Implémentation du Titre Transférable Electroniquement selon la MLETR

Abstract

La loi type de la **CNUDCI** sur les **Titres Transférables Électroniquement (TTE)** dite **MLETR** (**UNCITRAL Model Law on Electronic Transferable Records (2017))** vise à définir une version dématérialisée fiable de documents ayant des propriétés égales ou supérieures au papier : non substituables, transférables comme exemplaire original unique, signés, approuvés, versionnés. Le texte prévoit également le suivi des modifications et l'aller retour entre version papier et version numérique.
Ce document décrit l'implémentation par KeeeX de la MLETR en argumentant de façon très précise sur la façon dont la technologie et l'approche **KeeeX** satisfont à chacune des exigences formulées dans la loi type.

Author: Laurent Henocque

Introduction

La loi type MLETR vise à définir les exigences applicables à une version dématérialisée fiable de documents ayant des propriétés égales ou supérieures au papier : non substituables, transférables comme exemplaire original unique, signés, approuvés, versionnés. Le texte prévoit également le suivi des modifications et le passage de version papier à version numérique et réciproquement.

La proposition de cette loi type visait à inciter les gouvernements à accepter l'utilisation de documents numériques dans le contexte notamment du commerce international, encore trop peu dématérialisé. De nombreux pays ont déjà adapté leur règlementation à cet effet. En France, un rapport intitulé "Accélérer la digitalisation des activités de financement du commerce international" a été remis au gouvernement en Juillet 2023. Ce rapport indique que le commerce international n'est encore aujourd'hui dématérialisé que de façon extrêmement marginale.

Cet article décrit l'implémentation par KeeeX[KeeeX] de la MLETR (*UNCITRAL Model Law on Electronic Transferable Records (2017)* - Loi type de la CNUDCI sur les documents électroniques transférables (2017)).

Il s'appuie sur les Chapitres II. Dispositions relatives à l'équivalence fonctionnelle (Chapter II. Provisions on functional equivalence) et III. Utilisation d'enregistrements électroniques transférables (Chapter III. Use of electronic transferable records) détaillés dans le e-book explicatif officiel [MLETR] obtenu sur le site UNCITRAL[UNCITRAL].

Le titulaire des droits attachés à la possession d'un titre détient potentiellement une valeur économique considérable (comme c'est le cas dans la supply chain). Cela demande de proposer une solution :

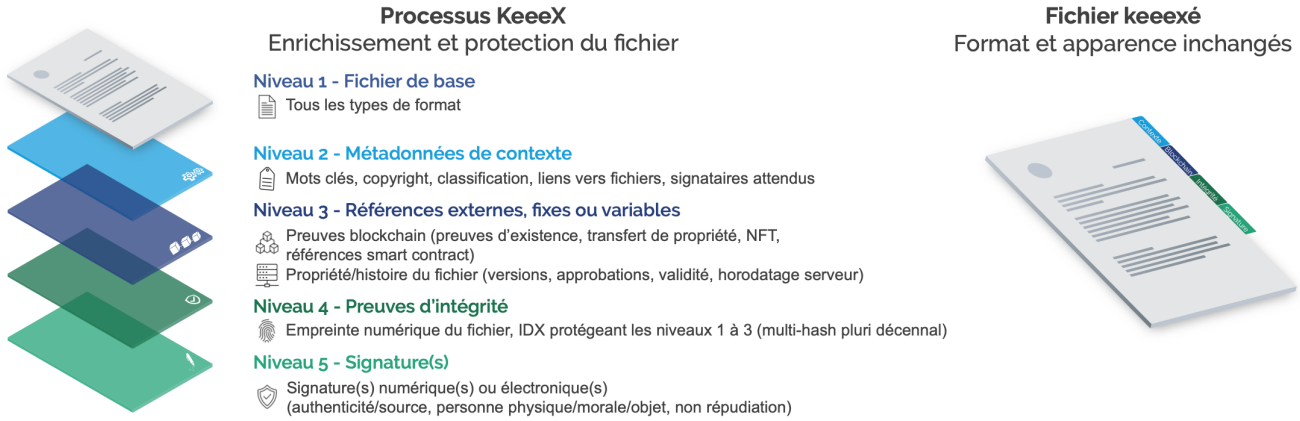
- facilement auditable et vérifiable sans tiers de confiance appuyée sur des documents facilement vérifiables par tous,
- qui réalise de façon efficace la continuité avec l'existant papier dans les deux sens
- qui prouve qui est propriétaire (ou "en contrôle") d'un document et permettre de transférer cette possession ou contrôle sans possibilité de contrefaçon ou usurpation d'identité (un effet comparable à ce qui est atteint par les NFT).

Ces éléments recouvrent largement les fonctionnalités des solutions issues de la technologie brevetée et de la blockchain KeeeX, dont ce document présente de façon détaillée la mise en oeuvre.

La présentation suit l'ordre des articles 8 à 18 de la loi type. Les textes originaux en anglais US sont en italiques. Ils sont traduits pour en faciliter la lecture.

Préambule - Au sujet de KeeeX

Ce document s'appuie sur les propriétés de la technologie KeeeX[keeex].



Cette technologie permet que tout fichier ou document auto-porte sans altération de son contenu visible des preuves de son intégrité par un multihash appelé IDX, de sa provenance par

une ou plusieurs signatures numériques, d'un horodatage légal et de preuves d'existence sur une ou plusieurs blockchains.

Ainsi équipé, un fichier est protégé sans limite de durée et vérifiable sans tiers de confiance. Il peut être conservé et archivé sans recours à une infrastructure spécifique et préserve sa force de preuve même sur une clé USB ou dans un mail.

Energie - KeeeX compense intégralement ses émissions

Avant toute chose, KeeeX utilise depuis 2014 la blockchain Bitcoin "en layer 2" comme source ultime de preuve par des écritures bi-quotidiennes mutualisées. Les émissions de CO2 résultant de cette activité restent modérées (150T eCO2) et sont comprises dans la compensation de l'intégralité des émissions de KeeeX (165T eCO2) déclarées à l'Adème depuis 2022 (dont celles de nos serveurs et de la blockchain KeeeX Chain).

Cette initiative fait de KeeeX à notre connaissance la seule ou première solution blockchain compensée au monde.

L'identifiant unique du fichier - son IDX autoporté

KeeeX attache à chaque document keeexé un identifiant unique inviolable et humanisé pouvant être utilisé par les usagers ou dans d'autres documents pour le référencer. Cet identifiant injecté dans le fichier est appelé son IDX - comme ici celui de cet original html :

xupes-dohik-dodyn-lecut-pizir-pasyr-ninyv-cizos-ryzys-tynac-lycot-fadel-mofik-bagan-lyvum-tehat-zaxux.

Cet IDX est calculé depuis la version 2 de KeeeX Fusion à l'aide d'un algorithme de multi-hash innovant conçu pour démultiplier sa durabilité (sachant que les empreintes cryptographiques sont de toutes façon résistantes au quantique).

Les signatures

Un fichier keeexé porte habituellement une combinaison de signatures de son émetteur et de la raison sociale émettrice qui rendent le document impossible à contrefaire dans l'état actuel de la technologie, y compris par un ingénieur ayant le contrôle des systèmes. Ces signatures jouent un rôle considérable pour interdire la création de faux, tant au niveau du fichier transférable lui même que dans les transactions émises sur le registre pour matérialiser les transferts de propriété et les déclarations de versions nouvelles.

Blockchain

Ces propriétés sont complétées par une infrastructure blockchain combinant :

- **des certificats d'ancrage mutualisés** bi-quotidiens sur la blockchain Bitcoin comme source de piste d'audit "perpétuelles" pour les documents keeexés. Ces derniers sont en layer 2 de

Bitcoin. KeeeX permet que les preuves d'ancrage soient elles même injectées dans les fichiers (par l'utilisation de branches de Merkle) ce qui rend les fichiers totalement autonomes y compris jusqu'à l'accès aux preuves d'existence.

- **une blockchain à noeuds observers et explorer publics** (https://blk.keeex.me/) pour exécuter des smart contracts à haute vitesse sans frais de gaz. Cette blockchain est également en layer 2 de Bitcoin.
- **des registres historisés auditables en mode fichier** qui compensent la faiblesse des blockchains sur cet axe et permettent de donner accès à des documents (versions de fichier). Ces registres permettent de créér les dossiers de preuve auditables sous forme de fichiers attestant de la réalité et de la séquentialité d'un processus, pour des données ne devant ou ne pouvant être inscrites en blockchain. En effet les smart contracts, qu'ils soient opérés sur des blockchains publiques ou privées, sont très inadaptés à l'historisation.
- **des smart contracts dédiés à l'enregistrement de propriétés variables** ("propriétaire", "version la plus récente", "transfert vers le papier réalisé", "statut d'expiration" ...) désignés dans les fichiers eux mêmes. Ces smart contracts doivent idéalement être opérés sur une blockchain publiquement auditable.
- **des preuves zero knowledge injectées dans les fichiers** permettant de n'en révéler que des composants choisis sans perdre la force de preuve.

Cette approche combine ainsi la vérifiabilité statique perpétuelle portée par les fichiers, la protection temps réel apportée par la blockchain KeeeX, l'historisation auditable permise par KeeeX Stories, la sécurisation permanente de l'ensemble des états valides par Bitcoin et l'association intangible d'un document inviolable à ses propriétés variables.

Liaison vérifiable entre le fichier et les registres.

Dans le contexte de la MLETR, KeeeX permet d'associer de façon inviolable un fichier certifié cryptographiquement et l'enregistrement dans un ou plusieurs registres (blockchain ou non) de propriétés variables de ce fichier dont la Titularité (qui est propriétaire?) du document. Dans ce contexte :

- l'information décrivant le registre à interroger pour connaître la valeur d'une propriété variable est enregistrée dans le document et rendue inviolable par les preuves KeeeX.
- la clé d'enregistrement de la propriété utilisée dans le registre (typiquement un smart contract sur la blockchain KeeeX Chain) est précisément l'empreinte unique et inviolable (IDX) du fichier.

Ces éléments permettent l'association bi-directionnelle inviolable certaine entre le registre et le fichier, et ainsi le changement de propriétaire vérifiable et auditable sans limite de durée ni tiers d'un titre transférable électroniquement, ce qui lève un verrou technologique considérable à la mise en oeuvre de la MLETR.

Ces fonctionnalités et services sont protégés par plusieurs brevets CNRS obtenus (FR/US/UE) ou déposés (KeeeX).

Le document poursuit maintenant par une analyse détaillée des exigences de chaque article clé de la MLETR.

Article 8. *Writing* - L'écrit

> *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.*

> Lorsque la loi exige que l'information soit consignée par écrit, cette exigence est satisfaite en ce qui concerne un document transférable électronique si l'information qu'il contient est accessible de manière à pouvoir être consultée ultérieurement.

Support de l'exigence par KeeeX

KeeeX permet que le fichier keeexé reste inchangé dans son apparence, son usage et ses propriétés, donc donne accès au contenu natif du document d'origine. De plus les métadonnées éventuelles ajoutées au contenu sont accessibles en texte clair et extraites lors de la vérification du fichier sur un vérifieur disponible en ligne comme https://services.keeex.me/verify, également archivé sur l'Archive d'Internet (https://archive.org/).

Enfin, le fichier étant autoporteur de ses preuves peut être conservé par chacun de ses ayants droit sans limite de durée, sous la garantie de pouvoir constater son intégrité et son origine sans limite de durée ni tiers de confiance. Les registres des propriétaires (ayant le contrôle), des versions et des retours au papier sont rendus disponibles et vérifiables par le biais de smart contracts sur la blockchain KeeeX Chain et/ou d'enregistrements sur KeeeX Stories (ou sur toute blockchain publique ou non, ou registre garanti par un tiers de confiance, pourvu que les états en soient également publiquement auditables).

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.*

> Lorsque la loi exige ou autorise la signature d'une personne, cette exigence est satisfaite par un document transférable électronique si une méthode fiable est utilisée pour identifier cette personne et pour indiquer son intention concernant l'information contenue dans le document transférable électronique.

Contexte

Cet article touche deux sujets : le KYC d'une part (identification certaine de la personne physique) et la qualité du consentement à signer d'autre part.

KYC - Qualité du signataire

L'identification du sujet se fait d'une part dans une étape initiale d'enrôlement, et se répète de façon habituellement simplifiée lors de chaque signature. Le sujet général du KYC est traité par de nombreux dispositifs ou services, le plus simple consistant à démontrer la bonne réception d'un email ou d'un SMS aussi bien au moment de l'enrôlement qu'à celui de la signature. Des processus d'enrôlement plus complets demandent la vérification de papiers d'identité (vidéos de reflets des hologrammes et informations techniques) et des preuves de vie (vidéo selfie avec mouvements et expressions du visage).

Qualité du consentement à signer

L'évaluation de la qualité du consentement à signer requiert que soit partagée l'identité du document à signer (la certitude que ce qui est signé est ce qui est considéré comme proposé à la signature) et que soit obtenue une preuve sans contrefaçon possible que l'usager souhaite signer le texte. Obtenir comme on le voit souvent la lecture de l'intégralité du texte par un artifice technique ne renforce pas cette preuve.

Support de l'exigence par KeeeX

Signataire

Lors de son enrôlement KeeeX permet que l'identité d'une personne soit attestée par un enregistrement keeexé à effet de KYC. Habituellement il peut s'agir de photos ou scans de preuves de domicile, carte d'identité ou autres documents officiels. Si les conditions le demandent et le permettent (RGPD) cela peut même consister en une vidéo selfie. L'usager enrôlé signe alors numériquement ces preuves d'identité et/ou de vie par une identité numérique sous son seul contrôle (matérialisée par une adresse Bitcoin) obtenue sur le moment ou préalablement détenue.

Lorsque l'enrôlement est réalisé par un tiers, il peut aboutir à la délivrance d'un certificat électronique à une personne physique ou morale. La solution KeeeX permet de signer les fichiers avec ce type de signatures en complément ou remplacement des identités Bitcoin. Elle est donc compatible avec les trois niveaux de signature du règlement eIDAS (simple, avancé, qualifié).

Dans les échanges futurs (signature intégrée au fichier ou consentement externe), la preuve de détention de la clé privée correspondant à cette identité matérialisée par la création d'une signature numérique valide suffira en pratique à identifier l'usager.

Consentement numérique seul

Au premier niveau, la preuve du consentement d'un usager à signer une action ou un texte est obtenue par sa signature numérique au moyen d'une clé publique dont il est le seul à pouvoir

déverrouiller la clé privée, dans un contexte qui fait que cette clé privée ne quitte jamais le navigateur, ou l'application mobile ou enfin le dispositif physique (ledger wallet) ayant servi à la produire. Une telle signature est du même niveau que la signature d'une transaction Bitcoin. Ne pouvant être contrefaite, elle démontre que l'usager a eu l'intention de déverrouiller sa clé privée pour signer.

Consentement avec preuve de vie

L'engagement d'un usager certain sur un texte certain est permis également par KeeeX par exemple par un enregistrement (texte, audio ou vidéo) qui fasse référence par son idx à un contenu ainsi désigné de façon certaine, cet enregistrement étant signé par son identité numérique personnelle. De la sorte, l'usager a le moyen de vérifier l'identifiant du document avant signature (https://services.keeex.me/verify) et en ayant nommé cet idx aucun litige ne peut émerger sur la réalité du document signé. La signature numérique suffit à prouver que le signataire est bien la personne attendue car elle avait déjà été mobilisée lors du KYC.

Cette approche interdit toute attaque ou contrefaçon, ce qui n'est le cas d'aucune solution à base d'envoi de mail ou de SMS qui n'empêchent ni un litige sur le contenu du document proposé à signature ni la signature par un tiers non autorisé.

Article 10. *Transferable documents or instruments* - Documents ou titres transférables

> *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.*

> 1. Lorsque la loi exige un document ou un instrument transférable, cette exigence est satisfaite par un document électronique si : (a) le document électronique contient l'information qui devrait être contenue dans un document ou un instrument transférable ; et (b) Une méthode fiable est utilisée : (i) Pour identifier ce document électronique comme étant le document électronique transférable ; (ii) pour rendre ce document électronique susceptible d'être contrôlé depuis sa création jusqu'à ce qu'il cesse d'avoir un effet ou une validité ; et (iii) conserver l'intégrité de ce document électronique.
> 2. le document électronique transférable, y compris toute modification autorisée survenant depuis sa création jusqu'à ce qu'il cesse d'avoir un effet ou une validité, est

> resté complet et inaltéré, à l'exception de toute modification survenant dans le cours normal de la communication, du stockage et de l'affichage.

Support de l'exigence par KeeeX

1.a Égalité d'information

Cette exigence est généralement atteinte par défaut, le document papier étant normalement le résultat de l'impression d'un document électronique qui en constitue le véritable original. Certains documents sont des formulaires portant des mentions manuscrites. Dans ce cas le scan d'un document papier satisfait également l'exigence 1.(a) s'il est lisible et complet. Le scan qui plus est peut être amélioré pour contenir une version électronique du texte obtenue par reconnaissance de caractères.

1.b(i) Identification

Le fichier keeexé est identifié de manière unique et inviolable par son IDX (hash), lui même signé par de multiples sources dont son emetteur. L'existence de ce document en tant que "Document Electronique Transférable" est attestée par un smart contract dédié sur la blockchain. Noter que même l'emetteur du document est identifié de façon inviolable par sa signature numérique auto-portée et le cas échéant comme signataire de la transaction blockchain attachée à la déclaration du document.

1.b(ii) Contrôle

Chaque version du titre transférable est inviolable. Chaque changement d'état (version) ou de détenteur des droits est attesté par la blockchain. Si les choses sont bien faites, les transactions déclarant ces changements d'état sont elles même signées par le détenteur des droits, qui mobilise pour ce faire son identité numérique. A tout moment, un fichier peut être vérifié comme non corrompu, comme participant à un process de TTE, peut donner accès à l'IDX de sa version la plus récente, à la suivante ou à la précédente par lecture dans une blockchain publiquement auditable. La dernière phase de son utilisation est également enregistrée et publiquement auditable.

1.b(iii) Vérifiabilité

L'intégrité et l'authenticité du fichier sont attestées par le keeexage, qui y injecte des preuves cryptographiques auto-portées vérifiables sans limite de durée et sans tiers.

2. Intégrité

Ici encore l'intégrité est attestée de façon intrinsèque par le keeexage et la blockchain. Noter que si des versions dérivées d'un contenu sont requises pour adresser des modalités de présentation, ces versions doivent elles mêmes être keeexées et faire référence à leur original. Rappelons que KeeeX permet la révélation probante d'une partie d'un document par des preuves Zero Knowledge reposant sur l'utilisation de branches de Merkle elles mêmes injectées dans les

fichiers. Cette fonctionnalité adresse il nous semble une partie des besoins anticipés par l'exigence 2.

Article 11. *Control* - Contrôle

> *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.*

> 1. Lorsque la loi exige ou autorise la possession d'un document ou d'un instrument transférable, cette exigence est satisfaite en ce qui concerne un document électronique transférable si une méthode fiable est utilisée : (a) pour établir le contrôle exclusif de ce document électronique transférable par une personne ; et (b) pour identifier cette personne comme étant la personne ayant le contrôle.
> 2. Lorsque la loi exige ou autorise le transfert de la possession d'un document ou d'un instrument transférable, cette exigence est satisfaite en ce qui concerne un document électronique transférable par le transfert du contrôle de ce document électronique transférable.

Support de l'exigence par KeeeX

1.(a) Contrôle exclusif

Le smart contract opéré sur la blockchain pour tracer la titularité du TTE garantit que **seule la personne qui contrôle la clé privée correspondant à la clé publique ou à l'adresse identifiée comme ayant le contrôle peut signer un transfert de propriété.**

1.(b) Identification de l'acteur

L'autorité qui contrôle la clé privée correspondant à la clé publique ou à l'adresse identifiée comme étant le propriétaire actuel sur la blockchain est de facto identifiée comme étant la personne qui a le contrôle puisqu'elle est la seule personne à pouvoir initier un transfert ou un changement. Comme cette identité numérique est associée à l'identité physique de l'usager obtenue lors de l'enrôlement, on obtient une identification formelle de "la personne ayant le contrôle".

2. Transfert du contrôle

Cette exigence s'adresse au législateur. Elle vise à demander d'accepter la validité d'un transfert si les conditions du 1. ci dessus sont satisfaites. C'est possible dans notre cas : les éléments qui précèdent montrent que sous les conditions permises par KeeeX, tout document référencé

comme document électronique transférable possède une force probante égale ou supérieure à celle du papier. En effet les signatures numériques utilisées pour signer les documents et les transactions réalisées dans la blockchain ont une résistance à la contrefaçon connue aujourd'hui comme inviolable. En témoignent les fonds considérables verrouillés par cette technologie sur la blockchain Bitcoin par exemple.

Article 12 *General reliability standard* - Standard général de fiabilité

> *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.*

> Aux fins des articles 9, 10, 11, 13, 16, 17 et 18, la méthode visée doit être : (a) Aussi fiable que possible pour l'accomplissement de la fonction pour laquelle la méthode est utilisée, à la lumière de toutes les circonstances pertinentes, qui peuvent comprendre : (i) Toute règle opérationnelle pertinente pour l'évaluation de la fiabilité ; (ii) La garantie de l'intégrité des données ; (iii) La capacité d'empêcher tout accès et toute utilisation non autorisés du système ; (iv) La sécurité du matériel et des logiciels ; (v) La régularité et l'étendue de l'audit par un organisme indépendant ; (vi) l'existence d'une déclaration d'un organisme de contrôle, d'un organisme d'accréditation ou d'un système volontaire concernant la fiabilité de la méthode ; (vii) toute norme industrielle applicable ; ou (b) Il est prouvé en fait qu'elle a rempli la fonction par elle-même ou avec d'autres preuves.

Support de l'exigence par KeeeX

KeeeX utilise une combinaison de sa technologie, qui garantit intégrité et provenance des fichiers sans limite de durée ni tiers et de blockchains qui sont soumises à un audit permanent par leur écosystème et possèdent une résilience liée au nombre de noeuds opérés et au protocole de consensus. Selon ces termes, elle satisfait l'exigence de standard général de fiabilité par l'alinéa **(b)**. Toutefois il est possible de détailler :

(i) Règles d'évaluation de la fiabilité

Une solution opérationnelle de TTE repose sur un certain nombre d'éléments : web services, portails, infrastructures naturellement soumis aux **procédures de contrôle SOC2** ou équivalents. Ces éléments mettent en oeuvre des fichiers protégés et des composants blockchain divers quand à eux éligibles à des mécanismes de contrôle supplémentaires.

KeeeX Chain

KeeeX propose un explorer de la blockchain KeeeX Chain (https://blk.keeex.me) et offre la possibilité d'opérer des nœuds observers sur cette blockchain permettant un backup et un audit permanent.

Certificats d'ancrage

Les certificats d'ancrage sont publics et vérifiables par tous, et les branches de Merkle associées aux fichiers par ces certificats peuvent être injectées dans les fichiers pour une vérification indépendante de tout tiers ou service, et ce quelle que soit la blockchain utilisée (Bitcoin mutualisé par défaut - dont les émissions sont compensées).

Vérification des fichiers

Chaque fichier indépendant peut donc être audité à tout moment, par tout acteur, par simple glisser déposer sur un vérifieur accessible sur un portail web mais fonctionnant en mode offline, sans transfert de données vers un service tiers. A l'instar d'autres utilisateurs de KeeeX, un vérifieur peut être déployé sur le site de l'organisation opérant des TTE.

Historisation KeeeX Stories

L'état de l'ensemble des structures de données du système d'historisation KeeeX Stories est auditable par export de zips vérifiables en mode fichier et verrouillé en layer 2 de Bitcoin.

Smart contracts des propriétés variables des TTE

Les propriétés variables attachées aux TTE peuvent être implémentées sur KeeeX Chain ou sur la blockchain choisie par l'usager, dont bien sûr EBSI (https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home). Ces smart contracts restent très simples et sont auditables par des organismes tiers. KeeeX ne déploie sur KeeeX Chain que des smart contracts dont le code est publié et rendu inviolable par une inscription sur IPFS selon les standards en usage dans l'écosystème Ethereum.

(ii) Garantie d'intégrité des données

La garantie d'intégrité des données est intrinsèque à KeeeX

(iii) Accès et utilisation non autorisée

KeeeX interdit toute création de contenu par usurpation d'identité issue d'un insider ou hacker car les clés privées des propriétaires sont sous leur seul contrôle. Les smart contracts interdisent toute écriture si l'on ne détient pas la capacité de signer une transaction valide. Nos portails sont permissionnés ou accessibles par signature numérique.

(iv) Sécurité du matériel et des logiciels

Nos serveurs sont hébergés chez OVH sur des machines à disques chiffrés et accédés par des signatures à base de certificats. Les mises à jour de sécurité sont immédiates et les mises à jour de versions sont hebdomadaires. Nos systèmes font l'objet d'un monitoring temps réel 24/7 et de backups automatisés croisés et multi sites.

(v) Audit indépendant

Nous faisons auditer nos processus et systèmes de façon régulière.

(vi) Attestation

KeeeX détient le label France Cybersécurité depuis 2018, renouvelé en 2022.

Nos pratiques de sécurité ont été validées par de nombreux groupes industriels (CAC40 : Société Générale, Engie, Enedis, EDF, SNCF...).

(vii) Normes applicables

Les services opérant une solution de TTE reposant sur la technologie KeeeX peuvent être certifiés selon tous les schémas SOC ou ISO applicables.

Pour ses propres services, et indépendamment des procédures d'audit listées plus haut, KeeeX se conforme aux meilleures pratiques de l'état de l'art (Services Node JS, React, TypeScript...).

Article 13 *Indication of time and place in electronic transferable records* - Indication du temps et du lieu dans les enregistrements électroniques transférables

> *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.*

> Lorsque la loi exige ou autorise l'indication de l'heure ou du lieu en ce qui concerne un document ou un instrument transférable, cette exigence est satisfaite si une méthode fiable est utilisée pour indiquer cette heure ou ce lieu en ce qui concerne un document transférable électronique.

Support de l'exigence par KeeeX relativement au temps

Le langage de métadonnées et le système KeeeX proposent par défaut:

- l'injection de la date système dans les fichiers, cette information étant verrouillée dans le fichier
- l'injection dans le fichier de l'horodatage du GPS signé par le satellite lorsque cette information est disponible (téléphone mobile, véhicule)

- l'obtention d'une preuve de temps (TSR RFC 3161) pour l'IDX du fichier qui peut-être qualifiée eIDAS selon le niveau souhaité
- l'obtention d'un ancrage blockchain de l'IDX du fichier fournissant une date de bloc. L'ancrage est habituellement multiple, car dans le contexte TTE le fichier seul est ancré une première fois, et toutes les inscriptions des propriétés variables dans des registres séparés donnent lieu à des ancrages secondaires (pour le propriétaire, la version la plus récente, le statut).
- l'injection dans les fichiers si nécessaire du TSR rendant cette information indépendamment vérifiable sans tiers (toutefois au prix d'un surcoût de taille de fichier allant jusqu'à 4 Kilo Octets.
- l'injection dans les fichiers d'une branche de merkle rendant l'ancrage blockchain indépendamment vérifiable sans tiers.

Support de l'exigence par KeeeX relativement au lieu

Certains documents comme les photos ou vidéos permettent l'enregistrement d'informations géographiques. Le langage de métadonnées de KeeeX[metadata] propose par défaut :

- la réplication d'informations comme celles fournies par un GPS habituel dans les métadonnées KeeeX injectées dans tout format de fichier
- l'injection d'informations géographiques rarement présentes pour exploitation automatisée : altitude, précision du signal, timestamp GPS

Comme indiqué KeeeX permet d'attacher à tout fichier de tout format des informations de position selon les besoins. Cela permet notamment l'inclusion dans les documents ou dans les propriétés variables d'un codage symbolique des lieux comme le GLN (Global Location Number) proposé par GS1 : https://www.gs1.fr/identifier-vos-entites-entreprises-lieux

Le langage de métadonnées permet par ailleurs l'injection dans les TTE de propriétés de sémantique et contenus arbitraires (classification, licences, etc...).

Article 14. *Place of business* - Lieu d'affaires

> *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.*

> 1. Un emplacement n'est pas un lieu d'affaires simplement parce que c'est : (a) où se trouvent l'équipement et la technologie soutenant un système d'information utilisé par une partie en rapport avec les documents électroniques transférables ; ou (b) où le système d'information est accessible à d'autres parties.

> 2. Le seul fait qu'une partie utilise une adresse électronique ou un autre élément d'un système d'information connecté à un pays spécifique ne crée pas une présomption que son établissement est situé dans ce pays.

Cet article ne possède à notre sens qu'une seule portée de droit. Les GLN de GS1 couvrent la sémantique de "Place of Business".

Article 15. *Endorsement* - Endossement

> *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.*

> Lorsque la loi exige ou autorise l'endossement, sous quelque forme que ce soit, d'un document ou d'un instrument transférable, cette exigence est satisfaite en ce qui concerne un document électronique transférable si les informations requises pour l'endossement sont incluses dans le document électronique transférable et si ces informations sont conformes aux exigences énoncées aux articles 8 et 9.

Support de l'exigence par KeeeX

Toutes les parties ne peuvent pas toujours être présentes en capacité de signature numérique active au moment de la production d'un document. KeeeX permet donc la signature retardée en mode simple et en mode délégué.

Rappelons techniquement que la clé publique des signataires attendus d'un fichier est incluse dans le fichier avant son verrouillage par le keeexage, ce qui interdit toute revendication de signature future par un tiers non prévu. La signature d'un document par un tiers non initialement prévu ne peut se faire que dans une nouvelle version du fichier, habituellement chainée cryptographiquement avec la précédente, et renseignée dans un historique de versions pouvant être traversé dans les deux directions et audité.

Toutefois il existe des cas ou l'identité numérique du signataire réel du document (définie par sa clé publique) est inconnue au moment de la création du fichier car elle intervient dans un mécanisme de délégation de signature selon un rôle (Président, Directeur, Conducteur etc..). KeeeX permet alors dans ce cas de désigner par sa clé publique l'identité d'un tiers endosseur pour ce rôle attendu dans une signature du fichier. Ce tiers endosseur peut ensuite, sans limite de délai, injecter dans le fichier une déclaration signée de l'identité réelle mobilisée pour ce rôle dans cette signature. Le détenteur de l'identité peut alors injecter sa propre signature de l'élément demandé.

En résumé le langage de métadonnées de KeeeX[metadata] permet :

- d'injecter dans le fichier lors de son keeexage la déclaration d'une autorité d'endossement optionnelle pour une signature
- d'injecter dans le fichier la déclaration d'une identité signataire réelle désignée signée par l'autorité précédente
- d'injecter dans le fichier la signature par l'identité désignée

Cette fonctionnalité peut être provisionnée pour des endossements multiples. Le fichier résultant est alors auto-porteur de ses preuves d'endossement. Le procédé est conforme aux exigences des articles 8 (Ecrit) et 9 (Signature).

Article 16. *Amendment* - Modification

> *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.*

> Lorsque la loi exige ou autorise la modification d'un document ou d'un instrument transférable, cette exigence est satisfaite en ce qui concerne un document électronique transférable si une méthode fiable est utilisée pour modifier l'information contenue dans le document électronique transférable de sorte que l'information modifiée soit identifiée comme telle.

Cet article énonce d'abord la possibilité qu'un document électronique transférable possède plusieurs versions. Il énonce ensuite que les changements appliqués entre deux versions doivent être documentés.

Toutefois le texte reste ambigü sur la portée du concept de version dans le contexte des propriétés variables attachées à un TTE (notamment le propriétaire) : cette information est elle "dans" le TTE ou en dehors?

Considérons en préambule que le procédé breveté KeeeX s'applique indifféremment à tous les formats de fichiers.

Support de l'exigence par KeeeX relativement aux versions

KeeeX permet à un acteur :

- d'ouvrir un fichier en étant certain que c'en est la version la plus récente et de détenir les droits de le modifier (utilise notre smart contract MLETR)
- d'en créer une nouvelle version avec l'éditeur de son choix (cette action pourrait être réservée au seul propriétaire du fichier, ou à un éditeur identifié dans le fichier par son identité numérique signataire
- de keeexer cette nouvelle version puis de la publier en conservant les droits de contrôle

- d'en transférer si nécessaire la propriété

Le chainage des versions de fichiers est bidirectionnel sous forme brute dans un smart contract et/ou avec des métadonnées publiques de contexte dans KeeeX Stories

Support de l'exigence par KeeeX relativement au suivi des modifications

Etant compatible avec tous les formats de fichier, KeeeX supporte nativement les formats de bureau (office notamment) qui prennent en charge le mode révision pour le suivi des changements. Ces fichiers peuvent être keeexés tels quels, et ainsi permettent le suivi des changements. Cette approche évite le recours inutile au format pdf.

Lorsque le format de fichier ne permet pas le suivi des modifications (pdf) notamment, le langage de métadonnées KeeeX permet d'utiliser la propriété description, ou des propriétés définies par l'usager, pour informer sur la nature des modifications effectuées. Au plan technique cela peut aller jusqu'à l'injection dans le fichier des résultats d'une comparaison (diff) entre les deux versions.

Support de l'exigence par KeeeX relativement au suivi des modifications de propriétés variables

Le TTE keeexé désigne de façon inviolable le registre utilisé pour tracer les changements de valeur d'une propriété variable comme son propriétaire, la version la plus récente connue de ce fichier, son statut (actif, expiré) etc.

Chacun de ces registres, smart contract blockchain ou non, identifie clairement la valeur courante d'une propriété comme ayant modifié la valeur précédente. Les valeurs successives sont historisées dans les deux directions. Dans le cas où des métadonnées de contexte doivent accompagner cette historisation, l'utilisation de KeeeX Stories peut s'avérer utile.

Article 17. *Replacement of a transferable document or instrument with an electronic transferable record* - Remplacement d'un document ou d'un instrument transférable par un document électronique transférable

> *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.*

> 1. Un document électronique transférable peut remplacer un document ou un instrument transférable si une méthode fiable de changement de support est utilisée.
> 2. Pour que le changement de support prenne effet, une mention indiquant un changement de support doit être insérée dans le document électronique transférable.
> 3. Dès la délivrance du document électronique transférable conformément aux paragraphes 1 et 2, le document ou l'instrument transférable est rendu inopérant et cesse d'avoir tout effet ou toute validité.
> 4. Le changement de support conformément aux paragraphes 1 et 2 n'affecte pas les droits et obligations des parties.

Support de l'exigence par KeeeX

Le moyen le plus immédiat d'atteindre les obligations de l'article 17 consiste à

- scanner l'original papier détenu par l'acteur ayant le contrôle (nouveau support)
- keeexer le scan obtenu en y intégrant les informations décrivant la procédure (paragraphes 1 et 2)
- reporter sur l'original son IDX (comme par exemple l'idx de ce html original : xupes-dohik-dodyn-lecut-pizir-pasyr-ninyv-cizos-ryzys-tynac-lycot-fadel-mofik-bagan-lyvum-tehat-zaxux). Cet IDX est obtenu lors du keeexage ou par simple glisser déposer [sur le vérifieur KeeeX][https://s.keeex.me].
- reporter sur l'original les informations permettant d'accéder à la chaîne de traçabilité du TTE issu du changement de support
- mentionner sur l'original la perte de sa validité au profit du TTE (paragraphe 3)

Le cas échéant un nouveau scan de la première page de l'original portant les inscriptions précédentes peut être intégré dans le registre de traçabilité du TTE.

Article 18. *Replacement of an electronic transferable record with a transferable document or instrument* - Remplacement d'un document électronique transférable par un document ou un instrument transférable

> *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.*

> 1. Un document ou un instrument transférable peut remplacer un document électronique transférable si une méthode fiable de changement de support est utilisée.
> 2. Pour que le changement de support prenne effet, une mention indiquant un changement de support doit être insérée dans le document ou l'instrument transférable.
> 3. Dès l'émission du document ou de l'instrument transférable conformément aux paragraphes 1 et 2, le document électronique transférable est rendu inopérant et cesse d'avoir tout effet ou toute validité.
> 4. Le changement de support conformément aux paragraphes 1 et 2 n'affecte pas les droits et obligations des parties.

Le besoin d'une procédure de sauvegarde dite "back to paper" est attesté et avait été implémenté par KeeeX en 2017 au sein d'un pilote réalisé par KeeeX pour CMA-CGM avec la société BuyCo.

Support de l'exigence par KeeeX

Pour atteindre les conditions de l'article 18 KeeeX permet :

- l'impression de l'ETR dans sa version vérifiée comme la plus récente (action automatique ou manuelle) (article 1)
- le report sur le fichier papier des éléments (dont son IDX, ou un hash encodé de façon humanisée) donnant accès à la chaîne de traçabilité du fichier numérique à date (action manuelle ou potentiellement automatisée par l'imprimante) (articles 1 et 2)
- l'invalidation de l'ETR sur sa chaîne de traçabilité avec mention du changement de support (procédure de sauvegarde "back to paper") (article 3). Cela se fait par le changement de valeur d'une propriété variable "back to paper", dont le registre interdit le retour en arrière.

Conclusion

La technologie KeeeX associée à un smart contract MLETR opéré sur la blockchain KeeeX implémente l'intégralité des conditions définissant la MLETR. Cet ensemble de services est accessible par API et via un portail de démonstration. Une partie du savoir faire de KeeeX dans le transfert de titularité de documents transférables est en production et visible dans le contexte des NFT sur nft.keeex.art.

Annexe : KeeeX (anglais)

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). 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, including on some snapshots by way-back machine (Internet Archive).

Crédits

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

Les traductions ont été assistées par DeepL.com.

La version html originale de ce fichier a été produite avec https://kaaas.keeex.me et a pour idx :

xupes-dohik-dodyn-lecut-pizir-pasyr-ninyv-cizos-ryzys-tynac-lycot-fadel-mofik-bagan-lyvum-tehat-zaxux

Ce fichier devrait être vérifié sur https://s.keeex.me/verify

Réferences:

- 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-