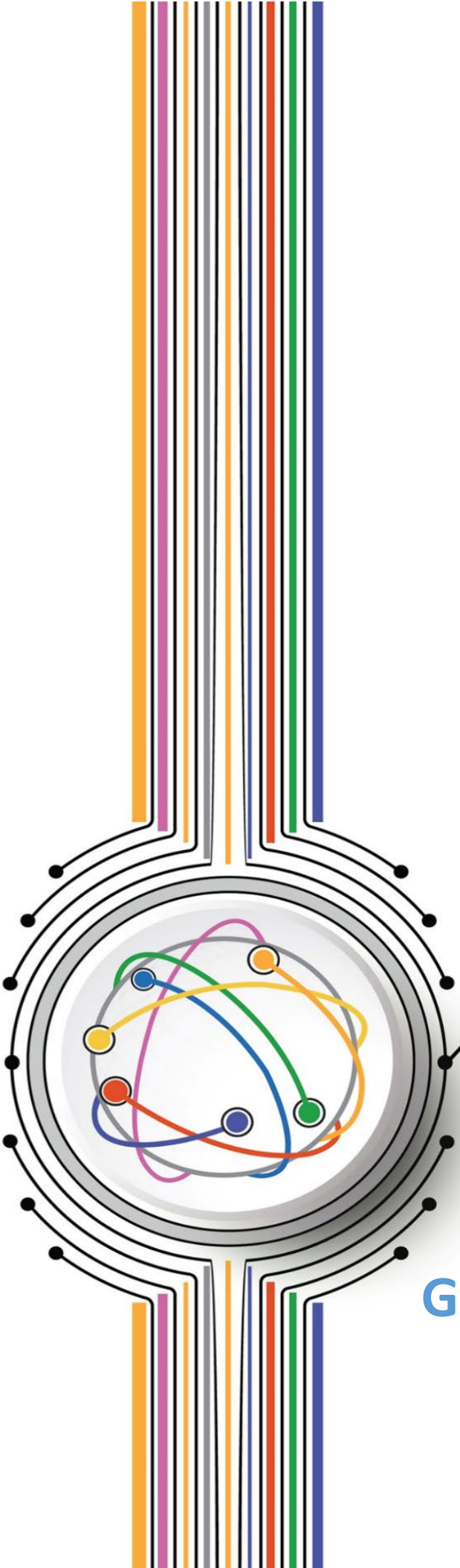


UNECE

White Paper

Globally Unique Identifiers in Supply Chains

April 2025

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Achnowledgement

The UNECE Trade Facilitation Section and UN/CEFACT would like to express their gratitude to the experts who contributed to the development of this paper.

We extend our appreciation to Clare Rowley (project leader), Eduardo Leite (Regional Rapporteur), Hans J. Huber, Henri Barthel, Ian Watt, Jaco Voorspuij, Jacobo Iribarnegaray, Kevin Shakespeare, Nuria Vegas, and Virginia Cram for their valuable input.

We also acknowledge the contributions of Hanane Becha (Vice Chair), Lois Tullo, Miriam Goldby, Stephan Wolf, Steve Capell (Vice Chair), and Tej Contractor as key contributors to this work.

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)

Simple, Transparent and Effective Processes for Global Commerce

UN/CEFACT's mission is to improve the ability of business, trade and administrative organizations, from developed, developing and transitional economies, to exchange products and relevant services effectively. Its principal focus is on facilitating national and international transactions, through the simplification and harmonization of processes, procedures and information flows, and so contribute to the growth of global commerce.

Participation in UN/CEFACT is open to experts from United Nations Member States, Intergovernmental Organizations and Non-Governmental Organizations recognised by the United Nations Economic and Social Council (ECOSOC). Through this participation of government and business representatives from around the world, UN/CEFACT has developed a range of trade facilitation and e-business standards, recommendations and tools that are approved within a broad intergovernmental process and implemented globally.

www.unece.org/cefact

TABLE OF CONTENTS

1 Overview and Key Insights: Globally Unique Identifiers in Supply Chains. Discoverable, Resolvable, Verifiable

"Moving from paper chaos to digital clarity"

1.1 The Supply Chain Information Layer is Outdated

The challenge: Pushing information downstream and excessive reliance on paper as the only interoperable protocol for data exchange in supply chains	 Image by Ag Ku from Pixabay

1.1.1 The Challenge:

Pushing information downstream and excessive reliance on paper as the only interoperable protocol for data exchange in supply chains.

Data Pull as the solution:

Despite ever-advancing technologies that facilitate electronic data exchange, most trade data is still conveyed through paper[1] (i.e., PDF). For trade and transportation stakeholders — traders, transporters, and service providers— the goal of trade digitization should be to eliminate paper use[2] entirely and exchange trade data in structured, digital formats. This approach would enable transacting partners and consumers to access specific data on demand by using unique identifiers to pull only the information they need.

If subjects (who trades or transports, who helps with trading or transport?) and objects (what is being traded/transported, what helps with trading or transportation?) had discoverable identifiers, a trade and transport ecosystem could emerge where transacting partners and consumers could pull data on demand, as needed. In other words, downstream participants could use identifiers to request information and only receive the information that they need.

Achieving this pull-based information system requires identifiers with three key characteristics: Discoverability, Resolvability, and Verifiability (D-R-V).

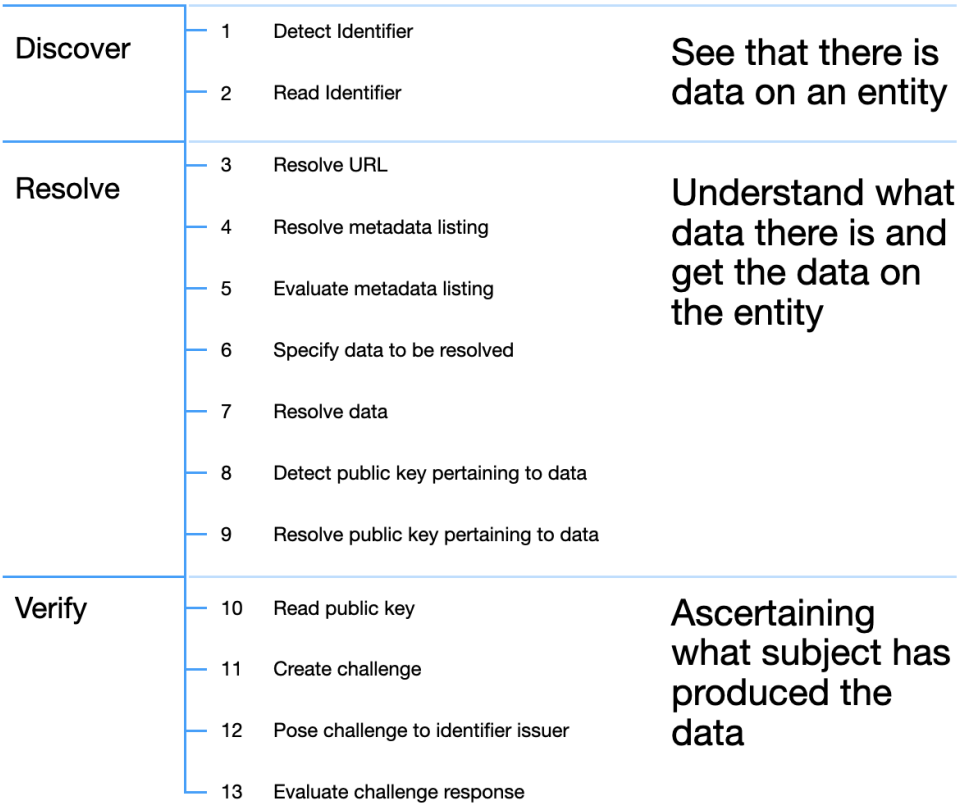
- Discoverability is the extent to which the source of an identifier can be easily detected. Discovery of an identifier is the first step and a prerequisite to resolvability.
- Resolvability is obtaining reference data associated with the identifier.
- Verifiability is a demonstration of the authenticity of the identifier and associated reference data. Verifiability of an identifier provides confidence (or even certainty) about the entity that controls the identifier. Controlling an identifier means to have the authority to determine and possibly edit the data behind it.

If the identities of those who provide identifiers and linked data are verifiable – then so are the identities of those who provide false data. See section 2.1 and Appendix 1 for further details on D-R-V.

[1] According to the Cross-border Paperless Trade Toolkit co-published by World Trade Organization (WTO), in collaboration with the United Nations Economic and Social Commission, cross-border paperless trade measures had a global implementation rate of only 34 percent in 2017. Available: https://www.wto.org/english/.

[2] See "Trust in Trade" report by ICC DSI, section 7, for an explanation of paper substitutes and their effects. Available: https://www.dsi.iccwbo.org/_files/ugd/8e49a6_5a75a77950d7474da772bf9cfc2d985b.pdf.

Figure 1: Defining Discoverability, Resolvability and Verifiability



Identifiers serve as signposts to enable a party or object to learn more about the identified entity. The discoverability of identifiers, and the ability to find and verify the authenticity of the associated reference data[3] are prerequisites for moving ecosystems of trade and transport from push to pull information retrieval for trading partners and consumers.

The data-pull flow-model (see Figure 2) opens a wide range of opportunities for the business community, governments and all supply chain actors having with legitimate interests in trade data. Its simplicity makes it easier, more transparent (e.g. counter greenwashing) and suitable for a real time economy. The use of verifiable identifiers using this model can be an effective tool against fraud. Additionally, it enhances financial inclusion[4] for SMEs and MSMEs by streamlining identity verification and onboarding processes. This model further supports integration with global markets, such as compliance in areas like Environmental, Social and Governance (ESG)

[3] See "Trust in Trade" report by ICC DSI, section 11, for an explanation of public key infrastructure, decentralized public key infrastructure and zero trust. Available: https://www.dsi.iccwbo.org/_files/ugd/8e49a6_5a75a77950d7474da772bf9cfc2d985b.pdf

[4] As an example, please refer to "More Transparency for Better Business – the Potential of Legal Entity Identifiers for African Economies," authored by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ): giz2020-0293en-transparency-legal-entity-identifiers-africa.pdf

reporting[5], which involves disclosing a company's performance on these critical factors. ESG reporting often involves integrating data from different sources, sectors and jurisdictions. Having D-R-V identifiers will help supply chain actors assess and report the sustainability and ethical impact of their activities, foster accountability, and encourage businesses to adopt responsible practices that can lead to long-term value creation.

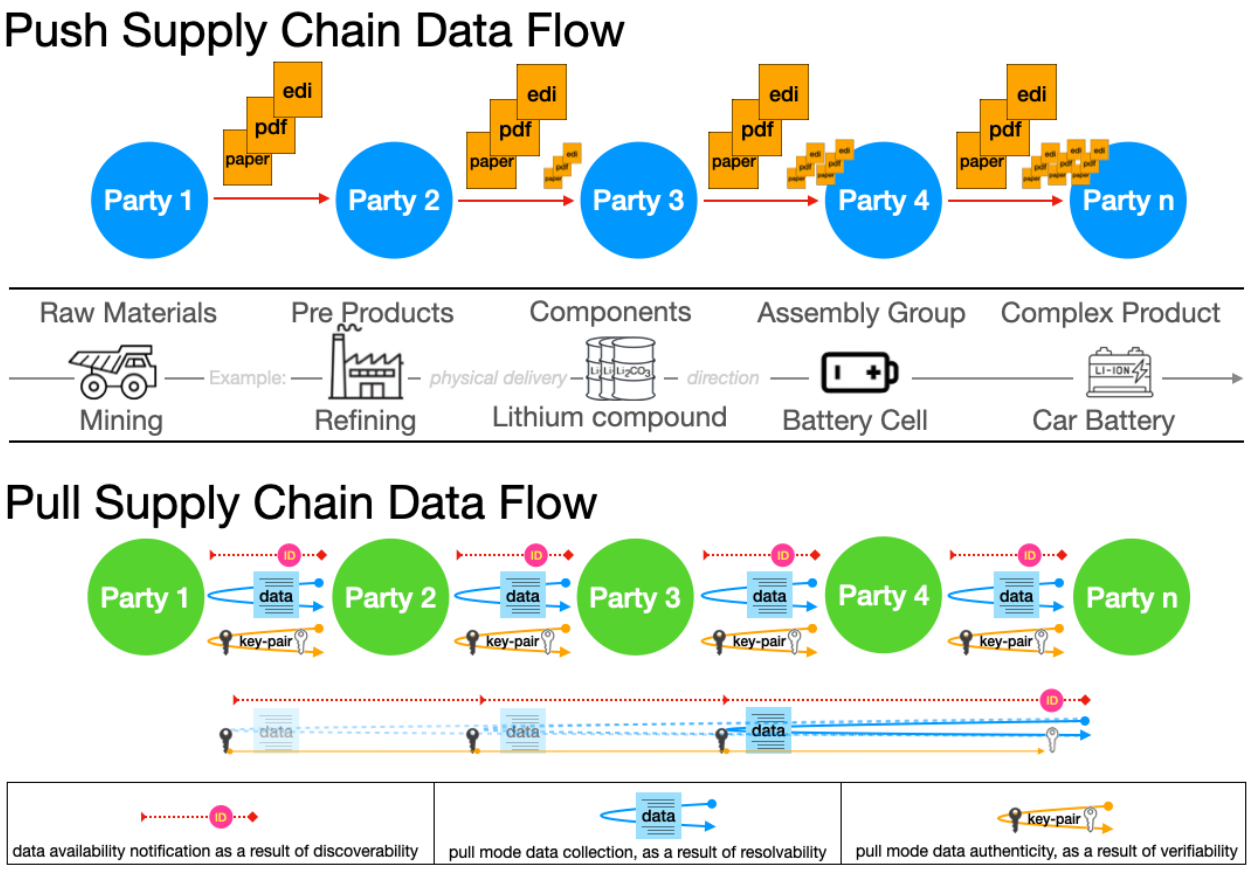
Pull-based approach for data within customs and other operators could support the Information Security Policies of many organizations involved in such operations. Key among these are the "Need-to-know[6]" principle, which ensures individuals have access only to essential information for a limited period, based on the level of information sensitivity (e.g., restricted or secret data), and the "Minimum Privilege" principle, which minimizes permissions to the lowest necessary level to mitigate risks from potential system vulnerabilities. Specifically, by implementing role-based access, encryption, and permission layers within the pull-based system, it is possible to enforce strict compliance with principles like "Need-to-know" and "Minimum Privilege," minimizing access and exposure risks while allowing authorized data retrieval when necessary. For instance, the pull system could leverage Verifiable Credentials and Verifiable Identifiers to ensure that only authenticated and authorized users can access certain data as it will be later explained in this paper.

This shift to a digital ecosystem would streamline processes, reduce errors, and foster a more responsive trade and transport network.

[5] For further reading please check the White Paper on Project Savannah: Common ESG Metrics for Generating Digital Sustainability Credentials for MSMEs authored by United Nations Development Programme (UNDP), Monetary Authority of Singapore (MAS) and GLEIF: https://www.undp.org/sites/g/files/zskgke326/files/2024-03/white_paper_on_project_savannah.pdf

[6] The principles of "Need-to-know" and "Minimum Privilege" are foundational components of ISO/IEC 27001, which is the international standard for information security management systems (ISMS) : https://www.iso.org/standard/27001.

Figure 2: Push vs pull data flow in the supply chain



1.2 Supply Chain Entity Types: The Who and What

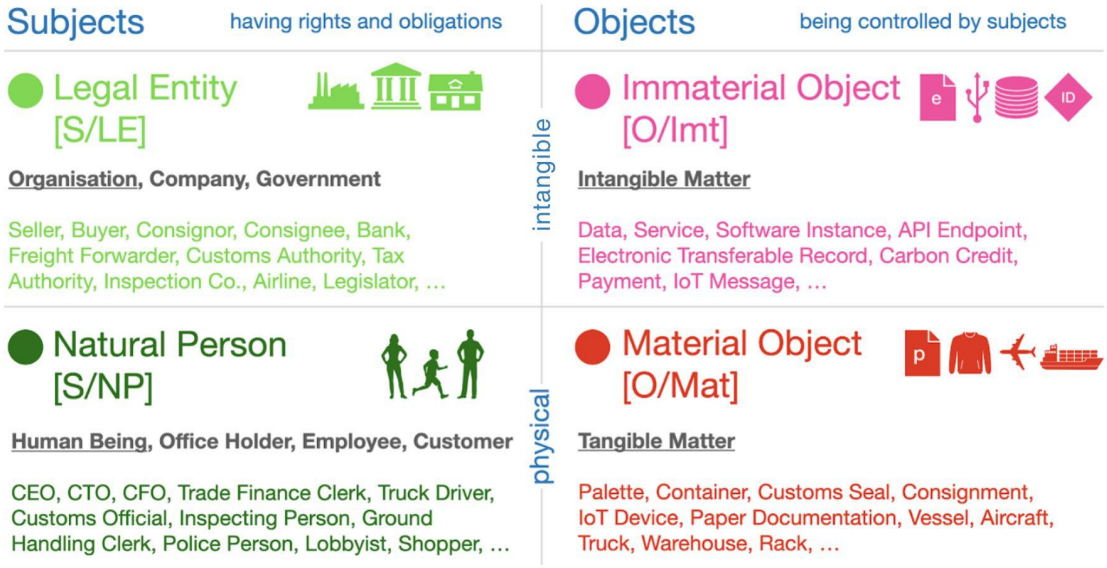
1.2.1 Supply Chain Entities

Supply chain events involve both subjects and objects, each of which can have either physical or intangible subtypes. Figure 3 provides a graphical overview of the resulting four categories of supply chain entities. Regardless of whether the entity is physical or intangible, all entities require unique identification in data exchanges. This is the purpose of identifiers.

Subjects answer the questions: “Who is trading or transporting?” and “who helps us in those transactions?” Subjects can be either a Natural Person (S/NP) or a Legal Entity (S/LE). In commercial terms subjects are referred to as parties. Subjects can bear rights and obligations. Subjects can own objects.

Objects answer the questions: “What is the transaction about?” and “What is helping us to execute the transaction?” Objects may be Material Objects (O/Mat) and Immaterial Objects (O/Imt). Objects cannot bear rights and obligations. Objects cannot own subjects or other objects.

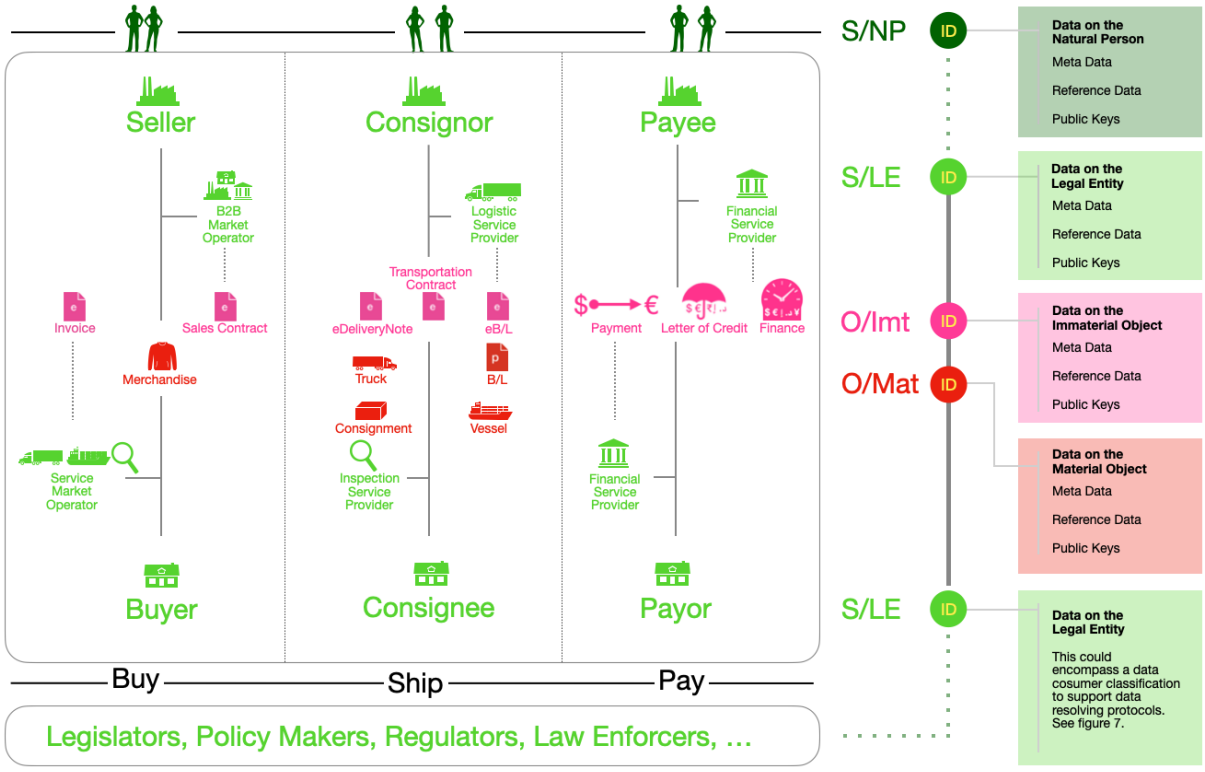
Figure 3: Demonstration of supply chain entities – intangible and physical



1.2.2 Relationships Between Supply Chain Entities

Trade is nearly always initiated between two subjects – a seller and a buyer. In most cases, the relationships between the two subjects are about an object (see Figure 4). Hence, a very common graph particle is Subject-Object-Subject. The relationship between subjects – seller, buyer, customs authority, tax authority, etc. is also an important topic in legal instruments. Legal instruments define the parameters of legally recognized digital identity and therefore the digital exchange of identity credentials describing the subjects in trade. Appendix 2 provides a review of legal texts which describe digital identity in trade and the challenges and considerations for advancing a global digital identity standard for legal persons and their authorized representatives.

Figure 4: Examples of relationships



1.3 Information Pull Supply Chain

It would be a big step towards the dematerialization of trade documentation and a great facilitation of trade data exchanges, if:

- All entities, the subjects and objects, have unique identifiers.
- Identifiers are easy to find (discoverability) in any supportable interaction.
- The associated reference data can be accessed and retrieved easily by authorized parties (resolvability), and,
- The data provenance can be confirmed (verifiability) and data hereby became reliably authentic.

As described in section 2.2, issuers of identifiers may choose to implement the above principles or link to identifiers that are D-R-V.

1.4 Using identifiers as signposts for finding data

Instead of retrieving data from Transport Management Systems (TMS) or similar platforms to put them on paper, into a PDF, or into an EDI data transmission, a party can create and share only an identifier.

The "*Cross-Border Paperless Trade Database, Key Trade Documents and Data Elements*[7]" compiles the trade data elements used in 36 key trade documents. This toolkit helps us to imagine what future structured data exchange could look like.

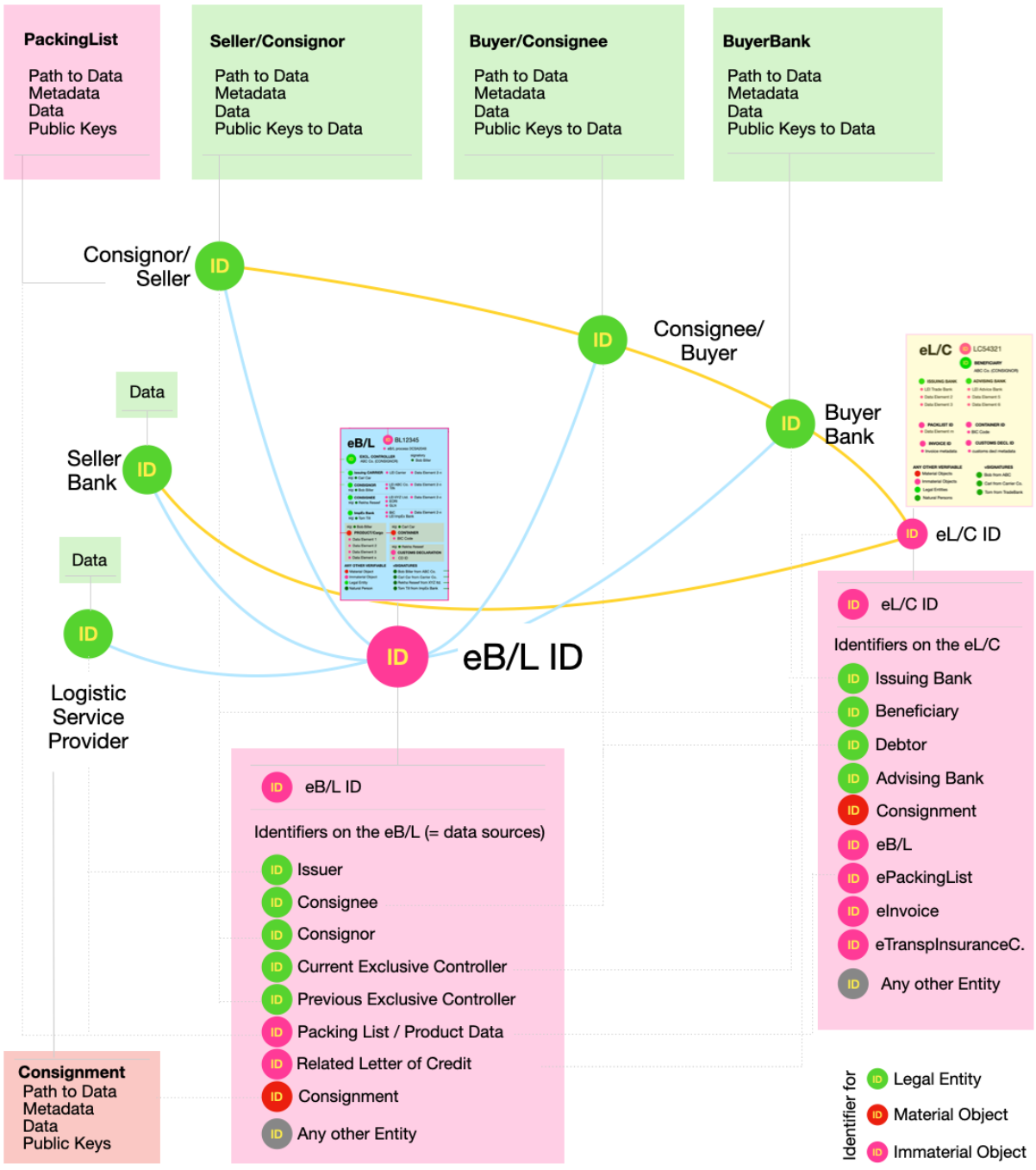
Imagine data exchanges using chains of identifiers referencing key trade documents. These identifiers would be resolved to their associated data elements, for authorized parties. The identifier may be verifiable[8] meaning the party controlling the identifier can be determined (beyond doubt), which makes the data resolved from the identifier authentic.
For example, a bill of lading would consist of only the identifier for the Transport Contract Document / Bill of Lading (see Figure 5 below). This identifier would then reveal further details to authorized parties on the terms of the bill of lading such as issue date, estimated time of departure, etc. It would also reveal other identifiers like the Sales Contract identifier. Authorized parties could then access the Sales Contract concluded between the Buyer and Seller and the associated data. It would also reveal other identifiers like the Freight Forwarder identifier or and the Carrier (transport services provider) identifier. Authorized parties could then find the further details on the identified parties and the cargo by resolving linked data.

Appendix 3 provides a use case example of an import case of apparel into the European Union and the UK. This use case example shows the automation potential of customs proceedings in pull mode.

[7] The Key Trade Documents and Data Elements (also called the KTDDE) initiative (https://www.digitalizetrade.org/ktdde) produced a report that encompasses the efforts of international trade experts and the International Chamber of Commerce Digital Standards Initiative in defining 36 key trade documents which are vital to the health of the international trade ecosystem
Source: https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf

[8] i.e. the identifier may be linked to data that verifies its correctness. For example, it may be linked to an electronic signature or electronically signed certificate from a trust service provider

Figure 5: Chaining data via identifiers - example for a Bill of Lading



1.5 Recommendations

This paper demonstrates how identifiers are a foundational building block for a digital supply chain where data can be pulled by authorized trade participants. However, few identifiers currently issued to supply chain subjects and objects fulfill the criteria of being D-R-V. As a result, the recommendations presented here are for issuers of identifiers as well as identifiers' users.

Issuers include but are not limited to organizations such as commercial registries, customs authorities, tax authorities, security authorities, transportation safety regulators, sectoral associations and certification authorities. Users include potentially any organisation or natural person.

1) **Understand D-R-V for identifiers:** Issuers of identifiers should take note of the characteristics of discoverability, resolvability and verifiability and conduct a self-assessment to determine if the identifiers they issue meet these criteria.

2) **Take action towards D-R-V:** When an identifier does not meet these criteria, issuers of identifiers should consider (a) the ability to adjust issuance processes to achieve these criteria, or (b) binding the issued identifier to globally unambiguous identifiers[9] that meet these criteria.

3) **Cross Referencing or binding identifier schemes:** Cross referencing or binding locally prevalent identifiers with globally prevalent identifiers, especially for subject identifiers, extends the reach of locally and regionally used identifiers and can greatly facilitate interoperable data exchange in supply chains (see Appendix 3 for example trade use case).

4) **Unify tagging:** Issuers of identifiers should strive to align globally on how to name tags in structured data files, which is important for interoperability. The alignment should extend into unifying the process of resolving data. In the interest of verifiability, or data authenticity, and the therefore required identifiers for legal entities, the activity seems urgent especially for subject identifiers. The KTDDE Working Group within the Industry Advisory Board of the Digital Standards Initiative (DSI) of the International Chamber of Commerce (ICC) was established with a similar mission: to streamline key trade document standards and align industry practices in trade digitalization. This forum provides a critical platform for issuers of identifiers to engage in these efforts[10].

5) **Communicate:** Issuers of identifiers should create a roadmap for achieving these criteria for their identifiers and share this roadmap with their stakeholders.

[9] A globally unambiguous identifier is an identifier that is globally recognized and refers to a single unique data object (based on ISO 23950:1998); identifiers may be registered, but don't have to be. Global unambiguity (uniqueness) is a prerequisite for resolvability of the identifier

[10] For further details: https://www.digitalizetrade.org/ktdde#msdynttrid=t-AwnolQqdJHbGvaBHpHJZbHDR4iC4QvwvELPYOOClE

Additionally, the legal instruments for digital identity dictate the acceptable[11] digital identity standards for global trade. As such a recommendation is presented for governments, especially their customs and security authorities:

6) **International alignment of frameworks**: The concepts of Neutrality, Reliability, and Interoperability that underlie international frameworks like those noted in Appendix 2 must be supported by identifiers that are discoverable, resolvable, and verifiable.

1.6 Conclusion

The journey towards a paperless society requires a deeper understanding of the challenges and opportunities in modernizing supply chains. We propose a gradual migration towards structured data exchanges based on "Pull" rather than "Push" models that support increasingly higher levels of verification, facilitated by identifiers that serve as signposts to relevant information.

Discoverability, resolvability, and verifiability are crucial properties of identifiers to support this model. By leveraging identifiers effectively and embracing structured data exchange, we can enhance interoperability and pave the way for a more efficient, transparent, and inclusive trade ecosystem to drive economic growth and development, in support of the UN Sustainable Development Goals (SDGs).

2 In-depth Analysis

2.1 Discoverability, Resolvability, Verifiability (D-R-V)

This section outlines the key principles of Discoverability, Resolvability, and Verifiability (D-R-V)—essential properties for structured data exchanges in a paperless trade ecosystem.

2.1.1 Discoverability

Discoverability is the ability to detect an identifier. It is the first step towards obtaining the data linked to it, also referred to as resolvability. The identifier takes the role of a signpost to the reference data associated with the identifier. During discovery the identifier is technically found and read. Supporting software can then resolve the identifier to its additional reference data.

[11] Most recent examples include United Kingdom Electronic Trade Documents Act (ETDA). The UNCITRAL Model Law on Electronic Records (MLETR) adoption can be followed at the MLETR Tracker: https://www.digitalizetrade.org/MLETR

Examples

[O/Mat] A GTIN Barcode can be read by a barcode scanner at the checkout point of a super-market to resolve the product name and the product's current price.

[O/Imt] A port community system receives the identifier of a master bill of lading of a container with several Less-than-truckload (LTL) consignments. The master bill of lading identifier resolves to the identifiers of the respective house bill of ladings. The system requests a list of the current exclusive controllers of all house B/Ls, which could consist of only identifiers of legal entities [S/LE].

[S/LE] A software system of a bank is parsing through pain.001 payment files in XML format, finds LEI tags for the beneficiary and creates a list of payments made to a certain legal entity (beneficiary). The list could contain only identifiers of payment files [O/Imt]

[S/NP] An employee access card is swiped via a reader to ascertain access rights to enter a building.

Data carrier assisted discoverability

An identifier is represented by a data carrier which is designed to be read as easily as possible. The data carrier can be normal numbers and letters in an OCR assisted discovery process, for example as it is used for the BIC code on containers. It can also be a barcode which includes the GTINs like those found on products in supermarkets. A QR-code is another example of a data carrier. When scanned a QR-code often returns a URL. Further, there are radio assisted data carriers like RFID-tags and NFC-transponders. IoT devices must be discovered by collectors to enable resolvability (where authorized) to the associated data flows.

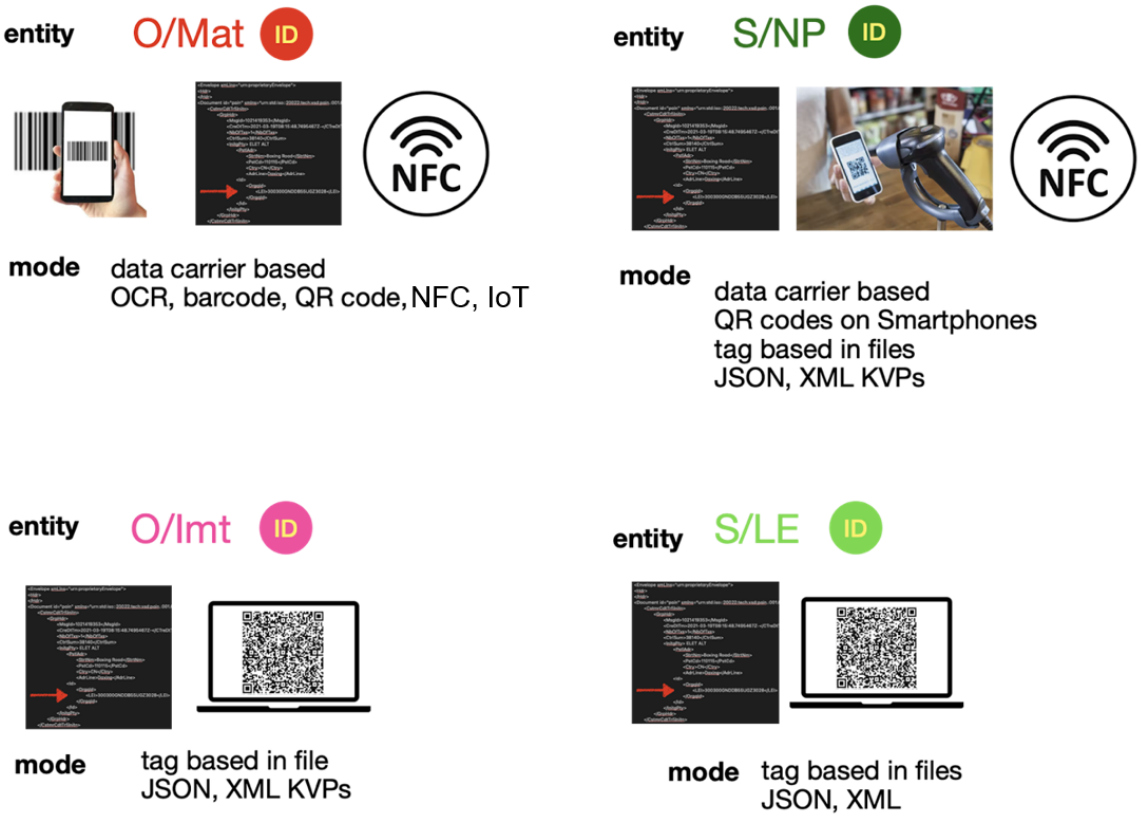
Tag based discoverability

An identifier can also be part of structured data file like XML or JSON and can then be discovered as the key of a key-value pair. A key containing the name of an identifier is then called a tag. A software instance reading ("parsing") the structured data then needs to discover these keys and extract the corresponding value, which is the identifier.

Discoverability differences for entities

All four entity types can be discovered via tag-based solutions or data-carrier-based solutions. The difference lies in the requirements of the service interaction to be supported.

Figure 6: Example ways to discover identifiers



2.1.2 Resolvability

Given an identifier can be discovered, the next question is accessing the reference data associated with the identifier. Resolvability is the ability for authorized parties to obtain the data linked to an identifier (see Figure 7).

Path to the data

A structured URL indicates a location of the data linked to the identifier. This URL often allows a requestor to resolve a metadata listing of the data.

Authentication and access privileges

Authentication may be required to determine which data is available to the data requestor. The authentication could be made dependent on the role the data requestor assumes in the trade.

Metadata

A metadata listing is like the menu in a restaurant, which one can choose from. The listing will inform the data requestor (i.e. an API which enquires) about the data available and maybe also

about properties of the data, i.e. the last update time. The metadata listing may depend on who is the data requestor, so a prior authentication may be taking place.

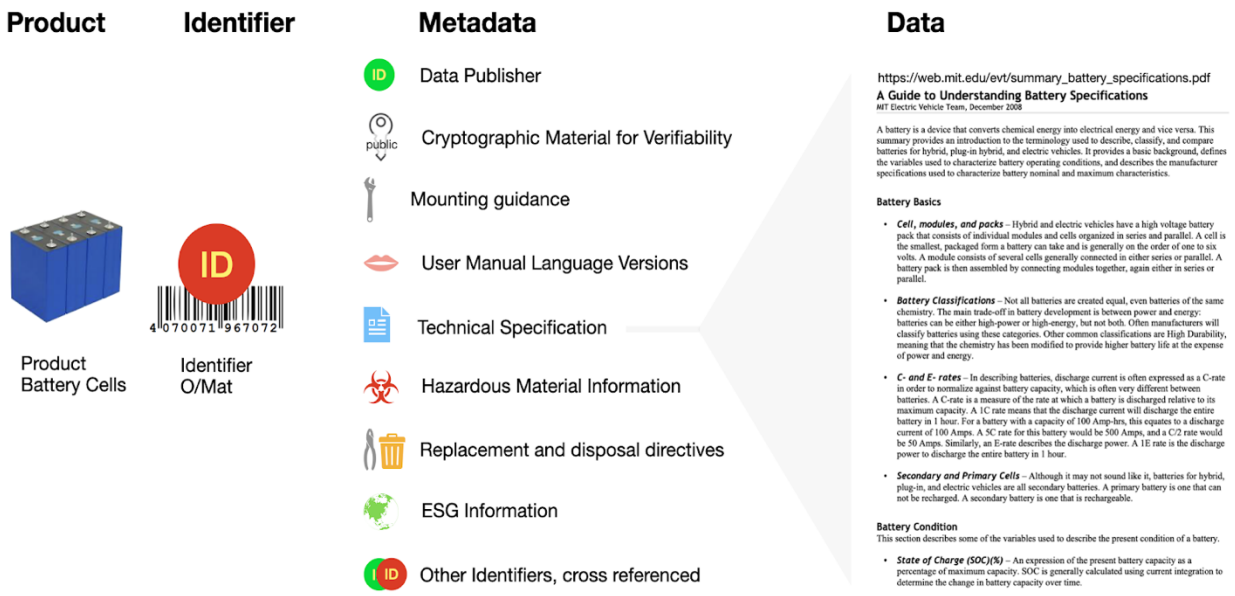
The actual data

Data can now be resolved by modifying the structured URL in a way to request certain items from the list of metadata. Data can be delivered as actual values or another identifier for which another resolving process would need to start.

Public key

One or more public keys can be resolved. Public keys can be for an entire data set or each individual data element. A public key is being used to challenge the originator of the data. The challenge can only be mastered using the corresponding private key, which the exclusive controller of the identifier has. This makes data authentic. Note that this requires a subject identifier as well, to identify the "Who".

Figure 7: Identifiers may provide access to wide ranges of data



2.1.3 Verifiability

Verifiability is the ability to determine the true identity of the controller of an identifier and therefore the authenticity of the reference data linked to it.

Authenticity versus veracity

Verifiability always looks at the Who and not at the What. It answers the question of Who controls the identifier and therefore Who has created the data. In more formal terms: Verifiability renders data authentic, but it does not produce data veracity.

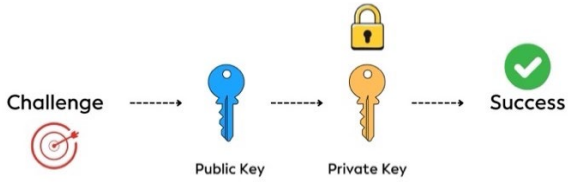
Public and private key

To render data authentic a cryptographic key pair is being used. Private and public key are mathematically entangled. A public key can be sent anywhere, while the private key needs to be kept strictly secret, i.e. in a wallet.

Challenge and Response

A challenge is a mathematical task designed using the public key, which can only be correctly solved when knowing the private key. Hence, only the controller of the identifier (who exclusively knows the private key) can master the challenge (see Figure 8 below).

Figure 8: Demonstration of Challenge and Response



Evaluation

The result of the response to the challenge determines the further processing of whatever process is being supported by verifying. A correct result says: Go ahead! An incorrect result says: Stop here!

2.2 Cross-referencing and Binding: Increasing Utility of Identifiers

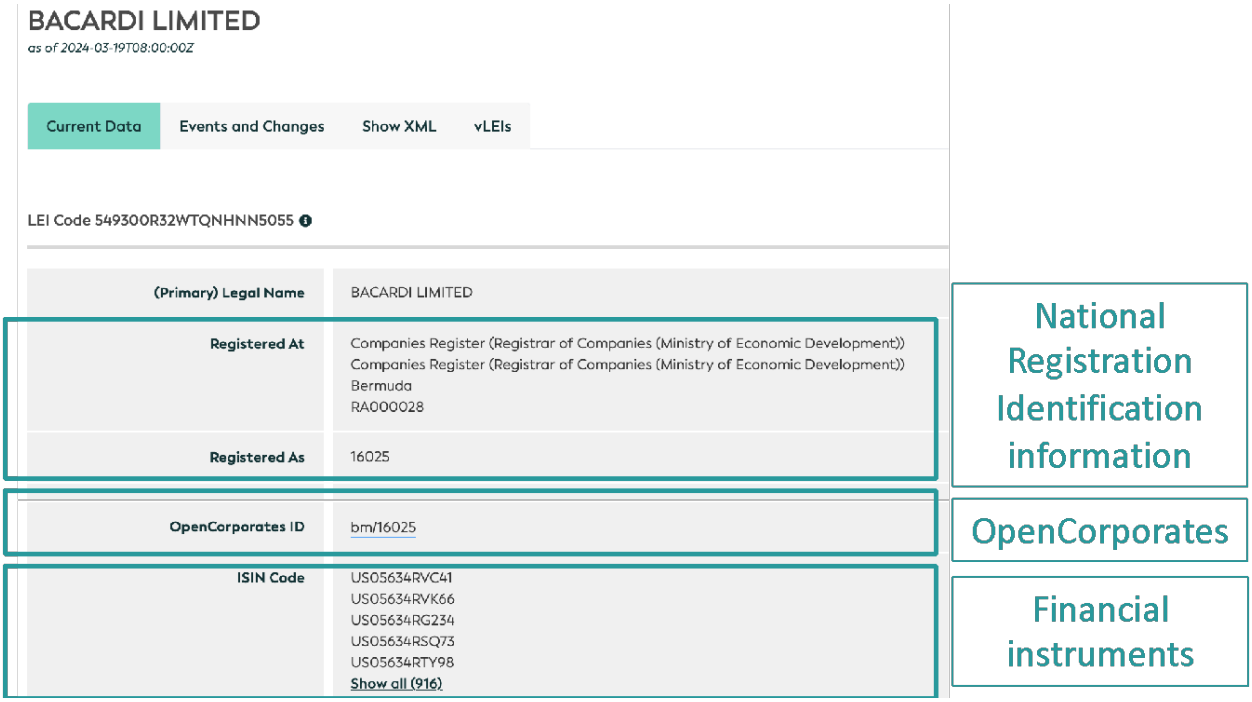
In an ideal world all identifiers should be D-R-V in a globally unique fashion. Given this ideal world is not achievable, issuers of identifiers may choose to link to identifiers that are D-R-V.

Organizational identity

The Global LEI System provides an example of how a system offering a D-R-V identifier can be extended to cross-reference other identification systems (see Figure 9).

Figure 9: Cross-referencing identifiers – Example Bacardi Limited

https://search.gleif.org/#/record/549300R32WTQNHNN5055



Within the LEI reference data there is already a reference to the local registration authority and the local identifier (the <National Registration Identification> block in the figure above).

GLEIF has added additional mappings through a certification of mapping service which certifies that organizations which map the LEI to their own identifiers use state of the art methodologies and / or processes to do so accurately. Organizations that achieve certification are then included in the Global LEI System data model.

The <OpenCorporates> block provides the identifier value and this also serves as the link (https://opencorporates.com/companies/bm/16025) to the OpenCorporates service[12] for more information related to this organization.

Imagine extending the available mappings to include a national Tax-ID, which is currently not resolvable in any standardized manner, to the LEI. Another example is the EORI Number[13]. Given the EORI number were linked to an organization's LEI, the EORI number could be resolved to organizational reference data.

[12] OpenCorporates claims to have approximately 223 million organizations/companies in their database. https://opencorporates.com/

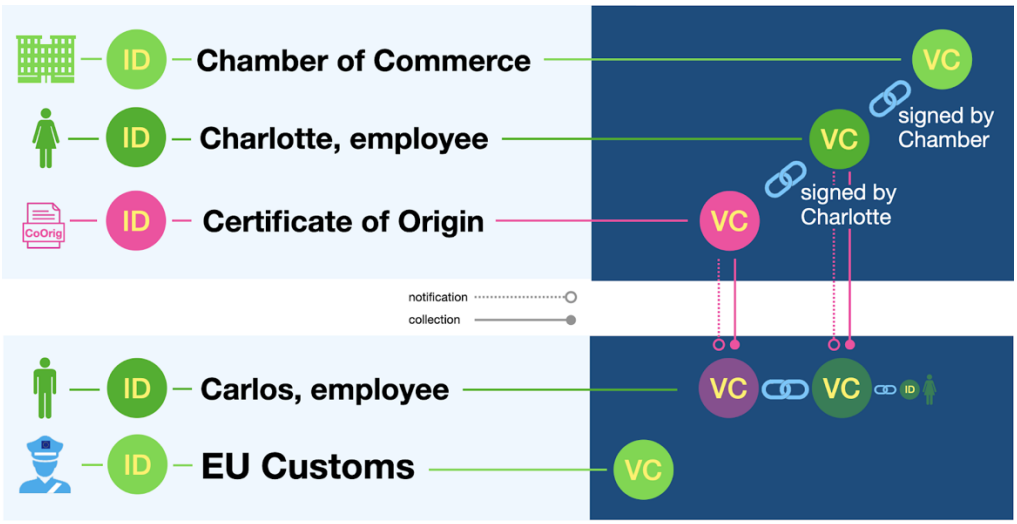
[13] EORI Number: Economic Operators Registration and Identification. An EORI number is mandatory for customs clearance in the customs territory of the European Union

Organizational identity and delegated authority

The verifiable Legal Entity Identifier (vLEI)[14] is a verifiable credential containing identifiers. The identifier can be an LEI, it can be the identifier of an employee, but it could be any other payload. The vLEI is in the format of an Authentic Chained Data Container (ACDC), which has several identifiers in its header and usually there are more identifiers in the payload.

As displayed in Figure 10 a Certificate of Origin is being issued by a local chamber of commerce and signed by the employee Charlotte. The vLEI is a cryptographic binding of Charlotte's natural person's identifier, the identifier for a functional role and the LEI of the employer. By signing the issued Certificate of Origin, the chamber of commerce and employee authorized to act on behalf of the chamber of commerce are now cryptographically bound to the Certificate of Origin. Carlos, who is a clerk with import custom, may request access to the Certificate of Origin using his vLEI credential to prove his is an authorized representative of the Customs Authority. Carlos may confirm the Certificate of Origin was signed by an authorized representative of the Chamber of Commerce and collect the person data (if authorized to do so).

Figure 10: Delegating authority by linking D-R-V identifiers

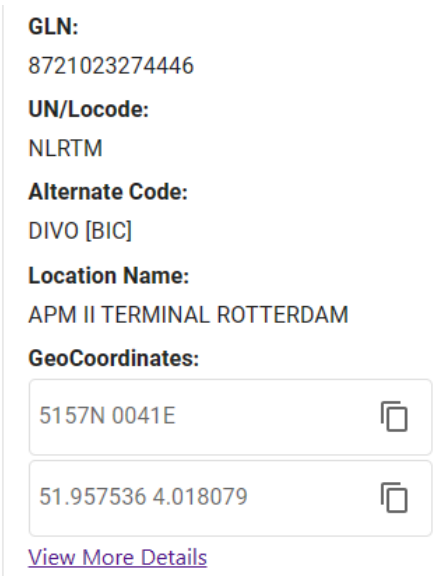


[14] See Introducing the vLEI: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei

Location Identifiers

The GS1 Resolver[15] or other resolver service based on GS1 standards can be used for any of the GS1 ID Keys. Consider the example of the <APM II terminal> location in Port of Rotterdam. Below is a screenshot of the data available via the Global Location Data Resolver.

Figure 11: Binding Location Identifiers



This location records connects three identifiers. The first one mentioned in the figure is the GS1 GLN (Global Location Number). The second, is the UN/Locode. This Locode (NLRTM) identifies the geographical area within which the location is situated. The UN/Locode itself is unique, but it generally covers a significant number of locations. For example, NLRTM covers the Port of Rotterdam, the city of Rotterdam, half a dozen or so suburbs as well as the airport of Rotterdam/The Hague.

The third is the BIC facility code, which is composed of the UN/Locode plus the alternate code shown third from the top in the figure (NLRTMDIVO). The View More Details link (also mentioned above) actually uses that code to access the specific record in the BIC Facility code online service.

There is in principle no limit to the number of different location identifiers that may be linked with one specific location. Consider a specific location such as “APM Terminals Maasvlakte 2”, which is an Ocean Terminal in the Port of Rotterdam, The Netherlands.

There are two widely used codes (identifiers) that are linked to this location.

- NLRTMNLMVII = **SMDG** Terminal Code for APM Terminals Maasvlakte 2[16]
- NLRTMDIVO = **BIC** Facility Code for APM Terminals Maasvlakte 2[17]

For each of those links, it would also be possible to indicate the nature of the link between the location and the associated identifier. However, that goes beyond the scope of this document.

[15] The GS1 Resolver may be used for any of the GS1 ID Keys. https://www.gs1.org/standards/resolver and https://ref.gs1.org/standards/resolver/

[16] https://www.bic-code.org/facility-codes/smdg/NLRTMNLMVII/

[17] https://www.bic-code.org/facility-codes/nlrtmdivo/Or the API / json response

3 Appendices

3.1 Appendix 1: Examples of (D-R-V)

Object/Material: Transport Unit Identifier
GS1 Serial Shipping Container Code (SSCC)

The Serial Shipping Container Code EPC scheme is used to assign a unique identity to a logistics handling unit, such as the aggregate contents of a shipping container or a pallet load. The SSCC is fully compliant with "ISO/IEC 15459 – part 1: unique identifiers for transport units". This is often referred to as the ISO license plate and is a prerequisite for tracking and tracing logistic units in many international supply chains[18].

General Syntax using urn approach:
urn:epc:id:sscc:CompanyPrefix.SerialReference
Example:
urn:epc:id:sscc:9521141.1234567890

Discoverability

In an XML or JSON file the URN may be used to tell a software system reading it to find a transport unit instance identifier, namely a serialized shipping container code, for which the SSCC is "195211412345678900".

While the GS1 system of standards still supports the urn approach (mostly for RFID contexts), GS1 prefers that the URI[19] approach based on URL is used to "tag" identifiers.

Using the URL-based approach, the "tag" in a structured data file for the SSCC would read:
https://example.com/00/195211412345678900.
The GS1 Scan4Transport (S4T) standard, provides a way to pack a significant number of data elements into a 2D barcode such that the individual data elements can all be discovered easily. This S4T standard also builds on this URI approach. A sample barcode is included below (as well as the text string contained in it). You may scan the barcode (with your mobile phone) to check the contents; this example URI does not resolve anywhere (see Resolvability section below also).

[18] Serial Shipping Container Code (SSCC) : https://www.gs1.org/docs/idkeys/GS1_SSCC_Executive_Summary.pdf

[19] URI: Uniform Resource Identifier and URL: Uniform Resource Locator and URN: Uniform Resource Name; the URI identifies a resource in the internet, the URL, being a URI itself, designates the resource's location, a URN, also being a URI, identifies a resource by a name in a particular namespace. The URI has become a foundational standard for IT solutions that make use of the World Wide Web.

https://example.com/00/195212342345678909?4300=Municipality+Meierijstad&4302=Stadhuisplein+1&4304=Veghel&4305=Meierijstad&4306=Noord-Brabant&4307=NL&420=5461+KN+&4309=14161436320055462573&401=9521234ABC12345&402=95212340000000012&s4t	

In effect, the text string is a structured data file (that "lives" also inside the 2D barcode). The text string is compliant with the URI standard. The structure of this set of data consists of two main sections, separated by the question mark character "?". The section before the question mark (highlighted with yellow background) is where the identifier for the object can be found (discovered). In this case the SSCC associated with the transport unit.

The first part of the first section in this structure is called the URI stem; in this example "https://example.com/".

The second part of that first section that runs up to the question mark includes the identifier for the object.

In this example the SSCC (signaled by the "/00/") with a value of "195212342345678909".
GS1 refers to these numerical tags as "Application Identifiers" (aka AI).

Therefore, the discovery is based entirely on global data standards that are well-established also in modern Web-based IT environments.

The section behind the question mark is not relevant for discovery of the identifier, but it offers massive benefits for Supply Chains. This second section is structured according to the GS1 Digital Link standard. The data elements have been included as so-called attribute-value pairs. They always appear as follows: Each attribute is "tagged" with an Application Identifier, followed by an equal sign "=", which is followed by the value associated with that attribute. The attribute-value pairs are separated by the ampersand sign "&".

This standards-based approach using standardized tags at every level within the structured data enables all stakeholders to easily and correctly interpret all the data elements included within the structured data (including any identifiers that are in the structured data).

The structured data above includes two additional identifiers in the attribute-value pairs: 9521234ABC12345 (Global Identification Number for Consignments) and 95212340000000012 (Global Shipment Identification Number).

Resolvability

The access to data related to a logistic unit identified with an SSCC is generally restricted to the parties directly involved in the trade and transport of these items. The information related to the nature and the movements of logistics units is sensitive from a business perspective. Resolution services are however widely implemented by various parties. The GS1 EPC Information Services (EPCIS), also known as ISO/IEC 19987, enables disparate applications to create and share visibility event data, both within and across enterprises. Ultimately, this sharing is aimed at enabling users to gain a shared view of physical or digital objects within a relevant business context.

Verifiability

The shipper may be the supplier or a logistic service provider (LSP) acting on behalf of the supplier[20]. Stakeholders can verify the issuer of the SSCC (and any other GS1 ID Key). The "Verified by GS1" online service[21] allows anyone to enter any GS1 ID Key.

The service validates the format and the identity of the licensee (issuer)[22].

Object/Immaterial: FIATA eBill of Lading (eFBL)

FIATA is a global Freight Forwarders association that has successfully implemented what they call the "electronic FIATA Bill of Lading" (eFBL). It consists of an ecosystem of dozen/s of software providers and an ever-increasing number of freight forwarders and their clients.
The eFBL standard is available as open source for all and it is aligned with the UN/CEFACT semantic, which facilitates interoperability across all stakeholders involved.

[20] GS1 Logistic Label Guideline : https://www.gs1.org/docs/tl/GS1_Logistic_Label_Guideline.pdf

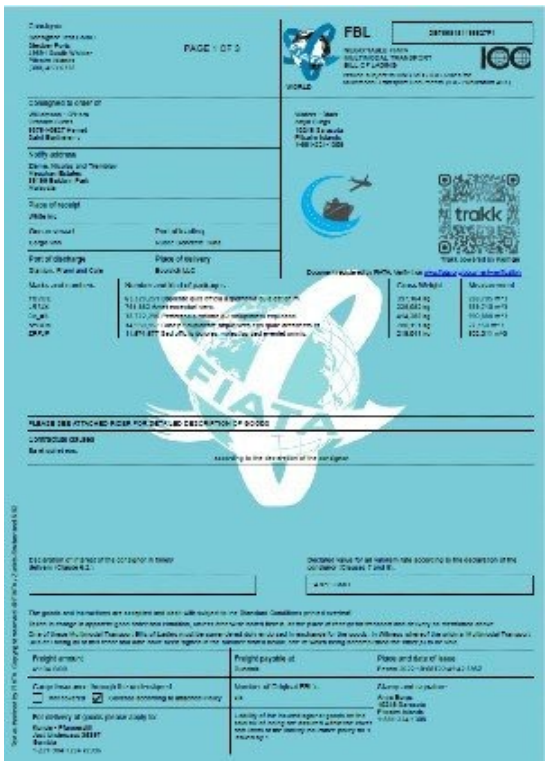
[21] Service available via Verified by GS1 | Barcode GTIN GLN Company Lookup Verification; https://www.gs1.org/services/verified-by-gs1

[22] The licensee is not necessarily the issuer; warehouse service providers working on behalf of a shipper may issue and assign the SSCC for the transport units based on the licensee's identifier-range.

How does the eFBL work?

1. Freight-Forwarders input FBL data through their everyday tool (TMS & other software).
2. The software shares the FBL data together with the identity of the document issuer with FIATA, through a dedicated API.
3. FIATA checks the identity of the issuer, through its FIATA Verified Digital Identity and registers the digital FBL document, stamped with a unique tracking QR code that contains the globally unique identifier issued by FIATA (e.g. AD962931CBD3DD5A7) - see figure to the right.
4. Freight-Forwarders can decide how they wish to share the document with their stakeholders: as a printed document or as a secured digital BL.
5. All stakeholders interacting with the document can access the immutable audit trail to verify the validity of the document, the identity of its issuer and the integrity of its content.

Figure A1-1: FIATA eFBL example



Discoverability

Stakeholders scan a QR code (if they receive a paper document) or upload the document on FIATA's *verification page*[23].

The QR-code is compliant with the URI-standard and it contains both the URL for the verification service and the attribute-value pair that enables to discover the eFBL identifier.

[23] Accessible via https://fiata.org/document-verification/.

Resolvability

The FIATA verification service is the only service that is publicly available (free of charge) that offers access to the information related to eFBL identifier. The FIATA service may be found via a scan of the QR-code. Alternatively, the service may be accessed via API for authorized partners.

Verifiability

The FIATA eFBL does not use any public key infrastructure (PKI) and relies only on a 2D barcode (printed on the physical document) that enables the holder of the physical document to check the online PDF copy of the document (a service hosted by FIATA) with the physical paper document. That level of verification is apparently sufficient for the industry in which FIATA operates. On the FIATA eFBL you will find identifiers for Subjects and Objects (both material and immaterial). None of those identifiers are directly verifiable. The eFBL-implementation is simply making it easy for users of the eFBL to increase their confidence in the paperwork and information presented to them.

Subject/Legal Entity: Organizational identity – Legal Entity Identifier (LEI) and verifiable Legal Entity Identifier (vLEI)

The Global Legal Entity Identifier Foundation (GLEIF), as manager of the Global LEI System, has created the vLEI ecosystem. A trusted network of Qualified vLEI Issuers (QVIs) issue Organizational Credentials – vLEIs. Each vLEI requires an underlying LEI – an ISO standard (17442) for legal entity identification. GLEIF is the root of trust for the vLEI ecosystem.

Discoverability

Referring to an organization digital exchanges works via tags that indicate and designate a Legal Entity in files which are being exchanged digitally. One example is entity identification in payment messages. ISO 20022 format includes a structured tag for the LEI, so parties involved know that this identifier is associated with the Global LEI System. A software system reading an ISO 20022 structured payment message can discover the OrgID-Tag, and read the LEI.

Figure A1-2: Discovery Example 3 - Legal Entity Subject (S/LE):

xmlns="urn: iso:std: iso:20022: tech:xsd:pain.001.001.09
LEI=300300GNDD855UGZ3028

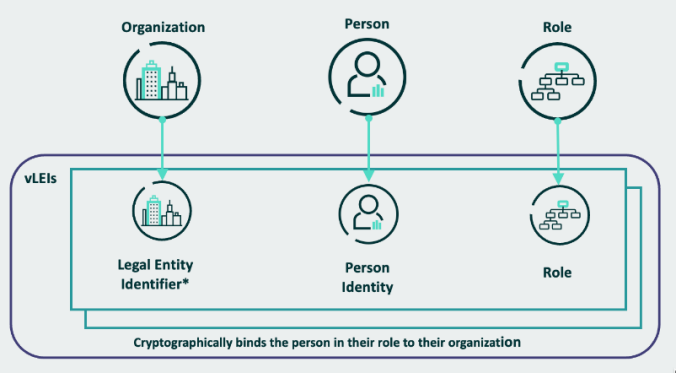
vLEIs are based on the Trust over IP Authentic Chained Data Container (ACDC) specification (based on the Key Event Receipt Infrastructure (KERI) protocol[24]. Discoverability and interoperability are achieved through the use of the did:webs DID Method.

```
<GrpHdr>
  <MsgId>1021419353</MsgId>
  <CreDtTm>2021-03-19T08:15:48.7495467Z</CreDtTm>
  <NbOfTxs>1</NbOfTxs>
  <CtrlSum>38140</CtrlSum>
  <InitgPty>
    <Nm>北京奔驰汽车有限公司</Nm>
    <PstlAdr>
      <StrtNm>Boxing Road</StrtNm>
      <PstCd>110115</PstCd>
      <Ctry>CN</Ctry>
      <AdrLine>Daxing</AdrLine>
    </PstlAdr>
    <Id>
      <OrgId>
        <LEI>300300GNDDB55UGZ3028</LEI>
      </OrgId>
    </Id>
  </InitgPty>
</GrpHdr>
```

Resolvability

vLEI credentials resolve to 3 concepts – the organizations identity represented by the LEI, a person's identity and the role that person plays for the organization.

Figure A1-3: Three-way resolving of vLEI



The LEI can be resolved via the Global LEI Index published by GLEIF[25]. Easy access to the data associated with the LEI to all stakeholders is a prerequisite to achieving all potential benefits from DRV identifiers. GLEIF, as operator of the Global LEI System, offers access to the Global LEI index

[24] github.com/trustoverip/tswg-keri-specification; github.com/trustoverip/tswg-acdc-specification
[25] Described above, see also figure 8

via a web-based LEI search tool, a file download service and application programming interface (API). All access points are free of charge and without the need to register.
Easy access to the data associated with the LEI to all stakeholders is a prerequisite to achieving all potential benefits from DRV identifiers. GLEIF, as operator of the Global LEI System, offers access to the Global LEI index via a web-based LEI search tool, a file download service and application programming interface (API). All access points are free of charge and without the need to register.

Person identity is resolved the person-name or some other relevant information like an employee number.

Role may be either Official Organizational Roles (ISO 5009) that are referenced in local legislation (e.g. Managing Director) or Engagement Context Roles that are specific to the organization and use case. The code list associated with the ISO 5009 standard is accessible online[26].

Verifiability

The vLEI follows Zero Trust Architecture[27] meaning it is developed around the "never trust, always verify" mantra, which is rapidly growing within the cybersecurity industry. The vLEI Ecosystem Governance Framework is a Layer Four Ecosystem Governance Framework of the Trust over IP Foundation (ToIP). The purpose of the vLEI Ecosystem Governance Framework is to deliver a global infrastructure that enables decentralized verifiable digital identity of legal entities in all use cases where it is required and can enable industry and participant benefits[28].

[26] https://www.gleif.org/en/about-lei/code-lists/iso-5009-official-organizational-roles-code-list

[27] Zero Trust Architecture: Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters (firewalls) to focus on users, assets, and resources. See: https://csrc.nist.gov/pubs/sp/800/207/final

[28] vLEI ecosystem governance framework : https://www.gleif.org/en/vlei/introducing-the-vlei-ecosystem-governance-framework

3.2. Appendix 2:
Digital identity standardization for trade facilitation – a legal review

3.2.1. Introduction

The purpose of this legal review is to analyze the legal framework in which the project "Digital Identity Standardization for Trade Facilitation" is embedded. This analysis is crucial due to the importance of digital identity in global trade and its regulation by several legal instruments at various levels. The goal is to align the standard with international conventions, agreements, model laws and data ecosystems (World Customs Organizations Data Model, ASYCUDA, Trade Single Window, Maritime Single Window, and Port Community Systems), as well as ongoing negotiations in intergovernmental organizations such as the United Nations (UN) and World Trade Organization (WTO).

Digital identity is essential in today's digital age, facilitating secure and efficient online interactions and transactions. Its global importance lies in promoting digital inclusion, ensuring information security, and fostering trust in digital interactions, especially with the growth of e-commerce, digital financial services, and e-government.

3.2.2. Background

Digital Identity, often associated with digital signatures and authentication, plays a significant role in both domestic and international business transactions. It validates contracts, electronic transferable records, and electronic communications. Digital identity is integral to various legal instruments and the broader electronic commerce ecosystem.

Current legal instruments under negotiation include regulations for warehouse receipts, negotiable cargo documents, and electronic commerce, where digital identity is a key component. For instance, the WCO Data Model[29] incorporates digital identity, reflecting its importance in trade facilitation.

The UN/CEFACT recommendation[30] emphasizes the removal of manual signatures in trade documents and the adoption of electronic authentication methods to streamline international trade processes." In addition, the Financial Action Task Force (FATF) recommends[31] that financial institutions are prohibited from keeping anonymous accounts or accounts in obviously fictitious

[29] https://www.wcoomd.org/DataModel

[30] https://unece.org/trade/uncefact/tf_recommendations. See recommendation 14.

[31] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

names and that they should Identify and verify the customer's identity using reliable, independent source documents, data or information.

In trade digital identity for legal entities and the persons acting on behalf of legal entities is of primary importance because these are the subjects that execute legal contracts and legal obligations. They are the foundation of the Business-to-Government and Business-to-Business relationships.

3.2.3. Need for a global standard

Existing legal instruments do not establish standards or guidelines for Digital Identity for legal entities and the persons acting on behalf of legal entities, necessitating collaboration among countries and intergovernmental organizations (IGOs) to establish protocols that are discoverable, resolvable, verifiable, and interoperable.

A globally accepted standard for Digital Identity for legal entities and the persons acting on behalf of legal entities can bring numerous benefits, including improved transportation safety, security and efficiency in international trade. The ASYCUDA program[32] by UNCTAD, adopted by 102 countries, is an example of a system compatible with global standards like the WCO Data Model[33], facilitating international trade through standardized electronic communication.

3.2.4. Regulatory and Legal Aspects

It is important to point out that not all standards are good, some are ugly, and others are bad, according to a relevant study carried out by UNCTAD[34]. Thus, we highlight some aspects that a good standard for Digital Identity for legal entities (subjects) and the persons acting on behalf of legal entities could address.

[32] https://asycuda.org/en/data-model/
[33] https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/data-model.aspx
[34] Trade barriers: picking the good from the bad and the ugly: https://unctad.org/news/trade-barriers-picking-good-bad-and-ugly

3.2.4.1 Harmonization

Harmonization ensures equivalence of standards across different jurisdictions. Given the diversity of countries, harmonization is crucial for creating standards that accommodate local adaptations while achieving global objectives

3.2.4.2 Standardization

Standardization involves creating consistent procedures and regulations. Private and and Public standards, such as those from IGOs like WCO and UN/CEFACT, are essential. Terms and definitions to achieve semantic interoperability and data exchange formats like XML and JSON are vital to ensure technical interoperability. Unambiguous digital identifiers are a prerequisite for technical interoperability. Semantic and technical interoperability achieve that *"what is sent is what I understood"*[35]. Other technologies such as blockchain may be deployed to add a layer to detect whether the data exchanged has been tampered with, in effect verifying the information originates from a reliable source.

3.2.4.3 Legal Status

A standard for identifiers used in electronic documents, as described in the main body of this paper, must have legal recognition, which can be achieved through laws, technical regulations, or judicial decisions. The 13 legal instruments listed in point 5, require or utilize digital identity standards for trade facilitation and electronic business, highlighting the need for a standardized approach.

3.2.4.4 Mutual Recognition Agreements (MRA) for Cross-border Paperless

MRAs enable harmonization by recognizing different but compatible standards across countries. An example is the UNESCAP Framework Agreement on Cross-border Paperless Trade[36] adopted by member states in 2016.

[35] https://joinup.ec.europa.eu/interoperable-europe (latest version)
[36] https://www.unescap.org/projects/cpta

3.2.4.5 Compatibility with Existing Frameworks

Standards like the WCO Data Model, IMO Maritime Single Window[37],IATA Cargo-XML[38], IATA ONE record are essential. The WCO Data Model, used by 183[39] countries, provides a comprehensive data framework for cross-border trade.

3.2.4.6 Interoperability Neutrality, Reliability and D-R-V

Interoperability ensures smooth information exchange between different countries. An excellent work in this direction is the European Interoperability Framework[40].

Figure A2-1: Interoperability Layers

Neutrality refers to choice of technologies. This White Paper does not define a technology, it rather suggests ways to achieve the goals of interoperability and reliability via D-R-V identifiers. Discoverability, resolvability, and verifiability are crucial for identifying, accessing, and authenticating digital identities as well as objects referred to in electronic documents and therefore for enabling interoperability.

Reliability, in a technological sense, is the ability for the identity solution to meet the working use expectations over time. However, reliability in legal texts must be achieved by fulfilling many requirements and tests.

37 https://www.imo.org/en/OurWork/Facilitation/Pages/MaritimeSingleWindow-default.aspx
38 https://www.iata.org/en/programs/cargo/e/cargo-xml/
39 https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/data-model.aspx
40 https://ec.europa.eu/isa2/eif_en/.

3.2.4.7 Development and Implementation of the Standard

Depending on which path you choose to follow, the process of developing a standard (holistically speaking) includes written norms, governance infrastructure, the private sector and skilled personnel.

Written Norms

Developing standards requires international agreements, conventions, and local laws. Existing legal frameworks, such as the WTO-TFA (Trade Facilitation Agreement), WCO-RKC (Revised Kyoto Convention) and UN conventions, support the creation of global standards. Regional and bilateral agreements further facilitate mutual recognition of digital identities for legal entities (subjects) and the persons acting on behalf of legal entities.

Government Infrastructure

Governments also have an important role in providing data infrastructure, especially regarding Data Pull and Public Key Infrastructure. It should be noted that developing and least developed countries may have budget and technological infrastructure constraints.

Private Sector

The private sector must be prepared to offer services, requiring information and consultation to provide effective solutions. As indicated in Appendix 1, several private sector organizations have started to offer required services. Nevertheless, more services from more organizations will be needed to realize the full potential benefits of DRV identifiers.

Skilled Personnel

Training personnel to operate the systems is essential, especially with new technologies integrated into existing ecosystems. Systems include Information technology, operations as well as interactions with other organizations. Personnel needs to understand and accept the effect of the use of electronic documents and the DRV identifiers used within those documents in all those contexts.

3.2.5 Compilation of Legal Instruments

Global trade regulation is guided by legal instruments approved or under negotiation by organizations such as the UN and its agencies, WCO, and WTO. These instruments are crucial for trade facilitation and the development of electronic business.

Key Instruments Include:

- UNCITRAL Model Law on Electronic Signatures (MLES).
- UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT).
- UNCITRAL Model Law on Electronic Transferable Records (MLETR).
- UNCITRAL Model Law on Electronic Commerce (MLEC).
- UNCITRAL working group I Warehouse Receipts.
- UNCITRAL working group IV Negotiable Cargo Documents.
- UNCITRAL working group VI Electronic Commerce.
- United Nations Convention on Contracts for the International Sale of Goods (CISG).
- United Nations Convention on the Use of Electronic Communications in International Contracts (ECC).
- IMO FAL Convention.
- WCO Revised Kyoto Convention
- WTO Trade Facilitation Agreement.
- WTO Joint Initiative on E-commerce

3.2.6 Challenges and Considerations

Implementing a global digital identity standard involves addressing challenges such as legal compatibility, technological infrastructure, and inclusivity of developing countries.

Initially, it is important to mention that each legal instrument deals with a different theme. To simplify, it is possible to separate the issues into customs (Business-to-Government relationship) and commercial (Business-to-Business relationship). They are different contexts, although interconnected.

Given legal entities and the persons representing them are highly important for the execution of legal contracts and legal obligations and the foundation of the Business-to-Government relationship and Business-to-Business relationship, we highlight some of the challenges specific to digital identity for legal persons and their authorized representatives.

Challenge 1: How to confirm that a person signing/attesting to a document or transaction is an authorized representative of a valid legal entity (and the expected legal entity)?

Using Brazil as a demonstration, there are two types of digital signatures that are recognized nationally:

Digital signature: it is the one made using the public key infrastructure. It can be used both in public systems (single window) and to sign documents in .DOC or .DOCX or. ODT or .JPG or .PNG or .PDF. It has both customs (Business-to-Government relationship) and commercial (Business-to-Business relationship) validity. Rigorous and reliable validation process related to the identity of the party that acquired the PKI, it has legal value.

Electronic signature: it is the one made **without** using the public key infrastructure. Signatures made with validation by email are not accepted for access in public/customs systems and only have commercial validity (Business-to-Business relationship). The validation process is unreliable, because anyone who receives an email can sign a document, but it has legal value.

If the operation is being performed within the single window, only the digital signature is valid.

Thus, what is missing is a system that fills this gap of operations outside the single window but is interoperable with it. How to confirm that a person signing/attesting to a document or transaction is an authorized representative of a valid legal entity (and the expected legal entity)? This missing system needs to be reliable, because reliability is part of legal texts. It is also important that this gap (missing system) is filled with an automated information exchange system (validating only documents does not address trade facilitation).

The D-R-V identifiers are aimed to close exactly that gap. A D-R-V identifier in an electronic document enables any party to find and access the data associated with the identifier and determine that the data came from a trustworthy source. This approach relies on the various sources of data to make that available through D-R-V identifiers, which is currently not widely done.

Challenge 2: How to recognize the subjects to a contract – both the legal entity and the delegated authority or person acting on behalf of the legal entity?

If the operation is within the single window, the recognition is done by the system. However, sensitive trade information is private and is made available only to the importer, exporter, and some are extended to the warehouse and carrier.

If the operation is outside the single window, it is necessary to fill the gap mentioned above (in Challenge 1). Note that it is a gap outside the single window but can be filled with Data Pull from the single window and/or using identifiers. Currently this is not possible as single window is not designed with interoperable digital identity for legal persons and their authorized representatives.

3.2.7. Conclusion and Recommendations

Effective digital identity standardization hinges on collaboration among international organizations, governments, and the private sector. Standards must be grounded in principles of Neutrality (non-discrimination and functional equivalence), Reliability (transparency and integrity), and Interoperability – principles upheld by leading international frameworks. These principles must be supported by identifiers that are discoverable, resolvable, and verifiable.

The Data Pull model exemplifies this by enhancing digital signature capabilities within legal instruments, where discoverable and interoperable identifiers allow for the seamless validation of numerous aspects of commercial negotiations. This approach reduces the reliance on document generation, instead using distributed ledgers and authenticated Single Window systems for access and verification.

Analyzing this framework reveals several key insights:

1. Each legal instrument possesses its own distinct scope and application requirements.
2. Digital identity, digital signatures, and authentication are integral to Trade Facilitation and are central to the instruments discussed.
3. For digital standards to align fully with these legal instruments, they must incorporate methods that address integrity, reliability, transparency, neutrality, legal effect, interoperability, support for data messages, and non-discrimination of foreign electronic transferable records.

References and Sources related to identifiers and their use in information exchanges

United Nations System

UN/CEFACT

Buy-Ship-Pay Reference Data Model (BSP-RDM)

Multi-Modal Transport Reference Data Model (MMT-RDM).

UN/EDIFACT

United Nations Convention on the Use of Electronic Communications in International Contracts (ECC).
United Nations Convention on Contracts for the International Sale of Goods (CISG).
UNECE International Convention on the Harmonization of Frontier.
UNECE TIR Convention.
ICAO Convention for the Unification of Certain Rules for International Carriage by Air
(Montreal Convention of 1999 or MC99)
IMO/FAL Convention. FAL.5/Circ.42/Rev.3.

UNCITRAL Model Law on
Electronic Signatures (MLES).
The Use and Cross-border Recognition of Identity Management and Trust Services (MLIT).
Electronic Transferable Records (MLETR).
Electronic Commerce (MLEC).
UNCITRAL working group I Warehouse Receipts.
UNCITRAL working group IV Negotiable Cargo Documents.
UNCITRAL working group VI Electronic Commerce.

UNCTAD ASYCUDA.
UNESCAP The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific.

World Trade Organization
Trade Facilitation Agreement.
Joint Initiative on E-commerce.

World Customs Organization
Revised Kyoto Convention.
WCO Data Model.

International Air Transport Association
Cargo-XML
ONE record

3.3 Appendix 3:
D-R-V Identifiers in an Import Case of Apparel into the EU and the UK

3.3.1 Automation potential of customs proceedings in pull mode

In this appendix, we present an example that illustrates how interactions between a European or UK apparel importer and customs authorities could be streamlined. This example demonstrates how shifting from an information "push" model (sending paper, PDFs, or EDI transmissions) to an "information pull" model could work. In this model, data availability is signaled by Verifiable Identifiers, which allows for secure retrieval of data using Verifiable Credentials. This example highlights the complexity of these interactions, involving various parties, diverse data types, and cross-industry processes.

The case is also designed to be expanded in future UN/CEFACT work in areas such as:

ESG:
Tracking and reporting the materials that make up a product (e.g., cotton, buttons, dyes), exploring how D-R-V identifiers can support digital product passports.

Trade Finance, Letter of Credit:
Managing trade risks, especially during the maritime leg, and examining how the pull approach might streamline document presentation for letters of credit.

Online B2C customs declaration:
Customs declaration[41] and customs compliance related to the avalanche of small low-value consignments (LVC) resulting from online B2C orders.

VAT Perspective:
E-Commerce VAT Regulations case addressing the “avalanche” of small e-commerce consignments and how to ascertain VAT compliance in affordable manner.

[41] Customs compliance related to low value consignments is still a problematic issue to solve. Authors like Antov, M. comment on simplified customs, One-Stop-Shop schemes (IOSS), « These options greatly facilitate both importers and customs authorities, but at the same time, they create some new challenges for customs authorities, which need to be addressed. The customs formalities currently in force do not sufficiently cover the risks of fraud and error, as full physical control of these consignments is not possible. » Source : https://worldcustomsjournal.scholasticahq.com/article/72636-challenges-to-customs-imposed-by-the-new-european-union-value-added-tax-rules-on-cross-border-e-commerce-the-case-of-bulgaria

Delegation of authority between subjects (S/LE to S/NP):
Demonstrating how employees can be verifiably identified to take actions on behalf their employers, such as in authentic fashion, i.e., signing customs declarations.

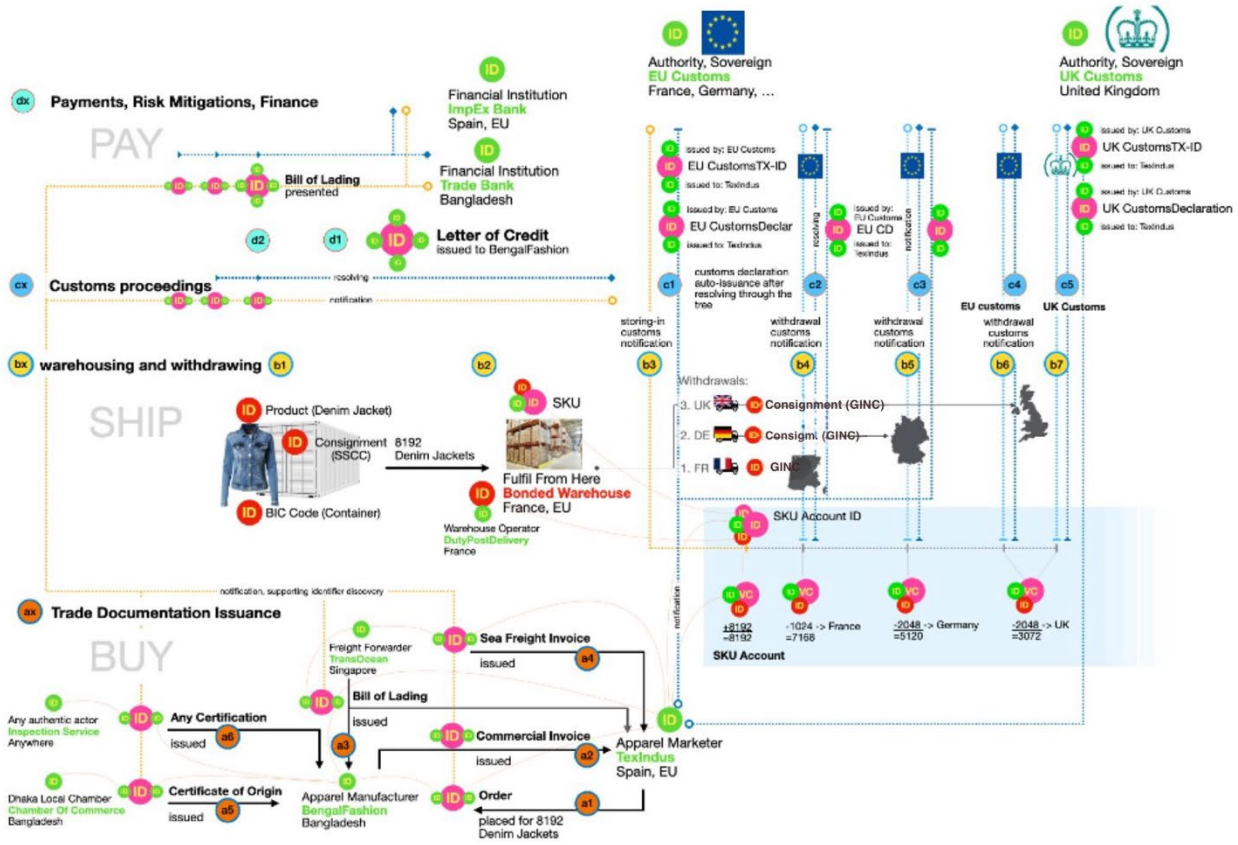
IoT device management:
Elaborating how IoT devices in containers or on palettes and the single software processes running on these devices are being made identifiable, discoverable and attributable to their respective operators.

Logistics Management:
Focusing on the information required for cargo movement alone.

This case study centers on a shipment of denim jackets ordered from Bangladesh, transported by sea to Marseille, and then distributed within the EU and the UK. Once the container is unloaded in Marseille, the goods are stored in a bonded warehouse as a Stock Keeping Unit (SKU), with customs duties deferred until items are withdrawn from the SKU for circulation.

Additionally, this case aims to describe how the lack of globally verifiable identifiers for legal entities hinders a full shift to pull-based information management supply chain, as this lack gets in the way of data authenticity.

Figure A3-1: Overview of the Use Case



a: Document issuance (Trade and Transport)

b: Transport, warehousing and withdrawing for transport

c: Customs proceedings

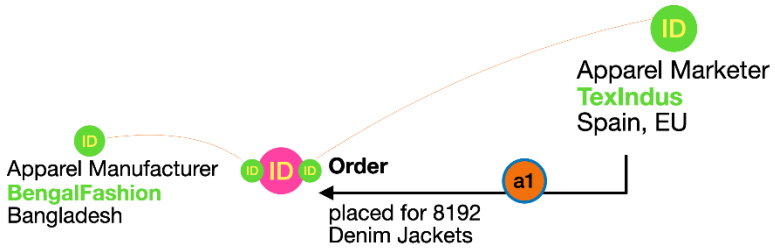
d: Payment, Risk Mitigation, Finance

The remainder of this appendix provides a detailed walkthrough of the activities and data flows.

a1: Placing an order (Trade Transaction started)

Apparel Marketer "TexIndus" places an order for Denim Jackets to Apparel Producer "BengalFashion" in Dhaka, Bangladesh, on a B2B system for apparel.

TexIndus and BengalFashion receive a notification with an identifier for the order placed through the apparel marketplace.

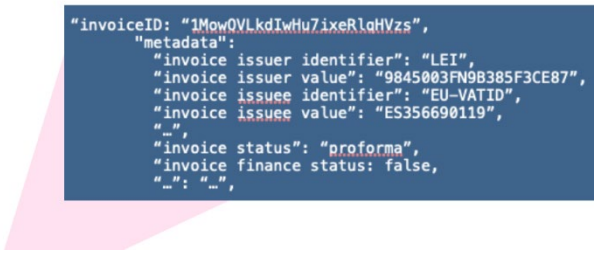


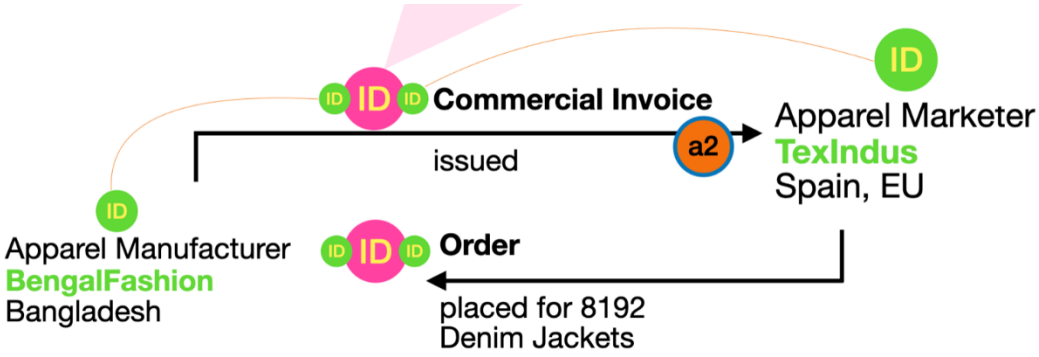
a2: Accepting order, invoice issuance (Trade Transaction agreed)

BengalFashion accepts the order, creates the goods shipment for dispatch and replies with an identifier for a Commercial Invoice issued to TexIndus for the Denim Jackets in the shipment.

TexIndus' systems can discover this identifier and resolve to access the entire invoice data. The metadata of the invoice contains important data:

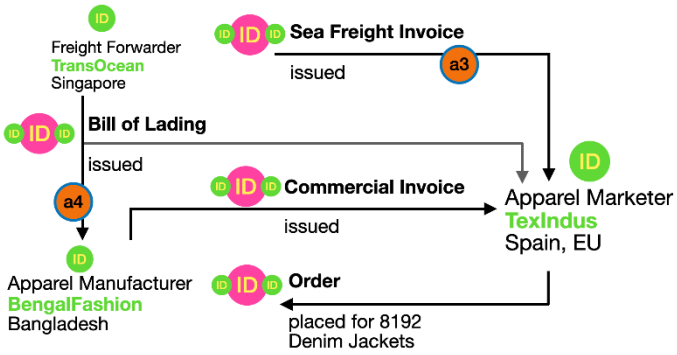
The 'issuer' field contains the LEI of BengalFashion
The 'issue' field contains the Spanish TaxID of TexIndus
The 'invoice status' field reads "proforma"
The field 'invoice finance status reads "false"





a3: Ordering maritime transport, invoice issuance (Transport Contract agreed)

Texindus orders a maritime transport (simplified) and receives an identifier of the invoice for the transport service. The invoice status field in the resolved metadata of the invoice reads “proforma”.



a4: Starting maritime transport, bill of lading issuance

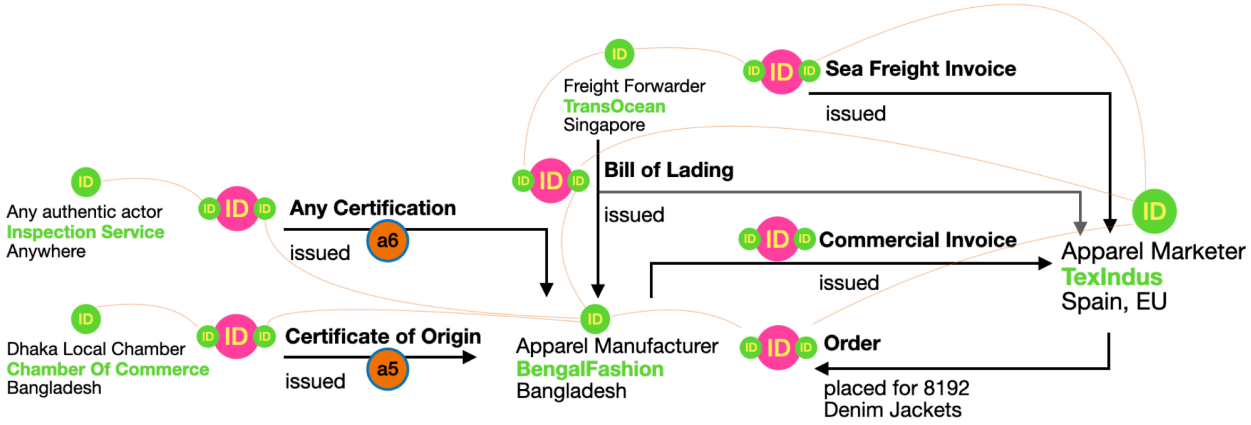
After receiving the cargo consignment, TransOcean, the maritime carrier, issues a Bill of Lading to BengalFashion. BengalFashion provides TransOcean with a product data identifier and an identifier for the packing list dataset. Using this data, TransOcean generates the electronic Bill of Lading (eB/L). Both BengalFashion and TexIndus are then notified with an identifier for the eB/L, with BengalFashion designated as the exclusive controller of the eB/L.

a5: Certificate of Origin issuance

The Dhaka Chamber of Commerce issues a Certificate of Origin to BengalFashion for the Denim Jackets, documenting the transaction details according to the Chamber's internal systems. The certificate includes an identifier that allows BengalFashion, and any party with a legitimate interest, to locate and access relevant data linked to the certificate. This identifier is also cryptographically bound to the Chamber, ensuring its authenticity. It’s important to note that this certificate may reference the local export invoice issued by BengalFashion, which may differ from the invoice received by the importer.

a6: Issuance of any other certificate

This could apply to any type of certificate, such as one issued for an inspection service. For example, it might involve a mandatory certificate verifying the safe use of hazardous chemicals in production or a certification of compliance with minimum workplace safety standards at BengalFashion's factories. Notably, only some—though not all—potential recipients of a certification, or future data consumers, can be identified at this stage. Others may express interest later. The information pull approach accommodates this by allowing additional recipients to be added over time, with documentation identifiers being discoverable and access rights granted as needed for data retrie.



b1: Executing maritime transport and delivery to the Marseille warehouse

The container carrying 8192 Denim Jackets, packed in cardboard crates on palettes, arrives in Marseille and is transported by truck to a Bonded Warehouse run by DutyPostDelivery Co., an operator certified by both EU and UK customs.

b2: Creating an SKU and SKU account to keep track of the bonded inventory

The consignment of 8192 Denim Jackets is stored in a Bonded Warehouse in the port of Marseille. The buyer and importer TexIndus record a SKU in their system and creates an identifiable account for it. The SKU is now prepared for distribution into the various retail outlets of TexIndus across Europe. Each partial withdrawal from the SKU into free circulation requires a customs declaration and clearance process.

b3: EU customs notification of storing-in into bonded warehouse

The warehouse operator "DutyPostDelivery Co" submits an identifier (O/Imt) to EU customs in France to notify about storing-in the jackets into its Bonded Warehouse in Marseille. The identifier resolves to a Verifiable Credential of an account of an SKU.

The SKU file shows the current amount of merchandise left to be withdrawn and could still be brought into free circulation (provided they are released into France and the EU).

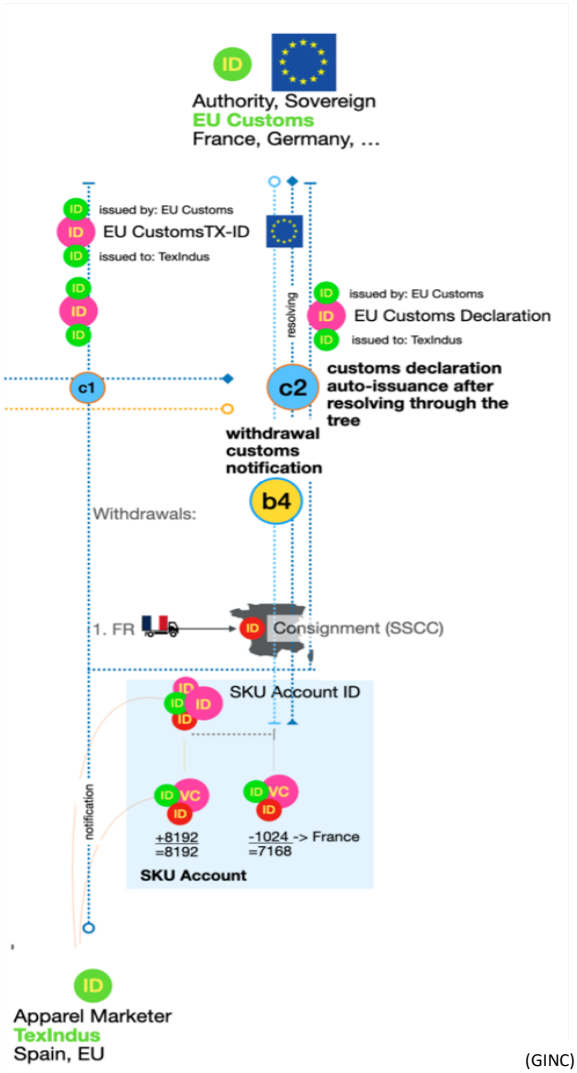
The below identifiers are also all linked to the SKU file:

1. SKU identifier (O/Imt)
2. Identifier TexIndus (S/LE), the owner of the Denim Jackets
3. Identifier of the bonded warehouse (O/Mat), within which the Denim Jackets are stored
4. Identifier of the Warehouse Operator (S/LE)
5. The identifier of the maritime consignment that was received into the warehouse along with the entire tree of identifiers for all the trade documentation filed so far.

Resolving this tree structure requires appropriate access rights, granted to parties with a legitimate interest. In this case, EU customs have a valid business interest, as TexIndus seeks to streamline customs proceedings. Therefore, TexIndus aims to provide EU customs with the necessary access to enable data resolvability.

c2: Import customs invoice issuance

Based on the notification of withdrawal, EU customs can see that 1024 jackets have been taken off the SKU inventory into free circulation, destined for France. French customs calculate the duties based on the Customs value associated with the SKU file and issues an import customs invoice to the warehouse operator.



(GINC)

b4: Withdrawal from bonded warehouse into free circulation, destination EU, France

1024 Denim Jackets are dispatched from the warehouse to a destination in France. The warehouse operator sends a notification to EU customs in France with an identifier for the shipment (GSIN) and an identifier for the SKU file from which the Denim Jackets have been taken. The remaining inventory in the SKU is now at 7168.
This is visible to EU customs at any time, by allowing them resolvability into the data linked to the SKU identifier.

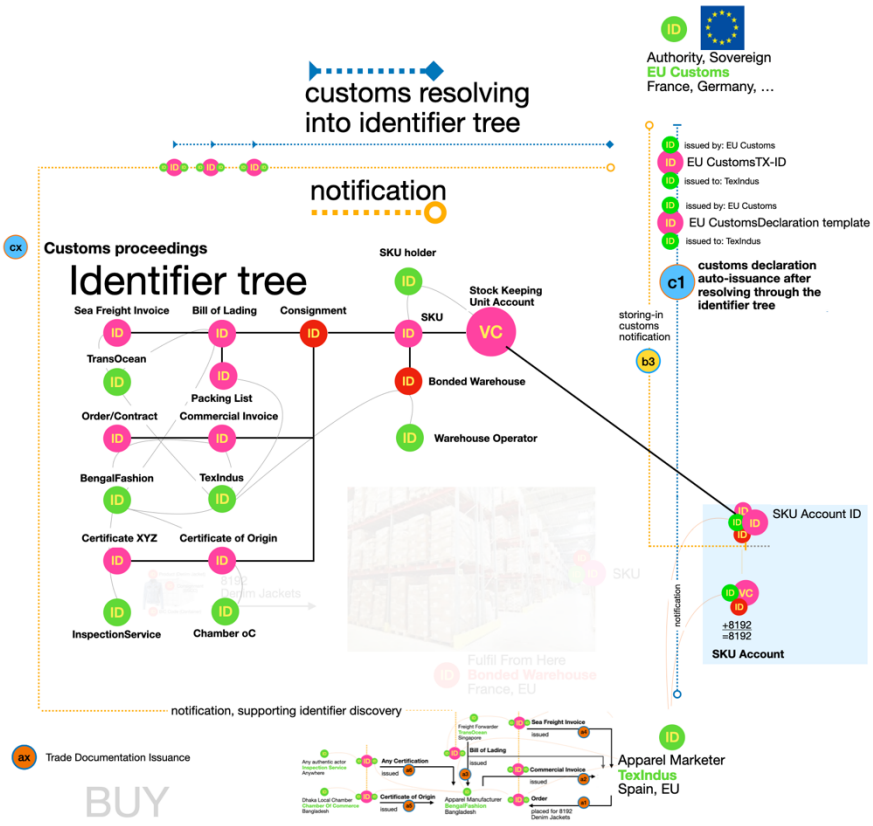
The carrier transporting the consignment (GINC) associated with the shipment (GSIN) is being granted access to all data required for executing the transportation by allowing discoverability of the collection of identifiers at hand.

c1: Opening a customs procedure, assignment of a customs process identifier

EU customs take note of the storing activity and replies with a transaction identifier[42] for the expected customs proceedings to follow.

EU customs:

1. resolve into the linked data behind the SKU,
2. discover all identifiers,
3. resolve through the entire identifier tree and
4. resolve all data, and
5. propose a custom declaration for all future withdrawals from the bonded warehouse.



TexIndus can resolve the identifier of the customs declaration which is linked to the transaction identifier that EU customs has shared with them. Hence, TexIndus can access the data of the customs declaration and populate their systems.

This way EU customs (or any other custom authority) can propose and produce customs declarations automatically.

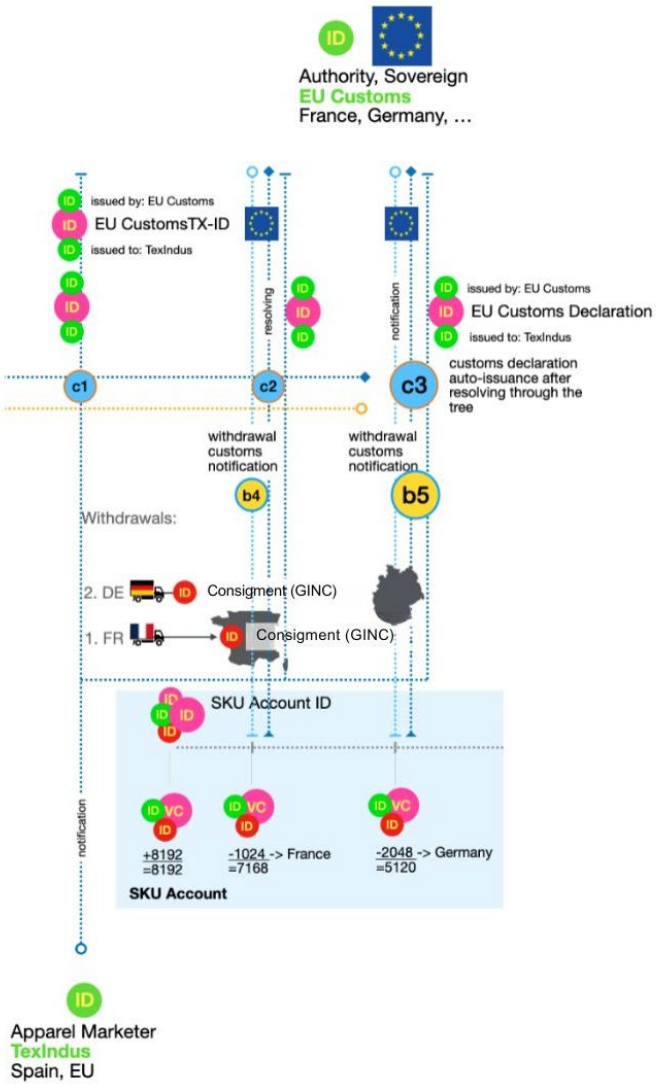
[42]Customs processes identifiers are, in general, the Movement Reference Number (MRN) assigned by the customs authorities after the declaration is received and accepted. In general, the data included in the MRN (customs declaration) is only accessible via a digital certificate which identifies the declarant/importer. In some cases, the customs authorities/importers can make these declarations publicly available through a *Secure Verification Code* -which can be shared by the declarant/importer with other operators. Example of the Spanish Tax Office *Secure Verification Code* Panel: https://www2.agenciatributaria.gob.es/wlpl/inwinvoc/es.aeat.dit.adu.eeca.catalogo.vis.VisualizaSc?COMPLETA=NO&ORIGEN=J

c3: Withdrawal from bonded warehouse into free circulation, destination EU, Germany

EU customs pull a VC containing the remaining stock. They can see that another 1024 jackets have been taken off the SKU inventory into free circulation, destined for Germany.

The remaining inventory on the SKU file is 5120.

EU customs prepare a custom declaration for TexIndus signature and calculates the duties under reference to the commercial invoice from BengalFashion and the freight invoice from OceanTrans.

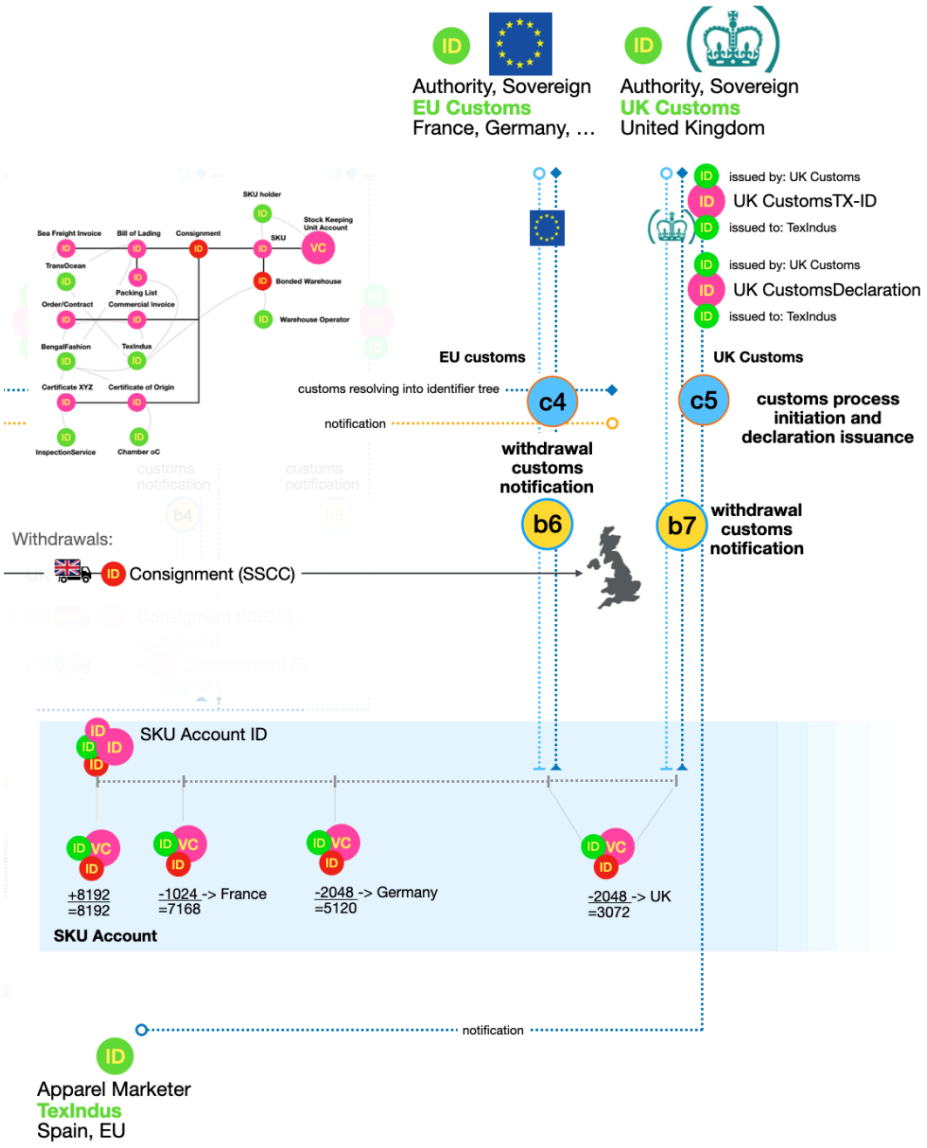


b5: Withdrawal from bonded warehouse into free circulation, destination EU, Germany

Another withdrawal occurs with destination Germany. The same process runs.

c4: Updating EU customs

French customs are notified of a further withdrawal from the bonded warehouse, which is not destined for free circulation in Europe to update them with the latest inventory balance on the SKU. EU customs confirm receipt of the notification and automatically open a digital Carnet TIR.



b6: Another withdrawal occurs, this time destined for the UK.

c5: UK customs starting customs process

UK customs take note of the upcoming import, automatically reply with a transaction identifier for the expected following customs proceedings, resolve into the identifier tree and linked data and auto-register TexIndus for the GVMS procedure and prepare an import customs declaration for TexIndus signature.

b7: Notifying UK customs

UK customs are notified by TexIndus with an identifier of the digital Carnet TIR and UK Customs are granted appropriate access rights to resolve into the linked data of the whole identifier tree associated with the digital Carnet TIR.

d: Payments, Risk Mitigations, Finance

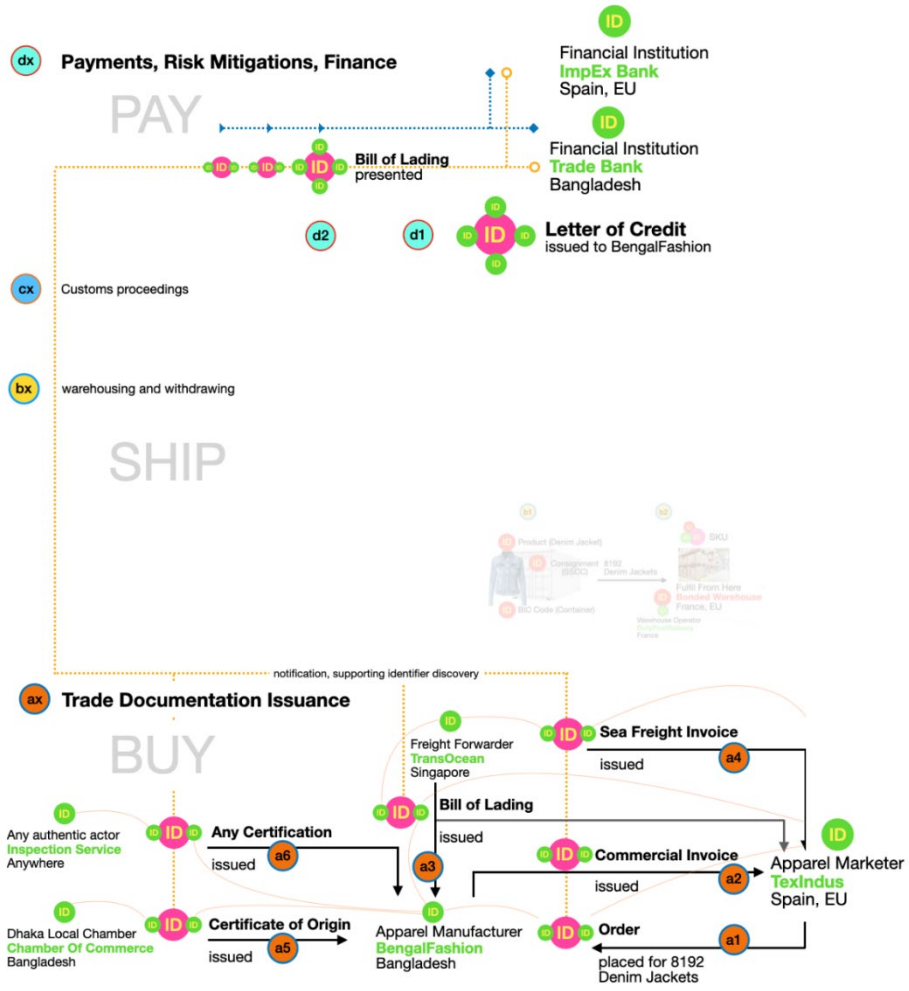
The same principles of pushing an identifier and pulling the data linked to it can be applied for any area in supply chain data management.

d1: A bank which has issued a letter of credit will ask the beneficiary to present documents.

d2: Instead of producing the documents, the beneficiary will notify the bank of identifiers of the documentation along with appropriate access rights. The bank will then be able to resolve the data.

The bank will strive to have legal certainty on…

1. who sent the data
2. who controls the electronic Bill of Lading?



3.4 Appendix 4:
D-R-V Principles and the United Nations Transparency Protocol (UNTP)

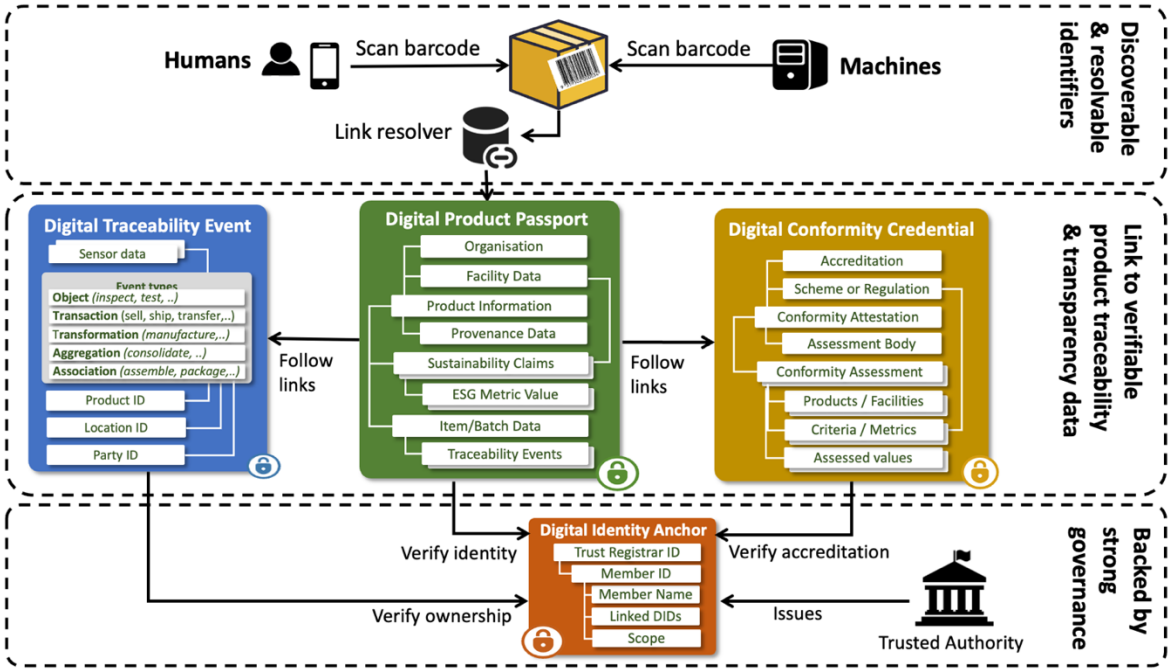
The **United Nations Transparency Protocol (UNTP)**[43] is an interoperability framework designed to enhance supply chain transparency and traceability, thereby combating greenwashing and promoting sustainable practices.

By utilizing decentralized events and existing business systems, UNTP enables stakeholders to link data across supply chains without relying on centralized platforms. This approach allows for the seamless integration of various software solutions, facilitating the participation of diverse actors in digitized supply chains.

- UNTP supports the creation of **Digital Product Passports (DPPs)**, which carry essential product information and conformity data, including sustainability assurances. These passports enable buyers to make informed decisions based on verified product claims.
- Additionally, **Digital Conformity Credentials (DCCs)** issued by independent auditors provide assessments of products or facilities against defined criteria, enhancing trust and compliance.
- The protocol also incorporates **Digital Traceability Events (DTEs)**, allowing for the tracking of product batches throughout the value chain, thereby ensuring provenance and authenticity.

[43] https://uncefact.github.io/spec-untp/

Figure A4-1: UN Transparency Protocol



By implementing UNTP, governments and industries can effectively meet supply chain due diligence obligations, empower software providers to support sustainable digitized supply chains, and enable certifiers to offer verifiable proofs of Environmental, Social, and Governance (ESG) compliance.

3.4.1 D-R-V Principles in UNTP

The **UNTP Identity Resolver (IDR)** specification[44] is a key component of the **UNTP** enabling seamless access to sustainability data using **resolvable identifiers**. The IDR is designed to accommodate existing natural identifier schemes such as

- **Business** identifiers such as national tax registration numbers managed by national business registers such as the Australian Business Register[45] or global registers such as GLEIF[46].
- **Land** parcel identifiers such as cadastral lot numbers managed by national or local authority land registers such as the Spanish land register[47].

[44] https://uncefact.github.io/spec-untp/docs/specification/IdentityResolver
[45] https://abr.business.gov.au/
[46] https://www.gleif.org/en
[47] https://land-registry.es/

- **Facility** identifiers such as farm, mine-site or manufacturing facility identifiers managed by facility registers such as GS1 Location or commercial registers such as open supply hub[48]
- **Equipment** identifiers such as vehicle registration numbers, vessel numbers and container IDs managed by authorities such as BIC[49] or IMO[50].
- **Product** identifiers for such as consumer item barcodes or upstream material identifiers managed by product registers such as the Verified by GS1 Register[51] or the Australian National Livestock Identification System (NLIS) register[52].

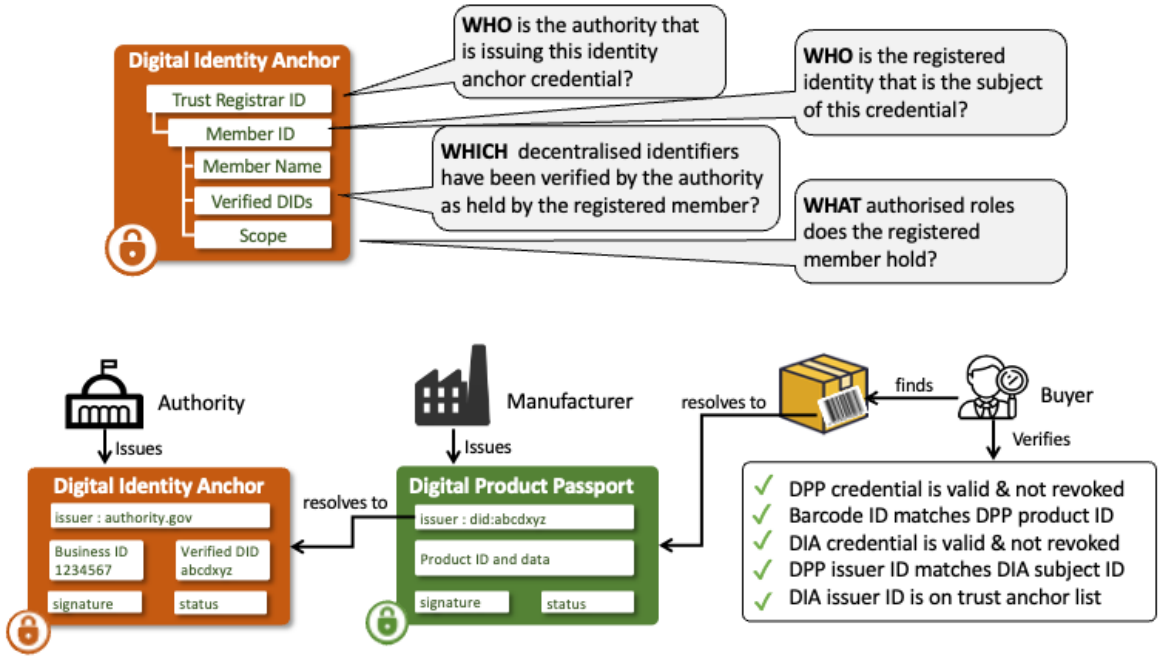
These identifiers link digital records to verifiable data sources like product certifications, regulatory compliance reports, and supply chain events. When a resolver processes an identifier, it retrieves associated information from authoritative registers, ensuring transparency and traceability in global trade.

The UNTP Identity Resolver specification, which itself is based on ISO and IETF standards, provides a simple way for every register to become discoverable, resolvable, and (with the digital identity anchor) verifiable.

The **UNTP Digital Identity Anchor (DIA)** specification[53] strengthens identity integrity by linking credential issuer decentralised identifiers to formal identifiers. Issued by recognized authoritative entities, such as national registers or certification bodies, the DIA confirms the legitimacy of businesses, products, or facilities. This eliminates reliance on paper-based certificates, reducing fraud and counterfeiting risks. Together, the UNTP IDR and DIA specifications create a trusted ecosystem, allowing stakeholders to confidently validate sustainability claims and compliance data, advancing accountability and sustainability in international supply chains.

48 https://opensupplyhub.org
49 https://www.bic-code.org/bic-codes/
50 https://gisis.imo.org/Public/Default.aspx
51 https://www.gs1.org/services/verified-by-gs1
52 https://nlis.com.au/
53 https://uncefact.github.io/spec-untp/docs/specification/DigitalIdentityAnchor

Appendix A4-2: UNTP Digital Identity Anchor



The Digital Identity Anchor is used for purposes such as:

- Business registers to assert that the holder is genuinely the business that they say they are.
- Accreditation authorities issue DIA to assert that a conformity assessment body is accredited against a given scheme.
- IP Offices issue DIA to assert that a registered party is the genuine owner of a trademark.
- Land registers issue DIA to assert that a regulated party is the owner of a geo-located property.
- Product registers to assert that the registered party is genuinely the owner of the product ID.

Call to action

Operators of business, trademark, facility, asset, or product registers have already done all the hard work to manage rigorous processes for identity, enrolment, maintenance, and ultimate deletion of member records.
Adding digital discoverability, resolvability and verification through implementation of UNTP IDR and DIA specifications is a relatively simple step that multiplies register value.