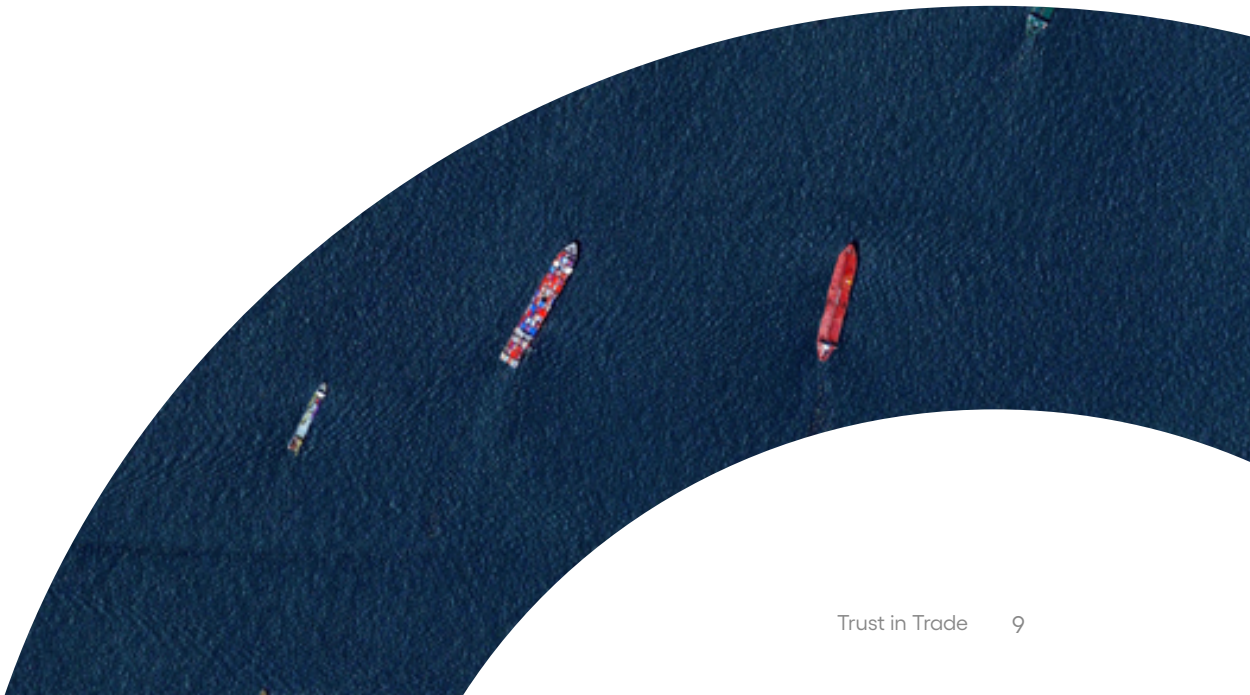
[2] W3C: World Wide Web Consortium, an international community that develops open standards to ensure the long-term growth of the Web

[3] ToIP: Trust over IP, a confluence of multiple efforts in the digital identity, verifiable credential, blockchain technology, and secure communications spaces to converge and create an interoperable architecture for decentralised digital trust

[4] IETF: Internet Engineering Task Force, producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

[5] ISO: International Standards Organization, an independent, non-governmental international organisation with a membership of 167 national standards bodies. ISO/IEC JTC 1, entitled "Information technology", is a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission. Its purpose is to develop, maintain and promote standards in the fields of information and communications technology.

[6] ITU: The International Telecommunication Union (ITU) is the United Nations specialised agency for information and communication technologies – ICT.



5 Identity, authentication, authorisation

A digital identity is information used by computer systems to represent an external agent – a person, organisation, application, or device. Digital identities allow access to services provided with computers to be automated and make it possible for computers to mediate relationships.

Authentication is the act of proving an assertion, such as the identity of the user of a computer system. In contrast with identification - the act of indicating a person or thing's identity - authentication is the process of verifying that identity. It might involve validating personal identity documents, verifying the authenticity of a website with a digital certificate, determining the origin of a document by verifying the latter appropriately, or ensuring that a product or document is not counterfeit.

Authorisation is the function of specifying access privileges to resources, which is related to general information security and computer security, and to access control in particular. More formally, "to authorise" is to define an access policy. For example, human resources staff are normally authorised to access employee records and this policy is often formalised as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be granted or rejected. Resources include individual files or an item's data, computer programs, computer devices and functionality provided by computer applications, like an electronic Bill of Lading (eB/L) as a service.

6 The Trade Ecosystem

6.1. Stakeholders in trade

A trade transaction is usually conducted between a seller and a buyer. The two parties, however, make use of many service providers, without whom a trade transaction cannot be executed.

Service providers comprise

- **Logistic service providers** undertake transport and storage of merchandise, but also offer services like labelling and packing of goods to name just two.
- **Financial service providers** help with payments, mitigate payment risks and help bridging liquidity by financing transactions.
- **Insurance companies** offer protection against damage, loss, and theft.
- **Inspection agents** help to fulfil the numerous rules and regulations imposed on traders.
- **Customs authorities** impose tariffs on imports and exert limits on export of certain goods.
- **IT service providers** conceive, build, and to an ever-greater extent also operate applications and application landscapes that allow for information flows required in conducting trade.
- **Business associations** like IPCSA, ICC, Chambers of Commerce and consortia like DCSA, IDSA help to convene the parties in trade to mutually shape the future landscape of trade.
- Finally, **policy makers** and **legislators** in the national legislations and supranational organisations create rules, directives and shape statutory conditions.

All these parties need and want legal certainty and therefore rely on trust technology to maintain digital interactions. In ever more digitalised environments, cryptography-based verifiable trust becomes a key factor.

In our use case example below the stakeholders are exemplified as listed and described below:

- **Seller**
  Batavia B.V, Amsterdam, Netherlands – wholesaler of wine and more delicious produce. Trades globally on selected B2B networks.
- **Buyer**
  CentreShop Ltd., Singapore – runs a chain of supermarkets in Singapore and Malaysia offering high quality grocery products and more. Sources globally via B2B networks.
- **Seller bank**
  GIN Bank, Amsterdam, Netherlands – advising on and confirming the Letter of Credit (L/C) for the seller. Maintaining a correspondent banking relationship with SDB Bank and offers Letter of Credits on L/C Quick.
- **Buyer bank**
  SDB Bank, Singapore – issuing a Letter of Credit as a payment risk mitigation on behalf of the buyer and for the seller in correspondence with the seller bank and offers Letter of Credits on L/C Quick.
- **Logistics service provider and shipping co.**
  MarineLog, Hamburg, Germany – procuring transport on SeaTrans and elsewhere and issuing Bills of Ladings (BL).

- **Transport insurer**
  MarineCover, San Francisco, USA, issuing Transport Insurance Certificates for sea transports, including pre- and post-carriage on TranSafeNet.

- **Chamber of Commerce**
  Rotterdam Chamber of Commerce, Rotterdam, Netherlands. Issuing Certificates of Origin on the ICC-Origin network to be used in customs clearance processes to obtain preferential origin and to be presented in the L/C process.

- **Sea port operator**
  Jurong Port Ltd., Singapore – operating the port facilities in Singapore's main seaport.

6.2. Trade Assets

Bill of Lading – 1. Contract of carriage, 2. Receipt for shipped goods, 3. Document of title. A Bill of Lading (BL) is a contract of carriage between the carrier and consignee for ocean or overland imports and exports. The Bill of Lading contains the terms and conditions of transportation. It provides evidence that the carrier has agreed to transport the freight to its destination as per the agreement between the seller and buyer. At the point of origin, a Bill of Lading confirms that the seller has transferred the freight to the carrier in good condition. The carrier confirms receipt of the goods on board their cargo vessel in optimum condition as per contractual terms. The Bill of Lading acts as a title to the goods. Whoever is receiving the goods must show the bill to secure the release of the freight from the carrier. Access to the contents can only be gained by producing the Bill of Lading. The Bill of Lading must often be submitted when making an insurance claim. A Bill of Lading is key to the Letter of Credit process.

Certificate of Origin – A Certificate of Origin (CoO) is usually submitted to customs authorities in the importing country to prove the product's eligibility for entry. It is also used to establish whether the goods are eligible for preferential treatment under the terms of any trade agreement existing between the countries of origin and import. Information on the certificate will determine the level of duty applicable to the goods and can, if a trade ban or sanctions are in place, determine whether goods can be legally imported. CoOs are particularly useful for customs teams in nations that:

- Restrict imports from certain countries
- Limit the quantity of goods that can be imported
- Give preference to products manufactured in certain territories

Commercial Invoice – The Commercial Invoice is a key document in trade which often contains a vast amount if information also found on other trade documents. It enumerates the funds owed from a trade transaction, lists up the goods delivered and contains details about the sender and recipient of a consignment. It supports taxation processes, is used to determine customs duties owed, is being financed against and needs to be presented in a Letter of Credit transaction.

Customs Declaration Form – Specifies the quality and quantity of merchandise to be imported following a goods classification scheme. Many countries nowadays offer and demand electronic means for customs declarations.

Packing List – Who is sending the package, the destination of the cargo, which and how many items the package contains.
A packing list is compiled by whoever is responsible for packing the goods - usually the seller, exporter, or freight forwarder. It is essential for both ocean and air shipments. The document includes details about the

nature, weight, and dimensions of the goods in the consignment. It also carries information about how the goods were packed, and notes any marks or numbers present on the exterior of the box, crate, or other container used to protect the goods during transit. The details on the form will be used by freight forwarders, customs officials, and others involved in the supply chain. Customs teams at ports of origin and arrival will refer to a packing list when checking that the product and packaging comply with local rules and regulations. The document helps customs officials at the destination port calculate import duties or taxes payable and determine whether reduced tariffs or preferential treatment should be applied to a consignment. A packing list also provides a source of vital information required to complete a Bill of Lading.

Purchase Order - A commercial document and first official offer issued by a buyer to a seller, indicating types, quantities, and agreed prices for products or services. It is used to control the purchasing of products and services from external suppliers. Purchase orders can be an essential part of enterprise resource planning system orders. The issue of a purchase order does not itself form a contract. If no prior contract exists, then it is the acceptance of the order by the seller that forms a contract between the buyer and seller.

Trade Contract – Legally binding agreement to deliver specified merchandise or service in return for a payment.

Warehouse Receipt – negotiable instrument securitizing proprietorship of merchandise stored in a warehouse or storage pile. Receipt of having taken over the merchandise for storage.

Transport Insurance Certificate – Negotiable instrument certifying the right to draw insurance coverage for merchandise in transit. Coverage can be transferred to the buyer during risk passing in CIF or CIP[7] deals.

[7] Incoterms which include an obligation to procure for transport insurance. CIF: Cost, Insurance, Freight (to named destination); CIP: Carriage and Insurance Paid To (named destination)

7 Trade digitisation vs. trade digitalisation

Like in many other industries the application landscapes established in the past 30 years have been built mainly to fulfil specified functions in organisations and companies. Although the advent of the internet and its precursor, the telecommunication infrastructure, brought about enormous connectivity capabilities. Applications have been deployed in organisations fulfilling similar functions, but these applications very often still constitute digital islands. Interconnectivity to up- and downstream applications along the business processes across organisations was rarely a development goal, or if so, many hindrances prevented good results.

The lack of common data format standards and algorithmised standard business processes, the lack of legal recognition of electronic records, tardiness in adopting real time system architectures (i.e. replacing end of day processing by straight through processing), the absence of powerful database architectures being able to concurrently process and provide data from within one single instance, and the shortage of a common trust layer employing transitive verifiable trust have prevented functional process interconnectivity between organisations and have resulted in tenacious survival of legacy processes.

The reverse conclusion is perfectly valid in this case: there was never an incentive to make structural changes to legacy processes, even if identified as outdated. In a networked economy without a working trust layer, inventing and selling products based on business processes that are overarching organisations' boundaries is hard, or a nonstarter.

Especially the lack of transitive trust provisions during data exchange posed a seemingly unsurmountable barrier.

This conserves breakpoints in cross-company process flows, which have long been and are still being bridged by exchanging paper documentation.

7.1. Trade digitisation

The rise of the internet brought about progress on the "connectivity layer", which was used to speed-up conveyance of information by replacing wet ink signed paper and fax with electronically signed (or unsigned) PDFs dispatched via email or file-transfer-APIs. However, the process breakpoints continue to exist. Progress on the "logic layer" was not achieved in large scales. Traditional process flows have hardly been changed, but only accelerated.

A PDF based "digital" documentation may be digitally signed, but it remains hard to determine who produced the data items contained in it. The PDF may even contain structured data, but its authenticity ends at the "container level". The single data items cannot be traced back to their originators, so the "palette or crate level" remains unauthentic.

This is trade digitisation. Trade digitisation leaves the biggest portion of the digital dividends untapped by ignoring most of digitalisation's change potential.

7.2. Trade digitalisation

To fully digitalise trade, paper substitutes need to be replaced by structured data, which can be conveyed via APIs, directly processed, and consumed in real-time

by downstream applications, which can directly acknowledge receipt and return process feedback on the fly, again via APIs. A fully digitalised structured trade data conveyance and processing system, we call a data supply chain. This data supply chain may be stand-alone for digital goods or may be used to facilitate an associated physical goods supply chain.

Data being conveyed between applications using APIs will need to retain its attributability to its source, no matter how often it has been forwarded and what further processing the data has been made subject to. However, data in the form of JSON or XML files cannot be practically signed using electronic signature products like DocuSign or Adobe Sign, let alone with ink.

For short we describe the secure attributability of data to its source along a data supply chain including any transformations of that data, its provenance.

Analogously to how the authenticity of a classic work of art is provenanced via the establishment of an unbroken chain-of-custody back to its origin, the authenticity of data may be provenanced via an equivalent chain of cryptographically verifiable commitments back to its source(s).

To exemplify this: a trade receivable, i.e. an invoice, having been issued in the Enterprise Resource Planning (ERP) system of a vendor in Germany, will need to be attributable to this vendor in the ERP system of a buyer in Singapore to which it has been conveyed for further processing. The invoice also needs to continue to be attributable to its original issuer, in the likely case it has been routed via a B2B system prior to being conveyed to the buyers ERP system. Data items in that invoice having been provided by an upstream provider, i.e., a manufacturer of a pre-product, need to remain attributable to this supplier.

Fig. 2: Verifiability across networks

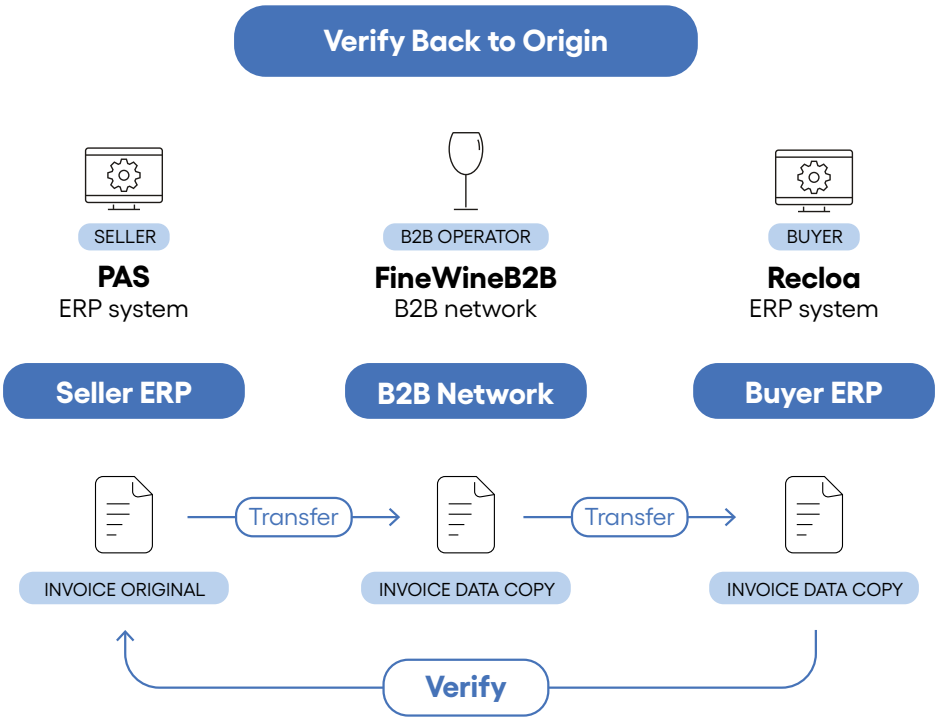
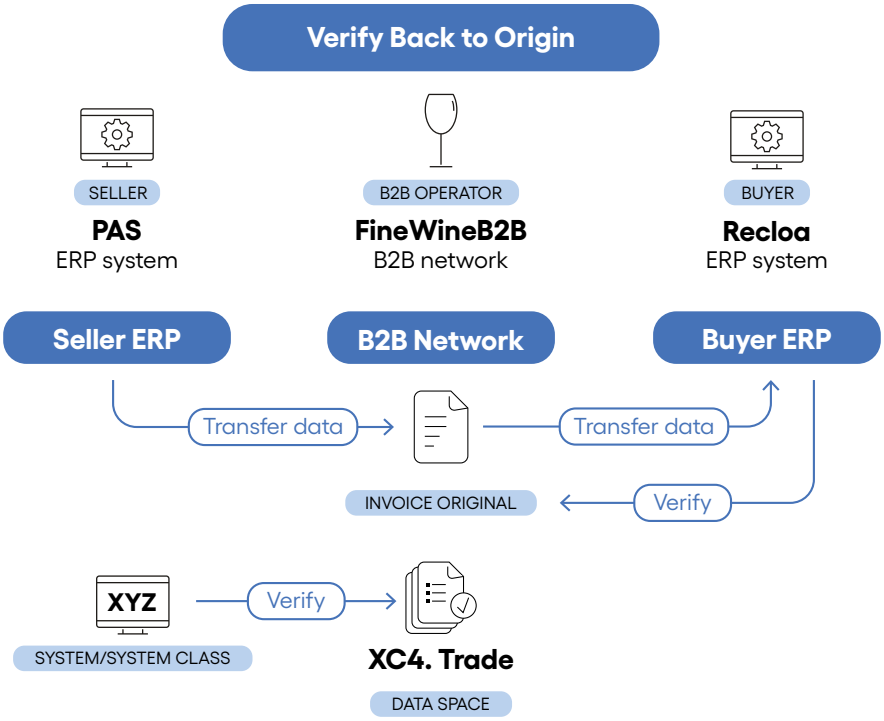


Fig. 3: Verifiability on a data space



The same maintenance of attributability applies to all further process ramifications the invoice may end up in, i.e. into a supply chain finance network providing receivables discounting.

To conclude, authentication and authorisation, and certification requiring the former two, needs to sink down on data level, rather than remain on the level of the individual networks, being the source of the information.

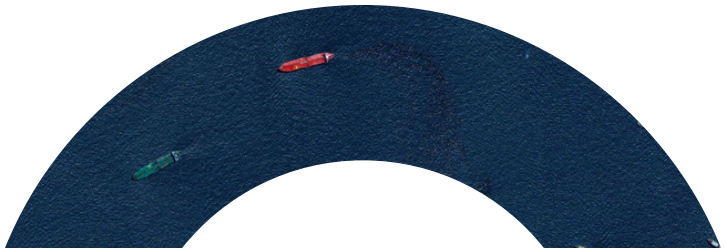
Certificates may help to authenticate and authorise sessions but making certificates work on dataset level or even on subsets of datasets seems close to impossible.

This is trade digitalisation.

Another, less data provenance-, but more process-oriented part of trade digitalisation would be to look at how a transitive verifiable trust layer would allow for re-architecting of information transmission processes in trade.

Do we really need to convey an invoice between systems as indicated above? Or could the invoice just remain in the ERP system which it originates in, accessible and verifiable for subjects (people) or objects (people's computer systems) having a stake?

If the identity of the subject or object accessing the invoice can reliably be proven at the time of access, authentication and authorisation follow up and if legitimate access could be granted.



8 An example use case of transitive (verifiable) trust in trade digitalisation

8.1. Introduction

On 21st October 2028 the container ship "Digital Age" embarks on a journey from the port of Rotterdam in the Netherlands to Jurong port in Singapore.

On board it carries 16,384 containers stacked with machinery, chemicals, pharmaceuticals, batteries, wine, and many other produces. All containers on board are equipped with IoT devices fulfilling several different functions. All IoT sensors form a mesh network and communicate among each other and in real-time with the ship's IT infrastructure. The ship itself is in constant exchange with either satellite constellations in the sky, communicates with mobile phone networks when close to coast lines or connects to port infrastructures.

It will cross the Suez Channel and is scheduled to arrive in Singapore on 06th November 2028.

The respective ports' digital infrastructures will query all containers onboard via the ship's infrastructure for information upon arrival and send updates.

A closer look at an FTL[8] consignment aboard the ship "Digital Age" reveals:

Case: Cool Wine

Container 2048, a 40 foot reefer, contains 22,176 bottles of French red wine on 22 palettes, each holding 84 crates of 12 bottles. The wine is delivered from Batavia B.V., a Dutch exporter of European wine. In transit the container's inner temperature may never exceed 18 degrees celsius and the buyer, CentreShop Ltd, a food retailer, demands a tight temperature recording regime to safeguard the quality of the wine. Any temperature excess event will trigger an insurance claim. Furthermore, every delay in delivery shall result in a penalty of 5,000 USD per day. The consignment has a trade value of 254 TUSD and a retail value of 685 TUSD or 938 TSGD

The wine is being traded on FineWineB2B, a wholesale B2B network convening sellers and buyers of large quantities of wine from all over the world.

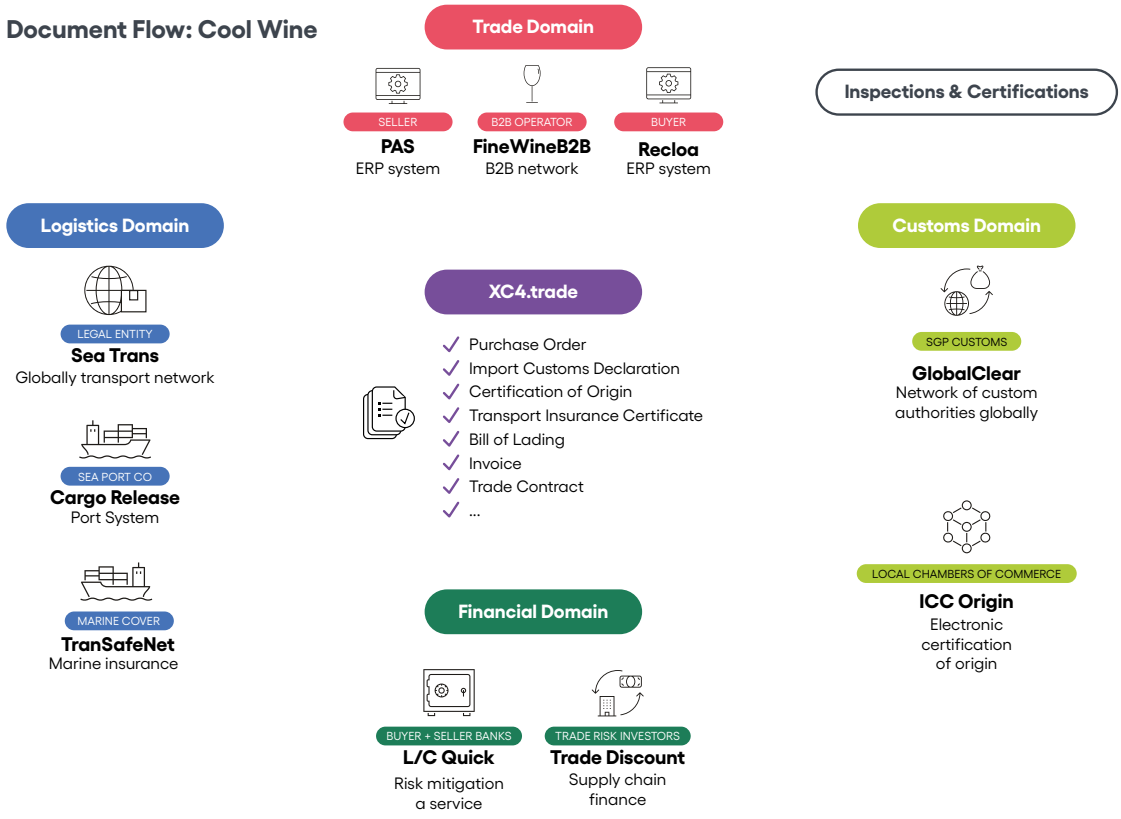
Batavia B.V. has asked CentreShop Ltd. to have its bank SBD Bank to issue a Letter of Credit as a payment risk mitigation. SBD Bank issues the Letter of Credit and determines trade documentation to be presented as specified below:

Trade documentation and documentation flow relying on verifiable trust in future

- **Trade Contract –** the contract underpinning the trade, closed on the B2B network FineWineB2B
- **Purchase Order –** the order placed by CentreShop Ltd. following the trade contract
- **Commercial Invoice –** issued by Batavia B.V.

[8] FTL (Full truck load). A consignment that occupies an entire freight container, as opposed to LTL (less than a truck load), where several consignments are grouped in a container.

- **Certificate of Origin -** issued by Rotterdam Chamber of Commerce on behalf of Batavia B.V. by using the Chamber's instance on ICC-Origin
- **Packing list –** produced by Batavia B.V.'s ERP System PAS using product data therein and the purchase order placed by CentreShop Ltd. on FineWineB2B
- **Import Customs Declaration -** produced by CentreShop Ltd.'s ERP System Raceloa according to templates and data sourced from Singapore's instance on GlobalClear
- **Bill of Lading –** issued by the logistic service provider MarineLog on the network SeaTrans to the order of Batavia B.V.
- **Certificate of Transport Insurance –** issued by the Marine Insurer SeaCover on the insurance network TranSafeNet on behalf of the applicant Batavia B.V.



All documentations are digitally signed by their respective issuers and acknowledged by their respective applicants or beneficiaries by digital signature. All documentation is being put onto XC4.trade, a data space for trusted trade documentation exchange.

A documentation's digital signature on XC4.trade allows for unambiguous attribution to its issuer and current controller at any time. The controller is the current holder of the electronic record being the documentation. There is only one controller of a trade documentation at any given time to satisfy the `exclusive control` and `singularity` requirements proposed by the ML-ETR[9] that the respective national legislations are asked to derive from it. A full history of all digitally signed changes made is being kept and placed into the metadata layer of the documentation, so that any downstream system consuming and processing the trade documentation knows who has contributed which data objects in each documentation provided, and who at any time is the exclusive controller of the instrument, and who has signed it for which purpose and at which process step. The metadata could also entail information on purpose and function within the respective stake holding organisation. Each instrument's content will only be modifiable through the identity layer controlling access to the instrument, its content, and its metadata.

To avoid any discrepancy between trade documentation with the L/C requirements, SBD Bank may offer a documentation a largely automated pre-check service on the condition of fully electronic and digitalised presentation on the Financial Network "L/C Quick". L/C Quick supports this service.

SDB Bank further asks for the Bill of Lading and transport insurance to be put to their order by Batavia B.V. for the time of the transport. SDB bank herewith assumes exclusive control over the Bill of Lading.

Batavia's bank, GIN, will confirm the L/C based on the electronic presentation.

L/C-Quick offers extensive matching capabilities for documentation presented in an L/C transaction. A feature, which is facilitated by its trusted position in the network, following its reputation to fully respect data sovereignty assertions imposed by the trading parties. This in turn means, that not every party has full visibility into the entire set of documentation, but only to the extent required to provide the respective service. Extended visibility may be granted against subordination to data sovereignty assertions and may be at a price.

Any temperature excess above 18° C will be reported by the container's IoT device as a condition violation into the metadata of the Transport Insurance Certificate. The IoT device will sign this event report using its digital identity. Hence, the condition violation event report will be verifiable and authentic. It will always be attributable to the IoT device from container 2048.

8.2. Example documentation flow

8.2.1. Commercial Invoice

1A The seller issues a Commercial Invoice in his ERP system for the wine to be dispatched and digitally signs it. The invoice is being stored on the trade data space XC4.trade and referenced in FinWineB2B.

1B The buyer is being notified and digitally signs the invoice in FineWineB2B to acknowledge the invoice. FineWineB2B updates the invoice on XC4.trade.

2A The buyer presents the invoice on L/C Quick as requested in the Letter of Credit by amending the L/C Quick transaction with a reference to the invoice on XC4.trade.

2B The buyer bank is being notified and signs the invoice on L/C-Quick as 'subject to risk mitigation'.

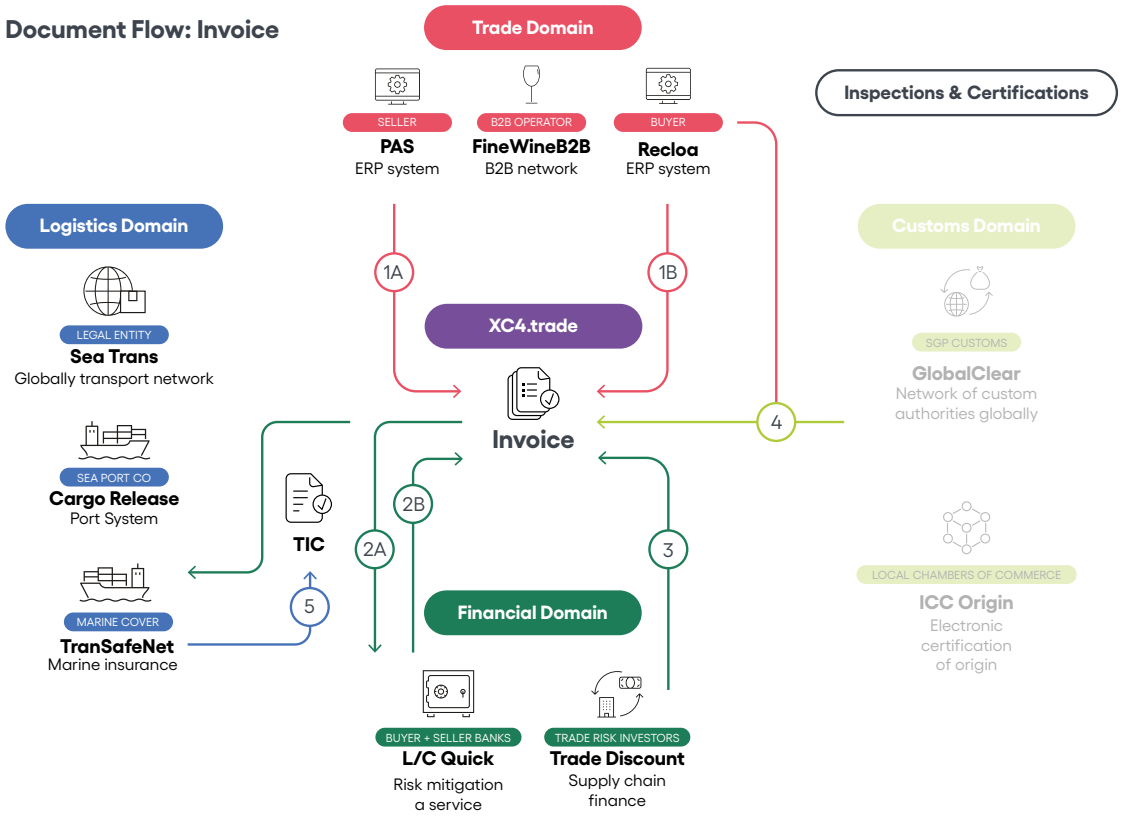
3 An investor in trade risk on the network 'TradeDiscount', which offers refinancing of trade receivables for the

[9] ML-ETR: Model Law on Electronic Transferable Records, a recommendation by UNCITRAL on national statutory implementation of Electronic Transferable Records in the interest of harmonising trade legislation pertaining to digital trade internationally.

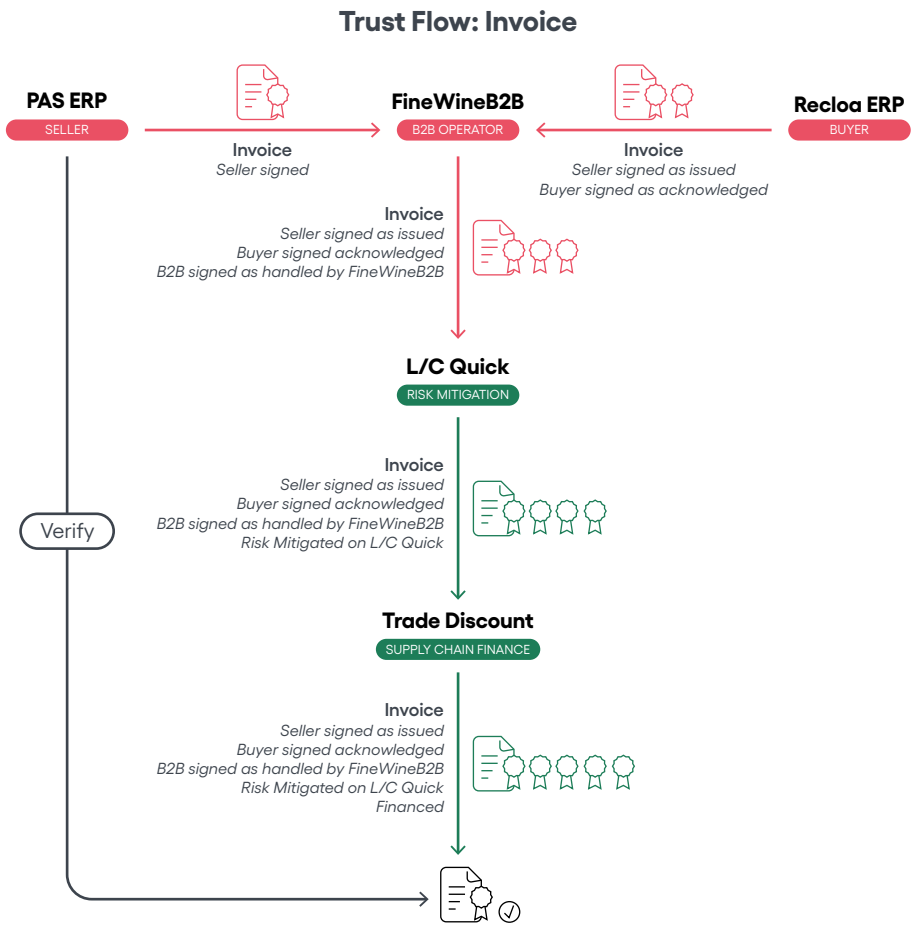
customers of seller bank, checks for the veracity of the CoolWine invoice and positively verifies the digital signature of the seller and the acknowledgement of the buyer. The investor also takes note of the 'subject to risk mitigation'-flag. She finances the invoice for its remaining days outstanding and signs it as `financed'.

4 On behalf of the importer the Singapore customs authorities can access the invoice from within their GlobalClear instance to support determination of import duties. Singapore customs will read all required data for customs clearance from the invoice and other documentation already provided on XC4.trade. Singapore customs will also see, who is importing and what.

5 A Transport Insurance Certificate is being issued based on the data of the Commercial Invoice.



In a fully digitalised trade environment architecture copies of the invoice need not be produced. Instead, there could be only one version, which is accessible and fully verifiable for anyone having a stake and being able to prove it. This primary version may be placed on a data space, but it could as well remain in the system of origination, as long as the invoice (or any other instrument) remains accessible, and its authenticity remains verifiable. Still (subset) copies of the dataset can be drawn to update downstream systems in the respective parties' domains, serving any supposable purpose. These copies, however, will be marked as such, while the original, the primary version, must always be recognisable as being the primary.



8.2.2. eB/L

1 **a.** MarineLog takes over the transport of CoolWine and issues a SeaTrans e/BL to the order of the seller on XC4. trade (Issuance and Control Transfer). MarineLog digitally signs the eB/L, the seller acknowledges receipt by digitally countersigning the eB/L.

b. The seller's ERP system automatically uploads a reference to the eB/L onto FineWineB2B

c. MarineLog notifies SeaPort Co. in Singapore via the network SeaTrans of the consignment.

2 The seller presents the eB/L on L/C-Quick on behalf of the buyer to the buyer bank and digitally signs this action. The seller also puts the eB/L to the order of the bank (Control Transfer), as requested in the Letter of Credit. The buyer is being notified by FineWineB2B and acknowledges all that by digitally countersigning each act.

3 SeaPort Co.'s CargoRelease system notifies

a. the buyer,

b. the seller, and

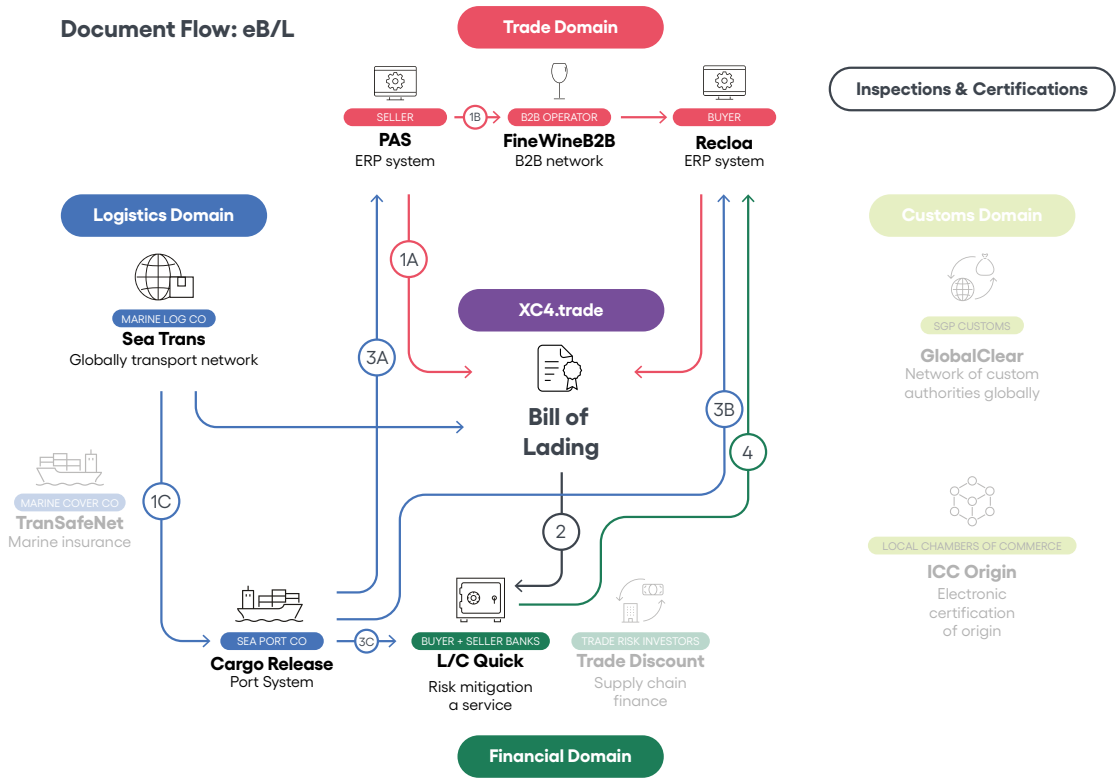
c. the buyer bank via XC4.trade of the merchandise having arrived and being ready for release.

The eB/L has in the meanwhile been continuously updated on XC4.trade with the process IDs of the transactions of the systems the eB/L has been made instrumental in. The digital signatures provided also serve as means of authorisation to effect this.

4 The buyer bank, who is the current controller of the eB/L, puts the eB/L to the order of the buyer and digitally signs this act. The buyer is again notified and digitally signs this act as acknowledged.

The buyer bank debits the account of the buyer and credits the seller's account with seller bank.

5 The buyer, who now controls the eB/L presents it to SeaPort Co's CargoRelease system at the seaport and receives the merchandise. The eB/L assumes the status 'spent' and is being archived for future reference according to retention periods specified by its stakeholders.



8.3. Trade systems relying on transitive verifiable trust

All systems and interconnection scenarios below are fictitious. Some may already have representations in today's world, some are in the process of being built, some are a vision of what would be beneficial to have to fully digitalise trade.

PAS ERP – the seller's enterprise resource planning system. Commercial invoices originate here, next to other trade instruments.

Recloa ERP – the buyer's enterprise resource planning system. Purchase orders originate here, next to other trade instruments.

FineWineB2B – a B2B Network and marketplace for wine. FineWineB2B offers product catalogues maintained by sellers, enriched with all downstream required product information. It also features a trade contract editor and consults on using favorable incoterms. FineWineB2B assists with customs declarations by interconnecting with GlobalClear and is a selling point for digital Certificates of Origin of ICC-Origin.

L/C QUICK – a decentralised system to orchestrate Letter of Credit interactions between seller, seller bank, buyer, and buyer bank on a distributed ledger.

It is interconnected to XC4.trade and accepts references to trade documentation stored and governed in there.

TranSafeNet – a decentralised marketplace for sea transport insurance. It stores Transport Insurance Certificates on XC4.trade on behalf of its customers. The Transport Insurance Certificate can be transferred alongside an eB/L at the time of risk passing on XC4.trade. TransSafeNet allows for integration with IoT devices on board of containers.

SeaTrans – a logistic service provider network offering pre-carriage, sea transport and post carriage services of goods around the globe. SeaTrans also offers issuance of electronic Bills of Ladings and has them governed on XC4.trade, which accesses and executes the eB/L process libraries of SeaTrans eB/L.

ICC-Origin – a future decentralised system of ICC WBO allowing local Chambers of Commerce to issue globally verifiable electronic Certificates of Origin to support preferential custom clearance. ICC Origin sells on B2B systems like FineWineB2B.

GlobalClear – a global custom clearance network operated by participating national custom authorities on mutuality. FineWineB2B sources its HS-code product classifications from GlobalClear.

FinTrade – a cloud-based trade finance front and back-office as a service system for banks. FinTrade seamlessly integrates services of L/C-Quick, and XC4.trade, among others. FinTrade connects into the back-offices of banks.

CargoAccept – part of a system suite covering the processes in seaports for accepting containers for carriage on sea vessels. It integrates with stowage planning systems of sea vessel operators and port systems.

CargoRelease – part of a system suite covering the processes in seaports for releasing containers to their consignees against presentation of a Bill of Lading.

XC4.trade – a trade data space that accepts authenticated trade documentation and allows for traceable transfer of control of Electronic Transferable Records. XC4.trade solves the singularity requirement, which asserts that there can at any time only be one primary version of a trade documentation, while all copies are to be considered secondary. XC4.trade also solves the exclusivity of control requirement, which asserts that there can only be one controller of a trade documentation at any given time. Control Transfers between two parties can be performed on the identity layer of the trust supply chain. Further, XC4.trade allows weaving process interactions between different Electronic Transferable Records, e.g. a Bill of Lading and a Promissory Note, or a Delivery Note and a Warehouse Receipt. XC4.trade can also group documents for presentations to a Letter of Credit orchestrated in L/C-Quick. Or interact with CargoRelease to reclaim a container in its port of destination.

XC4.trade wraps trade instruments in a data container, which are controlled by fully decentralised digital identities. It interconnects the information supply chain with the trust supply chain.

8.4. Table of Interactions: Instruments, subjects, systems

Documentation	Originators (Subject)	Source System	Destination Systems	Receivers (Subject)
Trade Contract	• Batavia B.V. • CentreShop Ltd.	FineWineB2B	L/C Quick	• SBD Bank • GIN Bank
Purchase Order	CentreShop Ltd.	Recloa ERP	• FFineWineB2B • PAS ERP • L/C Quick • FinTrade	• Batavia B.V. • SBD Bank • GIN Bank
Commercial Invoice	Batavia B.V.	PAS ERP	• FineWineB2B • Recloa ERP • L/C Quick • FinTrade	• CentreShop Ltd. • SBD Bank • GIN Bank
Packing List	Batavia B.V.	PAS ERP	• FineWineB2B • Recloa ERP • L/C Quick • FinTrade	• CentreShop Ltd. • SBD Bank • GIN Bank
Certificate of Origin	Rotterdam Chamber of Commerce	ICC-Origin	• FineWineB2B • PAS ERP • L/C Quick • Recloa ERP • GlobalClear	• Singapore Customs • SBD Bank • GIN Bank
Import Customs Declaration	CentreShop Ltd.	Recloa ERP	GlobalClear (SGP Instance)	• Singapore Customs • SBD Bank • GIN Bank
Bill of Lading	MarineLog S.E.	SeaTrans	• PAS ERP • L/C Quick	• Batavia B.V. • CentreShop Ltd. • SBD Bank • GIN Bank
Certificate of Transport Insurance	MarineCover S.E.	TranSafeNet	• PAS ERP • Recloa ERP • L/C Quick	• Batavia B.V. • CentreShop Ltd. • SBD Bank • GIN Bank

9 Privacy engineering and data sovereignty

9.1. What is data sovereignty

Data is said to be the new oil. In digitalised business processes it is being exchanged and made available to others to an ever-greater extent. Divesting structured data makes it easy for the receiver to use data as intended, but also in other ways. To maintain control over data yielded, technical limitations of the usage of data to certain, pre-defined and agreed upon processes is required.

In future dataspaces a lot of data will be accumulated. The often-stressed term “full transparency”, however, is not always a desired property of an exchange environment. Parties making data available are often eager to protect an array of interests and desire to draw back data which has been shared as a requirement for a service provision. Secondary uses of data, of which there can be many, shall often be prevented.

9.2. Data sovereignty example in the trade context

Consider SBD bank issuing a series of L/Cs for CentreShop Ltd., being presented with a series of trade documentation in digital form. CentreShop Pte Ltd. may not want this documentation to be made subject to data mining, to hide trade secrets from service providers or competitors. CentreShop Pte Ltd. may fear that identity tagged data could put service providers like banks in a position to apply discriminating pricing schemes against it and wants to rule this out.

Since SBD bank may have to respect retention periods for transaction documentation, deleting presented documentation after transaction closure may not an option.

But how else would the bank exclude CentreShop’s import information from their prescriptive analytics processes?

Identity data attached to business data may help SBD bank to reliably exclude customer data from certain processes, while concurrently making the same data subject to other, indispensable processing.

This way identity information may become a facilitator for data sovereignty.

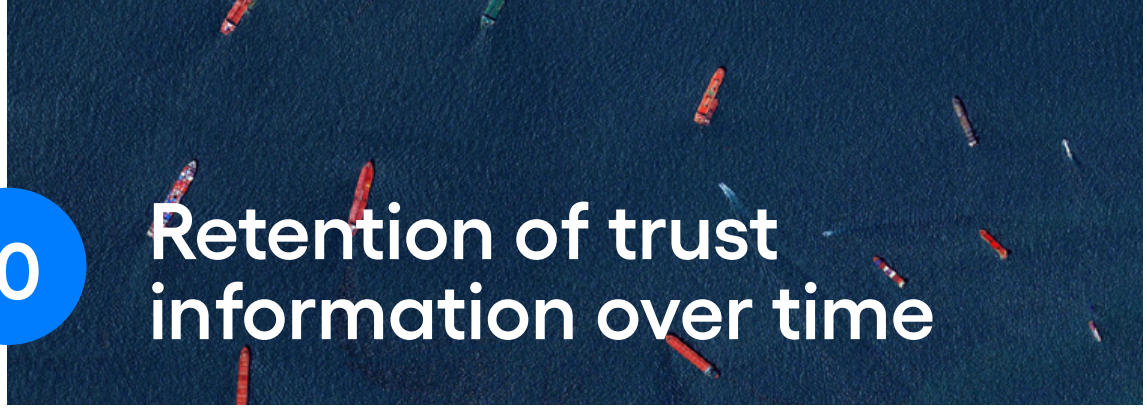
9.3. Verifiable trust as a facilitator for data sovereignty

CentreShop has signed the invoice and other documentation which was presented in the L/C process. CentreShop may have added a “do not analyse” tag to the documentation.

The bank may have added their own “do not analyse” tag during their processing and after reading CentreShop’s tag.

This was only made possible on the fly by CentreShop having digitally signed the invoice before it was presented, and the bank has been able to evaluate this information automatically.

Both digitally signing the invoice as well as adding tags for downstream processing would happen on the meta layer. The core data of the invoice remains unchanged.

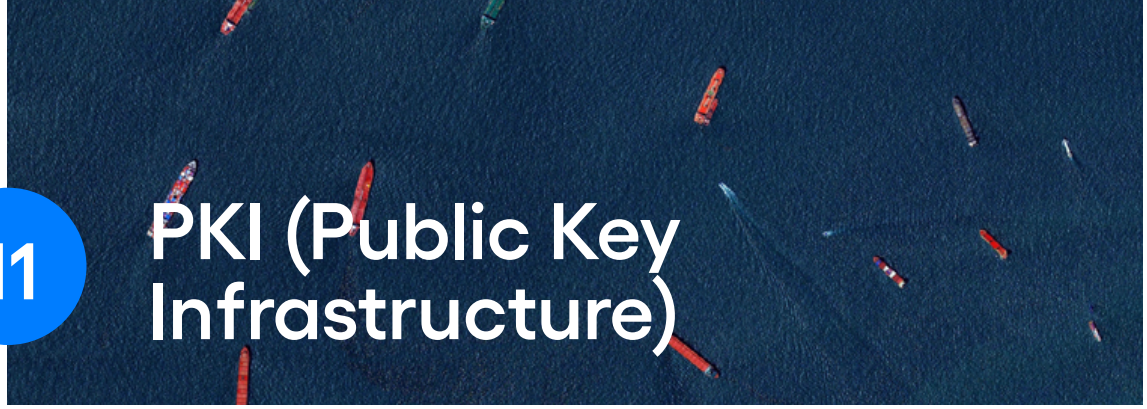


10 Retention of trust information over time

Legally and regulatory relevant information is frequently subject to retention periods. Business data needs to be archived and may not be deleted for periods of time determined by the law or regulations and depending on the subject matter background.

Trust services facilitating authentic data exchange can help alleviating this and simplify meeting the multitude of requirements.

Verifiability and attributability to originators on data level helps to flag data as being subject to retention and also to not being the latter any longer and therefore be released for deletion.



11 PKI (Public Key Infrastructure)

With the arrival of cryptographic algorithms for the creating of private/public key pairs it became possible to create standards around these algorithms. One standard deals with digital certificates. The International Telecommunication Union (ITU) standardised digital certificates in their X.509 standard in the 1980ies. It took some time before rule books and governance models arrived, resulting in Public Key Infrastructures (PKI) and the establishment of certificate authorities (CA). CAs are responsible for the issuance and revocation of digital certificates.

PKI is a technology for authenticating users and devices in the digital world. In its centralised form one or more trusted parties, certificate authorities, digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device. The key can then be used as an identity for the user in digital networks.

Its decentralised form, Decentralised Public Key Infrastructure (DKPI) does not require a certificate authority, the certificate is replaced by a Decentralised Identifier (DID) or an Autonomic Identifier (AID) which are self-certifying and self-sovereign and contain the public key. Upon request, the owner of the DID can prove its control over the DID/AID using the private key.

Users and devices holding keys are called entities. In general, anything can be associated with a key that it can use as its identity. Besides a user or device, it could be a program, process, manufacturer, component, or something else. The purpose of a PKI is to securely associate a key with an entity.

An entity in trade can be either a subject, having rights and obligations, hence a natural person employed by a legal entity or the legal entity itself, in the form of a trading party or a service provider. Attributable to these subjects are objects, like trucks, containers, pallets, IoT sensors, computing resources or data.

11.1. Centralised vs. decentralised PKIs

PKI as we know it today is largely centralised. The advantages of decentralised over centralised PKI in global trade are explained here.

11.2. Asymmetric vs. symmetric cryptography

The core technology underlying PKI is called asymmetric cryptography. It's asymmetric with respect to cryptographic keys. Unlike symmetric cryptography, whose operations use a single shared secret key, asymmetric cryptography uses a pair of keys, which are mathematically entangled. One key in the pair is the private key and the other key is the public key, forming a public-private key pair. The main advantage of asymmetric cryptography is that only the public key is shared, while the private key is never and must never be shared. This enables security without having to trust in some other entity.

One of the important operations enabled by asymmetric cryptography is a non-repudiable digital signature. Non-repudiable digital signatures enable more secure attribution of data to its source. With an asymmetric digital signature, the signature is created by the unshared private key. The signature may be verified by anyone who has the shared public key. An attacker cannot forge a signature without the private key. This means a signer cannot repudiate a signature made with their private key. This means that any verifier can verify without having to trust the signer and the signer can prove it signed without having to trust the verifier.

A symmetric key signing operation, on the other hand, is repudiable because the signing key must be shared with whomever needs to verify the signature. Thus, the signer can repudiate any signature because any verifier is enabled to be a forger. Symmetric cryptography is only secure

amongst a set of mutually trusting parties and only to the degree that those parties act in a mutually trustworthy manner.

11.3. Trust across trust domain boundaries

A related key insight underlying security is about trust and who must be trusted. A trust domain can be loosely defined as the set of trusted infrastructure that is shared by every organisation that operates within that domain. The hard problem is enabling trust to cross trust domain boundaries. Symmetric cryptographic operations are only secure within the same trust domain. In contrast, asymmetric cryptographic operations have the potential to be secure across trust domain boundaries. This points to the crux of why one should care about decentralised PKI versus centralised PKI.

Centralised PKI largely defeats the main potential advantage of asymmetric cryptographic, that is, its ability to allow trust to cross trust-domain boundaries. In the limit the best infrastructure is Zero Trust Infrastructure. Zero trust is short for: never trust, always verify. What it really means is that any operation or communication from a given source must be verifiable by the end user. This is called end-verifiability. This means that as information crosses from the source entity to another to yet another to eventually the end user, the path taken doesn't matter. The middle does not need to be trusted because the end can verify the information back to the source.

11.4. Trust imposed transaction cost in trade

In the context of international trade, trust domain boundaries are strong boundaries. These boundaries impose high degrees of friction and hence cost. These costs may be more formally classified as transaction costs. Transactions costs may be divided into three categories, that are: triangulation, transfer, and trust.

- Triangulation costs include finding, filtering, and matching of the parties, products, and services associated with a transaction.
- Transfer costs include transportation, fulfilment, and payment of exchange of goods and services associated with the transaction.
- Trust costs include identification, authentication, authorisation, and reputation of the parties to the transaction as well as ascertaining the risks associated with the parties fulfilling their obligations under the transaction.

It is the latter, trust transaction costs, that PKI impacts. In a strong sense, lowering trust transaction costs enables transactions that would not have been possible or economical otherwise.

For example, a Bill of Lading on paper cannot be processed in two locations concurrently. A digitised Bill of Lading (i.e. on PDF) may be swiftly conveyed but cannot seamlessly be included into a ramified process thread. A digitalised eB/L, maybe offered on a blockchain based system, can be called and manipulated from anywhere in immutable fashion, but all stakeholders around it would be required to make use of the same trust provider. Unless the trust provision is transitive between the large variety of systems to be found among the seemingly infinite permutations of systems having to interoperate. This has been addressed as open interoperability problem.

11.5. Transitive trust

Clearly enabling trust to cross trust domain boundaries is essential to reducing trust transaction costs in the arena of international trade. This is called transitive trust. Indeed, in the limit Zero Trust Infrastructure could approach the lowest possible trust transaction costs. So how does a more decentralised PKI better provide transitive trust compared to a more centralised PKI?

The vital function of a PKI is to bind controllers, identifiers, and key pairs. A controller is a person that controls an identifier with a (public, private) key pair. If any of the bindings are weak then the infrastructure is subject to attack. The infrastructure is therefore weak.

11.6. Centralised vs. decentralised PKI

In a centralised PKI, the bindings between identity and a subject or object are asserted by some trusted entities like DNS/CA registrars and certificate authorities, or a given shared ledger. The trusted entity controls the shared infrastructure supporting those bindings that everyone must trust. This makes it difficult for the trust in one trust domain to securely cross over to another trust-domain. However, exactly this is a requirement in supply chains, where a multitude of actors are interacting and will in future have to interlink their business processes across domain boundaries. This is the interoperability assertion.

In a decentralised PKI the bindings are based on verifiable cryptographic operations. This makes the bindings strong. Because all operations are verifiable, they require no trust into any given, centralised trust provider and therefore that verifiability is transitive across trust domains. The most important operation is determining the state of the controlling keys for a given identifier. The difficulty for decentralised PKI is ensuring that all operations are duplicity evident. This means that duplicity by a given party to a transaction is detectable by the other party or parties to that transaction. Ensuring duplicity evident operation in a totally decentralised way may be accomplished by splitting the infrastructure into two parts. These are the promulgation infrastructure and the confirmation infrastructure. What is being promulgated is the key state which underlies the bindings between the controller, identifier, and key pair. What is being confirmed is that there is no evidence of duplicity or irreconcilable duplicity in that promulgated key state. Each controller controls its own promulgation infrastructure; each verifier controls its own confirmation infrastructure.

This split enables what is called shared data without shared control over the infrastructure. There is no shared control over the infrastructure. What is shared, however, is the key state. This is the shared data. The key state is provable using a verifiable data structure. All that needs to be agreed upon is the protocol for sharing the key state as verifiable data structure and not who controls shared infrastructure.

Shared control over the PKI is what makes it centralised to some extent and makes transitive trust difficult. Clearly, in an international setting, shared control may be extremely problematic. By splitting the infrastructure into two parts, shared control is no longer needed. Each controller controls its own key state promulgation infrastructure, and each verifier controls its own key state confirmation infrastructure. This makes the system totally decentralisable.

This split fosters competitive differentiation and innovation which drives lower cost-for-performance and in turn lowers trust transaction costs.

In a decentralised PKI there are two classes of identifiers. The first class consists of self-certifying identifiers. These are cryptonymous (crypto-pseudonymous) identifiers that are cryptographically derived from key pairs. There is no practical limit to the number of cryptonymous identifiers and only the holder of the private keys can prove control over such an identifier. These form a cryptographic end-verifiable root-of-trust to the bindings between the controller, identifier, and key pairs. The second class consists of human meaningful identifiers. Because human meaningful identifiers are scarce, they require some entity to issue them. This is inherently centralising to that entity. However, if the infrastructure that supports them is otherwise decentralised, their trust may securely cross trust domain boundaries, i.e is transitive.

Global Legal Entity Identifier Foundation (GLEIF)'s Legal Entity Identifier (LEI) is already accepted as a cross-jurisdictional human-meaningful identifier. The Verifiable Legal Entity Identifier (vLEI) is a credential based on decentralised PKI that enables cryptographic verification of the association between an LEI and the controllers of an AID (cryptonym). Thus, a vLEI imbues a LEI with cryptographic verifiability of the bindings between controller, identifier, and key pairs in a cross-trust-domain friendly way. The protocol to exchange and verify public keys as well as their status as issued or revoked is called Key Event Receipt Infrastructure (KERI). KERI allows for bridging trust domains, e.g. across multiple blockchain applications or APIs, by anchoring any credential on the target system. The infrastructure for this network-of-networks is called Witness Network.

11.7. Similarities of digital certificates and verifiable credentials

Both digital certificates and verifiable credentials use crypto-algorithms for binding the content to a pair of keys, the private and public keys created by a PKI. In both cases the content is verifiable which means it is tied to the holder and it cannot be changed without compromising the hash code. The latter means that there is certainty about the data contained has not been modified or tampered with. This is called authenticity of the data, in this case the identity information.

The crypto-algorithms are foundational. In general, all different types of crypto-algorithms and key lengths (important for protection against hacking the keys) can be used in digital certificates and verifiable credentials. Additional standards are in place to define them in a specific context. The underlying software is usually open source and can be used equally for digital certificates and verifiable credentials.

Both come with templates describing the content of the digital representation:

- The x.509 standard defines a skeleton of attributes to be used. Contents of certificates can be enhanced by additional attributes based on additional standards. Good examples are electronic Identification, Authentication and Trust Services (eIDAS) compliant certificates in the European Union. There, the content template is defined by a corresponding European Telecommunications Standards Institute (ETSI) standard. It is important to recognise that both sender and receiver of digital certificates must agree on the standards and protocols. This leads in many cases to different types of certificates used only in a certain context.

- Verifiable credentials also contain content linked to the key pair. The standards, e.g., VC 1.0 by W3C, ACDC 1.0 by Trust over IP foundation (now a draft specification at the Internet Engineering Task Force (IETF)) and market standards such as AnonCreds on Hyperledger, allow the definition of templates. In principle, the templates for digital identity could be similar.

To use an analogy, digital certificates as well as verifiable credentials are in fact containers for data, sealed with the private key of the holder.

11.8. Differences

Digital certificates are used mainly for identity information. Typical examples are transport layer security (TLS) certificates on the internet, or qualified seals in eIDAS. They are usually used for encryption and authentication when accessing a resource, e.g,. web service, or for digital signing, e.g., machine-readable contracts, invoices, reports etc.

Certificate issuance is the domain of certificates authorities (CA) and trust service providers (TSP). The underlying PKI is centralised PKI. To obtain a certificate for a certain use case, it must be applied for with a CA. The certificate itself contains the content as well as the trust chain of the CA. Chain of trust means the hierarchy of issuers. So, if the certificate coming from a TSP in Europe, it contains the trust chain of the certificate of the holder, linked to the certificate of the issuer, which is linked to the root certificate, e.g., of a European jurisdiction.

Certificates have a fixed time to live. Encoded within the certificate is the date from which on the certificate is invalid and cannot longer be used. This can create an issue with the integrity and accuracy of the contained information compared to the real world. For instance, a name could change but the holder may continue to use certificate which carries the old value until they become invalid. In some use cases, the validity is restricted to very few minutes, in others up to a year or longer.

To overcome this referential integrity issue between certificates and the real world, certificates can be revoked at any time. The certificate is added to a central revocation list with all revoked certificates of a certain trust domain. Downstream applications can access the revocation list to prove the validity. This results in the need for having multiple certificates for multiple domains, and over time multiple certificates for the same underlying identity. And all certificates have a different cryptographic identifier which makes it impossible to have a complete trace

for all certificates issued for the same entity or person. To solve these problems requires rigorous rules and infrastructure which must be controlled for compliance. In the end, verification of all aspects is complex, and delegated to applications and infrastructures which makes it more error prone and costly than it should be.

Verifiable credentials are more flexible. For easier read, the differences between the various types of credentials will not be discussed here. Basically, any ecosystem could define templates for credentials as described in a governance framework. In case of the vLEI the content is restricted to very basic information such as the LEI and/or the role of the holder. All other information can be provided outside as the embedded LEI points to the most up to date information on identity of an organisation. Data privacy constraints can be managed outside the credential.

Verifiable credentials are decentralised by nature. Both the issuance and the use can be distributed among autonomous systems or nodes in a network, aka the internet. A required standard is the protocol between all nodes and across trust domains. In case of the vLEI this protocol is KERI, also a draft IETF standard.

Verifiable credentials can but do not need to have an expiration date. In case of the LEI we see a life-long unambiguous identifier that will never change or get re-used. The digital twin vLEI should be valid as long as the LEI is issued and renewed. However, this requires the possibility of real-time revocation. In the event of newer information, e.g., if the company ceases trading and the LEI is retired, the information about the revocation must be available to downstream applications immediately. Furthermore, each derived credential is rendered invalid as well. If a company cease to exist, all credentials for all employees, customers, members etc. will become invalid at once. This is guaranteed by the KERI protocol. Each request for verification includes the check for revocation. It should be noted that the verification happens against distributed nodes. The credentials contain information regarding the path for verification. A central blockchain or ledger is not needed.

12 Zero Trust Architecture

Organisations have for long operated applications they require to perform business functions - application landscapes – within their own networks, often called intranet. This was, and to an extent still is, being done in dedicated company owned data centres or private clouds. The networks are typically enclosed by software instances controlling access to applications on certain ports, the so-called firewalls, and helped by role-based access limitations. Several lines of defence were defined to protect the network and keep attackers out of private networks and data centres.

12.1. Directory service federation spaghetti

Employees are usually being given access to a set of applications in an organisation. They're being assigned dedicated roles to perform certain functions while using their subset of applications.

The roles are being assigned by the organisation's identity access management team for all the organisation's personnel. A person in a bank working on Letter of Credit has access to a trade finance back-office system and a variety of other applications required.

This mode of operation has long worked rather poorly than ideal, but another mode of operation just didn't exist, though there was often the need to allow for access for external people to interact with internal applications. A trade example would be for a bank's employee working on a Letter of Credit to access a Bill of Lading that has been stored in a logistics service provider network.

How could this access be granted? Attempts to federate directory services, providing foreign identity information, have mostly failed over the exponential permutation growth in the number of services to be interconnected. And there will be ever more interconnection requirements.

What's more, the accelerating trend to cloudification has gradually perforated the security perimeters of organisations, following the need to connect and integrate more and more internally and externally operated applications with those of external service providers.

12.2. Security threats

There is another downside to the traded model of operating "private central identity". An organisations internal network security parameters resemble a castle's wall. From outside no access is possible, but once an attacker has surmounted the perimeter, there is often little limits to further "lateral movement". This type of criminal activity is on a raise globally with devastating effects for affected organisations.

Often access to a network is attained by phishing attacks. An attacker gains access in a staggered approach, tempting an internal user to click on a link or open a forged file attached to a mail, eventually gaining knowledge of the user's credentials and then continues to move laterally alongside the attacked user's authorisation spectrum. In many cases, internal users who either lack skills or can socially be tricked into conducive behaviour are the target for attacks regardless how careful the security perimeter has been designed.

12.3. Zero Trust

An environment built following Zero Trust Architecture principles does not pose vulnerability of that kind. Access privileges are not centred around users, but always around the resources that are being used.

A resource can be anything. A data object like a file, an IoT device or just the data it makes

available, calculation power rendered by either a server cluster or an edge instance like small computing unit in a car or a container.

Let us assume the resource in consideration is an electronic Bill of Lading, which represents a consignment.

Let us further assume that access to this eB/L, or a subset of its information shall be granted to a port authority, but only at the time the container is in the port. An IoT device in the container would connect to the port authority's network and be asked for authentication. The reference to retrieve the eB/L from a data space would only be sent by the IoT device once a two-way authentication and authorisation process has successfully completed and the port authority has proven their access right.

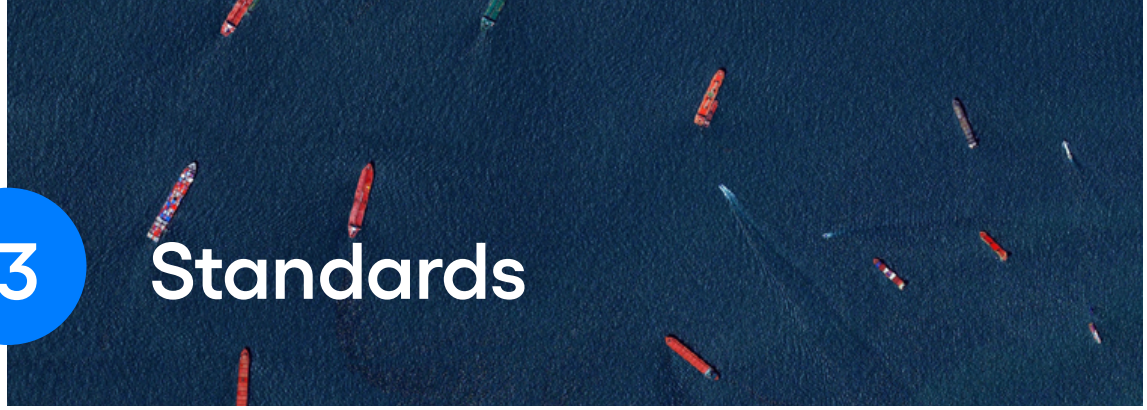
As soon as the container is released and left the port, no further access to the eB/L is possible, since the reference to the eB/L is a single-use token.

The single-use token could also be limited to a certain process or purpose. Or only allow for certain required sections of the eB/L to be revealed, while others remain hidden.

This way Zero Trust Architectures and transitive trust support the right to use certain data for a certain process at a certain time, but not for anything else or at a later point in time.

This is data sovereignty.

Zero Trust Architectures are based on verifiable credentials and address this and a multitude of other issues. The methods for resolution between foreign networks are always build-in.



13 Standards

13.1. Technical Standards

13.1.1. X.509 Certificate

An X.509 Certificate, often just called certificate, is a digitally signed file binding an identity to a public key. The identity can represent a hostname (a specified computer), an organisation (i.e. a company participating in a trade) or a human being (a natural person). The certificate is usually issued and signed by a commonly known, reputable, and trusted certification authority, i.e. Let's Encrypt (not for profit) or IdenTrust (commercial).

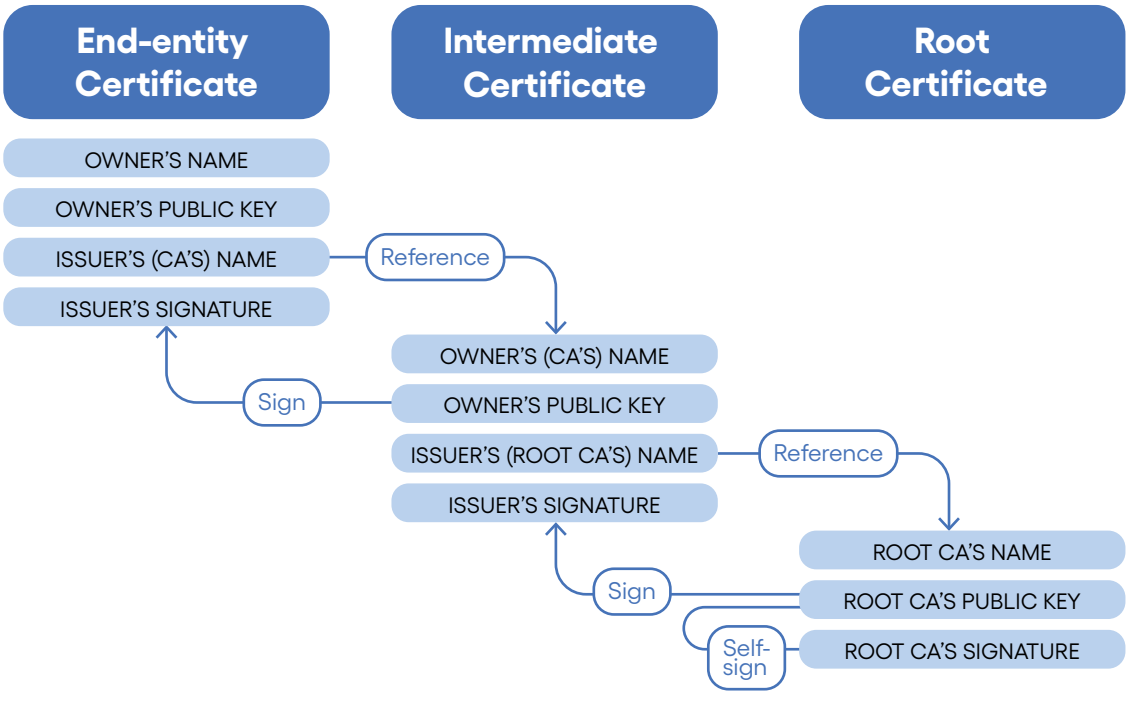
A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. In other words: a trade documentation that has been signed with the private key of a x.509 certificate and thus can be verified by its recipient to having been issued by the subject specified in the certificate.

The X.509 standard has been set by the International Telecommunication Union in 1988.

Since a X.509 certificate relies on the trust put into the certificate authority the PKI it supports has a centralised component.

Certificates come with an expiry date, after which they must be re-issued.

A trust chain can be formed from an end-entity certificate via one or more intermediate certificates through to a root certificate, typically held by the certificate authority.



In case a certificate is discovered to have been improperly issued, or if a private key is thought to have been compromised, certificates can be irreversibly revoked by the CA by adding it to a certificate revocation list, which are usually updated on a daily basis. Software relying on certificates thus need to check against revocation lists every time trust in a certificate is being asserted.

X.509 certificates are used in many internet protocols, including TLS/SSL, forming the basis for HTTPS, the secure protocol for browsing the World Wide Web. They are also used for electronic signatures.

13.1.2. Decentralised Identifiers (DID)[10]

Decentralised Identifiers are based on the model that the controller of an identity keeps a private key which is used for authentication, assertions and other use cases.

All DIDs resolve to a DID document, which includes the corresponding public key.

This way, anyone can verify that an entity claiming to control a given identifier holds its private key.

This removes the need to map between multiple identity provider representations; the DID is essentially its own identity provider[11]

DIDs are currently mostly used in blockchain/DLT solutions, but do not rely on DLT.

Decentralised Identifiers[12] enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are Uniform Resource Identifier (URI), a unique resource identifier, that associate a DID subject with a DID document allowing trustable interactions associated with that subject.

Each DID document, being a set of data describing the DID subject, can express cryptographic material, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject via service endpoints. A DID might provide the means to return the DID subject itself, if the DID subject is an information resource such as a data model.

This document specifies the DID syntax, a common data model, core properties, serialised representations, DID operations, and an explanation of the process of resolving DIDs to the resources that they represent.

A DID uniquely identifies any subject, like a trading party, be it an organisation or a natural person, or an object, which can be data, a machine, a software process, or a trade documentation in the form of transferable record. There is no need for a central trusted authority to issue a DID.

The DID subject is the entity identified by a DID and described in a DID document.

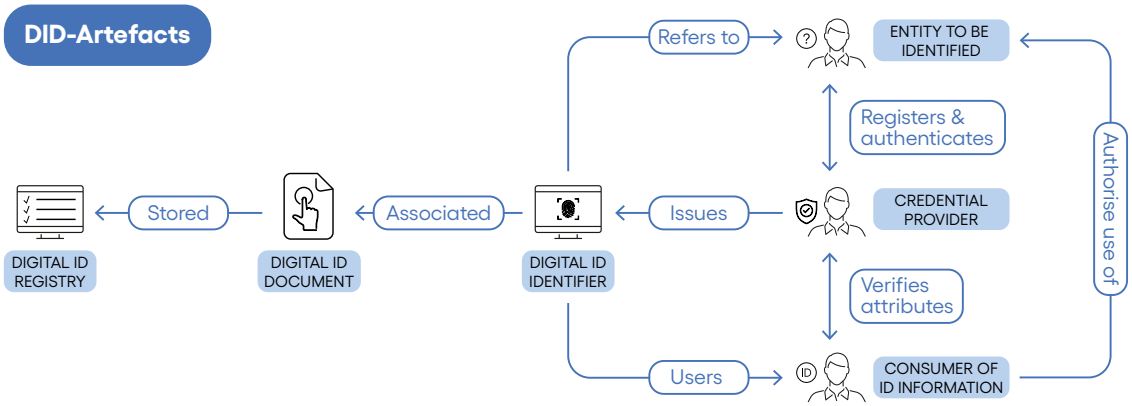
Anything can be a DID subject: A person employed by a bank, a seller Co. operating on FineWineB2B, a physical thing like an IoT device, a digital thing like an electronic Bill of Lading, a logical thing like a process library running on XC4.trade to govern allowed operations on the eB/L stored, or a trade itself, represented by its trade contract entered into on FineWineB2B.

The DID subject is usually, but not necessarily the DID controller, who can make changes to the DID document. In case the DID identifies an object, as a trade documentation, its controller may be another object, a software process, whose DID is then controlled by a DID subject being a natural person, and therefore legally a subject.

[10] Source: W3C - https://www.w3.org/TR/did-core/

[11] Source: Nis Jespersen, 28th plenary Meeting UN/CEFACT. https://unece.org/sites/default/files/2022-10/Nis%20Jespersen%20-%20Solving%20International%20Trade%20ChallengeswithEmerging%20Web%20Technologies.pdf

[12] https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers



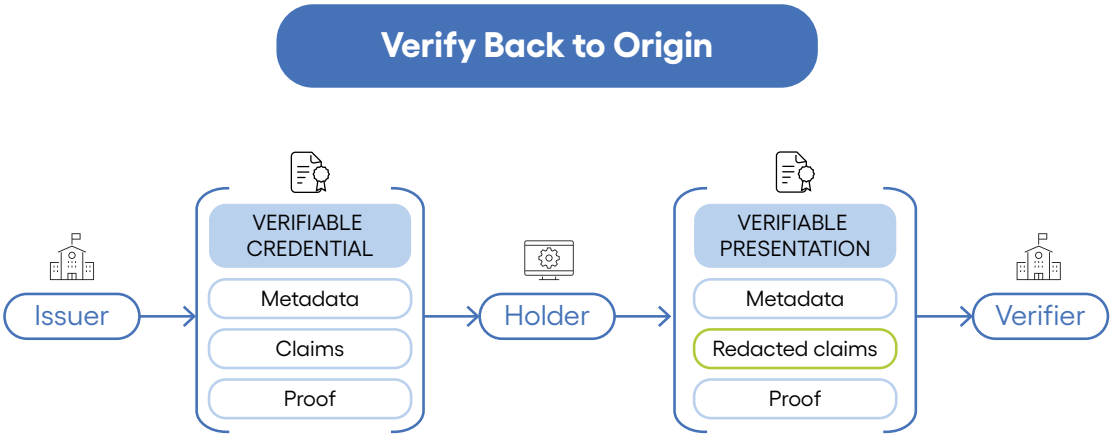
13.1.3. Verifiable Credentials

The Verifiable Credential (VC) standard of the World-Wide-Web Consortium (W3C) explains[13]:

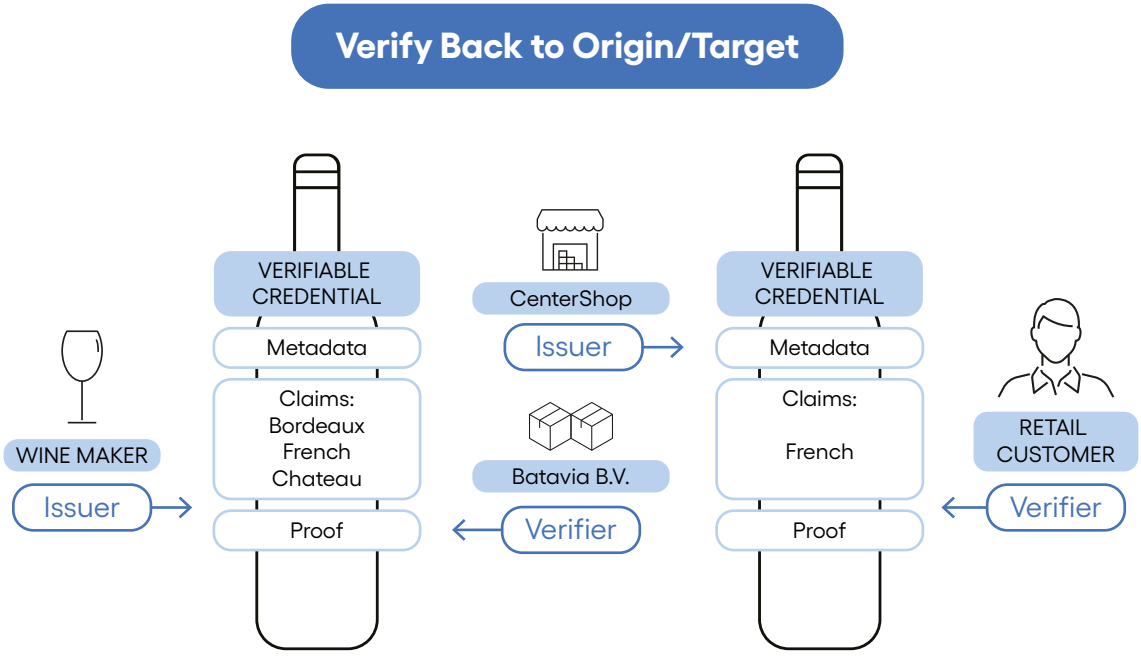
"Credentials are a part of our daily lives; driver's licenses are used to assert that we learned how to operate a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. This specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine verifiable"

A credential is a set of one or more claims made by an issuer. A VC is a tamper-evident credential whose authorship can be cryptographically verified. VC can be used to build verifiable presentations, which can also be cryptographically verified. Authorship of data can hence be trusted.

Example: A VC issued for a bottle of wine by a winemaker and specifying a certain quality of wine can be verified to having been issued by this winemaker. It doesn't guarantee that the wine meets the quality features that have been claimed. Someone else, a wine inspector of good reputation could issue another VC, which would be provably issued by her.



[13] https://www.w3.org/TR/vc-data-model/



13.1.4. Authentic Chained Data Container (ACDC)

An authentic chained data container is an IETF[14] internet draft focused specification being incubated at the Trust over IP foundation. An ACDC is a variant of the W3C VC specification. One primary purpose of the ACDC protocol is to provide granular provenanced proof-of-authorship (authenticity) of their contained data via a tree or chain of linked ACDCs (technically a directed acyclic graph or directed acyclic graphs (DAG)). Like the concept of a chain-of-custody, ACDCs provide a verifiable chain of proof-of-authorship of the contained data.

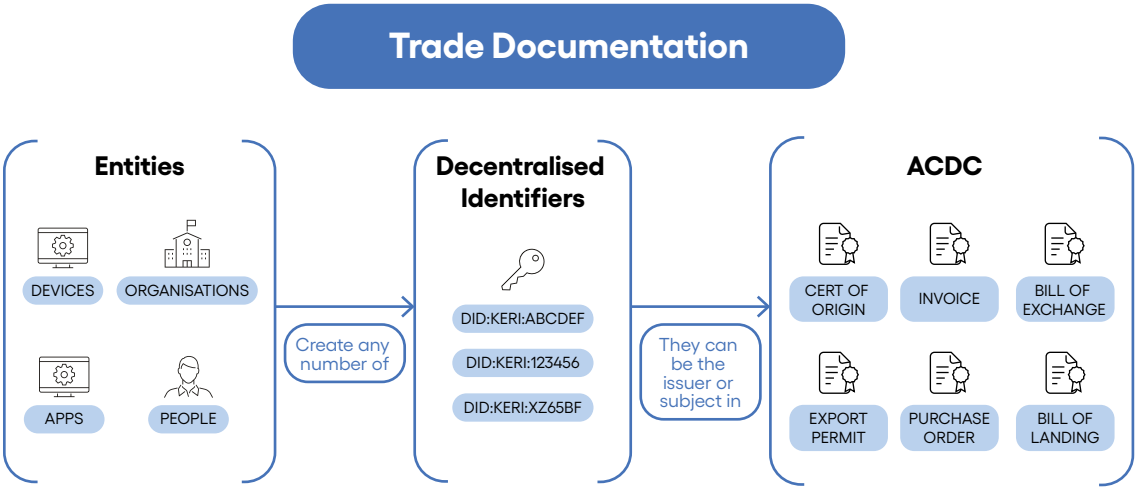
Chains of ACDCs that merely provide proof-of-authorship (authenticity) of data may be appended to chains of ACDCs that provide proof-of-authority (delegation) to enable verifiable delegated authorised authorship of data. This is a vital facility for authentic data supply chains. Furthermore, any physical supply chain may be measured, monitored, regulated, audited, and/or archived by a data supply chain acting as a digital twin.

Hereby ACDCs provide the critical enabling facility for an authentic data economy and by association an authentic real (twinned) economy.

An ACDC is a data container that provides a verifiable proof of origin linked to an identifier. This origination identifier is called the Issuer. It identifies the entity that the ACDC is issued by. Optionally an ACDC can also be linked to another identifier called the Issuee that it is issued to. It then identifies the entity the ACDC issued to. The Issuee can provide a verifiable proof of its identity at the time of presentation. Each ACDC can also be chained to other ACDCs. Interdependencies between several ACDCs, like different trade instruments wrapped in ACDCs and contracts relating them can this way be woven.

This combination of features enable a set of ACDCs to provide a verifiable chain of provenance of the contained data and optionally a verifiable chain of authority from Issuer to Issuee to Issuer and so forth. Thus an ACDC can convey both verifiably authoritative data and authorised entitlements.

[14] IETF – Internet Engineering Task Force, https://www.ietf.org



13.1.5. Composable Event Streaming Representation (CESR)

Composable Event Streaming Representation (CESR) is a protocol allowing to sign subsections of a documentation. More than one person (or software process) can sign the same or different sections of a documentation provided.

The CESR specification and proof format were developed within a ToIP working group and currently are drafts of the Internet Engineering Task Force (IETF)[15].

Content in sections of a report or a documentation, can be signed by one or more officers and employees/managers of an organisation using their Official Organisation Roles (OOR) and Engagement Context Role (ECR) vLEIs.

The entire content of the same report, for example, also can be signed in its entirety by one or more officers and employees/managers of organisations using their company issued credentials.

A Bill of Exchange (BoE) is frequently multi-signed on different sections. The drawer (debtor) signs the BoE, as well as the drawee (creditor) and every consequential endorser of the instrument signs a separate section. Similar procedures apply to Bills of Lading, Warehouse Receipts, and other negotiable instruments.

In case standardised credentials for company roles were to be used in trade on a global level to multi-sign trade documentation, ACDC and CESR could provide means to dramatically simplify exchange of documentations, which i.e., securitise property or represent documentation required for a trade related process, i.e., hazardous goods information.

GLEIF's vLEI offers such a standard.

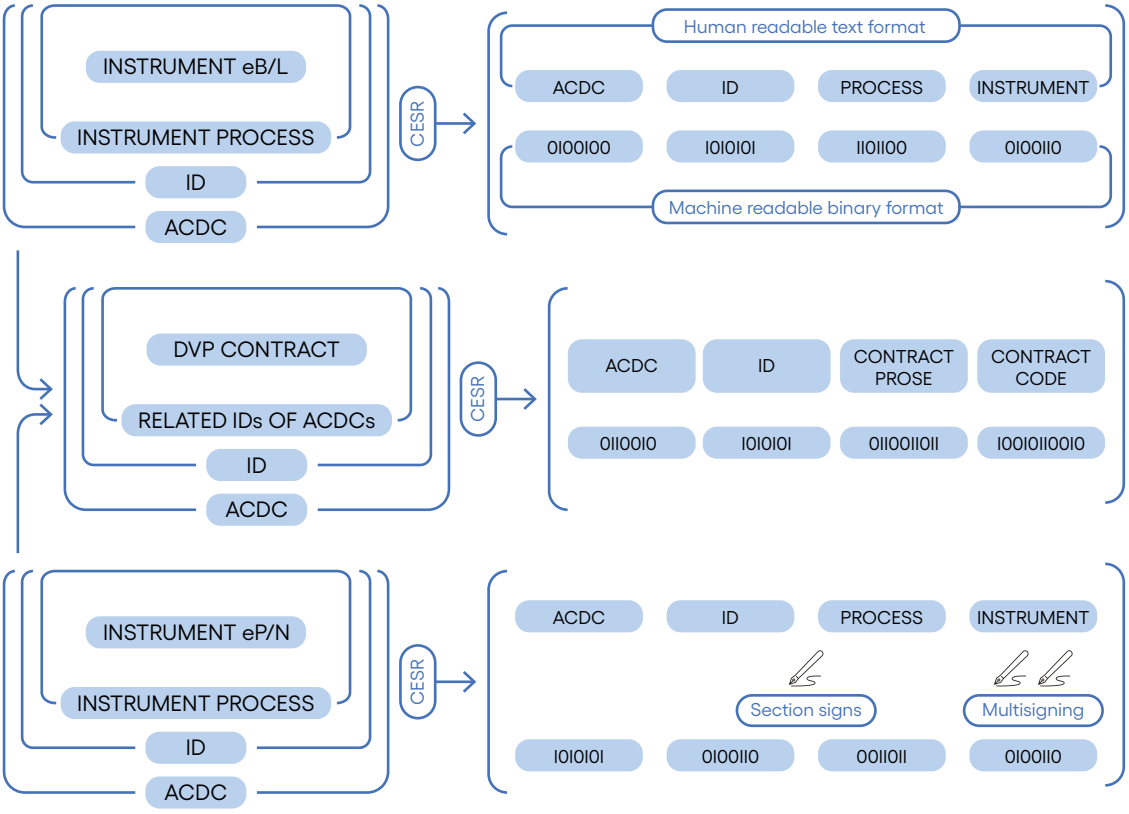
The CESR protocol allows for swift transport of data containers between different systems while preserving the unique features of the data containers and supporting human readable and machine-readable data representations concurrently, while preserving the identity context of the information provided. In more plain words: CESR allows retaining of who has provided what information regardless of how many times the information was conveyed to a downstream system.

Further CESR enables signing of entire data containers or subsections of its content. It even allows multi-signing of sections and subsections.

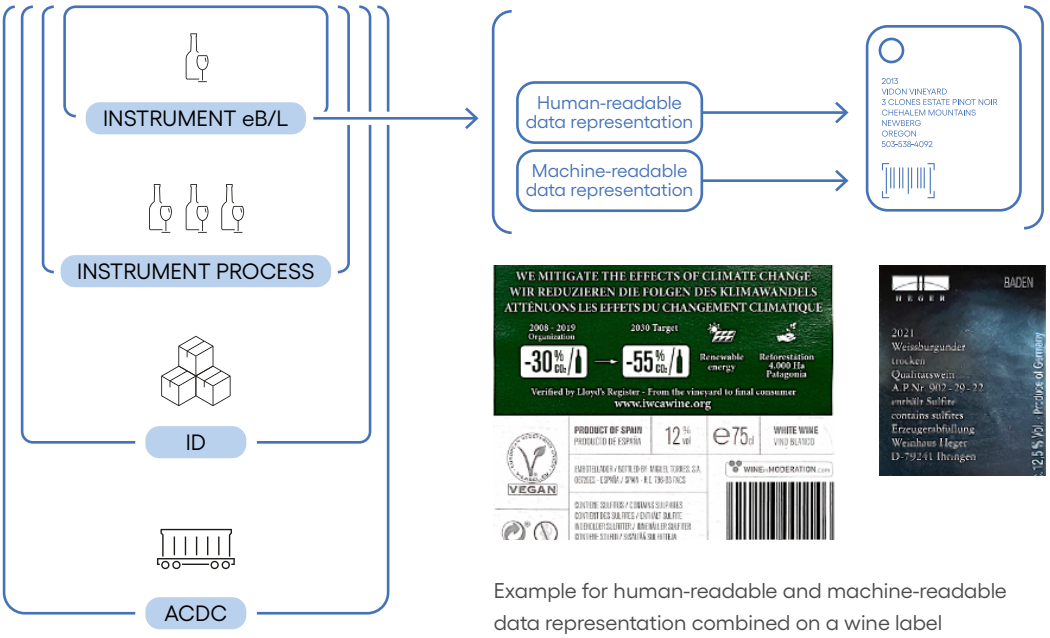
As an example, a Promissory Note is being signed by its issuer and can in a downstream process become endorsed by multiple endorsees on its endorsement section.

[15] https://weboftrust.github.io/ietf-cesr/draft-ssmith-cesr.html

Interrelated ACDCs, CESR serialised



Nested information containerisation and representation



Example for human-readable and machine-readable data representation combined on a wine label

As another example a Bill of Lading is being signed in full by the carrier and countersigned in full by the shipper and consequently put to the order of a succeeding proprietor of a traded commodity by signing it again.

13.2. Combining ACDC and CESR

The combination of ACDC as an instrument bearing credential and CESR as a conveyance facilitator may be a powerful solution to alleviate the interoperability challenge of digital trade documentation while at the same time introducing a cryptographically strong bond between the information supply chain and the trust supply chain. ACDC and CESR can be used in blockchain, cloud or any other technical application.

13.3. Identity relevant standards in trade

13.3.1. Legal Entity Identifier (LEI)

The LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure and thus answers the questions of 'who is who' and 'who owns whom'. Simply put, the publicly available LEI data pool can be regarded as a global directory or business register, which greatly enhances transparency in the global marketplace. Data about a LEI holder can be obtained free of charge from https://search.gleif.org/#/search/

13.3.2. Verifiable Legal Entity Identifier (vLEI)

The vLEI is the secure digital counterpart of a conventional LEI. It is a digitally trustworthy version of the 20-digit LEI code which can be automatically verified, without the need for human intervention.

The vLEI is a digitised LEI service, utilising digitally verifiable credentials containing the verified organisation identity to provide automated identity verification between counterparties. The vLEI provides a cryptographically secure chain of trust that can replace manual processes needed to access and confirm an entity's identity across industries.

vLEI is delivered in an agnostic method able to support self-sovereign identity (SSI) platforms. This ensures the identity holder has control of his/her personal data over how, when, and to whom that data is revealed.

13.3.3. Role Credential

A verifiable credential certifying the official role of a person acting on behalf of an organisation in a machine-readable way.

The standard, ISO 5009, is used to verify the identity and position of individuals who represent an organisation (like a business or company) and is intended for inclusion in current and future digital assets. This will be achieved through global uniformity of two kinds of digital assets under the LEI digital ID umbrella: vLEI and digital certificates embedded with LEIs.

Role Credential allow to assert information on people associated with the organisation. An Official Organisation Role Credential (OOR) links an individual with an organisation in a well-known role. The roles are limited to an official set of 'official' roles as defined by an ISO standard (ISO 5009_2022). This list includes roles such as 'Director', 'Chief Executive Officer', 'Chief Financial Officer'. With an OOR credential an individual is able to present themselves as holding an official role for a given organisation, and all the claims presented can be electronically verified in real time.

An Engagement Context Role Credential (ECR) is very similar to the OOR except that the role is custom, the legal entity can define any role they wish and place that in the ECR. For example, "customer of", "supplier to", "contractor for".

13.3.4. Global Location Number (GLN [GS1])

The GLN[16] provides a globally unique, standardised identifier that allows companies to answer the questions “who” and “where” within their own organisation and throughout the entire supply chain.

Parties identified by GLN include legal entities and functions. For example, a legal entity could be a corporation, subsidiary or government body. Functions are organisational subdivisions or departments, such as accounts receivable or quality assurance.

Locations include both physical and digital locations found throughout business. Locations identified with a GLN include places like warehouses, pharmacies, dock doors, ports, farms and ERP systems. When needed, locations inside larger facilities, like a room or shelf, can be assigned GLNs as well.

13.3.5. Global Trade Item Number (GTIN [GS1])

A Global Trade Item Number (GTIN)[17] can be used by a company to uniquely identify all of its trade items. GS1 defines trade items as products or services that are priced, ordered or invoiced at any point in the supply chain.

14.3.6. Data Universal Numbering System (DUNS [D&B])

DUNS is a proprietary system developed and managed by Dun & Bradstreet, a commercial provider of company identification, that assigns a unique numeric identifier, referred to as a "DUNS number" to a single business entity.

13.3.7. Decentralised Identifier (DID)

A W3C[18] standard[19] for Decentralised Identifiers. All DIDs resolve to a DID document, which includes the corresponding public key. This way, anyone can verify that an entity claiming to control a given identifier indeed holds its private key.

This removes the need to map between multiple identity provider representations; the DID is essentially its own identity provider.

13.4. Standards Inflation

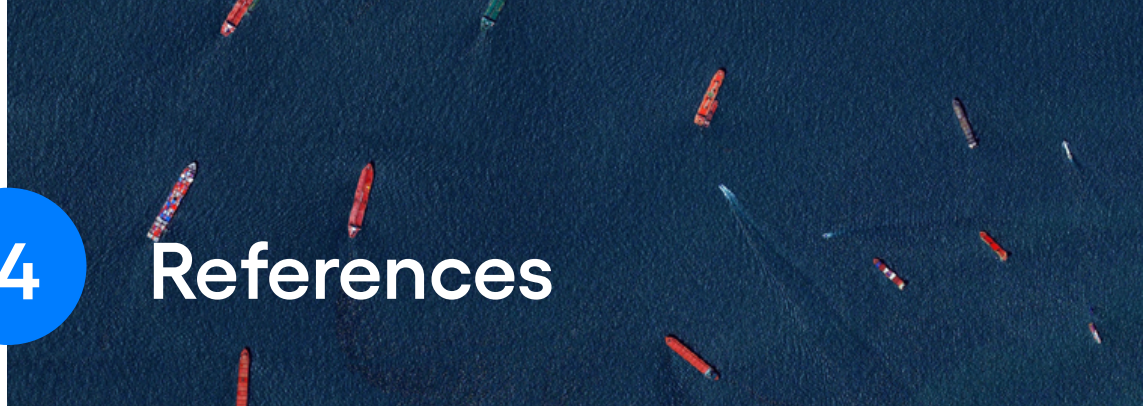
While standardisation is mostly beneficial, having a multitude of standards serving the same or very similar purpose can be detrimental to the original intention of standardising: producing interoperability.

Identifiers for legal entities cannot be done without in digitalising supply chains. We have found this situation and suspect a considerable overlap between the standards:

- ISO/IEC 6523 specifies a structure for globally and unambiguously identifying organisations, and parts thereof for the purpose of information interchange.
- ISO 8000-116 specifies the requirements for representing Authoritative Legal Entity Identifiers (ALEI).
- ISO 17442 specifies the minimum elements of an unambiguous LEI scheme to identify the legal entities relevant to any financial transaction.

This may display how difficult it can be to convene people to undertake communal efforts, even in the presence of a sizeable intersection of interests.

[16] Source: https://www.gs1.org/docs/idkeys/GS1_GLN_Executive_Summary.pdf
[17] https://www.gs1.org/standards/id-keys/gtin
[18] https://www.w3.org
[19] https://www.w3.org/TR/did-core/



14 References

ICC DSI Standards Toolkit for Cross-Border paperless trade

https://iccwbo.org/publication/standards-toolkit-for-cross-border-paperless-trade/

ICC Identity Management Guide

https://iccwbo.org/content/uploads/sites/3/2020/11/icc-identity-management-guide.pdf

Digitisation vs. Digitalisation

https://www.truqcapp.com/digitization-vs-digitalisation-differences-definitions-and-examples/

Model Law on Identity Management by United Nations Commission on International Trade Law

https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/009/38/PDF/V2200938.pdf?OpenElement

Model Law on Electronic Transferable Records

https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf

NIST (National Institute on Standards and Technology, US Department of Commerce) on Zero Trust Architecture

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Bank for International Settlements on "Corporate Digital Identity"

https://www.bis.org/publ/bppdf/bispap126.pdf

McKinsey Technology Trends Outlook 2022

https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202022/mckinsey-tech-trends-outlook-2022-full-report.pdf

See page 94-106 for "Trust architectures and digital identity"

15 Appendices

15.1 Appendix 1 - Definitions

The following definitions are essential for this paper, outlining the multiple opportunities there are in digitising trade and using appropriate standards supporting the trusted means in every stage or trade processes.

ACDC (Authentic Chained Data Containers) provide a verifiable chain of proof-of-authorship of the contained data. The ACDC protocol is to provide granular provenanced proof-of-authorship (authenticity) of their contained data via a tree or chain of linked ACDCs (technically a directed acyclic graph or DAG). The ACDC specification was developed within a ToIP working group and currently is a draft specification of the Internet Engineering Task Force (IETF).

CA (Certificate Authority)

A Certificate Authority (CA), also sometimes referred to as a Certification Authority, is a company or organisation that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.

Composable Event Streaming Representation (CESR) is a dual text-binary encoding format that has the unique property of text-binary concatenation composability. The CESR Specification and Proof Format were developed within a ToIP working group and currently are drafts of the Internet Engineering Task Force (IETF).

Digital Authentication[20] refers to an electronic process that allows for the electronic identification of a natural or legal person. Additionally, authentication may also confirm the origin and integrity of data in electronic form, such as the issuance of a digital certificate to attest to the authenticity of a website.

An electronic Certificate of Origin could be seen as a use case for electronic certification, whereby an issuing chamber of commerce.

Decentralised Identifiers (DIDs)[21] are a new type of identifier that enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID.

Digital Certificates

An X.509 certificate binds an identity to a public key using a digital signature. A certificate contains an identity and a public key and is either signed by a certificate authority or is self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can use the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

DUNS Number is a unique, proprietary nine-digit identifier for businesses issued and managed by Dun & Bradstreet.

Global Location Number (GLN) can be used by companies to identify their locations, giving them complete flexibility to identify any type or level of location required. The GS1 GLN is recognised by the ISO/IEC 6523 standard.

KERI is a protocol for a truly decentralised identity system. It is ledger-less which means it does not need to use a ledger at all or ledger-portable which means that

[20] Source: https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics

[21] Source: https://www.w3.org/TR/did-core/

its identifiers are not locked to any given ledger and may switch as needed. In other words KERI identifiers are truly portable. The KERI specification was developed within a ToIP working group and currently is a draft specification of the Internet Engineering Task Force (IETF).

The **Legal Entity Identifier (LEI)** is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO).

Object (Legal)

Objects are entities **without rights and obligations** according to the legislation of UN members.

Examples for objects in trade are trade documents like invoices (or their dataset representations in fully dematerialised trade), IoT sensors, containers, or consignments.

Public Key[22] is a cryptographic key that can be distributed to the public and does not require secure storage. Messages encrypted by the public key can only be decrypted by the corresponding private key.

Public Key Infrastructure (PKI)[23] is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-private-key-pairs. There can be centralised as well as decentralised Public Key Infrastructures (PKIs).

A public and private keypair are mathematically entangled. For an identifier which is based on a public-private-key-pair only the holder of the private key can prove control over the identifier.

Private Key is a cryptographic key which must be kept secret and requires sure storage. A private key is being used to decrypt messages being encrypted using a public key.

Role Credential is a verifiable credential attached to the identity of the holder, which allows proving tenancy of an official role in an organisation. The Role Credential is based in an "official role standard" in the process of being standardised within the ISO TC 68 as ISO standard 5009.

The **Society for Worldwide Interbank Financial Telecommunication (SWIFT)** is a global member-owned cooperative and the world's leading provider of secure financial messaging services. https://www.swift.com

Subject (Legal)

Subjects are entities with rights and obligations according to the legislation of the UN members. There are two categories of subjects in any country: natural persons and legal entities.

Examples for legal entity subjects in trade are companies that sell and buy or companies that provide services.

Examples for natural persons in trade are employees of these companies.

Verifiable credentials are digitally signed credentials capable of being verified in decentralised manner.

vLEI is short for "verifiable Legal Entity Identifier" and a Verifiable Credential which contains a LEI issued in accordance with the vLEI Ecosystem Governance Framework requirements.

vLEIs are based on the Trust over IP Authentic Chained Data Container (ACDC) specification (based on the Key Event Receipt Infrastructure (KERI) protocol, both Internet Engineering Task Force (IETF) draft specifications.

W3C stands for World Wide Web Consortium. The standardisation of the DID and VC occurs in the W3C context.

X.509 Certificate

A standardised machine-readable certificate format for certificate documents. The standard is called X.509v3. Originally, it was an ISO standard, but these days it is maintained by the Internet Engineering Task Force as RFC 3280

[22] Source: https://www.securew2.com/blog/public-key-infrastructure-explained

[23] Source: https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki

Zero Trust[24] is a strategic approach to cybersecurity that secures an organisation by eliminating implicit trust and continuously validating every stage of a digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular, "least access" policies. (Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture)

Trust Domain

A trust domain is a domain that the local system trusts to authenticate users. In other words, if a user or application is authenticated by a trusted domain, this authentication is accepted by all domains that trust the authenticating domain.

15.2 Appendix 2 – identity terms

The terms are defined in Article 1. Definitions in the 'Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services' (ML-IdM[25]) of UNCITRAL.

Attribute means an item of information or data associated with a person

Data message means information generated, sent, received or stored by electronic, magnetic, optical or similar means

Electronic Identification ["Authentication"], in the context of identity management services, means a process used to achieve sufficient assurance in the binding between a person and an identity

Identity means a set of attributes that allows a person to be uniquely distinguished within a particular context

Identity Credentials means the data, or the physical object upon which the data may reside, that a person may present for electronic identification

Identity Management Services means services consisting of managing identity proofing or electronic identification

Identity Management Service Provider means a person who enters into an arrangement for the provision of identity management services with a subscriber

Identity Management System means a set of functions and capabilities to manage identity proofing and electronic identification

Identity Proofing means the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a person within a particular context

Relying Party means a person who acts on the basis of the result of identity management services or trust services

Subscriber means a person who enters into an arrangement for the provision of identity management services or trust services with an identity management service provider or a trust service provider

Trust Service means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services

Trust Service Provider means a person who enters into an arrangement for the provision of one or more trust services with a subscriber

[24] Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

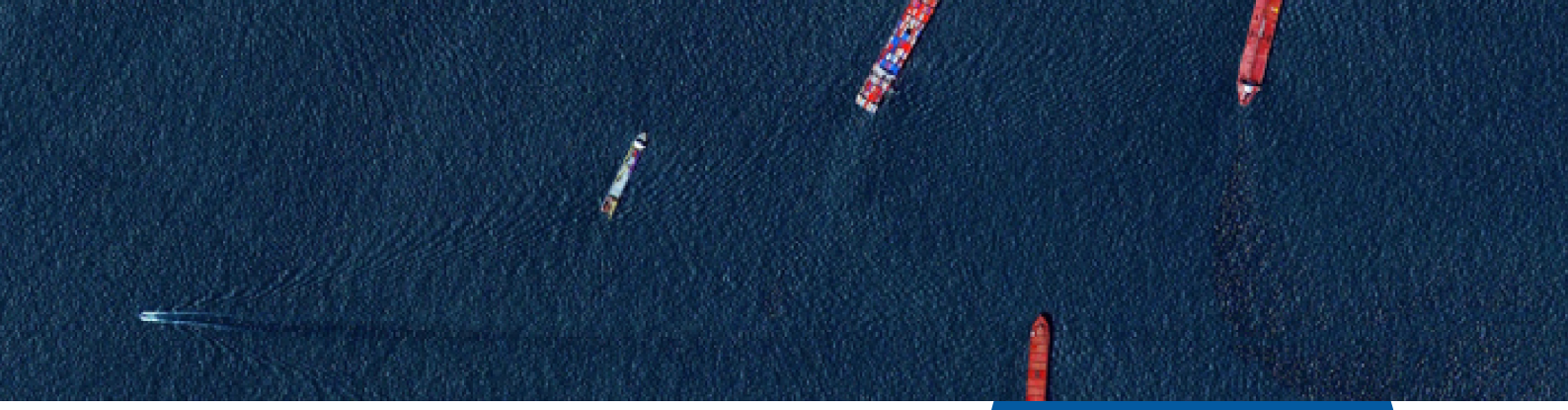
[25] ML-IdM – Model Law on Identity Management, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf

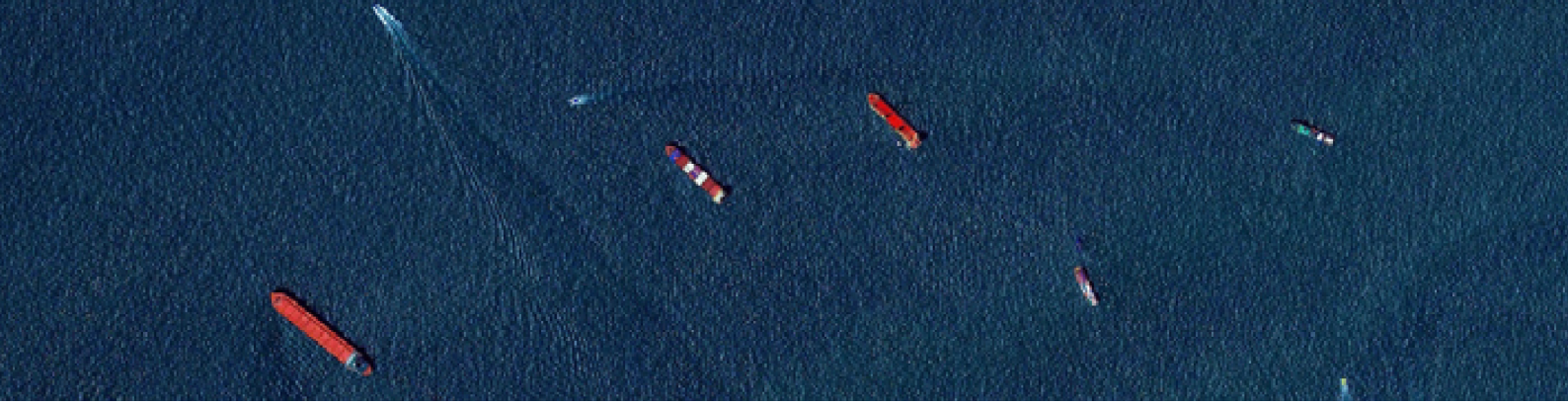
15.3 Appendix 3 – an example for an X.509 certificate

bitkom.org	
Subject Name	
Common Nam:	bitkom.org
Issuer Name	
Country or Region:	US
Organisation:	Let's Encrypt
Common Name:	R3
Serial Number:	04 3B D0 02 47 E7 36 6F B3 DF D2 1F 90 5B E5 B0 AF 1F
Version:	3
Signature Algorithm:	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters:	None
Not Valid Before:	
Not Valid After:	
Public Key Info	
Algorithm:	RSA Encryption (1.2.840.113549.1.1.1)
Parameters:	None
Public Key:	256 bytes : CB CF 2F 80 FA EF E9 0C E6 F9 48 45 F9 11 55 8C 8C 25 60 7D 7A 6F E8 6A C3 03 A7 DD 97 5E 32 C7 61 75 38 4F 78 56 8A 2B 0B B4 D3 C4 4A 4B C3 15 E0 3D F9 EF F8 B8 20 72 CC 58 0C D5 E3 24 76 FA C4 40 B1 9E A5 D5 65 14 E6 6D CA A2 C3 80 CE 1B EA 0F D7 CF 10 92 8D 87 AA 8E 17 AC E1 77 DA FD FC AE 4F 41 84 00 4E 66 F8 DC CD 89 A2 AD B6 4B 9A A5 E7 26 9D B2 20 E7 01 DB 06 DB BF 78 D8 2F 48 46 64 59 C4 AD 34 8B 29 CC 8F 25 8E 38 CC C7 9A 78 A4 94 4E 57 06 00 8B A5 BC 4D 8B C8 48 FF C9 13 41 2A 82 B0 30 46 5E F1 8B CA 9A 33 E2 F1 5E FE EB 5E 73 CA 68 24 8C 37 C5 03 B0 24 82 A6 31 70 2D 27 E2 5F 51 1D 08 7C 45 C4 E2 8E 11 5E 6D 0A DB BA C9 B4 32 6B 8F 69 54 42 3F 94 C4 7F 33 2C F5 84 D7 AB 9E 0D 09 2E C1 FA 77 E2 E2 DC F4 04 1D 15 8F 17 CE 2C 44 13 07 3F EB 02 11 3B
Exponent:	65537
Key Size:	2.048 bits
Key Usage:	Encrypt, Verify, Wrap, Derive
Signature:	256 bytes : 88 03 08 66 BB 64 42 46 EC 6E 1E E9 03 E5 04 BC 28 70 00 C8 34 CB DC 39 06 97 BB A8 D7 93 F8 25 DF 3D 36 7A 05 F5 66 D9 08 9F 71 91 61 B2 DC 08 F3 F3 AC 5A 7E 1F A1 C9 0C 19 64 CC 96 B7 84 22 9F A3 A7 62 16 C3 EB E2 A6 E9 EB 81 1C 5A E2 ED 67 1F 28 D0 11 F6 02 0D 40 4E 6C 30 EA CD 72 EE E9 CC 69 12 68 C7 AF 6D 30 D2 5B 6F 3D 18 2D 83 87 D7 F4 03 CD 14 41 A5 2B 30 E5 6F 91 DC 40 DD AA 43 9C A6 1D D8 6F 6E E3 C9 80 D7 9D 23 92 B4 90 98 99 BC CA 51 39 6A B2 2D B6 BA D5 F4 FB C3 E3 23 31 EC FA 54 D7 F8 1B 36 32 F0 BC 7C 87 90 E5 35 41 6A 39 A8 EB 8E 69 19 56 E6 EB C5 81 02 E1 BB A1 BA CE 2A F6 69 B6 94 02 90 CF 3C A9 11 96 E7 D5 D8 3B 61 D1 F6 91 DA E6 89 EF 0B 93 24 08 3F CD 55 2A 03 6B 3C 48 8C B1 36 D7 E8 37 4A A6 33 7C 17 24 6D D2 F8 FE A5 FB 15 79 E2 EF C3
Extension:	Key Usage (2.5.29.15)
Critical:	YES
Usage:	Digital Signature, Key Encipherment

Extension:	Basic Constraints (2.5.29.19)
Critical:	YES
Certificate Authority:	NO
Extension:	Extended Key Usage (2.5.29.37)
Critical:	NO
Purpose #1:	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2:	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension:	Subject Key Identifier (2.5.29.14)
Critical:	NO
Key ID:	DD A0 66 49 5C 68 71 AF 16 99 2D 3B 41 10 FB 0D F6 32 94 22
Extension:	Authority Key Identifier (2.5.29.35)
Critical:	NO
Key ID:	14 2E B3 17 B7 58 56 CB AE 50 09 40 E6 1F AF 9D 8B 14 C2 C6
Extension:	Subject Alternative Name (2.5.29.17)
Critical:	NO
DNS Name:	bitkom.com
DNS Name:	bitkom.de
DNS Name:	bitkom.eu
DNS Name:	bitkom.net
DNS Name:	bitkom.org
DNS Name:	digitalestadt.org
DNS Name:	digitalwahl.de
DNS Name:	live.bitkom.org
DNS Name:	live.digitalestadt.org
DNS Name:	live.digitalwahl.de
DNS Name:	onboarding.bitkom.org
DNS Name:	www.bitkom.com
DNS Name:	www.bitkom.de
DNS Name:	www.bitkom.eu
DNS Name:	www.bitkom.net
DNS Name:	www.bitkom.org
DNS Name:	www.digitalestadt.org
DNS Name:	www.digitalwahl.de
Extension:	Certificate Policies (2.5.29.32)
Critical:	NO
Policy ID#1:	(2.23.140.1.2.1)
Policy ID#1:	(1.3.6.1.4.1.44947.1.1.1)
Qualifier ID #1:	Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URL:	http://cps.letsencrypt.org
Extension:	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical:	NO
SCT Version:	1
Log Operator:	Let's Encrypt
Log Key ID:	B7 3E FB 24 DF 9C 4D BA 75 F2 39 C5 BA 58 F4 6C 5D FC 42 CF 7A 9F 35 C4 9E 1D 09 81 25 ED B4 99
Timestamp:	Wednesday, 12. October 2022 at 22:28:50 Central European Summer Time
Signature Algorithm:	SHA-256 ECDSA
Signature:	70 bytes : 30 44 02 20 3A 3B DE 10 84 95 47 E3 0A 32 5A 4E 71 F7 ED 39 98 C6 01 45 45 92 BA A1 44 D6 12 55 CE 16 FD 66 02 20 01 B7 05 8B CF B9 1B 55 9F 3A 65 92 E8 E0 B8 22 BC C5 FC 90 14 74 27 B4 CF 09 4B B4 0C 1B 4B C0

SCT Version:	1
Log Operator:	Cloudflare
Log Key ID:	7A 32 8C 54 D8 B7 2D B6 20 EA 38 E0 52 1E E9 84 16 70 32 13 85 4D 3B D2 2B C1 3A 57 A3 52 EB 52
Timestamp:	Wednesday, 12. October 2022 at 22:28:50 Central European Summer Time
Signature Algorithm:	SHA-256 ECDSA
Signature:	70 bytes : 30 44 02 20 25 26 D4 01 27 9E C4 4B 51 3D CB 45 CB A8 87 DE 0C 45 2A C4 E6 C9 E9 D9 4C 77 9C 4D A0 61 AC 71 02 20 2A 85 8D 0A E9 57 CF 48 D6 E5 C7 75 97 C8 23 80 DD 1B F1 2D 6B 6E 32 13 64 FD 55 33 A7 6E 04 17
Extension:	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical:	NO
Method #1:	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URL:	http://r3.o.lencr.org
Method #2:	CA Issuers (1.3.6.1.5.5.7.48.2)
URL:	http://r3.i.lencr.org/
Fingerprints:	
SHA-256:	BD E8 1D D3 B9 35 40 C7 4D 69 C8 E6 B3 97 1A C4 E9 38 78 DE 6A 8F 0A 68 48 B1 63 06 78 7F 04 C5
SHA-1:	F2 EB 56 84 70 FD 2E AF BC 26 FD 52 DE 67 FE C5 C7 07 FD 9D





This paper is dedicated to **Richard Morton**, who co-chaired the Trusted Technology Environments (TTE) working group, which has produced this paper.

Richard, the Secretary-General of the International Port Community Systems Association, passed away on September 9, 2022 at the age of 50 after battling illness for many months.

He remained positive and enthusiastic to the end, and his drive undiminished as he continued to support IPCSA members to achieve their ambitions. for IPCSA's and the whole industry's future.

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 130 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

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

DSI is a collaboration between Enterprise Singapore, the Asian Development Bank and ICC, and works closely with the World Trade Organization and the World Customs Organization. Together, these five institutions form the Governance Board for the DSI.

BCG is a global management consulting firm and the world's leading advisor on business strategy. BCG partners with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. BCG's expertise in the financial institutions sector spans all major topic areas to give global, regional, and local banks detailed insight, knowledge, and analysis across markets. Trade finance is an established and growing topic area for BCG's wholesale and transaction banking practices. BCG has worked on more than 40 recent trade finance-related projects globally on industry questions and challenges such as market entry and growth, pricing, cost reduction, operations, and digital change and transformation. In addition, BCG's Global Trade Model, which analyses and forecasts global trade flows and trade finance revenues, is in its seventh year, and now includes services trade as well as goods trade.

Beyond its work with ICC, BCG continues to actively support the trade finance community with thought leadership, including recent and a pipeline of future publications covering topics such as the digital, regulation, geopolitics, and increasingly importantly sustainability in trade.

BCG was founded in 1963. It is a private company with more than 90 offices in 50 countries. For more information, please visit www.bcg.com.


ICC
Digital
Standards
Initiative