Implementing Electronic Transferable Records according to MLETR

Abstract

The **2017 UNCITRAL Model Law** on **Electronic Transferable Records (ETR)** aims to define a reliable dematerialized version of documents with properties equal to or superior to paper: non-substitutable, transferable as a single original copy, signed, approved, versioned. The text also provides for the tracking of modifications and the round-trip between paper and digital versions.
This document describes KeeeX's implementation of the MLETR, arguing in great detail how the **KeeeX** technology and approach satisfy each of the requirements set out in the model law.

Author: Laurent Henocque

Introduction

The MLETR (*UNCITRAL Model Law on Electronic Transferable Records (2017)*) aims to define the requirements applicable to a reliable dematerialized version of documents with properties equal to or superior to paper: non-substitutable, transferable as a single original copy, signed, approved, versioned. The text also provides for the tracking of changes and the transition from paper to digital versions and vice versa.

The proposal for this model law was intended to encourage governments to accept the use of digital documents, particularly in the context of international trade, which is still not very dematerialized. Many countries have already adapted their regulations to this effect. In France, a report entitled "Accelerating the digitization of international trade finance activities" was submitted to the government in July 2023. This report indicates that international trade is still only extremely marginally dematerialized today.

This article describes KeeeX[KeeeX]'s implementation of the MLETR.

It is based on Chapters II. Provisions on functional equivalence and III. Use of electronic transferable records detailed in the official explanatory e-book [MLETR] obtained from the UNCITRAL website[UNCITRAL].

The holder of the rights attached to the possession of a title potentially holds considerable economic value (as is the case in the supply chain). This calls for a solution that :

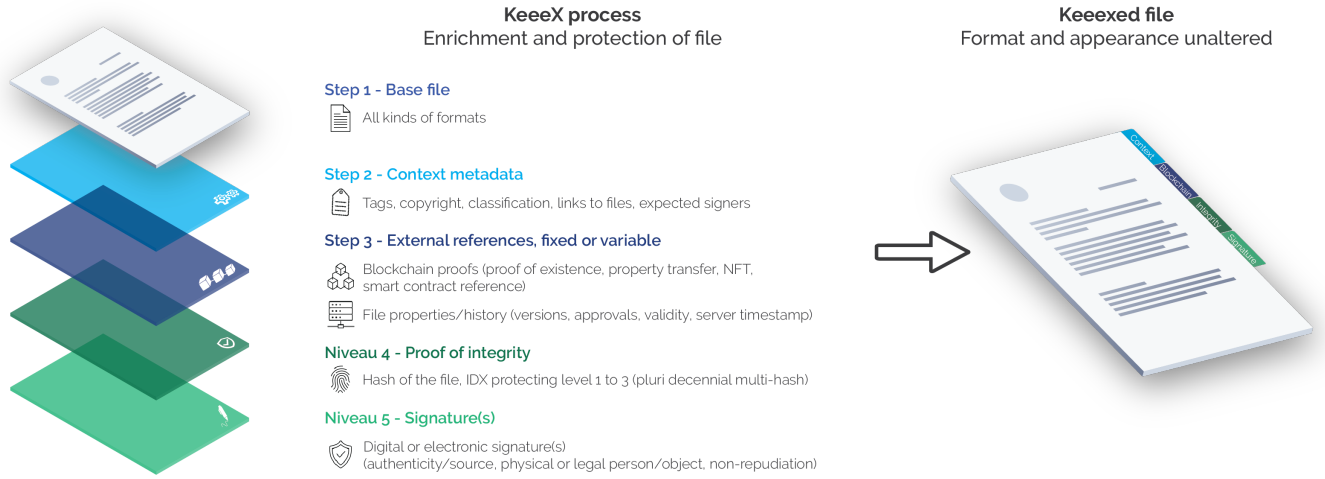
- is easily auditable and verifiable without a trusted third party, based on documents that can be easily checked by everyone,
- effectively ensures continuity with existing paper-based systems in both directions
- proves who is the owner (or "in control") of a document, and enables this possession or control to be transferred without the possibility of forgery or identity theft (an effect comparable to that achieved by Crypto Currencies or NFTs).

These elements fall within the scope of the functionalities of solutions based on the patented KeeeX technology and blockchain, whose implementation is presented in detail in this document.

The presentation follows the order of articles 8 to 18 of the model law. The original texts in US English are in italics.

Preamble - About KeeeX

This document is based on the properties of KeeeX[keeex] technology.



This technology enables any file or document to self-carry evidence of its integrity via a multihash called IDX, its provenance via one or more digital signatures, a legal timestamp and proof of existence on one or more blockchains, without altering its visible content or exploitation.

Equipped in this way, a file is protected for an unlimited period of time, and can be verified without the need for a trusted third party. It can be stored and archived without recourse to a specific infrastructure, and preserves its evidential value even on a USB key or in an e-mail.

Energy - KeeeX fully offsets its emissions

First and foremost, KeeeX has been using the Bitcoin blockchain in "Layer 2" since 2014 as the ultimate source of proof through mutualized twice-daily writings. The CO2 emissions resulting from this activity remain moderate (150T eCO2) and are included in the offsetting of all KeeeX emissions (165T eCO2) declared to the french Ademe since 2022 (including those from our servers and the KeeeX Chain blockchain).

To the best of our knowledge, this initiative makes KeeeX the only or first clean blockchain solution in the world.

Unique file identifier - self-supporting IDX

KeeeX attaches to each keeexed document a unique, tamper-proof, humanized identifier that can be used by users or in other documents to reference it. This identifier, injected into the file, is called its IDX - as in this html original:

xiroz-fybul-cotyg-vesom-sulyz-lesyc-cudez-vizid-bitam-gutev-tegup-zihon-ratok-vidus-cemin-nehoh-voxox.

Since KeeeX Fusion version 2, this IDX has been calculated using an innovative multi-hash algorithm designed to multiply its durability (bearing in mind that cryptographic fingerprints are quantum-resistant anyway).

Signatures

A keeexed file usually bears a combination of signatures of its issuer and the issuing company, making the document impossible to forge in the current state of technology, even by an engineer with control of the systems. These signatures play a considerable role in preventing the creation of forgeries, both in the transferable file itself and in the transactions issued on the register to materialize transfers of ownership and declarations of new versions.

Blockchain

These properties are complemented by a blockchain infrastructure combining :

- **mutualized** twice-daily anchor certificates on the Bitcoin blockchain as a source of "perpetual" audit trails for keeexed documents. These are in Bitcoin layer 2. KeeeX allows the anchor proofs themselves to be injected into the files (using Merkle branches), making the files completely autonomous, including access to the blockchain proofs of existence.
- **a blockchain with public observer and explorer nodes** (https://blk.keeex.me/) for high-speed execution of smart contracts without gas costs. This blockchain is also in layer 2 of Bitcoin.
- **auditable historical registers in file mode** that compensate for the weakness of blockchains in this area and provide access to documents (file versions). These registers can be used to

create auditable proof records in the form of files (easily retrieved as a zip archive) attesting to the reality and sequentiality of a process, for data that should not or cannot be recorded in blockchain. Indeed, smart contracts, whether operated on public or private blockchains, are highly unsuited to historization.

- **Smart contracts dedicated to recording variable properties**("owner", "most recent version", "transfer to paper completed", "expiry status" ...) designated in the files themselves. Ideally, these smart contracts should be operated on a publicly auditable blockchain.
- **Zero knowledge proofs injected into the files** enable only selected components to be revealed, without losing the strength of the proof.

This approach thus combines the perpetual static verifiability provided by files, the real-time protection provided by the KeeeX Chain blockchain, the auditable historization enabled by KeeeX Stories, the permanent securing of all valid states by Bitcoin and the intangible association of a tamper-proof document with its variable properties.

Verifiable link between file and registers.

In the context of MLETR, KeeeX enables the tamper-proof association of a cryptographically certified file and the recording in one or more registers (blockchain or not) of variable properties of this file, including the Titularity (who owns?) of the document. In this context :

- the information describing the register that must be queried to find out the value of a variable property is recorded in the document and made tamper-proof by KeeeX proofs.
- the property registration key used in the registry (typically a smart contract on the KeeeX Chain blockchain but possibly others) is precisely the file's unique, tamper-proof fingerprint (IDX).

These elements enable the certain tamper-proof bi-directional association between the registry and the file, and thus the verifiable and auditable change of ownership without time limit or third party of an electronically transferable title, which lifts a considerable technological lock to the implementation of MLETR.

These functionalities and services are protected by several granted CNRS patents (FR/US/EU) or a more recently registered KeeeX patent.

The document now continues with a detailed analysis of the requirements of each key MLETR article.

Article 8. Writing

> Where the law requires that information should be in writing, that requirement is met with respect to an electronic transferable record if the information contained therein is accessible so as to be usable for subsequent reference.

Support of the requirement by KeeeX

KeeeX allows the keeexed file to remain unchanged in its appearance, usage and properties, thus giving access to the native content of the original document. In addition, any metadata added to the content is accessible in plain text and extracted when the file is verified on a verifier available online such as https://services.keeex.me/verify, also archived on the Internet Archive (https://archive.org/).

Finally, since the file is a self-supporting source of evidence, it can be kept by each of its rightful owners for an unlimited period of time, with the guarantee that its integrity and origin can be verified without any time limit or trusted third party. Records of owners (having control), versions and returns to paper are made available and verifiable through smart contracts on the KeeeX Chain blockchain and/or records on KeeeX Stories (or on any public or non public blockchain, or registry guaranteed by a trusted third party, provided that the statements are also publicly auditable).

Article 9. Signature

> Where the law requires or permits a signature of a person, that requirement is met by an electronic transferable record if a reliable method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic transferable record.

Background

This article deals with two subjects: KYC on the one hand (certain identification of the natural person) and the quality of the consent to sign on the other.

KYC - Quality of signatory

The identification of the subject is carried out at the initial enrolment stage, and is repeated in a simplified way for each signature. The general subject of KYC is addressed by a number of systems and services, the simplest of which is to demonstrate receipt of an email or SMS at both enrolment and signature stages. More comprehensive enrolment processes require verification of identity papers (hologram reflection videos and technical information) and proof of life (selfie video with facial movements and expressions).

Quality of the consent form

Assessing the quality of consent to sign requires sharing the identity of the document to be signed (the certainty that what is signed is what is considered to be offered for signature) and obtaining proof without possible forgery that the user wishes to sign the text. As is often the case, obtaining a reading of the entire text through a technical device does not reinforce this proof.

Support of the requirement by KeeeX

Signatory

When KeeeX is used for enrollment, it allows a person's identity to be attested by a keeexed record for KYC purposes. This usually involves photos or scans of proof of address, identity card or other official documents. If conditions require and allow (GDPR) this can even consist of a video selfie. The enrolled user then digitally signs these proofs of identity and/or life with a digital identity under their sole control (materialized by a Bitcoin address) obtained on the spot or previously held.

When enrollment is carried out by a third party, it may result in the issuance of an electronic certificate to a natural or legal person. The KeeeX solution enables files to be signed with this type of signature, either in addition to or in place of Bitcoin identities. It is therefore compatible with the three signature levels of the eIDAS regulation (simple, advanced, qualified) depending upon the properties of the issued certificate.

In future exchanges (file-integrated signature or external consent), proof of ownership of the private key corresponding to an identity materialized by the creation of a valid digital signature will in practice suffice to identify the user.

Digital consent alone

At the first level, the proof of a user's consent to sign an action or text is obtained by a digital signature using a public key whose private key remains on sole user's control, in a context where this private key never leaves the browser, or the mobile application, or the physical device (ledger wallet) used to produce it. Such a signature is on a par with the signature on a Bitcoin transaction. Since it cannot be forged, it demonstrates that the user intended to unlock his or her private key in order to sign.

Consent with proof of life

KeeeX also makes it possible for a verifiable user to commit to a verifiable text, for example by means of a live recording (text, or better an audio or video) that mentions the idx of the signed text, and which is signed by the user's personal digital identity. In this way, the user can verify the document identifier before signing (https://services.keeex.me/verify), and having named this idx, no dispute can arise over the reality of the signed document. The digital signature is enough to prove that the signatory is indeed the person expected, as it had already been mobilized during the KYC process.

This approach prevents any attack or counterfeiting, which is not the case with any solution based on sending e-mails or SMS, which do not prevent any dispute over the content of the document offered for signature, nor signature by an unauthorized third party. It was presented by KeeeX at CES Las Vegas 2018 with a mobile app called KeeeX Signatory.

Article 10. Transferable documents or instruments

> 1 Where the law requires a transferable document or instrument, that requirement is met by an electronic record if: (a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and (b) A reliable method is used: (i) To identify that electronic record as the electronic transferable record; (ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or valid- ity; and (iii) To retain the integrity of that electronic record. 2. the electronic transferable record, including any authorized change that arises from its creation until it ceases to have any effect or validity, has remained complete and unaltered apart from any change which arises in the normal course of communication, storage and display.

Support of the requirement by KeeeX

1.a Information equality

This requirement is generally met by default, as the paper document is normally the result of printing an electronic document which constitutes the true original. Some documents are handwritten forms. In this case, a scan of a paper document also satisfies requirement 1.(a) if it is legible and complete. In addition, the scan can be enhanced to contain an electronic version of the text obtained by character recognition.

1.b(i) Identification

The keeexed file is uniquely and tamper-proof identified by its IDX (hash), which itself is signed by multiple sources, including the issuer. The existence of this document as a "Transferable Electronic Document" is attested by a dedicated smart contract on the blockchain. Note that even the issuer of the document is tamper-proof identified by its self-carried digital signature and, where applicable, as the signatory of the blockchain transaction attached to the document declaration.

1.b(ii) Control

Each version of the transferable document is tamper-proof. Each change of status (version) or rights holder is attested by the blockchain. If things are done properly, the transactions declaring these changes of state are themselves signed by the rights holder, who mobilizes his or her digital identity to do so. At any time, a file can be verified as uncorrupted, as taking part in an ETR process, can give access to the IDX of its most recent version, to the next one or to the previous one by reading in a publicly auditable blockchain. The last phase (expiration or destruction) of its use is also recorded and publicly auditable.

1.b(iii) Verifiability

The integrity and authenticity of the file are attested by keeexing, which injects verifiable self-carrying cryptographic proofs with no time limit and without third parties as explained earlier.

2. Integrity

Here again, integrity is intrinsically attested by keeexing and the blockchain. Note that if derived versions of a content are required to address presentation modalities, these versions must themselves be keeexed and refer to their original. Remember that KeeeX enables the probative revelation of part of a document through Zero Knowledge Proofs based on the use of Merkle branches injected into files. In our opinion, this feature addresses some of the needs anticipated by Requirement 2.

Item 11. Control

> 1 Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used: (a) To establish exclusive control of that electronic transferable record by a person; and (b) To identify that person as the person in control. 2 Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

Support of the requirement by KeeeX

1.(a) Exclusive control

The smart contract operated on the blockchain to trace ETR ownership guarantees that **only the person who controls the private key corresponding to the public key or address identified as having control can sign a transfer of ownership.**

1.(b) Identification of the actor

The authority that controls the private key corresponding to the public key or address identified as the current owner on the blockchain is de facto identified as the person in control, since it is the only person who can initiate a transfer or change. As this digital identity is associated with the user's physical identity obtained during enrolment, we obtain a formal identification of "the person in control".

2. Transfer of control

This requirement is addressed to the legislator. Its purpose is to ask the legislator to accept the validity of a transfer if the conditions of 1. above are met.

This is possible in our case: the preceding elements show that, under the conditions permitted by KeeeX, any document referenced as a transferable electronic document has a probative value

equal to or greater than that of paper. Indeed, the digital signatures used to sign documents and transactions on the blockchain are known to be tamper-proof. Witness the considerable funds locked up by this technology on the Bitcoin blockchain, for example.

Article 12 General reliability standard

> For the purposes of articles 9, 10, 11, 13, 16, 17 and 18, the method referred to shall be: (a) As reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances, which may include: (i) Any operational rules relevant to the assessment of reliability; (ii) The assurance of data integrity; (iii) The ability to prevent unauthorized access to and use of the system; (iv) The security of hardware and software; (v) The regularity and extent of audit by an independent body; (vi) The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method; (vii) Any applicable industry standard; or (b) Proven in fact to have fulfilled the function by itself or together with further evidence.

Support of the requirement by KeeeX

KeeeX uses a combination of its technology, which guarantees file integrity and provenance without time limits or third parties, and blockchains that are subject to permanent audit by their ecosystem and possess resilience linked to the number of nodes operated and the consensus protocol. In these terms, it satisfies the requirement for a general standard of reliability under paragraph **(b)**. However, it is possible to detail:

(i) Reliability assessment rules

An operational ETR solution is based on a number of elements: web services, portals, infrastructures, naturally subject to **SOC2** or equivalent control procedures. These elements include protected files and various blockchain components, which are themselves eligible for additional control mechanisms.

KeeeX Chain

KeeeX provides an explorer of the KeeeX Chain blockchain (https://blk.keeex.me) and offers the possibility of operating observer nodes on this blockchain, enabling permanent backup and auditing.

Anchor certificates

Anchor certificates are public and verifiable by all (check https://services.keeex.me/timestamps), and Merkle branches associated with files by these certificates can be injected into files for independent verification by any third party or service, whatever the blockchain used (Bitcoin mutualized by default - whose emissions are cleared).

File verification

Each independent file can therefore be audited at any time, by any player, by simply dragging and dropping it onto a verifier accessible via a web portal (but possibly operating in offline mode), without data transfer to a third-party service. Like other KeeeX users, a verifier can be deployed on the site of the organization operating ETR.

KeeeX Stories historization

The state of all data structures in the KeeeX Stories historization system can be audited by exporting verifiable zips containeng all the metadata files in a given Story. The validity of KeeeX Stories states themselves is assessed by layer2 anchors on the Bitcoin and KeeeX Chain blockchains.

Smart contracts for variable ETR properties

Variable properties attached to ETRs can be implemented on KeeeX Chain or on the blockchain chosen by the user, including of course EBSI (https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home). These smart contracts remain very simple and can be audited by third-party organizations. KeeeX only deploys on KeeeX Chain smart contracts whose code is published and made tamper-proof by registration on IPFS in accordance with the standards used in the Ethereum ecosystem.

(ii) Data integrity guarantee

The guarantee of data integrity is intrinsic to KeeeX.

(iii) Unauthorized access and use

KeeeX prohibits the creation of content by insiders or hackers, as the owners' private keys are under their sole control. Smart contracts forbid any writing without the ability to sign a valid transaction. Our portals are authorized or accessible by digital signature.

(iv) Hardware and software security

Our servers are hosted by OVH on machines with encrypted disks and accessed by certificate-based signatures. Security updates are immediate and version updates are weekly. Our systems are subject to 24/7 real-time monitoring and automated cross-site backups.

(v) Independent audit

We have our processes and systems audited on a regular basis.

(vi) Certification

KeeeX has held the France Cybersécurité label since 2018, renewed in 2022.

Our security practices have been validated by numerous industrial groups (CAC40: Société Générale, Engie, Enedis, EDF, SNCF...).

(vii) Applicable standards

Services operating an ETR solution based on KeeeX technology can be certified according to all applicable SOC or ISO schemes.

For its own services, and independently of the audit procedures listed above, KeeeX complies with state-of-the-art best practices (Services Node JS, React, TypeScript...).

Article 13 Indication of time and place in electronic transferable records

> Where the law requires or permits the indication of time or place with respect to a transferable document or instrument, that requirement is met if a reliable method is used to indicate that time or place with respect to an electronic transferable record.

KeeeX support of the time requirement

The KeeeX metadata language and system offer by default:

- injection of the system date into files, this information being locked in the file
- injection into the file of the GPS time stamp signed by the satellite when this information is available (cell phone, vehicle)
- obtaining a proof of time (TSR RFC 3161) for the file IDX, which may be eIDAS-qualified depending on the level required
- obtaining a blockchain anchor for the file IDX, providing a block date. The anchor is usually multiple, since in the ETR context the file alone is anchored once, and all variable property entries in separate registers give rise to secondary anchors (for owner, most recent version, status).
- if necessary, TSR is injected into files, making this information independently verifiable without third parties (albeit at the cost of a file size overload of up to 4 kilobytes).
- injection of a merkle branch into the file, making the blockchain anchor independently verifiable without third parties.

KeeeX support of the location requirement

Some documents, such as photos or videos, allow geographic information to be recorded. KeeeX's metadata language[metadata] offers by default:

- replication of information like that provided by a regular GPS in KeeeX metadata injected into any file format
- injection of seldom available geographic information for automated processing: altitude, signal accuracy, GPS timestamp, etc.

As mentioned above, KeeeX enables positional information to be attached to any file in any format, as required. In particular, this enables the inclusion in documents or variable properties of symbolic location coding such as the GLN (Global Location Number) proposed by GS1: https://www.gs1.fr/identifier-vos-entites-entreprises-lieux

The metadata language also enables arbitrary semantic and content properties (classification, licenses, etc.) to be injected into ETRs.

Article 14. Place of business

> *1. A location is not a place of business merely because that is: (a) Where equipment and technology supporting an information system used by a party in connection with electronic transferable records are located; or (b) Where the information system may be accessed by other parties. 2. The sole fact that a party makes use of an electronic address or other element of an information system connected to a specific country does not create a presumption that its place of business is located in that country.

In our view, this article has only one legal scope. GS1 GLNs for instance cover the semantics of "Place of Business".

Article 15. Endorsement

> Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements set forth in articles 8 and 9.

Support of the requirement by KeeeX

Not all parties can always be present in an active digital signature process at the time a document is produced. KeeeX therefore supports delayed signature in both simple and delegated modes.

As a technical reminder, the public key of the expected signatories of a file is included in the file before it is locked by keeexing, thus preventing any future signature claim by an unintended third party. The signature of a document by a third party not initially expected can only take place in a new version of the file, usually cryptographically chained with the previous one, and recorded in a version history that can be traversed in both directions and audited.

However, there are cases where the digital identity of the document's real signatory (defined by his or her public key) is unknown at the time of file creation, as it is involved in a signature delegation mechanism granted to a role (Chairman, Director, Driver, etc.). In this case, KeeeX's public key can be used to designate the identity of a third-party endorser for this expected role in a file signature. This third-party endorser can then, with no time limit, inject into the file a signed

declaration of the real identity mobilized for this role in this signature. The identity holder can then inject his own signature for the requested element.

In summary KeeeX's metadata language[metadata] allows to:

- inject an optional endorsement authority declaration for a signature into the file when it is keeexed
- inject into the file the declaration of a designated real signatory identity signed by the previous endorsing authority
- inject into the file the signature by the designated identity.

This functionality can be provisioned for multiple endorsements. The resulting file then carries its own proof of endorsement. The process complies with the requirements of articles 8 (Writing) and 9 (Signature).

Article 16. Amendment

> Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such.

This article first sets out the possibility that a transferable electronic document may have several versions. It then states that changes applied between two versions must be documented.

However, the text remains ambiguous as to the scope of the version concept in the context of variable properties attached to an ETR (notably the owner): is this information "inside" the ETR or outside?

Let's start by considering that the patented KeeeX process applies equally well to all file formats.

KeeeX support for versioning requirements

KeeeX enables an actor to :

- open a file with the certainty that it's the most recent version, and with the right to modify it (for instance using our MLETR smart contract)
- create a new version with the editor of their choice (this action could be reserved for the owner of the file alone, or for an editor identified in the file by their digital signature)
- keeex this new version, then publish it while retaining control rights
- transfer ownership if necessary.

File version chaining and browsing is natively bidirectional in a smart contract and/or with public context metadata in KeeeX Stories.

KeeeX support for change tracking requirements

As KeeeX is compatible with all file formats, it natively supports office formats that implement revision mode for tracking changes. These files can be Keeexed as they are, and thus enable change tracking. This approach avoids the unnecessary use of pdf files.

In particular, when the file format does not support change tracking (pdf), the KeeeX metadata language allows for using the description property, or user-defined properties, to inform about the nature of the changes made. On a technical level, this can go as far as injecting into the file the results of a comparison (diff) between the two versions.

KeeeX support for tracking changes to variable properties

The keeexed ETR contains a tamper-proof designation for the registry used to track changes in the value of a variable property, such as its owner, the most recent known version of the file, its status (active, expired) etc.

Each of these registries, either smart-contract based or not, clearly identifies the current value of a property as having modified the previous value. Successive values are logged in both directions. In cases where contextual metadata must accompany this historization, the use of KeeeX Stories may prove useful.

Article 17. Replacement of a transferable document or instrument with an electronic transferable record

> *1. An electronic transferable record may replace a transferable document or instrument if a reliable method for the change of medium is used. 2. For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the electronic transferable record. 3. Upon issuance of the electronic transferable record in accordance with para- graphs 1 and 2, the transferable document or instrument shall be made inoperative and ceases to have any effect or validity. 4. A change of medium in accordance with paragraphs 1 and 2 shall not affect the rights and obligations of the parties.

Support of the requirement by KeeeX

The most immediate way to meet the obligations of article 17 is to

- scan the paper original held by the controlling party (new support)
- keeex the scan obtained, integrating the information describing the procedure (paragraphs 1 and 2)
- write on the original the scan IDX (for example, the idx of this original html: xiroz-fybul-cotyg-vesom-sulyz-lesyc-cudez-vizid-bitam-gutev-tegup-zihon-ratok-vidus-cemin-nehoh-voxox). This IDX is obtained during keeexing or by simple drag and drop on the KeeeX verifier https://s.keeex.me/verify.

- write on the original the information enabling access to the chain of custody of the ETR resulting from the media change
- mention on the original the loss of its validity in favor of the ETR (paragraph 3).

If necessary, a new scan of the first page of the original bearing the above entries can be integrated into the ETR traceability registry (using KeeeX Story) if enabled.

Article 18. Replacement of an electronic transferable record with a transferable document or instrument

> *1. A transferable document or instrument may replace an electronic transferable record if a reliable method for the change of medium is used. 2. For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the transferable document or instrument. 3. Upon issuance of the transferable document or instrument in accordance with paragraphs 1 and 2, the electronic transferable record shall be made inoperative and ceases to have any effect or validity. 4. A change of medium in accordance with paragraphs 1 and 2 shall not affect the rights and obligations of the parties.

The need for a "back to paper" backup procedure is attested and had been implemented by KeeeX in 2017 within a pilot carried out by KeeeX for CMA-CGM with the BuyCo company.

Support of the requirement by KeeeX

To meet the requirements of article 18 KeeeX enables:

- to print the ETR in the version verified as the most recent (automatic or manual action) (article 1)
- the transfer to the paper file of elements (including its IDX, or a hash encoded in a humanized way) giving access to the traceability chain of the digital file to date (manual action or potentially automated by the printer) (articles 1 and 2)
- the invalidation of the ETR on its traceability chain, with mention of the change of medium ("back to paper" backup procedure) (article 3). This is achieved by changing the value of a "back to paper" variable property, which the registry prohibits from being reset.

Conclusion

The KeeeX technology associated with a MLETR smart contract operated on the KeeeX blockchain implements all the conditions defining MLETR. This set of services is accessible via API and a demonstration portal. Some of KeeeX's know-how in transferring ownership of transferable documents is in production and visible in the NFT context on the KeeeX NFT service (https://nft.keeex.art).

Appendix: KeeeX

The KeeeX[keeex] technology allows for embedding probative metadata within files that warrant integrity (using hashes), origin (using signatures), time (up to RFC3161) and existence (using blockchain anchoring). This is possible with no perceivable functional alteration to humans in a vast majority of files, with a few exceptions being file formats that do not support comments or metadata (e.g. txt, csv) but still remain processable. This universal digital signature scheme is patented. Verification is extremely simple since it only relies upon the KeeeX metadata language[metadata] and not the format of the file itself.

Using KeeeX the file's hash is computed so as to account for all file bytes except the hash itself in all it's occurrences and the signatures of this hash. The Bitcoin addresses of signatories or delegators are embedded in the file prior to hash computation meaning that a file cannot be resigned. No addition to the file stays undetected which improves over most existing electronic signature algorithms (however later extensions are possible using explicit multi-phase keeexing).

The KeeeX metadata language provides support for properties (e.g. description, author, copyright, original file name, partial disclosure proofs) as well as cryptographic references to other files. If requested a keeexed file may also embed a Merkle branch leading to Data attached to a transaction over a choice of the Bitcoin network (OP_Return text), Ethereum smart contract (as an abi call parameter) or any other data aware blockchain. The file may also embed an RFC3161 timestamp.

The point here is that a keeexed file is totally autonomous for proving integrity, provenance and date, and when requested only requires a blockchain explorer to prove existence. The current file you're reading demoes the technology and can be verified easily in many places (for instance on https://services.keeex.me/verify), including on some snapshots by the way-back machine (or Internet Archive) https://archive.org/. Check this 2019 snapshot for instance : https://web.archive.org/web/20190226173726/https://services.keeex.me/verify/

Credits

Author : Laurent Henocque for KeeeX - [1NkZmqDcTKmAWJaJM957HJo84CFHe5JXZn](https://www.google.com/search?&q=1NkZmqDcTKmAWJaJM957HJo84CFHe5JXZn

Translations assisted by DeepL.com.

The original html version of this file was produced with https://kaaas.keeex.me and has idx :

xiroz-fybul-cotyg-vesom-sulyz-lesyc-cudez-vizid-bitam-gutev-tegup-zihon-ratok-vidus-cemin-nehoh-voxox

This file should be checked at https://s.keeex.me/verify

References:

- MLETR:https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf
- UNCITRAL:https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
- keeex:https://keeex.me
- metadata:https://keeex.me/wp-content/uploads/KeeeX-Metadata-Statement-Specification-V2.0-keeexed-xuzah-

This keeexed file is signed by 1NkZmqDcTKmAWJaJM957HJo84CFHe5JXZn and must be verified on https://services.keeex.me/verify. Its idx (hash) is: xifin-zumep-ryzin-titac-todal-zelyf-fipun-vaged-lohov-fihyr-zopyr-dekal-zutyb-hasag-punyh-dakod-saxyx