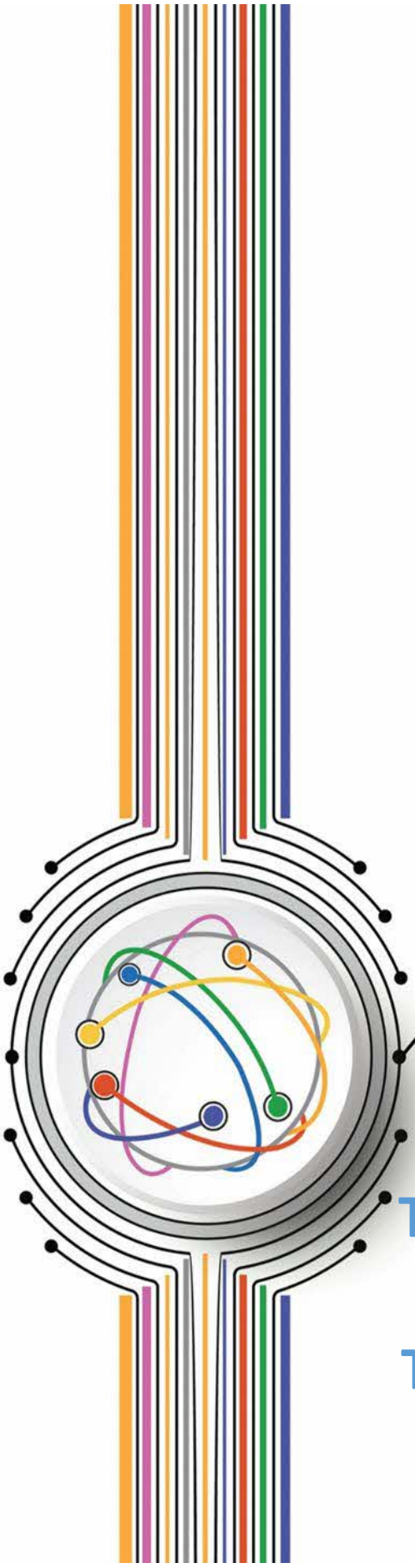


UNECE
UN / CEFACT

White Paper

Transfer of Model Law on Electronic Transferable Records - Compliant Titles

September 2023

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.

Acknowledgement

This document was prepared under the leadership of United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Supply Chain and Procurement Domain Coordinator Edmund Gray with the guidance of UN/CEFACT Vice Chairs Ian Watt and Tahseen Ahmad Khan; with support from Maria Rosaria Ceccarelli, Chief of Trade Facilitation Section, in the United Nations Economic Commission for Europe (ECE). ECE hosts the secretariat of UN/CEFACT, which develops standards and best practices for trade facilitation and electronic business. The project leadership would like to thank the following experts who contributed in their private and professional capacity to make this paper possible: Ren Yuh Kay (project lead and editor), Luca Castellani, Miriam Goldby, Simone Lamont-Black, Manuel Alba Fernández, David Saive, Jeanne Huang, Gunnar Collin, Lars Hansén, Sin Yong Loh, Serena Koh, Omer Guy, Sue Probert, Lance Thomson, Raymond Yeh, Andrea Tang, Meera Kumar, Aljosja Beije.

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

Simple, Transparent and Effective Processes for Global Commerce

The mission of UN/CEFACT 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 in order to 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 recognized 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

page

1. Executive summary

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Transferable Records (MLETR) legally enables the use in electronic form of transferable documents and instruments by complementing existing national substantive laws, under which each document and instrument comes with its own set of features that may vary amongst jurisdictions. This White Paper focuses on the specific type of electronic transferable record (ETR) corresponding to the transferable Bill of Lading. Since the use of transferable Bills of Lading spans international borders and multiple domains such as that of transport and finance, the project group recognises that clear guidance is valuable to those keen to realise and use the digital form of this transferable document.

A fully paperless trade environment can speed up many trade processes while lowering costs of trade. Transferable documents and instruments are essential commercial tools and the MLETR aims to enhance legal certainty and commercial predictability in electronic commerce by aiding the harmonization of certain rules on the legal recognition of electronic transferable records on a technologically neutral basis and according to the functional equivalence approach. The constraints with the paper process are briefly described and further references made to the reasons to digitalise the transferable Bill of Lading and other documents used generally in cross-border trade described in many publications by many organisations over many years.

This White Paper explains the key requirements laid out in the MLETR that an electronic record must satisfy to be an ETR so that its legal validity is preserved even when used across international borders through achieving the same legal effects as are achieved by use of its paper counterpart. These are the requirements of writing and signature, integrity, singularity, exclusive control to preclude double-spending, delivery and endorsement. The MLETR also provides for changes of medium where required.

In addition to explaining what the MLETR requirements entail in practical terms, this White Paper provides guidance on fulfilling the MLETR requirements to those implementing ETRs that are electronic Bills of Lading, for the benefit of the business users they serve. We contextualise this guidance on the relatively new technology of Blockchain (a.k.a. Distributed Ledger Technology), focusing on relevant aspects of the technology that meet the MLETR criteria and that are relevant in cross-border trade usage. These include the following: all parties with access to the ETR are able to, on a real-time basis, verify its authenticity and that the transferee is in control of it, while simultaneously preserving the confidentiality of commercially sensitive information.

Finally, since the MLETR can support dynamic information, it enables ETRs that can rise above the static constraints imposed by the paper medium. Some exposition is provided to give readers ideas of where the cross-border trade community may progress to by combining more technologies in a digitally enabled future.

The Annex of the White Paper points to various technical implementations and is provided solely for the purpose of letting readers explore for their own reference, technical methods that put this guidance into practice.

2. The business case for digitalising the Bill of Lading

The MLETR adopted by the UNCITRAL in 2017 was drafted with the view that legal certainty and commercial predictability in electronic commerce would be enhanced by the introduction of certain rules on the legal recognition of electronic transferable records. The MLETR is based on three fundamental principles, which have already been identified and formulated in other UNCITRAL texts:

- The principle of non-discrimination against electronic communications;
- The principle of functional equivalence between paper documents and their electronic form; and
- The principle of technological neutrality, ensuring that current and future developments are enabled providing they meet the criteria.

There are transferable documents commonly used in trade that function based on possession, in that transfer of physical possession of the document from one person to another can have the effect at law of transferring the right to claim performance of the obligation recorded in the document. The challenge that the model law addresses is to identify a functional equivalent to possession in the electronic environment and to set out the requirements that must be met in order that these documents are able to perform the same functions when issued in electronic form.

The MLETR is not intended to change the substantive law of a country, i.e., law which classifies or recognises a document as being transferable or determines the legal effects of its transfer. Countries implementing the MELTR therefore do so considering their existing substantive laws. When doing so, it remains open to countries to clarify which documents are covered or capable of falling within.[1]

There are numerous documents which fall within this description and the Explanatory Notes to the MLETR list bills of exchange; cheques; promissory notes; consignment notes; bills of lading; warehouse receipts; insurance certificates; and air waybills as possible examples.

While much of the guidance provided below is applicable to other types of these documents, this White Paper focuses on the Bill of Lading. The BL is used traditionally to allow parties to sell and buy goods in transit and to secure payment and finance, due to the BL being generally accepted as representing the goods. Presentation of the BL is required to obtain delivery of the goods, allowing the parties to pass possession and title in the goods. This traditionally was a paper-based approach and the MLETR and this white Paper are intended to facilitate its transition to and use in electronic form.

2.1 What is a Bill of Lading

A Bill of Lading (BL) is a legal document that is issued by a carrier (or its agent) and passed to the consignor when the goods are loaded. It functions as:

i) Receipt for the goods described therein;

ii) Evidence of contract of carriage; and

iii) Document of title when it is a negotiable BL.

Its role as a receipt for the goods described in the BL predates even the Middle Ages; as early as Roman times this was common practice.[2] Between ports it serves as a contract of carriage for the goods being transported, before being presented at its destination port for delivery of the goods to occur. Furthermore - and most importantly for this project - the negotiable BL can serve as proof of "ownership" of the cargo at each stage of the transit process. If the BL is made out "to order" or "to bearer" then the

[1] For example, the MELTR is capable of applying also to future transferable documents and instruments including a multimodal negotiable transferable document (see UNCITRAL Working Group VI on Negotiable Multimodal Transport Documents; the progress can be followed at https://uncitral.un.org/en/working_groups/6/negotiablemultimodaltransportdocuments [accessed 24.03.2023]).

[2] See page 550 of C .B. McLaughlin, *The Evolution of the Ocean Bill of Lading* (1925-1926) Vol.35 Yale Law Journal 548

BL is negotiable. In case of an "order bill", the original consignee, by endorsing (signing) the back of the BL and delivery of the document, transfers title in the goods to another named party who then becomes the new consignee. A "bearer bill" transfers title merely by delivery. This transfer of proof of ownership via digital means is the focal point of this white paper. Note, ownership in this paper is used in a technological sense. It bears pointing out that such an owner in the technological sense, is not necessarily the owner in the legal sense.[3]

2.2 The current paper process

When transferring ownership of a negotiable BL from one consignee to the other the following "proofs" are needed:

i) **Proof of Identity**

Is the organisation or person claiming to be the rightful owner of the goods, really the rightful owner? In the current paper-based system, this is ensured through physical possession of the original paper negotiable BL. It is, however, interesting to note that there exists a common industry practice of three original paper BLs being produced and that upon surrender of any one of these original paper BLs, the remaining two are rendered null and void.

ii) **Proof of Integrity**

Is the original (paper) negotiable BL really the original? In the current paper-based system, this is ensured through physically checking the original (paper) negotiable BL on its authenticity via mechanisms such as watermarking. This is of course sorely lacking as the technology applied is both minimal and not standardised.

iii) **Proof of Origin**

Has the original (paper) negotiable BL really been issued by the maritime transport operator (also commonly known as carrier)? Again, in the current paper-based system, this is ensured through physically checking the original (paper) negotiable BL on its authenticity via mechanisms such as watermarking and ink seals or chops. This is of course sorely lacking as the technology applied is both minimal and not standardised.

iv) **Proof of Existence**

Does the original (paper) negotiable BL represent a real physical transaction? Again, in the current paper-based system, this is ensured through physically checking the original (paper) negotiable BL on its authenticity, but further proofs can be provided by supporting documents such as a commercial invoice, packing list, customs declaration, and certificates of origin.

[3] In a legal sense, the negotiable BL represents the goods and enables transfer of possession of the goods from one person to another. This can then be used to transfer ownership providing the requirements of the applicable legal system are met.

2.3 Importance of digitalising the Bill of Lading

There are, however, several issues with this existing paper-based model:

i) The reality of global international supply chains means that information processing and the validation of the BL is not actually as smooth as is described in the high-level overview outlined above; transactions never involve only one combination of relevant parties, nor does it involve a simple transfer of goods from point A to point B. In reality, transactions often involve multiple parties who are mutually distrustful of each other, with goods travelling between multiple ports.

ii) The sort of validation involved in the above outlined process doesn't "go very deep"[4] with data travelling between "silos" controlled and owned by the companies involved in the transaction, and the validation itself only involving "some form of referencing with existing master-data such as addresses, product codes, quantities and checking whether the data transfer meets the data exchange message definition in terms of mandatory fields filled, field length, and whether the data in the fields is of the right type"[5]. Furthermore, the individual systems that each company uses, cannot be easily made interoperable, as there are many different standards for data exchange.[6]

iii) The limitations of the paper-based process have become glaringly visible in the recent COVID-19 crises. Finance of international trade relies heavily on paperwork and manual processes to provide proofs of integrity, origin and existence. Warehousing receipts, letters of credit and BLs depend on courier services for transfer between participants in a transaction. This was already an issue in the pre-COVID-19 era, but the cancellation of flights and consequent disruptions in courier services have made supply chain members painfully aware of the lack of digitisation efforts. Further complications arose from the fear of physical contact which further obstructed physical paper-based processes.

iv) The transfer of title and in particular the consequent use of the negotiable BL as collateral in trade finance is a strict "paper-only" process owing to statute law requirements in most countries. This has limited the application of existing electronic BL solutions, almost all of which rely on all users to contractually agree on the conditions under which to transact. Though perhaps still viable for trade between trusted entities, such as intercompany transactions, in a trustless environment however, certain parties (e.g., European banks) still require a collateral in the form of the original paper negotiable BL. Furthermore, the process of paper-based transfer of ownership is far from secure. A well-publicized fraud case involving warehousing receipts that acted as transferable documents of title led to combined losses of over a billion USD and a combined total potential exposure of three billion USD.[7]

---

[4] See N Vyas, A Beije, B Krishnamachari, *Blockchain and the Supply Chain: Concepts, Strategies and Practical Applications* (Kogan Page, 2019) , 98

[5] Ibid

[6] While various standards exist, the interoperability of these standards is limited. Recently we have seen a renewed push towards eBL standards, for example by the DCSA (Digital Container Shipping Association) that are based on UNECE work where UN/CEFACT holds the Core Component Libraries, Relational Data Maps and soon to be JSON-LD masters

[7] See https://www.gtreview.com/news/asia/qingdao-fraud-probe-ends-with-jail-term/

v) The impact on global supply chains of the inefficient nature of this document validation and transferal process is significant; although "a container takes approximately 36 hours to physically get from Singapore to Jakarta, Indonesia [...] information and financial settlement can take up to 7 days."[8]. This may then result in goods having to be detained at the ports, possibly causing damage and implying cost of demurrage and compensation for late delivery.

vi) The use of digital documents with standardised data can lend them to be more easily ingested by computer systems and thus be quicker and less prone to error when compared to human transcription or even Robotic Process Automation-enabled Optical Character Recognition technologies.

vii) Estimates abound on the monetary value of digitalising the Bill of Lading with a 2022 McKinsey article[9] estimating that it could save $6.5 billion in direct costs and enable between $30 billion and $40 billion in new global trade volume.

2.4 The focus of this White Paper

Leaving the substantive law untouched, the provisions of the MLETR only address the formal requirements in need of clarification in the law to enable the issuance of transferable records in electronic form with the same legal effects recognized for paper-based documents or instruments. The primary goal of this White Paper is to provide guidance on the implementation of these formal requirements of the MLETR for Bills of Lading. It attempts to illustrate how the resulting requisites can be satisfied in current practice and with existing technology.

3. Fulfilling the MLETR requirements

Article 10 of the MLETR lays down four functional requirements that must be achieved. First, per Article 10(1)(a), the electronic record must have the information that defines and fulfils the type of transferable document or instrument that it is (e.g., as is the focus of this paper, a bill of lading). Second, per Article 10(1)(b)(i), the record must be identified as being transferable; this introduces a need to "singularize" the record by giving it an identifier. Third, per Article 10(1)(b)(ii), the record must be subjected to control. Fourth, per Article 10(1)(b)(iii), the integrity of the record must be retained.

The first and fourth of these requirements is satisfied through fulfilment of the Writing, Integrity and Signature requirements discussed in sections 3.1 and 3.2 below. The second and third requirements may, at the time of writing, be fulfilled by at least two technological methods. This will be covered in sections 3.3 and 3.4.

3.1 The writing and signature requirements

Transferable documents or instruments like what is commonly known as negotiable Bills of Lading have always been typified or recognized in the law as written documents.[10] The purpose of Article 8 of the

[8] See N Vyas, A Beije, B Krishnamachari, *Blockchain and the Supply Chain: Concepts, Strategies and Practical Applications* (Kogan Page, 2019) 97.
[9] See McKinsey & Company *The multi-billion-dollar paper jam: Unlocking trade by digitalizing documentation* at https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/the-multi-billion-dollar-paper-jam-unlocking-trade-by-digitalizing-documentation#/
[10] See section 2.1 above.

MLETR is to enable compliance with writing requirements laid down in the law applicable to transferable documents or instruments, when issuing or in general using an electronic transferable record (ETR).[11]

As the rules on writing and signature are the same as or very similar to those in the UNCITRAL Model Law on Electronic Commerce and the Electronic Communications Convention, this means that they are in force in some 100 States and supported by case law.

As information in digital form may have different formats for being generated, stored, communicated, displayed or otherwise processed,[12] the basic requirement that this provision sets is that the relevant information in the ETR can be accessed so as to be readable in the required natural language.

Since several years ago, several technologies, applications and services satisfactorily cover this function for ETRs as well as for other types of documents or records in digital form. These include those based on centralized platforms or databases and as well as those built on distributed ledger technologies.

Signatures in general, are required for issue, acceptance and/or endorsement (amongst others) of the transferable document or instrument throughout the course of its life. As a provision aimed to enable compliance with signature requirements in this specific context, Article 9 of the MLETR requires that the method used for that purpose in an ETR fulfils the two functions usually fulfilled by handwritten or other signatures stamped in a tangible medium:

i) To identify the signatory; and

ii) Sufficiently express the intention of such person regarding the relevant information in the ETR.

Asymmetric cryptography is one of the methods used for electronic signatures. When used with a digital identity regime such as Public Key Infrastructure (PKI) or Self-Sovereign Identity (SSI) that allows participants to identify the person associated with the public key, electronic signatures on transactions recorded to say a blockchain, allow participants to identify the signatory as well as sufficiently express the intention of such person. The use of public key infrastructure also serves to make it tamper-evident.

In commercial transactions, non-repudiation is an important feature: this is where the signer cannot successfully dispute the validity nor the authorship of an associated contract. Two different keys, one privately held by the signatory and one publicly available to everyone else are used in the process to achieve this. The signer may use the private key to sign on a message to produce a signature which anyone with the message and the public key is able to verify. Anyone else not in possession of the private key will not be able to produce a valid signature. This thus achieves the non-repudiation property. It may be added that asymmetric cryptography, having higher global deployment, is used as a tool to explain the process.

---

[11] The UNCITRAL Model Law on Electronic Transferable Records (MLETR) available electronically at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf limits its scope for these and other purposes to transferable documents and records [see MELTR Explanatory Note, paragraph 74]. Moreover, Art. 8 MLETR has the same contents as other rules setting such requirements for all types of documents. Systems devised to allow issuing, transferring, and enforcing electronic transferable records will normally enable the use of other types of written documents employed in trade, and writing requirements applicable to each of them would be in substance be the same.

[12] The MLETR Article 2 defines “electronic record” as “information generated, communicated, received or stored by electronic means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not”.

3.2 The integrity requirement

Another important requirement is that the relevant information in the record maintains its integrity throughout the life of the ETR which may vary significantly depending on the situation. For example, in the case of disputes over goods covered by a document of title, the document might remain a live document of title for longer than expected (i.e., beyond that of just claiming the performance obligation when the goods arrive at the intended destination).

Preservation of the integrity of information contained in the ETR requires that the relevant information in the record remains unchanged or unaltered; that is to say, *that it retains the same contents it had when originally issued together with any ensuing authorised changes*. Indeed, information that becomes part of the record because of changes made after its creation must also satisfy writing requirements to maintain its integrity. Additionally, under Article 16, subsequent authorized changes must be identifiable as amendments.

Technically, integrity is achieved when all relevant information remains unaltered. The MLETR requires that the method used reliably ensures integrity. Several different methods are available to achieve this goal. One commonly used method to verify integrity relies on a hash function that creates a digest of the information ("hash value" or "hash") which is unique to the set of information. Any attempt to modify the information will result in its hash value being different.

Therefore, the use of digital signatures combined with the hash value, assist to ensure the integrity of the information in relation to its issuer's identity covered in section 3.1.

3.3 The singularity requirement

This relates to singularising the record by making a regular electronic record unique. The process of tokenization through the binding of a digital token to a regular electronic record, makes the record singular and thus enables it to satisfy this particular requirement to be an electronic transferable record. The record can be held on a register or ledger that provides, as it were, a 'single source of truth', eliminating the possibility that an ETR will be duplicated without the duplicate being recognisable as that.[13]

This Working Group recognises that as technology advances that there will be other methods that can do so but has chosen to devote their attention to two technological methods that are commonly used in the present context to achieve this:[14]

i) A centralised database where an authoritative register is kept and managed by a central service provider[15] (commonly known as a central registry system); and

[13] See S Brakeville and B Pherepa, *Blockchain Basics: Introduction to Distributed Ledgers – Get to Know this Game Changing Technology and How to Use It*, IBM, 18 March 2018, available electronically at: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/, 'Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable, immutable history of all transactions in the network.'

[14] D Saive, *Blockchain documents of title – negotiable electronic bills of lading under German law*, available electronically at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3321368 (accessed 3 February 2020).

[15] See e.g. the Bolero registry discussed in M Goldby, *Electronic Documents in Maritime Trade: Law and Practice* (2nd edn, OUP, 2019), Chapter 11.

ii) A distributed ledger which is decentralised, where each network participant has an identical copy of the ledger, a more recent development made possible by blockchain[16] and other distributed ledger technologies (DLTs).[17]

The two methods differ considerably in their various features and in the way they operate. Practitioners are urged to bear in mind implementation considerations which are addressed in the next Chapter. The differences have been discussed comprehensively elsewhere[18], however they may be summarized as follows.

In a centralised database, just one authoritative copy of the data exists and is held centrally. Thus, the 'source of truth' is found in the hands of a single intermediary, loss of which would result in loss of the only authoritative version of the information (so essentially there is a single point of failure).

In a distributed ledger, data is not held centrally but in synchronized ledgers held separately. Thus, there is still a single 'source of truth' as all ledgers are identical, but no single point of failure as in a centralised database notwithstanding various system engineering designs and best practices to increase the reliability of centralised IT infrastructure.

Furthermore, access to the single 'source of truth' is instantaneous and does not depend on the physical movement of a piece of paper. Finally, using cryptography and the hashing of individual transactions in a distributed ledger, the security and authentication features are built-in and integral to how the technology works rather than being an add-on (e.g., a centralised system that implements a security layer over the entire database). This also makes information on the distributed ledger immutable and censor-resistant – changes cannot be made, only updates appended.

3.4 The control requirement

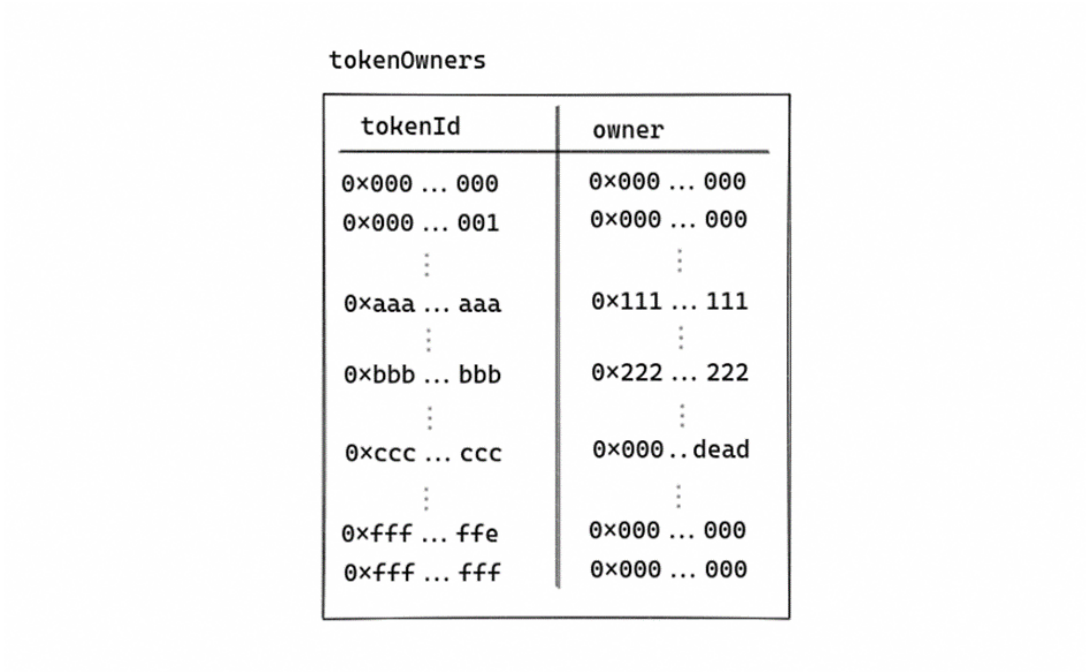
Another requirement in the MLETR is that the record must also be rendered subject to control until it ceases to have any effect or validity (MLETR Art 10 (1)(b)(ii)). That is, it must be capable of being controlled exclusively by a person (or persons acting concurrently[19]), control being the functional equivalent of factual possession for the purposes of MLETR. Regardless of whether the system is centralized or not, the underlying software should assert that at any given point in time, there should be no ambiguity as to who has control of the ETR. Asymmetric cryptography could be used to achieve this purpose where the public key (or wallet address) of the person in possession will be associated with the ETR. In a distributed ledger system, this may be achieved through a combination of tokenization and smart contracts.

[16] A blockchain is a series of records (called blocks) linked to each other in a chain using cryptography, with each block containing a cryptographic hash of the previous block as well as a timestamp and transaction data. For a full explanation see A Narayanan, J Bonneau, E Felten, A Miller, and S Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, 2016), xx–xxii and 11–12.

[17] For a discussion contrasting central registers with distributed ledgers see DA Zetzsche, RP Buckley and DW Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' [2017] *University of New South Wales Law Research Series* 52, 10–11.

[18] M Goldby, 'Substituting Data for Documents - a new meaning for "conforming tender"?' Chapter 7 in D Saidov (ed) *Research Handbook on International and Comparative Sale of Goods Law* (Edward Elgar, 2019), 152-179, esp. 165-168.

[19] MLETR Explanatory Note Para 111



A digital token can be associated with a wallet address to form the ledger of the ETR's owners. This can be visualized as a giant table (shown above) where each row contains in the left-hand column, the ETR's tokenID (which is a unique identifier of the digital token, and, in the righthand column, its owner (represented by his wallet address). A transfer of the ETR will be represented by appending a record of new ownership to the table.

As an example, the Ethereum Improvement Proposal, ERC-721 provides a widely used smart contract application programming interface (API) used for non-fungible tokens (NFTs) or deeds. The interface is widely used to represent digital assets from digital cats (virtual pets), digital art pieces and even title deeds, to virtual assets. Other than being used for representing assets on the blockchain, the API also enables other entities to build applications such as marketplaces to allow participants to buy, sell and auction these tokens.

Every individual ETR is therefore associated with a unique token and the association of the unique token to the person in control (termed the owner) ensures fulfilment of the exclusive control requirement discussed in section 3.5 below. However, the data constituting the document can be copied and shared with as many entities as needed, similarly to photocopies or scans of paper documents. The main difference between paper and an ETR created in above manner is that all the recipients of the ETR data will be able to verify the authenticity, integrity and provenance of the ETR data as well as query for the current "person" in control of the ETR.

3.5 Conferral of exclusive control and preclusion of double-spending

Article 11 of the MLETR[20] lays down two requirements for recognition:

i) a requirement that exclusive control be exerted over the electronic transferable record; and

ii) a requirement that the person in control be reliably identifiable.

[20] MLETR Explanatory Note Paras 84 and 85.

The concept of control adopted here is intended as being functionally equivalent to factual possession. Paragraph (2) of Article 11 provides that transfer of control will have equivalent effects at law to the transfer of possession of a paper document. Thus, one may infer a third, implied requirement that the system enables transactions whereby control is transferred between parties.

Both central registry and DLT systems can fulfil these requirements. In a central registry, exclusivity may be achieved by ensuring that only one person (or persons acting jointly or concurrently) is registered (identified) as the person(s) in control of a particular electronic record at any point in time. Transfer instructions are given and accepted over transaction platforms. The system will need to be designed so that only the person(s) registered as having exclusive control will be permitted to transfer, and control passes to the transferee upon acceptance of the transfer.

As for fulfilment of these requirements through a DLT system, as explained in section 3.3 above, the owner of the ETR will have exclusive control over the ETR. This means that only when the owner of the ETR invokes the transfer function of the ETR will the record update the existing owner to the new recipient. These constraints are enforced through a process known as "validation" based on digital signatures and can be enforced programmatically when writing the smart contract for the ETR. Whenever an entity claims to be the owner of the ETR, the entity may use the private key corresponding to the wallet address listed as the owner of the ETR to sign on a message to prove that s/he is indeed the controller of the owner wallet. Effectively, the person that the system allows to transact the ETR is the person in control of it and therefore the owner in the technological sense.

To transfer an ETR the current ETR owner will call the transfer function of the smart contract to register the current value of the owner in the smart contract with a new wallet address of the ETR receiver. This action will replace the owner value of the ETR with the new value and anyone who queries the smart contract for the "owner" will now know who the new owner of the ETR is. This is known as an anti-double-spending mechanism as only one person can have the token in their wallet at any time. While the current owner may send more than one transfer transaction to the blockchain, one transaction will be ordered before the other and the second transaction will fail, resulting in the ownership being transferred to the party named in the first transaction. This ensures that only one party will receive the ETR upon block confirmation.

3.6 Delivery and endorsement

Under MLETR article 15, while an endorsement is composed of writing and a signature, covered in articles 8 and 9 and discussed in section 3.1 above, it is worth bearing in mind the special purpose and function of endorsements. In an order document in paper form, the relevant obligation is expressed as being owed to a named person or their order. This makes the document transferable by endorsement.

Transferable documents and instruments may be transferred anonymously (or "to bearer") or to a named person (or "to order"). In the former case, the simple delivery of the paper-based document suffices, while in the latter case it is also necessary to endorse the document, usually by signing it on its back. The MLETR allows for both transfer methods: in the former case, it will be effected by transfer of control, while in the second it will require compliance with additional requirements (see section on endorsement below).

It is important to note that the requirement to identify the person in control does not prevent the anonymous circulation of the ETR to bearer: identification will not be used for commercial law purposes, and the last person in control will not have any action in recourse against the prior transferors as there is no chain of endorsements. However, identification may be used for other purposes, for e.g., compliance with regulation. This allows to fully preserve the flexibility of commercial law while overall improving governance and reducing compliance costs.

To transfer an order document the transferor must deliver the document to the transferee and address a signed instruction to the obligor, written on the back of the document, to render performance in favour of the transferee. Article 15 of the MLETR does away with the notion that the endorsement needs to be on the back of the document when the document is in electronic rather than paper form (although virtually the appearance of the document on the screen can still be given a front and back) but emphasizes that it must satisfy the requirements for writing and signature discussed above.

On the blockchain, the conditions for a transfer of an ETR by endorsement can be written in the smart contract that runs on it. By restricting the transfer function of an ETR to its owner, a correctly signed transfer with the owner's private key may automatically achieve the same effect of a written endorsement, if the record shows that the transfer has been properly authorized in all and each of the transfers made.

3.7 Change of mediums (digital and paper)

Articles 17 and 18 of the MLETR both provide for a change of medium; Article 17 from paper to electronic and Article 18 from electronic to paper.

The MLETR explanatory note states that "…article 17 of the MLETR does not require that all information contained in a transferable document or instrument be contained in the replacing electronic transferable record."[21] It also states that there is no requirement that the paper substitute reproduce information such as metadata from an ETR.[22] It is implicit in the reference to "change of medium" as well as in the provision of paragraphs (4) of both articles 17 and 18, that only the medium is being changed. Therefore, the core information that is needed for the doc to be legally relevant and valid needs to be reproduced. Information that is generated electronically out of that change of medium (i.e., metadata) however, does not have to be replicated on paper.

These provisions require that to fulfill MLETR requirements, electronic systems should enable users to request and obtain bidirectional swaps between paper documents and ETRs. To preserve singularity, a paper document and ETR should only be exchanged for one another and this could rely on the force of technical and/or process controls. For example, when swapping a paper document for an ETR, the owner of the paper document must surrender it to the issuer who will then proceed to take it out of circulation and replace it with an ETR. For an ETR to be exchanged for a paper document, the person in control of the ETR must surrender the ETR back to the issuer who will then proceed to replace it with a paper document. This latter option is particularly important for electronic bills of lading since these documents are typically used internationally and often need to be issued to shippers, accepted by receivers as well as processed by border control and customs agencies, in jurisdictions where ETRs may not be legally recognized as equivalent to paper documents of title.

However, it is worth noting that there is a fairly common practice in trade of issuing multiple originals due to limitations of the paper medium. As the MLETR does not change substantive law, so where issuance of multiple originals is possible in paper form, it is possible also electronically and even on mixed media.[23] However, issuers of transferable records (whether in electronic or paper form) should have the necessary mechanisms in place to prevent creating duplicate liabilities for themselves, as would happen if two records (one electronic and one paper) were in circulation simultaneously. Carriers as issuers of

[21] UNCITRAL, Explanatory Note to the UNCITRAL Model Law on Electronic Transferable Records, para 164. An identical statement is made about article 18 in para 179.
[22] UNCITRAL, Explanatory Note to the UNCITRAL Model Law on Electronic Transferable Records, para 179.
[23] UNCITRAL, Explanatory Note to the UNCITRAL Model Law on Electronic Transferable Records, paras 191-195.

bills of lading are already well versed in addressing such risks, in view of the practice of switching bills of lading.[24]

4. Practical considerations when implementing systems that fulfil MLETR requirements

4.1 Verifiability

Verifiability here refers to the situations where parties can be satisfied that the ETR is authentic, accurate, complete, and updated. For example, parties such as customs authorities or financiers using or accessing an ETR would want to be assured that a record presented to them throughout the course of an import/export process and documentary trade process is indeed a valid ETR.

One point that bears clarifying here is that per the World Trade Organization Trade Facilitation Agreement Article 10.2 which governs the acceptance of copies of supporting documents required for import, export, or transit formalities, border control agencies should not need to be provided the original supporting document.

The ETR's authenticity must be verifiable in all respects, in particular the identity of the person in control, the ETR's issuer and any other party whose identity may be relevant (e.g., an acceptor or a pledgee). Technically, either a trusted centralised system or a distributed ledger can be used, and this will allow anyone with access to an ETR and the ledger to know with certainty that the ETR is correct and has not been manipulated, even without ownership of the ETR. The ledger should of course strive to be resistant to manipulation (e.g., by being built based on a consensus mechanism using computer science principles).

Therefore, a public blockchain can be used as a notary service to evidence the existence and contents of an ETR so that a copy (which by definition is non-transferable) can be distinguished by comparing an ETR with its corresponding cryptographic references in the ledger. With all documents being identical and referencing the same register on the ledger, this means that all parties with access to the ETR will be able to verify that it is authentic.

If the verification is done while also being the owner of and presenting a private key, with evidence of the corresponding public key published as the owner key on the blockchain, the returning result would be that the ETR is the original and the owner is then able to manage the record according to allowed operations. The register on the ledger can be implemented with a smart contract to allow for actions like transferring the ownership to another.

Allowed operations for the owner of the original might have to include (depending on the type of ETR):

i) the possibility to add new information to the ETR, without changing what has already been written;

ii) allow the ETR to be electronically signed;

iii) endorse a transfer of ownership;

iv) terminate absolutely its ability to be transferred; and

[24] See discussion in M Goldby, 'Managing the Risks of Switch Bills of Lading' [2019] *Lloyd's Maritime and Commercial Law Quarterly* 457-480 available at https://qmro.qmul.ac.uk/xmlui/handle/123456789/61123

v) allow proper archiving according to relevant records keeping practices and audit requirements.

To give the owner of an ETR the ability to prove exclusive control, the solution could integrate an ownership verification service. This would allow the owner to transmit a copy, which can be verified, and a proof of ownership of the exact ETR that the verified copy is of.

Since all copies of the ETR will reference the register which has information on the public address/key of the owner, the owner will be able to prove ownership of the ETR by self-identifying as such through the private key (under the presumption that a public key is also the permanent cryptographic address). This is especially pertinent when one considers that the role of an operator of the ETR management system is separate and distinct from an owner of the ETR.

Having these functions available in an MLETR-compliant solution will reduce friction in transactions and decrease the level of reliability required between parties.

4.2 Business confidentiality and banking secrecy

Certain contracts, e.g., those between banks and their customers often contain obligations of confidentiality. In some jurisdictions these duties are implied by law even if the contract itself is silent regarding them. Certainly, though not specific to only ETRs, there may be trade secrets or business information on an ETR that corporates wish to keep confidential as they transact their business.

Technical solutions need to allow that such business secrets are kept confidential since otherwise these solutions risk being disregarded in favour of traditional paper documents where it may be easier to maintain confidentiality. Furthermore, an ETR functioning as a negotiable instrument will often circulate through financial institutions either as direct parties to the transaction or indirectly acting for the transferor or transferee. Compliance with banking secrecy laws would then be required. An ETR system therefore needs to be able to maintain confidentiality between the bank, its service providers, and its customers towards any third parties so that ETRs can be transferred subject to such regulations.

As a general note, there are technical solutions that can ensure privacy even when using a public blockchain by publishing only cryptographic evidence (e.g. hash as discussed above in section 2.2) of the existence and the public key of the owner of the document, thereby ensuring singularity and control while the ETR itself is stored off-chain. By using this method, local records containing ETR business data or personally identifiable information (PII) data can remain secret and hidden while the cryptographic evidence can prove the current contents of the ETR, the cryptographic identity of the current owner, and when it was published. The contents of the ledger make it impossible to reverse-engineer the contents of the record, so the ledger acts effectively as a notary service to ensure the integrity of the ETR contents which is what is critical.

In this manner of achieving privacy by design, the ledger is used solely as a digital verification service containing only anonymous cryptographic references to the ETR. Verifications of authenticity, integrity or ownership can be made mathematically without having to reveal the contents of the ETR itself, thereby preserving commercial confidentiality. The actual content can be held off-chain and can be shared by those who have the right to share it as a document or a file and only as needed.

The guiding principle of the MLETR is functional equivalence, therefore this would be a clear method to mimic the confidentiality achieved by limiting access to paper originals and copies to authorized persons.

Keeping data off-chain and storing only its hash on the blockchain only makes any changes evident but does not prevent them, hence care needs to be taken to check for such evidence of tampering. Although the alternative of storing the data on-chain makes it immutable to unauthorized changes (as a change is

subject to the consensus mechanism of the blockchain), this may unfortunately expose sensitive information and be problematic from a PII perspective.

4.3 Personal data regulation and the right to be forgotten

The holding and processing of personal data in electronic form may be subject to regulation.[25] This protection may include a "right to be forgotten", i.e., a right to have one's data purged from an electronic system where it is stored.[26] Thus, there may be data included in an ETR which some parties may not be permitted to see or to disclose publicly. The MLETR has left the question of storage and retention to existing domestic law, but any electronic system or platform over which ETRs are issued or transferred needs to take these obligations into account.

Distributed ledgers are very useful for evidentiary purposes because information cannot be deleted from the ledger; however, this has to be made compatible with data protection laws and the right to be forgotten if personal data or PII data is stored on the ledger. Thus, the storage of personal data on public blockchains should be avoided. For now, the right to be forgotten is limited to personal data though issues could arise when regulations change due to the immutable nature of the distributed ledger. Arguably, in the case of an electronic B/L, the vessel master's signature and the names of the relevant parties on an electronic B/L may be deemed necessary data thus processing them on a blockchain may be allowed.[27]

For distributed ledger systems, one suggested method of implementing the right to be forgotten is to encrypt the data on them but that may not be permitted in some jurisdictions because it is not certain that is not able to be decrypted. Therefore, one way to maintain confidentiality would be to only make generally available on systems, the associated cryptographic references (e.g. hash).

4.4 Procedural formalities for enforcement

Certain ETRs, such as Bills of Exchange, Promissory Notes or Cheques may need to be enforced through formal procedures such as protest when they are dishonoured. ETRs may also need to be used as evidence in court. Therefore, even after they are dishonoured, systems should be able to satisfy procedural requirements.

Procedural requirements often dictate that the original document itself is necessary to bring a claim. In many jurisdictions it may suffice to be able to demonstrate singularity and ownership in digital format, as the law generally[28] prohibits inadmissibility of evidence merely on the grounds that it is in electronic form. However, where necessary, there should be an option to use the ETR system to provide the relevant institution with access to the ETR in a way that allows verification of authenticity, integrity and control.

Where digital evidence is not accepted, the solution will depend on the kind of evidence required and the purposes for which it is required. Ultimately, where the original document is required in paper form, the ETR will need to be converted in accordance with the MLETR (as discussed in section 2.7) as well any applicable enforcement guidelines relating to electronic documents. Thus, having a technical solution able to support this will be crucial.

---

[25] EU General Data Protection Regulation (GDPR) Article 1

[26] EU General Data Protection Regulation (GDPR) Article 17

[27] D Saive, *Das elektronische Konnossement* (Mohr Siebeck 2020), p. 244.

[28] This should be the standard for countries that have adopted the UNCITRAL Model Law on Ecommerce (1996) Art.5, United Nations Electronic Communications Convention Art.8 and the UNCITRAL Model Law on Electronic Transferable Records (2017) Art.7

4.5 Long-term data preservation

There are many reasons to ensure that negotiable instruments and documents of title are retained and stored in original form even after the claim to performance has been exhausted. Such reasons may include evidentiary and tax purposes.

Technical solutions creating compliant ETRs must therefore reliably provide long-term data preservation for users of the solution and advancing technologies need to maintain backward compatibility to ensure that it would be available when the need arises.

Accordingly, the data format for the ETR must be in a *de jeure* standard format that is recognised by international standards bodies like UN/CEFACT[29] and the International Standards Organisation (ISO)[30], hence suited for long term preservation.

The Model Law does not contain specific provisions on storage and archiving. All applicable retention requirements are found in other law, including the law on privacy and data retention, and should be complied with. The notions of storage and archiving may apply to the information contained in the electronic transferable record, but not to the electronic transferable record as such.

Using distributed ledgers with immutable chains of evidence will go a long way towards providing security. If a distributed ledger or registry should cease to provide the service, each party to a transaction is still able to keep a locally stored copy of the entire ledger as a backup. The possibility of a secure backup stored with each transacting party speaks to the potential for blockchain based solutions to be well and truly immutable.

5. More than just an electronic variant of what is on paper

5.1 Dynamic information

An ETR can be much more than just a simple conversion of a paper transferable document into an electronic variant as new reliable information can be added to the record after it is issued, such as that providing visibility into the real-time status of the goods and the speedier resolution of issues that may arise during the goods' transportation. Of course, an ETR still needs to contain all the information required by law, but the MLETR leaves it open to the parties to provide for the inclusion of dynamic information[31] in the ETR.

Some idea of the possibilities that this creates can be gleaned from a report[32] by Lloyd's of London's Innovation team and the Centre for Commercial Law Studies, Queen Mary University of London that showcases how smart contract solutions could be implemented across a range of insurance products. One of the case studies included in the report is an examination of how different technologies could be combined to improve cargo insurance processes.

[29] See https://unece.org/publications/trade/cefact
[30] See https://www.iso.org
[31] See MELTR Explanatory Note, paragraph 58
[32] See *Triggering innovation: How smart contracts bring policies to life* available at https://www.lloyds.com/news-and-insights/risk-reports/library/triggering-innovation/

Where cargo is sold while in transit, unless parties agree otherwise, the legal presumption in cross-border sale contracts is that risk passes upon shipment[33] so that any loss or damage to the cargo that occurs while it is in transit is at the risk of the ultimate purchaser. For this reason, it is usual for the seller to transfer to the purchaser its rights under the cargo insurance cover. Where the applicable law permits, this transfer can take place by documentary assignment (indorsement and delivery of a cargo insurance policy or certificate).

The report notes that the presence of online sensors able to record real-time information about the cargo for example the temperatures, humidity, and vibrations it is exposed to, would enable cargo insurers to have early notice that the cargo was lost or damaged during the transit. This would enable greater automation in claims processes. For example, automated combination of data from sensors and geolocation devices (oracle data) with historical aggregated data relating to common causes of the kind of loss indicated by the oracle data would facilitate a speedier assessment of the extent to which further investigation of the loss may be required.[34]

Some of the oracle data referred to above can be obtained through traditional tracking methods, radio frequency identification-based tracking methods as well as Internet of things tracking methods, as discussed in a UN/CEFACT White Paper on Integrated Track and Trace for Multimodal Transportation[35] and a UN/CEFACT White Paper on Internet of Things for Trade Facilitation.[36]

[33] See Goldby, M., 2013. *Electronic documents in maritime trade: law and practice*. Oxford: Oxford University Press.
[34] See page 25 of *Triggering innovation: How smart contracts bring policies to life* available at https://www.lloyds.com/news-and-insights/risk-reports/library/triggering-innovation/
[35] See page 14 of *White Paper on Integrated Track and Trace for Multimodal Transportation* available at https://unece.org/info/Trade/CEFACT/pub/364129
[36] See *White Paper on Internet of Things for Trade Failitation* available at https://uncefact.unece.org/display/themepressdemo/Internet+of+Things+for+Trade+Facilitation

6. Annex: technical guidance

The MLETR-compliant Title Transfers White Paper has produced an annex of case studies to give practical implementation information for reference on the points made therein. These case studies do not constitute an endorsement of any kind by UN/CEFACT and the submissions are presented as is and were only checked for grammar and spelling.

This appendix is designed to support implementers with detailed technical information. Since such information is typically fast changing, this appendix provides only a summary of each topic and then links to sites that are maintained with the latest relevant information.

6.1 TradeTrust

Singapore developed TradeTrust (see https://www.tradetrust.io) which is an open framework adapted for global trade practices to help the typically long chain of business partners achieve the ultimate objective of fully digitalising their business processes even across borders through being able to cater for both normal documents and transferable documents like Bills of Lading. Given the complexities of cross-border trade, success requires a multi-prong and holistic approach. The technology underpinnings of TradeTrust are provided by OpenAttestation (see https://www.openattestation.com) to enable documents issued with this technology to be cryptographically trustworthy and able to be verified independently, as well as being able to effect title transfers through ETRs. OpenAttestation has been registered as a Digital Public Good with the Digital Public Goods Alliance (see https://digitalpublicgoods.net). Atop this **freely-available**, **open-source** technology, TradeTrust adds aspects such as acceptance by the global trade community and governments on the methods of document digitalisation as well as alignment on policy stances through Government-level arrangements such as Digital Economy Agreements. These efforts have resulted in the following features being implemented:

- The Title Transfer feature supports electronic transferable records and is designed to be compliant to the requirements laid out in the UNCITRAL Model Law on Electronic Transferable Records (2017).
- The Decentralised document rendering protocol enables users to choose their own document schema format, and to customise the look and feel of the trade documents produced.
- Selective Redaction provides a convenient method for intermediaries in the supply chain to hide sensitive data, which is critical for some use cases in the trade and traceability domains.
- The QR Code feature enables users to choose using paper or digital workflows, depending on their circumstances thus allowing issuers to execute digitalisation with minimal dependency on verifier technical capabilities.

The UN/CEFACT repository https://github.com/uncefact/spec-tradetrust provides additional guidance on the effective use of TradeTrust.

6.2 trace:original

The trace:original solution has been developed by Enigio AB, a document technology company from Sweden. The trace:original ETR is a freely transferable and verifiable electronic paper equivalent using the PDF standard (Portable Document Format). The trace:original solution is fully compliant with all requirements set out in the UNCITRAL Model Law on Electronic Transferable Records (2017), including

the possibility to endorse documents and provide the means for a reliable method to change medium from digital to paper and vice versa.

The trace:original document (the electronically transferable record) can carry any type of electronic signature and/or seal e.g., Adobe Sign, DocuSign and more, as well as structured data in predefined data standards. Additional documents, such as powers of attorney, vital for the verification and acceptance of the validity of the ETR, can be attached. The document can be freely transferable and updated by the current holder.

Through the ability to carry attachments, the trace:original document technology provides support for managing full electronic document presentations, as required in many trade and trade finance transactions.

All trace:original documents are both man and machine readable and can be processed manually by using a web browser as well as being subject to straight through processing if the document is carrying structured data.

The solution is use-case agnostic, and can be used in any situation where original documents are required by law or in cases where it is important to verify the authenticity of the documents. Use case examples range from documents of title, negotiable instruments, certificates, contracts to educational diplomas, where it is important to establish the authenticity of the document.

To enable a smooth and gradual transition from paper to digital, the trace:original[37] solution can be implemented in parallel with a current paper-based process without needing significant changes. This makes it possible for users to gradually move from paper to digital when their customers and counterparts are willing to change from paper to digital.

Enigio was awarded the status as 'Technology Pioneer' in June 2023 by the World Economic Forum.

[37] More information about trace:original is available at Enigio.com.