POSITION PAPER
Contribution to the drafting of the implementing decree for the French ETD law on Electronic Transferable Documents

Summary

This article lists recommendations to the legislator for the formulation of reliability requirements applicable to the implementation of the ETD law on the Electronic Transferable Document as formulated in the ADAFCI report "Accelerating the digitization of international trade finance activities" of June 29, 2023. These recommendations benefit from long-standing expertise in document and blockchain traceability solutions integrating the key issue of the UNCITRAL MLETR model law: exclusive control of the document and the possibility of transferring it without dual use. Our aim is to contribute to a formulation that does not create unnecessary regulatory hurdles in a context of operational urgency.

Author: KeeeX, https://keeex.me

1. Introduction

The report **"Accelerating the digitization of trade finance activities"[1]** (ADAFCI in the following) submitted on June 29, 2023 to Bruno Le Maire[2], Éric Dupond-Moretti[3] and Olivier Becht[4] aims to transcribe into French law the recommendations made by the UNCITRAL Model Law on Transferable Electronic Documents (MLETR, or Loi-Type in the following).

A considerable amount of work has gone into this project, culminating in the drafting of legislation to dematerialize the international trade sector, which is still largely paper-based, mainly due to the impossibility of having electronic negotiable (or transferable) securities, and the inability of players to commit to dematerialized processes in which they have only limited confidence. Paper-based securities are documents whose original incorporates a right (e.g. the right to a debt in the case of a bill of exchange or promissory bill; the right to

[1] See link and relevant extracts in appendix
[2] Minister for the Economy, Finance and Industrial and Digital Sovereigntý
[3] Keeper of the Seals, Minister of Justice
[4] Minister Delegate to the Minister of Europe and Foreign Affairs with responsibility for Foreign Trade, Attractivenesś and the French Abroad

delivery of goods in the case of a bill of lading), so that the exercise of the right incorporated in the paper original, or the transfer of that right, presupposes possession of the original. For electronic documents, the Model Law essentially provides that **exclusive control is the functional equivalent of possession** for tangible documents. ADAFCI recommends incorporating this and other derivatives of this essential principle into French law.

The current contribution builds upon EU and French regulations on electronic writing and electronic signatures, which introduce a first level of consideration of digital in the regulations, including an injunction to accept a digital signature process in place of a paper process.

This article is organized as follows: in 2, an overview of the current state of electronic writing, electronic signatures and blockchain; in 3, a description of the challenges to be met by the legislator to address the requirements of the MLETR; in 4, recommendations, including a proposal for an implementing decree for the law proposed in Appendix 7 of the ADAFCI report; in 5, a conclusion; and in 6, a presentation of the author.

All regulations and legal texts used in reference to this article are reproduced for convenience in the appendix. English translations of legal texts originally written in French may suffer from various biases and the reader is kindly redirected to the original sources in case of doubt.

- Reference: Text of the bill in Appendix 7 of the ADAFCI report
- Annex I: European "eIDAS" Regulation
- Appendix II: French Civil Code Articles 1365, 1366 and 1367
- Appendix III: Code of Civil Procedure
- Appendix IV: Decree no. 2017-1416 of September 28, 2017
- Appendix V: ANSSI references
- Annex VI: UNCITRAL Model Law on Electronic Transferable Records: Articles 10 and 12

Readers are warned that, despite numerous references to laws and regulations, this article has not been written by legal experts but by technical specialists.

2. The situation

The Model Law on Electronic Transferable Records (MLETR) was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 2017. It aims to enable the dematerialization of transferable records in international trade. This model law provides a frame of reference for states to incorporate the principles it lays down into national law. To date, some ten countries, including Singapore and the United Kingdom, have adapted their laws accordingly. France, for its part, should adopt the legislative provisions in the coming months, and the regulatory provisions should follow very quickly.

The ETD, or Electronic Transferable Document, is a relatively complex digital document designed to support the same processes as the paper document used in non-dematerialized documentary processes: endorsements, multiple signatures relating to the creation, acceptance or endorsement of the document, changes in status (expired, active,

etc.), annotations, under conditions allowing continuity with current processes, notably by returning to paper or switching to digital. The disharmony of regional regulations and the demand for security procedures adapted to the context of the value of the rights incorporated in titles justify the efforts required to create a regulatory framework acceptable to all, taking into account the most recent technological advances.

The general context of ETD is a continuation of the rich French and European regulatory work aimed at guaranteeing the acceptability of electronic writings and signatures and regulating the conditions of their use. ETD operates in an area that is predominantly inter-industrial (B2B), but also involves public services (customs, maritime affairs, etc.) and concerns the supply of documents representing rights to assets of arbitrary value. This last point justifies the refusal to use dematerialized solutions if the highest guarantees are not met, not only of the lowest possible risk of fraud, but also of the impossibility of multiple execution or transfer of the same document. In this context, we need to take a look at the current state of the art in terms of electronic writing and signatures.

Existing legislative and regulatory framework for electronic signatures

Articles 1365, 1366 and 1367 of the French Civil Code define the admissibility of an electronic document, of which the electronic signature is a key element.

Articles 1365 and 1366 provide that:

> "The writing consists of a series of letters, characters, numbers or any other signs or symbols with an intelligible meaning, regardless of their medium. "
>
> "An electronic document has the same evidential value as a paper document, provided that the person from whom it originates can be duly identified and that it is created and stored in conditions that guarantee its integrity. "

It should be noted straight away that article 1366 vaguely considers the notion of identification, so this notion can be assumed to be context-dependent. For example, in some cases, the sender of an e-mail may be considered as reasonably identified, while in others, the actor who has proved his ability to digitally sign a challenge sent by a server will also be. The notion of "digital" signature[5] in this context must be considered here as a technical tool distinct from the "electronic" signature[6] subject to specific obligations (qualification of operators and devices) but mobilized by the latter. For a brief reminder, a digital signature requires a pair of keys from an asymmetric cryptography system, and an algorithm which applied to a text to be signed (usually a short string of characters or a file hash) produces a signature in the form of a fixed-size number.

It should also be remembered that integrity can be preserved for a digital document in the absence of an external device (such as a digital safe), as long as this document (file) carries its own proof of integrity, generally combined with embedded digital signatures. This is

[5] https://en.wikipedia.org/wiki/Digital_signature
[6] https://en.wikipedia.org/wiki/Electronic_signature

notably the case for formats supported by the electronic signature and for all the usual formats addressed by the KeeeX technology.

Article 1367 states that:

> "The signature required to perfect a legal act identifies its author. It manifests his consent to the obligations arising from this act. [...] When it is electronic, it consists of the use of a reliable identification process guaranteeing its link with the act to which it is attached.
>
> The reliability of this process is presumed, in the absence of proof to the contrary, when the electronic signature is created, the identity of the signatory is assured, and the integrity of the document is guaranteed, in accordance with the conditions laid down by decree of the Conseil d'Etat".

This decree n° 2017-1416 was published on September 28, 2017 and refers to the European eIDAS regulation n°910/2014 (see Annexes). In particular, Article 1 states that.

> "The reliability of an electronic signature process is presumed, until proven otherwise, when this process implements a qualified electronic signature. A qualified electronic signature is an advanced electronic signature that complies with Article 26 of the above-mentioned Regulation (eIDAS) and is created using a qualified electronic signature creation device that meets the requirements of Article 29 of said Regulation, which is based on a qualified electronic signature certificate that meets the requirements of Article 28 of said Regulation. "

Although there is a distinction between "simple", "advanced" and "qualified" electronic signatures, they all have the same legal value, provided they are based on the use of a reliable identification process that guarantees their link with the act to which they relate. Only the charge of proof is reversed, as qualified electronic signatures are presumed to be valid by default.

Limits of existing regulations on electronic signatures

Article 26 of the eIDAS regulation states that:

An advanced electronic signature meets the following requirements:

- a) be uniquely linked to the signatory;
- b) identify the signatory;
- c) have been created using electronic signature creation data that the signatory can, with a high level of confidence, use under his exclusive control;
- d) be linked to the data associated with this signature in such a way that any subsequent modification of the data is detectable.

This last condition (d) is a very important point to bear in mind for ETD.

Concerning modification: this requirement is only partially met by PAdES signatures, which in the context of the current implementation of PDF signatures only protect part of the file and allow subsequent addition to the signed file.

Regarding detection: the general verifiability of signed documents is also very limited, as few people have easy access to an "official" verifier of signed PDF files. Many verification solutions do not reveal whether a signed file has been altered in any way that could change its appearance. Verification solutions do not make it easy to check the correspondence between a signature key used and an identity.

These factors argue in favor of a universal, easy-to-access verification solution.

Verifiable correspondence between the file submitted for signature and the signed file

This point is currently missing from the definition of the advanced signature. However, we feel that it is essential for electronically transferable documents to enable the signatory to verify the integrity and origin of the file offered for signature, and thus to make the exact state of what has been offered for signature opposable, independently of the signed result. This applies in all cases where a digital or electronic signature concerns a document. It should be noted that the endorsement of a paper document fully satisfies this condition and must be implemented for the ETD.

Universal file formats

The electronic signature solutions deployed integrate PDF (PAdES) and sometimes XML (XAdES) and JSON (JAdES) formats (case 1). Other formats can only be signed via an envelope (CAdES), which degrades the original format of the file (which remains extractable) (case 2), or in the form of a detached signature in a file to be stored separately (case 3).

In the first case, files retain their usual functions, but verifiability suffers from the limitations indicated above. In the second case, signed files are not immediately usable without processing. In case 3, files must be transmitted and stored in such a way as to preserve the correspondence between data and proof.

As the eIDAS regulation was drawn up before the emergence of blockchains, we feel it is necessary to analyze these "technologies", which are generally recognized as being necessary for ETD, and whose useful properties must therefore be presented in connection with CNRS patents and expected developments in the eIDAS regulation2.

The cryptographic and blockchain context of electronic signatures

The regulations applicable since 2016 were the result of years of work ignoring the rapid development of the Bitcoin blockchain (2009) and then the Ethereum blockchain (2015).

- Bitcoin: https://fr.wikipedia.org/wiki/Bitcoin
- Ethereum: https://fr.wikipedia.org/wiki/Ethereum

as well as the potential of the "Certification Keys" technology patented by CNRS in 2013 and 2014 and acquired in the US and EU.

- https://patents.google.com/patent/US10218714B2 (US patent) ("Method for checking the integrity of a digital data block")
- https://patents.google.com/patent/EP2949070B1 (EU patent)
- https://patents.google.com/patent/US10262026B2 (US patent)

About blockchain

A public blockchain such as Bitcoin is, in essence, a trust service provider not represented by a governance entity, not accountable for its use, and not qualifiable under European regulations. Yet Bitcoin is the world's most "advanced" signature and proof system, and is subject to constant, relentless quality auditing:

- a) a public key can only be used by the holder of a private key, which guarantees an unambiguous link between the signatory and the signed content.
- b) in all contexts where this is required, an advanced KYC system (as required by law) ensures that signature keys are associated with an identity. In the case of direct relationships, knowledge of the user's identity is validated by the parties themselves, using a horizontal rather than pyramidal approval process.
- c) blockchains have popularized the use of software "wallets" (e.g. "metamask") or hardware "wallets" (e.g. "Ledger"), necessary to prevent any usurpation and therefore theft of assets.
- d) the use of a publicly auditable blockchain to anchor the proof of existence of a file or signature guarantees the permanent verifiability of this proof, with no equivalent to that provided by qualified signatures.
- e) the user signing a transaction involving a document or its fingerprint knows this fingerprint and can check it before and after signing.

CNRS patents

The above patent ("Method for checking the integrity of a digital data block") makes it possible to deliver embedded digital signature services without functional alteration for all common formats, and by extension for all modern digital formats based on either zip or xml. This universal technology is available in the form of publicly accessible verifiers. Files are signed either by server seals and signatures based on certificates of the desired qualification level (eIDAS or RGS[7]) or signatures derived from blockchain algorithms (Bitcoin and/or Ethereum).

Expected developments in eIDAS2

The proposal for the future eIDAS 2 regulation includes a new section 11 which establishes a framework for trust services with regard to the creation and maintenance of electronic

[7] RGS is a French regulatory framework for digital and electronic signatures that existed before the implementation of eIDAS: https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

registers (this is mainly an alias for "blockchain") and qualified electronic registers. Electronic registers combine time-stamping and data sequencing with guarantees concerning the initiator, in a similar way to the electronic signature process, which has the added advantage of enabling more decentralized governance suited to multi-party cooperation. This is important for various use cases that may rely on electronic registers, such as MLTER.

Section 11 has been deleted by ITRE via a proposed amendment to the European Parliament. We encourage the Council and the European Commission to maintain this section 11, as it is necessary without taking a position on the underlying technologies in line with the technological neutrality intended by the framework law to support the creation of a framework conducive to the dematerialization of international commercial documents, particularly as regards the certification, security and interoperability of electronic registers.

The proposal also enshrines the European digital identity portfolio, which will enable users to store identity data in particular. This advance will enable the construction of an interoperable identity system within the European Union, with immediate practical applications to the supply chain and international trade.

3. Challenges

First and foremost, it is worth recalling the spirit of the historical and current use of "paper" Transferable Documents or Securities mentioned in the introduction:

> This type of document on a tangible medium incorporates a right in such a way that the exercise or transfer of this right implies the necessary possession of the original of the document (it should be noted that traditionally, to mitigate the risk of loss, certain documents, such as bills of lading, were drawn up in 3 "negotiable" originals, but the first of the "completed" originals rendered the other two invalid).
>
> The exercise (or completion) of the right implies the delivery of the original document to the debtor of the obligation (debtor of an obligation to pay for a bill of exchange or promissory bill; debtor of an obligation to deliver goods for a bill of lading).
>
> Rights are transferred by endorsement (a simplified form of transfer accepted in commercial law since the Middle Ages) or, if the title is a blank order, by physical delivery (jurists sometimes use the expression "manual tradition", which comes from the Latin "tradere" - to deliver).

Exclusive control requirement

The main difficulty lies in establishing the functional equivalent of possession of an original. The model law suggests "exclusive control" as the functional equivalent of possession. This requires to:

- identify the person having exclusive control;

- make sure it is the only one to have control and be able to transfer it;
- ensure that it loses full control when the transfer or exercise of the right takes place, and finally;
- ensure that it cannot exercise the right or its transfer more than once.

Finally, we need to be able to trace everything reliably.

The implementation of the ETD, as adapted to national law by the MLETR, must be based on existing regulations on writing and signature, although certain aspects could be strengthened. These provisions are necessary, but not sufficient, as the use of a transferable document in electronic form depends on the existence of rights linked to the physical possession of the paper medium. As an electronic document can exist in the form of multiple copies, the notion of original and exclusive control of an original need to be clarified by the legislator.

Exclusive control of a digital asset has been an integral part of the foundations of blockchains since 2009, first in a monetary context (Bitcoin) and then in a technical context (Ethereum smart contracts). It therefore seems essential to us that the French transposition of the Model Law evokes the notion of an electronic registry, while guaranteeing a certain technological neutrality.

Blockchain technology cannot be ignored

Today's legislators are well aware of the benefits of blockchain technologies, which are made indispensable by the very specifications of the MLETR: blockchain is the only potentially publicly auditable (or in this case "traceable") tool capable of guaranteeing the exclusive control of a Document by exercising the ability to produce the digital signature of a transfer transaction or of the exercise of a right (in this case, for example, by a transfer to the debtor of the right). The case of change of ownership is exemplary, as it has been used in real life in the world of crypto assets since 2009 by the Bitcoin protocol (transfer of ownership of digital units of account) and more recently and more visually by NFT initially on the Ethereum blockchain (transfer of ownership of Non Fungible Token identifiers).

More generally, the MLETR context suggests the public traceability of other document attributes such as status (active, completed), origin (digital or paper transfer), return to paper, most recent version. Here again, electronic registry technology enables the traceability of changes in the values of variable properties attached to a document, under all the required constraints (author of the modification, prohibited modifications, etc.).

However, the context of dematerialization of document flows is not that of public blockchains: there is no question of fighting censorship, and decentralization of writing (which most of the time remains an empty word) is therefore unnecessary. On the contrary, the industry needs scalability and access control for writing system status changes, while guaranteeing their absolute opposability, and in some cases their pseudonymity, through the effect of a digital signature effectively under the exclusive control of their issuer.

Blockchains have also given rise to the development of a huge number of signature tools under the exclusive control of users: software (Metamask, ZenGo...), physical (Ledger Wallet, Trezor...) and among the latter so-called "air gapped" systems (Ellipal...) requiring no connection between the signature device and the host software through the use of communication verifiable by QR codes.

In many cases, exercising the ability to sign a transfer transaction to the recipient's digital identity perfectly reproduces the hand-to-hand transfer of a paper Document. Instead of a handwritten signature of endorsement, the recipient's ability to digitally sign a future action using the digital identity designated by the previous owner materializes exclusive control.

More precisely, if we take up the above formulation of exclusive control requirements, we observe in the blockchain universe that:

- the ability to sign with the private key corresponding to an expected public key identifies the person with exclusive control;
- an appropriate smart contract guarantees that only this person is able to initiate a transfer;
- the same smart contract guarantees that once a transfer has been made, the person cannot repeat it;
- the blockchain protocol guarantees that no two simultaneous transfers are possible (on the same network).

No one should be able to create a false document or issue a false transaction.

First of all, we believe that the legislator must take two key requirements into account:

- No one can agree to interact with dematerialized documents entitling them to goods of arbitrary value (as in the case of the Bill of Lading) without the highest guarantee that no one will be able to cheat;
- There is no middle ground for the notion of *exclusive* control.

In the context of the MLETR, these requirements recommend ruling out any digital signature produced using a private signature key accessible to third parties[8], unless the user is provided with the necessary warnings or information on the limits of insurable value. This is all the more so in the case of interactions that only weakly identify a user (even if only by sending an e-mail or SMS), provisions that are nonetheless valid in the context of qualified electronic signatures.

An ETD requiring a signature interaction (digital or electronic) can therefore only be signed by an identity that has exclusive control over its means of signature, whether by a software device used in a portal or application ("software wallet"), or by a physical device ("hardware

[8] This is notably the case for a signature produced by an RGS** type physical device, whose unlocking password is accessible on a back end in a cloud-type remote interaction.

wallet"). It should be noted that this condition does not preclude a document process from authorizing several actors (presumably from the same company) to work on the same document process, notably for backup purposes (risk of loss of means of signature), in a context where the traceability of signatures and signatories is enforceable.

A few years ago, this requirement might have seemed excessive, but the accelerating democratization of signature methods in the world of crypto-currencies and blockchains, as well as the forthcoming eIDAS2 regulation and Estonia's experience, make it perfectly conceivable. Indeed, no one would object to the use of what looks like a Fido key or equivalent, already widespread as second-factor authentication tools.

Documents to be guaranteed are not just PDFs

The documents and data involved in a dematerialized process around transferable documents are extremely variable. This is true both for the documents themselves, which are the subject of the transfer, and for the appendices that support the decision-making process. Of course, there are image files, html files, csv files, json files, excel and other files, office files (e.g. Word), which are invaluable for tracking changes, etc. (and yes, they can also be pdf files - but why have to produce them if they can be avoided).

By way of example, the html files processed in accordance with the CNRS patents mentioned above may automatically display a QR code on a printed version, giving access to the digital original, the only source of truth.

Verifiability

Data, documents, sequences and proofs must be easily verifiable by anyone, anywhere, without time limits or business models. In particular, any element of a dematerialized process must be verifiable without the need for a third party to create an account or make a payment. This verifiability is closely linked to the notion of reliability, which is present in many articles of the Model Law: the more verifiable a solution, the easier it is to demonstrate its reliability.

In this context, any solution that gives the illusion of security through a complex device is inferior to one that provides easy access to verification. In the paper world, this is evidenced by the very poor ability to verify watermarks or filigrees (as in the case of Bills of Lading on special paper or banknotes) or holograms (banknotes in general), and in the electronic world by the general inability to verify PDF signatures.

Several conditions must be reliably verifiable in order for the holder of an ETD to have the same rights as a physical security:

- Contents
- Its original character
- Identification of its holder and signatories
- Its integrity
- Its date

- Its evolution

Finally, in certain contexts, the verifiability of a part of the document must be possible without revealing the entire document: for example to disclose the declaration of the absence of hazardous materials without exposing the total value of the goods. This is made possible by technical tools widely used and tested in the blockchain world, including "Zero Knowledge Proofs" and "Merkle branches".

4. Recommendations

Preamble

The action of transferring ownership of an asset represented by an Electronic Transferable Document must be able to be carried out as of right and without any regulatory impediment by the same mechanisms used today by holders of crypto assets: with a software or physical signature tool under the exclusive control of the user.

However, as recommended by the ADAFCI Report of June 29, 2023, the state of the art is constantly evolving, and this openness must not become a constraint.

The format of a file involved in an ETD process must not be constrained by the legislator, even implicitly (pdf).

The requirement for service providers to be qualified should not be retained on the sole grounds of a presumption of validity, since it would act as a barrier to innovation by de facto barring small companies from access to large groups, as we have seen in the case of electronic signatures.

Finally, as mentioned above, article 11 of the eIDAS2 regulation on the use of registers and/or blockchains must be retained.

Proposed wording for the decree on the reliable method

An Electronic Transferable Document (ETD) carries rights attributed to its owner alone. The ability of players to accept the use of this tool as a replacement for paper requires everyone to implement sufficiently reliable and auditable procedures guaranteeing that:

- each document is under the exclusive control of its owner, and that
- no one can create a fake

To these ends, this decree specifies the minimum reliability requirements expected for the implementation of the ETD law.

1. The integrity of the ETD and any version of it must be materialized by a unique identifier in the form of a cryptographic fingerprint with no known vulnerabilities, or

any future superior scheme. Ideally, this fingerprint should be able to be integrated into the file without altering its use, whatever its format.

2. The proof of origin and ownership of the creator of the first version of the ETD, and of any signatory, delegate or endorser, must be materialized by a digital signature of the identifier based on a pair of public and private keys under the exclusive control of its holder, using a digital signature calculation algorithm with no known vulnerabilities, or any future superior scheme. Ideally, this signature should be able to be integrated into the file without altering its use, whatever the format.
3. The calculation of the identifier must consider all the data in the file and must not allow any subsequent additions, except in the case of exceptions strictly provided for in the protocol (for delayed or delegated signatures, planned endorsements, etc.).
4. No alteration of the ETD (e.g. in the normal course of communication, display or storage) can be tolerated unless the verifiable digital original can be easily regenerated, or the altered version is registered as a valid version in the ETD life cycle. A version altered for display purposes must be verifiable and identify the original of which it is a copy.
5. The calculation of the identifier must consider at least the public keys of the document creator and of all the signatories or delegates expected at the time of creation, to avoid any reattribution.
6. The identification of a document as an ETD will have to be materialized by recording the identifier in a publicly auditable register with the evidential force of a smart contract on a blockchain with no known vulnerabilities, or any future superior scheme.
7. The recording of any value of a variable property of the ETD (owner, return to paper status, most recent version, expiry status, etc.) must be materialized by the registration of a correspondence between the identifier and the value of this property in a publicly auditable register with the evidential force of a smart contract on a blockchain with no known vulnerabilities, or any future superior scheme. This entry must be digitally signed and can only be signed by the owner or a delegate who is valid at the time of the transaction.
8. As far as possible, the registers required to manage the variable properties of the ETD should be mentioned in the ETD before creation, so that they cannot be altered, but also to ensure that if the file is discovered outside the technical context of its initial archiving, it provides access to the registers tracing its owners and variable properties. The information designating the register must be sufficient to identify it with certainty.
9. If a change of registry occurs for a property when a new version of the ETD is created, the previous registry must allow the change to be declared in a publicly auditable registry with the evidential strength of a smart contract on a blockchain with no known vulnerabilities, or any future superior scheme.
10. In the event of a switch to paper, at least one register linked to the ETD must enable this change of status to be designated in a publicly auditable register with the evidential strength of a smart contract on a blockchain with no known vulnerabilities, or any future superior scheme.
11. If a switch to paper is made, the paper document must visibly bear the identifier of the last known digital version used as the "Original" of the paper ETD, the words "back to paper" and, if possible, a QR code giving access to this original. If an item specified in the digital Original is missing from the paper version, the former will continue to be

the source of trust for this item (this may happen for instance if the paper version is not the result of a printout).

12. If a paper document is to be converted to a digital medium, the following conditions must be met:
    a. This possibility has been mentioned on the paper document since its creation.
    b. The paper document bears a unique identifier (e.g. the booking number in the case of a bill of lading).
    c. The status of the document must be publicly auditable in a register indexed by the document's unique identifier, this register having the evidential strength of a smart contract on a blockchain with no known vulnerabilities or any future superior scheme.
    d. The paper document and all its copies display a simple means of verifying the document's usability (e.g. via a QR code or any superior technology).
13. In the case of a paper-based switch to digital, the paper version must be visibly marked with the fact that it has been invalidated in favor of a digital ETD, with the identifier of the first version also printed on the paper and, if possible, a QR code giving access to the latter.
14. In the case of a switch to digital on the basis of a paper document, in order to prohibit the use of any paper duplicates in addition to the new digital document, the register mentioned in 12 c must be modified to simultaneously invalidate all paper versions potentially in circulation, the status of this invalidation being made accessible by the simple means of checking it as mentioned in 12 d.
15. Verification of file integrity must be possible without recourse to a third party imposing an economic or identification model. Verification of an ETD must be possible by anyone, anywhere, without technological dependency. It must be possible on services exposed to the public in at least two distinct geographical zones, and as a last resort this verification must be able to be carried out "manually".
16. Where conditions dictate, an ETD may be validly signed by several parties, potentially including in this case a signature identifying a company name and/or an industrial site. This signature must be performed using a qualified server seal, or a seal at RGS* or ** level.
17. Where the use of a counterfoil notebook is required by law for paper documents (as per law L522-25 of the French Commercial Code), this requirement will be validly fulfilled by writing into the ETD a unique code (sequential or random) also recorded in a publicly auditable register with the evidential force of a smart contract on a blockchain with no known vulnerabilities, or any future superior scheme.

Reminder: requirements set out in the report

1 At the very least, the decree issued by the Conseil d'état concerning the reliable method should:

- Address the issues covered by the provisions of the UNCITRAL Model Law, in particular Articles 10 and 12, while ensuring consistency with related provisions in French law;

- Preserve the approach of strict technological neutrality called for in the text of the ETD project:

one that links no transferable title to a specific technology, each of which is destined to become obsolete over time;

one that does not hinder the fluidity of trade and supply chains: transferable securities are governed by French law but are intended to be issued worldwide (as is currently the case for maritime bills of lading, a significant proportion of which are issued worldwide under French law): the reliability standard will therefore have to respect this fluidity requirement.

- Specify where applicable, the conditions for preserving the integrity of the electronic transferable security, depending on its use;

- Specify the parameters for paper/electronic conversion and vice versa, and, if necessary, the methods for notifying the various parties involved in the conversion, as well as the information that must appear on the converted title (old and new);

- Determine if there is a need to specify the address of service providers for certain procedures;

- Define the conditions for extracting receipts and warrants from the counterfoil register referred to in article L. 522-25 of the French Commercial Code, for electronic use.

5. Conclusions

Recent developments in technology make it possible to embark on a major dematerialization process in the industry, particularly in sectors which until now have been highly resistant to the idea, due to a justified perception of risk in the absence of appropriate technology.

The ETD law and its implementing decree provide a regulatory basis capable of dispelling any doubts, by defining for the first time the notion of transferable digital originals with greater force than paper. This law recognizes the considerable contribution of blockchain technology in defining "non-duplicable" original digital files. Indeed, any digital file is by its very nature clonable, but cryptography and blockchain finally make it possible, in a publicly auditable way to:

- make every clone a carbon copy of the original,
- make the variations applied to this original visible to all clone owners,
- deliver rights to a single holder.

In this respect, the ETD law is a lever for modernizing industrial activity that can be described as historic, in terms of its far-reaching effects on practices and the climate.

6. Author, credits

This article was written by the KeeeX team, which holds the exclusive license to the CNRS patents listed above and has had field expertise in document traceability since 2013. Since 2017, we have also carried out multiple applications and pilots on the subject of process

traceability including transfer of ownership or responsibility, including for CMA-CGM, Thales, BonjourLeBon, and the MeRS project at the initiative of the Minister in charge of Transport Madame Elizabeth Borne. We filed a new patent in 2023, which opens up unrivalled possibilities in terms of process reliability in electronically transferable document processes in particular, and more generally for data lineage.

More information on the KeeeX technology and company can be obtained at https://keeex.me

We would also like to thank the reviewers and contributors to this paper.

We apologize for any mistranslation that could occur in the following Reference and Annexes and kindly redirect the reader to the original linked texts, as well as the French original of this position paper (https://keeex.me/blog/).

This text was translated from French original with idx "xusaf-sisum-lerut-nezyc-tymys-numyh-tipet-zucem-dyvut-fynyv-cetuh-dabat-radav-zikem-kazan-penak-suxox".

Original text "xusaf" in French has been published as "Position Paper - Contribution KeeeX au décret DTE-MLETR en droit français-keeexed-LH-2023-10-04-xinot-pogel.pdf" with idx " xinot-pogel-fugip-hugic-mupim-zulym-zotem-rysep-mipiv-durev-tomen-tenir-dinon-tocuh-nacob-dylof-suxex"

7. Reference: June 29, 2023 report on electronically transferable securities

https://www.diplomatie.gouv.fr/IMG/pdf/rapporttrade-_vf-29.06.23_cle08ea4a.pdf

Appendix 7: Legislative provisions proposed by the mission

Article 1

A transferable document of title is a written document representing an asset or a right, which gives its holder the right to demand performance of the obligation specified therein and to transfer that right. Transferable securities falling within the scope of the present law include:

- bills of exchange and promissory bills governed by Title I of Book V of the Commercial Code;
- receipts and warrants governed by Section 4 of Chapter II, Title II of Book V of the Commercial Code;
- maritime bills of lading to order or to bearer governed by Section 2, Chapter II of Title II of Book IV of Part Five of the French Transport Code ;
- negotiable river bills of lading governed by the decree of July 20, 1960 creating a negotiable river bill of lading;
- order-based insurance policies governed by Chapter II, Title I of Book I of the French Insurance Code;

- professional receivables assignment slips governed by sub-section 1 of Section 3, Chapter III, Title I of Book III of the Monetary and Financial Code, when these slips are stipulated to order;
- any other writing, to order or to bearer, as defined in the first paragraph, with the exception of those mentioned in article 9 of the present law.

Article 2[9]

Any transferable document of title within the meaning of article 1 may be drawn up, signed and stored in electronic form under the conditions set out in articles 1366 and 1367 of the French Civil Code. Electronic transferable securities are transferred, delivered and modified in accordance with the reliable method set out in articles 4 and 5.

Article 3

The holder of an electronic transferable security is the person who has exclusive control over it, either for himself or for a third party. This control enables him/her to exercise the rights conferred by the security[10] , to modify it or have it modified, and to transfer it, under the conditions laid down in the present law. Endorsements, acceptances, endorsements or any other modifications that may be affixed to the security may appear in any appropriate place on the electronic transferable security if their nature and purpose are unambiguous from the terms of the endorsement concerned.

Article 4

The electronic transferable document has the same effects as a transferable document drawn up on paper, provided that it contains the information required for a transferable document drawn up on paper and that a reliable method is used to: 1°) identify it as the electronic transferable document; 2°) identify its successive signatories and bearers, from the moment it is created until the moment it ceases to produce effects or to be valid; 3°) establish the bearer's exclusive control over this electronic transferable document; 4°) identify this bearer as the person who has control over it. 5°) preserve its integrity and attest to any modifications made to it, such as additions, strikethroughs or deletions, permitted by law, custom, usage or agreement of the parties, from the moment it is created until the moment it ceases to produce its effects or to be valid. Integrity is assessed, in the light of article 1366 of the French Civil Code, by determining whether the

[9] An alternative wording had been envisaged by the mission. It read as follows: "A transferable document of title may be drawn up, signed, transferred, delivered, modified and stored in electronic form under the conditions laid down in articles 1366 and 1367 of the French Civil Code and by the present law". However, this alternative proposal was not adopted, as it appeared desirable to distinguish between the regime governing the creation of a document of title and that governing its transfer, given that transferable documents of title are not systematically transferred.

[10] (86) An alternative wording had been considered by the mission. It read as follows: "A transferable document of title may be drawn up, signed, transferred, delivered, modified and stored in electronic form under the conditions laid down in articles 1366 and 1367 of the French Civil Code and by the present law". However, this alternative proposal was not adopted, as it appeared desirable to distinguish the regime governing the creation of a document of title from that governing its transfer, given that transferable documents of title are not systematically transferred.

information contained in the title, including any modifications, has remained complete and unchanged.

Article 5

A Conseil d'Etat decree defines the characteristics of the reliable method provided for in article 4.

Article 6

I. Presentation or delivery of an electronic transferable security is made by any means of electronic communication to the electronic address indicated by the recipient. Such presentation or remittance may also be effected by communicating information enabling access to the electronic transferable security. This presentation or remittance is effective if the recipient acknowledges receipt by any means or, in the absence of acknowledgement, as soon as he/she is deemed to have been aware of it.

II. In the case of electronic transferable securities, the transfer or pledging of rights by endorsement or simple delivery of the security is effected by the transfer of exclusive control over the security. The blank endorsement of an electronic transferable security presupposes that the bearer is identified within the meaning of article 4° of the present law.

Article 7

A paper-based transferable security may be converted to an electronic medium and vice versa under the conditions laid down by the obligees and holders of rights under the security. A transferable security may, however, be created with the stipulation that it will not be convertible to another medium. The change of medium does not entail novation and does not alter the respective rights or obligations of the signatories, holders or persons having exclusive control of the security, nor its effects vis-à-vis third parties. The converted security retains, for all intents and purposes[11] , the properties of the initial security, and bears a reference to this conversion on the new medium. The old medium ceases to be valid from the date of issue of the new medium. The conditions of application of the present article are defined by decree of the Conseil d'Etat.

Article 8

Any stamp, seal, claw or other distinctive sign affixed in addition to a signature on a transferable paper document may be satisfied for an electronic transferable document by the time-stamped affixing of an image faithfully reproducing the said stamp, seal, claw or other distinctive sign.

[11] The phrase "as far as is reasonable" is inspired by the wording of article 1100-1 of the French Civil Code, which refers to the rules governing contracts for the validity of legal rules. It is justified here, as certain information in electronic format cannot be reproduced in a paper document.

Article 9

The provisions of this Act shall not apply to:

- financial instruments governed by Title I of Book II of the Monetary and Financial Code;
- cheques governed by Chapter I of Title III of Book I of the Monetary and Financial Code;
- special dematerialized payment instruments governed by article L. 525-4 of the French Monetary and Financial Code;
- promissory notes governed by article L. 143-18 of the French Commercial Code;
- warehouse receipts governed by article L. 522-37-1 of the French Commercial Code;
- enforceable copies of mortgage claims governed by law no. 76-519 of June 15, 1976.

Article 10

The French Commercial Code is amended as follows[12] :

1° After article L. 511-1, an article L. 511-1-1 is inserted as follows: "Art. L. 511-1-1 - Bills of exchange may be drawn up, signed, transferred, presented, delivered, modified and stored in electronic form under the conditions provided for by law [ETD]. "Section 12 of this chapter does not apply to electronic bills of exchange. It may not be drawn in several copies, nor may copies governed by articles L.511-75 and L.511-76 be made. "A document that must be drawn up at a person's domicile is drawn up in accordance with the conditions set out in article 2, paragraph I of the [ETD] law;

2° After article L.512-1, an article L.512-1-1 is inserted as follows: "Art. L. 512-1-1 - Promissory bills may be drawn up, signed, transferred, presented, remitted, modified and stored in electronic form under the conditions laid down by law [ETD]. "The provisions of article L.511-1-1 relating to electronic bills of exchange apply to electronic promissory bills insofar as they are not incompatible with the nature of this instrument;

3° After article L.522-24, an article L. 522-24-1 is inserted, worded as follows: Art. L. 522-24-1 - The receipt and warrant may be drawn up, signed, transferred, modified and kept in electronic form under the conditions laid down by law [ETD]. "The counterfoil register referred to in articles L.522-25 and L.522-27 is then an electronic register maintained using a reliable method, the characteristics of which are defined by a decree of the Conseil d'Etat. "No electronic receipt can be issued if the warrant is in paper format, and vice versa.

[12] Note: Articles L. 511-8, L.511-21, L. 511-15 and L. 511-18 of the French Commercial Code could also have been adapted to specify some of the specific conditions governing endorsement, guarantee and presentation for acceptance or payment in the case of an electronic bill of exchange. In the end, these clarifications seemed likely to make the text more cumbersome, given that not all the terms and conditions laid down for a paper document are necessarily applicable to an electronic document. For example, the length of the document, which is understandable for a paper document with a limited surface area, makes no sense for an electronic document, whose space is by definition unlimited.

Article 11

A new paragraph is added to article L.323-23 of the French Monetary and Financial Code: "The slip, when stipulated to order, may be drawn up, signed, transferred and stored in electronic form under the conditions laid down by law [ETD]".

Article 12

A new paragraph is added to Article L. 5422-3 of the French Transport Code: "The bill of lading may be drawn up, signed, transferred, modified, stored and delivered in electronic form under the conditions laid down by the law [ETD]".

Article 13

A new paragraph is added to Article L. 112-5 of the French Insurance Code: "The policy, when stipulated to order, may be drawn up, signed, transferred, modified and kept in electronic form under the conditions laid down by law [ETD]".

Article 14

The provisions of the present law apply under the conditions laid down by law, custom, usage or agreement between the parties. They do not apply to transferable titles issued prior to its entry into force[13] .

Notes on Article 2

In the course of its work, the mission came up against a difficulty relating to the establishment of the electronic form of the transferable document: could a possible challenge to the validity of the conditions necessary for transferability not, in fact, be such as to call into question the validity of the document as a whole?

This question has arisen in particular with regard to the "bordereaux de cession de créances professionnelles" (Dailly slips)[14] - governed by Articles L.313-23 et seq. of the French Monetary and Financial Code, insofar as these slips have, for some years now, been drawn up and signed in electronic form using the digitization and electronic signature methods permitted by law, and the introduction of new digitization methods may seem more complex and less secure, as they are not yet precisely known.

Dailly slips are a simple and effective way of mobilizing receivables (assignment or pledging), and have enjoyed considerable economic success, becoming one of the essential tools for financing companies' working capital requirements. In practice, slips very

[13] It seemed desirable to clarify in the text instituting a new system the terms and conditions of its application to current situations, hence this provision.

[14] The bordereau Dailly is the "model" for the bordereau used in securitization, the nature of which remains very similar. By law, this securitization slip can already be "drawn up, signed, stored and transmitted in electronic form" (article L. 214-169 and article D. 214-227 of the French Monetary and Financial Code), but the transfer method is not described.

frequently include the words "stipulation à ordre" (stipulation to order), which is copied mechanically by operators, whereas slips are almost never circulated by way of endorsement.

As a result, some members of the working group fear that the inclusion of bills of lading within the scope of the ETD Act would call into question the validity of the very many electronic bills of lading that include an order clause, even if this is rarely used: the validity of these electronic bills of lading could be called into question even though Articles 1366 (electronic writing) and 1367 (electronic signature) of the French Civil Code would be complied with, on the grounds that the provisions of the draft ETD text would then not be respected.

Admittedly, this fear is unfounded for slips issued and signed before the ETD Act came into force, and it is likely that operators will no longer include the stipulation to order in dematerialized slips that are not intended to circulate by way of endorsement. To avoid any doubt as to the application of the new law over time, it seemed useful to specify in article 14 of the draft that the provisions of the law "do not apply to transferable securities issued before its entry into force". Thus, the new law will not apply to transferable titles created prior to the law's entry into force. In addition, to take account of the lack of visibility regarding the technologies designed to ensure the identification of the bearer, the traceability of signatories throughout the life of the security and its exclusive control, Article 2 has been drafted in such a way as to distinguish between the procedures for establishing transferable securities and those for transferring them[15] . The former remain those currently in force (articles 1366 and 1367 of the French Civil Code), while the new law will only apply to electronic securities that may actually be transferred. The alternative wording not adopted is given in the footnote to article 2 (note 86).

Notes on digitizing bills of lading

The Customs Code stipulates that the master must deposit the bill of lading at the customs office within twenty-four hours of the ship's arrival at the port[16] and that the bill of lading must be presented at the request of any customs officer[17] . It may therefore be appropriate to seek the views of the customs authorities on the arrangements envisaged for the deposit or representation of an electronic bill of lading. 92 Article 72. 93 Article 117. 105

[15] The new wording separates the creation of a document from its transfer/endorsement/modification. This approach makes it possible to distinguish between what calls on well-known technologies (writing and electronic signature) and what will mobilize technologies whose reliability has not yet been established (transfer/endorsement and affixing of authorized mentions). This separation is intended to prevent any discussion of the conditions for transferring title and the reliability of the method used in this context from disrupting the validity of the title itself.

[16] Article 72 of the Customs Code

[17] Article 117 of the Customs Code

Appendix 8: Content of sub-legislative provisions proposed by the mission

Certain regulatory provisions will have to be adopted in addition to the legislative provisions presented in Appendix 7.

1. At the very least, the Conseil d'Etat decree on the reliable method should :

- address the issues covered by the provisions of the UNCITRAL Model Law, in particular Articles 10[18] and 12[19] , while ensuring consistency with related provisions in French law;
- preserve the approach of strict technological neutrality called for in the text of the ETD project, and thus :
    - not to link any transferable title to a specific technology, each of which is destined to become obsolete over time;
    - not hinder the fluidity of trade and supply chains: transferable securities are governed by French law, but are intended to be issued worldwide (as is currently the case for maritime bills of lading, a significant proportion of which are issued worldwide under French law): the reliability standard will therefore have to meet this fluidity requirement.
- specify, where applicable, the conditions for preserving the integrity of the electronic transferable certificate, depending on its use;
- detail the parameters for paper/electronic conversions and vice versa, and if necessary the methods for notifying the various parties involved in conversions, as well as the information that must appear on the converted title (old and new);
- Determine the possible need to specify the address of service providers for certain procedures;
- define the conditions for extracting receipts and warrants from the counterfoil register mentioned in article L. 522-25 of the French Commercial Code, in the case of electronic use.

2. In line with the legislative changes proposed by the mission in the Transport Code, article D. 5422-5 of the Transport Code should be amended to read as follows: *"When*

[18] 94 " 1. When the law requires the use of a paper transferable document or instrument, this requirement is satisfied, in the case of an electronic document: a) If the latter contains the information that would be required in a paper transferable document or instrument; and b) If a reliable method is used: i) To identify this electronic document as the electronic transferable document; ii) To ensure that this electronic document can be audited from the moment it is created until the moment it ceases to be effective or valid; and iii) To preserve the integrity of this electronic document. 2. The integrity of the electronic document is assessed by determining whether the information contained in the document, including any authorized changes that may have occurred since its creation until it ceases to be effective or valid, has remained complete and unchanged, except for any changes occurring in the normal course of communication, storage and display."

[19] 95 "For the purposes of Articles 9, 10, 11, 13, 16, 17 and 18, the method referred to must: a) Be sufficiently reliable to perform the function for which it is used, in the light of all relevant circumstances, which may include: i) Any operating 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 audits carried out by an independent body; vi) The existence of a declaration made by a control body, accreditation body or voluntary program concerning the reliability of the method; vii) Any applicable industry standards; or b) Have demonstrated in fact that it has fulfilled this function alone or in conjunction with other evidence. "

the bill of lading is issued on paper, it is drawn up in at least two originals, one for the shipper and the other for the master. The originals are signed by the carrier or his representative. They are dated. The number of originals issued is indicated on each copy. When the bill of lading is issued in electronic form, it is drawn up in accordance with the conditions laid down by law [ETD].

3. The decree of July 20, 1960 creating a negotiable river bill of lading should also be completed as follows: *"Goods transported by inland waterway vessels may be covered by a negotiable river bill of lading. The river bill of lading is to order. When the bill of lading is issued in electronic form, it is drawn up in accordance with the conditions laid down by the law [ETD]"*. It is also questionable whether the option provided for in article 2 of the decree to issue non-negotiable copies of the bill of lading should be maintained for electronic river bills of lading.
4. Article R. 522-20 of the French Commercial Code could also be adapted, as it stipulates that the front of the receipt-warrant must mention the insurance of the goods. In fact, the front/back distinction does not seem to be sustainable for electronic documents.

8. Annex I - EU Regulation no. 910/2014 'eIDAS

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910

In CHAPTER III - TRUST SERVICES :

SECTION 1 - Article 13 Liability and burden of proof

1. Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person as a result of a breach of the obligations laid down in this Regulation.

The burden of proving that the unqualified trust service provider acted intentionally or negligently lies with the natural or legal person claiming the damage referred to in the first paragraph.

A qualified trust service provider is presumed to have acted intentionally or negligently, unless he proves that the damage referred to in the first paragraph was caused without intention or negligence on his part.

2. Where Trusted Service Providers duly inform their customers in advance of the limits that exist to the use of the services they provide and where these limits can be recognized by third parties, Trusted Service Providers cannot be held liable for damages arising from the use of services beyond the limits indicated.

3. Paragraphs 1 and 2 shall apply in accordance with national rules on liability.

SECTION 4 Electronic signatures - Article 25 - Legal effects of electronic signatures

1. The legal effect and admissibility of an electronic signature as evidence in legal proceedings may not be denied solely on the grounds that the signature is in electronic form or does not meet the requirements of a qualified electronic signature.
2. The legal effect of a qualified electronic signature is equivalent to that of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State is recognized as a qualified electronic signature in all other Member States.

SECTION 4 Electronic signatures - Article 26 - Requirements for an advanced electronic signature

An advanced electronic signature meets the following requirements:

- a) be univocally linked to the signatory;
- b) identify the signatory;

- c) have been created using electronic signature creation data that the signatory can, with a high level of confidence, use under his exclusive control; and
- d) be linked to the data associated with this signature in such a way that any subsequent modification of the data is detectable.

SECTION 4 Electronic signatures - Article 27 - Electronic signatures in public services

1. If a Member State requires an advanced electronic signature to use an online service offered by a public sector body or to use it on behalf of that body, it shall recognize advanced electronic signatures, advanced electronic signatures based on a qualified electronic signature certificate and qualified electronic signatures in at least the formats or using the methods defined in the implementing acts referred to in paragraph 5.

2. If a Member State requires an advanced electronic signature based on a qualified certificate in order to use an online service offered by a public sector body or to use it on behalf of that body, it shall recognize advanced electronic signatures based on a qualified certificate and qualified electronic signatures at least in the formats or using the methods defined in the implementing acts referred to in paragraph 5.

3. Member States shall not require, for cross-border use in an on-line service offered by a public sector body, an electronic signature with a level of security higher than that of the qualified electronic signature.

4. The Commission may, by means of implementing acts, determine the reference numbers of the standards applicable to advanced electronic signatures. An advanced electronic signature shall be presumed to meet the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 where it complies with those standards. Such implementing acts shall be adopted in accordance with the review procedure referred to in Article 48(2).

5. By 18 September 2015, and taking into account existing practices and standards as well as Union legal acts, the Commission shall, by means of implementing acts, define the reference formats for advanced electronic signatures or the reference methods where other formats are used. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

9. Appendix II - French Civil Code Articles 1365, 1366 and 1367

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070721/LEGISCTA000006118074/#LEGISCTA000032042346

Article 1365 (Amended by Ordinance n°2016-131 of February 10, 2016 - art. 4)

Writing consists of a series of letters, characters, numbers or any other signs or symbols with an intelligible meaning, whatever their medium.

Article 1366 (Amended by Ordinance n°2016-131 of February 10, 2016 - art. 4)

Electronic documents have the same evidential value as paper documents, provided that the person from whom they originate can be duly identified and that they are drawn up and stored in conditions that guarantee their integrity.

Article 1367 (Amended by Ordinance n°2016-131 of February 10, 2016 - art. 4)

The signature required to perfect a legal act identifies its author. It expresses his or her consent to the obligations arising from the deed. When affixed by a public official, it confers authenticity on the deed.

When it is electronic, it consists of the use of a reliable identification process guaranteeing its link with the document to which it is attached. The reliability of this process is presumed, in the absence of proof to the contrary, when the electronic signature is created, the identity of the signatory is assured and the integrity of the document is guaranteed, under conditions laid down by decree in the Conseil d'Etat.

10. Appendix III - Code of civil procedure

Code of civil procedure - Chapter I: Disputes relating to private deeds. (Articles 287 to 302)

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070716/LEGISCTA000006149658/#LEGISCTA000006149658

Article 287 Modified by Decree no. 2016-1278 of September 29, 2016 - art. 1 (V)

If one of the parties denies the handwriting attributed to him or her, or declares that he or she does not recognize the handwriting attributed to its author, the judge verifies the contested handwriting, unless he or she can rule without taking it into account. If the contested handwriting relates to only certain aspects of the claim, the judge may rule on the others.

If the denial or refusal to acknowledge relates to an electronic writing or signature, the judge verifies whether the conditions set by articles 1366 and 1367 of the Civil Code for the validity of the electronic writing or signature have been met.

Article 288 Modified by Décret n°2002-1436 du 3 décembre 2002 - art. 8 () JORF 12 décembre 2002

It is up to the judge to carry out the handwriting verification on the basis of the elements at his disposal, after having, if necessary, enjoined the parties to produce all documents to be compared with him, and to have handwriting samples composed under his dictation.

In determining the documents to be compared, the judge may retain any useful documents originating from one of the parties, whether or not they were issued in connection with the disputed deed.

Article 288-1 of the Code of Civil Procedure

When an electronic signature is presumed to be reliable, it is up to the judge to decide whether the elements at his disposal justify overturning this presumption.

11. Appendix IV - Decree no. 2017-1416 of September 28, 2017

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000035676246/

Article 1

The reliability of an electronic signature process is presumed, in the absence of proof to the contrary, when this process implements a qualified electronic signature. A qualified electronic signature is an advanced electronic signature, in compliance with article 26 of the aforementioned regulation and created using a qualified electronic signature creation device meeting the requirements of article 29 of the said regulation, which is based on a qualified electronic signature certificate meeting the requirements of article 28 of the said regulation.

12. Appendix V - ANSSI references

ANSSI offers detailed resources on the eIDAS regulation:

https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

and a set of documentary resources listing the associated regulations and implementing decisions:

https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

It reads (as of 26 09 2023):

The eIDAS regulation focuses primarily on electronic identification and trust services. To a lesser extent, it also deals with electronic documents, giving them legal effect.

ANSSI has a dual role in implementing the regulation: as a security guarantor for the "electronic identification" component, and as a supervisory body for the "trust services" component.

Electronic identification

Objectives and principles of the "electronic identification" chapter of the regulation

The eIDAS regulation aims to establish a mechanism for mutual recognition of Member States' means of electronic identification on all online services in other Member States.

In order to benefit from this mutual recognition, an electronic means of identification must :

- Have been issued in accordance with an electronic identification scheme notified by the Member State concerned and appearing on the list published by the Commission.
- According to the regulation, an electronic identification scheme is a system for electronic identification under which electronic means of identification can be issued to natural or legal persons. Member States have been able to notify electronic identification schemes since September 29, 2015.
- Have a level of guarantee equal to or higher than that required by the public sector body concerned to access this online service, provided that this level is substantial or high.

This mutual recognition only applies to public sector bodies that require electronic identification meeting at least the requirements of the substantial level in order to access one of their online services.

The requirements applicable to the various guarantee levels that are provided for in the regulation are detailed in implementing regulation no. 2015/1502 of September 8, 2015.

These levels are granted on the basis of compliance with minimum specifications, standards and procedures. Three guarantee levels are provided for in the regulation:

- Low: at this level, the aim is simply to reduce the risk of misuse or alteration of the identity;
- Substantial: at this level, the aim is to substantially reduce the risk of misuse or alteration of identity;
- High: at this level, the aim is to prevent misuse or alteration of the identity.

Mutual recognition of electronic means of identification became mandatory on September 29, 2018.

Competent national bodies

In France :

DINSIC, the French government's interministerial directorate for digital information and communication systems, acts as a single point of contact for electronic identification;

the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is responsible for establishing a reference framework of requirements applicable to each level, and for assessing the guarantee level of electronic identification systems.

In addition, an eIDAS cooperation network was set up by implementing decision 2015/296 and issues opinions on the various electronic identification schemes notified by member states. These opinions are public and are available via this link https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Opinions+of+the+Cooperation+Network

Trusted services

Objectives and principles of the "trust services" chapter of the regulation

The eIDAS regulation also aims to establish a legal framework for the use of trust services. It lays down requirements for trust services relating to electronic signatures, electronic stamps, electronic time stamps, electronic registered mail and website authentication.

The regulation distinguishes between qualified and non-qualified trust services. Qualified trust services meet specific requirements and may benefit from specific legal effects. Qualified trust services are provided by qualified trust service providers.

Qualified trust service providers are subject to regular audits by conformity assessment bodies accredited in accordance with regulation no. 765/2008 of July 9, 2008. The eIDAS regulation has been applicable to trust services since July 1, 2016.

The list of ANSSI-qualified products and services is available in the "Liste nationale de confiance" tab.

Qualified trust services covered by the regulation

The qualified trust services provided for in the eIDAS regulation are as follows:

- Issuance of qualified certificates for electronic signature, electronic seal and website authentication;
    - Qualified electronic signature certificates attest to the identity of the natural persons to whom they have been issued. The legal effect of a qualified electronic signature is equivalent to that of a handwritten signature.
    - Qualified electronic seal certificates attest to the identity of the legal entities to which they have been issued. A qualified electronic seal benefits from a presumption of data integrity and accuracy of the origin of the data to which it is linked.
    - Qualified website authentication certificates attest to the identity of the natural or legal persons to whom they have been issued, as well as the name of the corresponding websites.
- Qualified validation of qualified electronic signatures and qualified electronic stamps ;
    - A qualified validation service for qualified electronic signatures or stamps guarantees the legal security of a qualified signature or stamp by providing proof of validation by a qualified third party.
- Qualified storage of qualified electronic signatures and qualified electronic stamps ;
    - A qualified storage service for qualified electronic signatures or qualified electronic stamps extends their reliability beyond their technological validity period.
- Qualified electronic time-stamping ;
    - Qualified electronic time-stamping makes it possible to certify that data in electronic form existed at a given moment. Such a process can be used to affix a date to the dispatch or receipt of mail, but also more generally to certify the existence of data at a given moment, or the date of an act carried out electronically.
- Qualified electronic registered mail.
    - Qualified electronic registered mail enables data to be transmitted electronically between third parties, providing evidence of the processing of transmitted data, including proof of sending and receipt, and protecting such data against loss, theft, alteration or unauthorized modification.

The creation of a "remote" qualified electronic signature (or "server signing"), when the signatory or creator of the seal keeps his or her key in cryptographic equipment implemented in a third party's environment, is not a qualified trust service within the meaning of the regulation.

Qualified products for electronic signature and electronic seal

The regulation specifies that qualified electronic signatures and qualified electronic stamps are achieved respectively by means of :

- Qualified electronic signature creation devices ;
- Qualified electronic sealing devices.

Within each Member State, certification of the conformity of these products with the requirements of the regulation is issued by a certification body designated by the European Commission.

The regulation provides that, in certain cases, signature or seal creation may be delegated to a trust service provider which, on behalf of the legitimate signatory or seal creator, generates or manages the signature or seal creation data. In this case, the service provider must be a trust service provider qualified to provide one of the aforementioned qualified trust services.

Competent national body

In France, ANSSI is responsible for overseeing trust services. As such, it is responsible for :

- the definition of technical procedures to ensure compliance with the requirements of the regulation;
- qualification of trustworthy service providers established in France.

In addition, ANSSI plays two other roles provided for in the regulation:

- it draws up and keeps up to date trust lists of qualified trust service providers and the qualified trust services they provide;
- it certifies the conformity of qualified electronic signature and sealing devices.

13. Appendix VI - UNCITRAL Model Law on Electronic Transferable Records (MLETR)

https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/mletr_ebook_f.pdf

Article 10. Transferable documents or instruments

1. When the law requires the use of a paper document or transferable instrument, this requirement is met, in the case of an electronic document:

a) If it contains the information that would be required in a transferable paper docu- ment or instrument, and

b) If a reliable method is used :

i) To identify this electronic document as the electronic transferable document

ii) To ensure that such electronic document can be audited from its creation until such time aṣ it ceases to be effective or valid; and

iii) To preserve the integritý of this electronic document.

2. The integrity of the digital document is assessed by determining whether the information contained in the document, including any authorized modifications that may have occurred since its creation until the moment when it ceases to be effective or valid, has remained complete and unchanged, with the exception of any modifications that occur in the normal course of communication, storage and display.

Article 12. General standard of reliabilitý

For the purposes of Articles 9, 10, 11, 13, 16, 17 and 18, the method must :

a) Be sufficiently reliable to perform the function for which it is used, in the light of all relevant circumstances, which may include :

i) Any operating rules relevant to the assessment of reliabilitý ;

ii) Ensuring data integritý ;

iii) The ability to prevent unauthorized access to and use of the system;

iv) Hardware and software security ;

v) The regularitý and scope of audits carried out by an independent body;

vi) The existence of a declaration made by an inspection body, accreditation body or voluntary program concerning the reliabilitý of the method ;

vii) Any applicable industry standards: or,

b) Have demonstrated in fact that it has fulfilled this function alone or in conjunction with other evidence.