Enforceability of electronic contracts and signatures under French law

By Luis Wolff Kono[1]

V1 – October 2020

As companies increasingly use electronic contracting tools, they should analyze whether the tools being used satisfy French legal requirements for enforceability of electronic contracts and signatures.

These requirements are in part determined by EU law, which has created a legal framework for electronic signatures.

Enforceability of electronic contracts is of particular importance, in light of the growth in litigation involving electronic documents and signatures.[2]

As the EU legal framework is under review and could be revised soon[3], the topic of electronic signatures has gained renewed interest.

This article discusses the enforceability of electronic contracts and signatures under French law, with a focus on the legal framework created by EU law on electronic signatures.

A questionnaire appears at the end of this article, as a practical aid for companies to assess the compliance of their electronic contracting service providers.

I. Key highlights

- *Although a "writing" is not always required to prove the existence or content of a contract, ideally every company should seek to have enforceable written contracts, and if these are electronic, a number of requirements apply.*

---

[1] Luis Wolff Kono is a corporate and commercial attorney based in Paris, France. He is admitted in Paris, New York and New Jersey, USA. Email: luis@wolffkono.com. Internet site: http://wolffkono.com. He welcomes peer review of this article and any comments or suggestions from readers.

[2] Caprioli, Vademecum juridique de la digitalisation des documents, Fédération des tiers de confiance, 2016, page 4, available at : https://fntc-numerique.com/fr/actualites/814/vademecum-juridique-de-la-digitalisation-des-documents.html.

[3] The European Commission is currently evaluating this regulatory framework and launched an open consultation until 2 October 2020. The aim of the consultation is to collect feedback on drivers and barriers to the development and uptake of electronic identification and trust services in Europe and on the impacts of the options for delivering an EU digital identity. See https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification.

- *The reliability of a process of electronic signature is presumed, where this process implements a qualified electronic signature. Companies with strong needs for enforceability of electronic contracts should therefore consider using qualified electronic signatures.*

- *Qualified electronic signatures are created based on certificates issued by qualified trust service providers, who verify the identity of the signatory. Qualified trust service providers must be certified by competent bodies.*

- *A qualified electronic signature is not, however, indispensable to enforceability of electronic contracts. Companies with lesser needs for enforceability of electronic contracts (such as B2B commercial transactions) may decide to use electronic signatures not meeting the high threshold of "qualified" status and avoid the costs, time and efforts required for qualified signatures.*

II. Writing requirement

Before turning to electronic contracts, it is helpful to recall the general principles on when a writing (paper or electronic) is required for a contract.

By virtue of the principle of "*consensualisme*", a writing is not, as a general rule, a condition of *validity* of a contract. But a writing is required, as a general rule, to *prove* a contract involving more than 1500 euros (*ad probationem*).[4]

Here the focus is on proving the existence or content of a contract, which falls in the category of legal instruments or "*actes juridiques*". By contrast, non-writing proof, such as witness testimony or emails (not meeting the conditions of reliability to qualify as electronic writings)[5], can be used to prove "facts" such as performance or breach of a contract.

An exception to the general writing requirement exists, however, for certain types of commercial transactions (*actes de commerce*) with commercial companies or persons. Such commercial transactions can be proved against the commercial company or person by all means, not just by a

[4] C. civ., art. 1359 (« A legal instrument [such as a contract] involving a sum or value exceeding an amount defined by regulation must be proved by writing …"); F. Terré, Ph. Simler, Y. Lequette, F. Chénedé, Les obligations, Dalloz précis 13e édition (« Terré »), n° 1831 and 1904. Regulation has defined this threshold amount as 1500 euros. Décret n° 2004-836 of 20 August 2004, art. 56.

[5] Cass. soc., 25 sept. 2013, n° 11-25.884 (email sent by employer could be used as evidence to prove a fact in case involving wrongful termination of employee, without the need to verify whether email complied with conditions of reliability as electronic writing).

writing.[6] To qualify for this exception, however, the commercial transaction must fall within the ordinary commercial activity of the company, such as the purchase of goods for resale.[7]

As an example, a company purchases equipment from a reseller. The purchaser can prove this contract by all means, without the necessity to produce a writing.

There are other exceptions to the general writing requirement, in which a contract may be proved by other means than a writing: (1) in case of fraud or illicit nature of the contract[8], (2) where common usage is not to use a writing (e.g. contract between doctor and patient)[9], (3) in case of "moral impossibility" to have a writing (e.g. contract between family members or friends)[10], and (4) in case the writing was lost by a "force majeure" event[11].

As a practical matter, companies should try to create "writings" to prove their contracts, as a writing may either be required as proof or (in situations where a writing is not required) be persuasive proof. The best type of writing, having the strongest evidentiary value, is a formal contract signed by both parties. As companies increasingly turn to electronic contracting tools, they have very good reason to verify that their selected tools comply with enforceability requirements, discussed below.

But in addition to a formal contract, other types of writings can be relied upon as evidence of a contract.[12] This important point should not be forgotten, as it places in the right perspective the question of enforceability of electronic contracts, whose importance must not be exaggerated.

These "other" writings can be of various types. Registers and documents which professionals must keep and issue, have the same evidentiary value against their authors as contracts would, under art. 1378 of the civil code.

Professional registers and documents, although unilaterally created, present guarantees of accuracy because they are of a mandatory nature, must obey detailed legal rules as to their content, can be the subject of administrative audits, and can result in heavy sanctions in case of inaccuracies.[13]

For example, a buyer could prove a sale by presenting the invoice issued by the professional seller.

---

[6] C. com., art. L110-3 ("With regard to commercial persons, commercial acts may be proved by all means unless otherwise provided by law.").

[7] If both parties are commercial companies or persons, but the transaction is outside their commercial activity, the rules of civil law apply, i.e. general requirement for a writing. Civ. 1re, 23 mai 1977, Bull. Civ. I, n° 246; Com., 19 janv. 1993, Bull. Civ. IV, n° 21.

[8] Terré, n° 1919 ("The rule "fraus omnia corrumpit" justifies sufficiently that fraud may always be proved by all means, including by the parties themselves.").

[9] C. civ., art. 1360 (the principle of written proof "is subject to exception in case of material or moral impossibility to obtain a writing, if usage is not to establish a writing, or where the writing was lost by force majeure").

[10] C. civ., art. 1360

[11] C. civ., art. 1360

[12] Terré, n° 1835 ("The expression proof by writing immediately evokes a writing constituting a pre-established legal instrument, signed by both parties and intended to serve as perfect proof of the instrument in question. Reality is more diverse. *All kinds of other writings, having variable evidentiary value, may be introduced in court as items of evidence."*).

[13] Terré, n° 1862.

Writings used as proof must comply with the general requirement under art. 1363 of the civil code that, "no one may create an instrument by oneself". In general, this means a party cannot rely on a document created by it alone, as an item of proof.

Following up on the same example above, although the buyer could prove a sale by presenting the professional seller's invoice, the seller could not prove the sale that way, as the seller cannot rely on its own invoice.

Another type of writing that may be used to prove a contract, is emails or other correspondence between the parties. But emails will likely be weak evidence, since they are not signed and in most cases may not offer assurances of integrity (i.e. their content can be modified).

A writing insufficient by itself to prove a contract (such as an electronic contract not complying with applicable requirements) still may have some value, as it may be considered by a court as "commencement of written proof" (*commencement de preuve par écrit*). Other types of evidence, such as witness testimony, emails or correspondence between the parties, or partial performance of the contract[14] could then be used, to complement this insufficient writing, in proving the existence or content of a contract.

These "other" methods of proof admittedly are of uncertain evidentiary value, depending on their content and surrounding circumstances. Courts enjoy wide discretion in determining how much weight to give to these other types of proof[15], so this creates unpredictability about how the court will rule. These other methods should be relied on as a "last resort". Ideally what every company should seek to do, is to have enforceable written contracts, and if these are electronic, a number of requirements apply.

III. Legal recognition of electronic contracts

Legal recognition of electronic contracts can be traced back to 2000, when an EU directive[16] had called on EU member states to "ensure that their legal system allows contracts to be concluded by electronic means":[17]

[14] Cour d'appel d'Orléans, 2 mai 2019, No RG 18/01350 (holding that car lease agreement was enforceable, where car lessee acknowledged having received the financed vehicle and paid lease installments for 7 months, "which sufficed to establish the existence of the contract voluntarily performed whose existence was furthermore not at all challenged by the defaulting debtor", even though the lower court had found the electronic signature of the contract did not meet applicable requirements for validity).

[15] Guinchard (dir.), Droit et pratique de la procédure civile, Dalloz action, 9ème éd., 2017-2018, n° 341.73 (noting with regard to the procedure of verification of writing, which applies when a party denies the authenticity of a writing or claims it has been falsified, that "the Code of civil procedure offers [to the judge] the broadest powers to settle the issue and he enjoys a discretionary power to assess the items of evidence furnished to him").

[16] DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[17] EU directive on electronic commerce, art. 9(1).

"Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

Not all types of contracts, however, enjoyed this principle of enforceability, as the EU directive allowed member states to exclude certain contracts: real estate transfers; suretyship granted by persons outside their trade or profession; and family law contracts.[18]

France implemented this European directive by legislation enacted in 2004, which states that "where a writing is required for the validity of a legal instrument, it may be created and preserved in electronic form under conditions provided in articles 1366 and 1367."[19]

Article 1366 of the French civil code states:

"An electronic writing has the same evidentiary value as a paper-based writing, on condition that the person from whom it emanates can be duly identified and that it be created and preserved under conditions guaranteeing its integrity."

Integrity of the electronic writing, which must be ensured throughout its entire life cycle, constitutes the cornerstone of the proof mechanism for electronic documents.[20]

Article 1367 of the French civil code deals, in relevant part, with electronic signatures:

"Where [signature] is electronic, it is made based on the use of a reliable process of identification guaranteeing its link to the instrument on which it is made. The reliability of this process is presumed, absent contrary proof, where the electronic signature is created, the identity of the signatory assured and the integrity of the instrument guaranteed, under conditions defined by regulation by the State council."

[18] EU directive on electronic commerce, art. 9(2).
[19] C. civ., art. 1174.
[20] Cass. soc., 25 sept. 2013, n° 11-25.884, F-P+B, Sté AGL finances c/ L., Comm. Com. Elec. n° 12, Décembre 2013, comm. 132, note E. A. Caprioli; see also http://www.caprioli-avocats.com/publications/54-dematerialisation-archivage/275-regime-juridique-du-courrierelectronique-selon-la-cour-de-cassation.

Whenever a person denies being the electronic signatory of a document, so that there is a dispute about its authenticity, the court must examine whether the conditions set out in article 1367 are satisfied[21], in a special procedure called "verification of writing"[22].

A subsequent EU regulation[23] reiterated the fundamental principle of enforceability of electronic documents: "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form."[24]

This principle has been affirmed also in the exceptional cases, where a writing is required for the validity (and not just the proof) of a contract or other legal instrument (such as an admission of debt).[25] There are, however, exceptions to this principle, for certain types of contracts which can never be in electronic form, namely in family law (prenuptial agreement, divorce agreement) and suretyship law (personal guarantees).

In summary, a contract can as a general rule be made by electronic means.[26] We can summarize the legal requirements for enforceability of electronic contracts, as follows:

1. Identification of signatory (art. 1366): Where signature is electronic, it is made through a reliable process of identification (art. 1367).

2. Integrity of the contract is preserved during its creation and conservation (art. 1366).

For internet consumer transactions, in which a professional seller offers goods or services online (e.g. such as an online bookstore taking orders over the internet), there are special requirements for information disclosure, ordering process, and languages under art. 1127-1 of the civil code, but these will not be covered by this article.

We turn next to consider the key concept of "qualified electronic signatures", which are the type of signature offering the highest level of assurance as to identification of the signatory.

---

[21] Cass. Civ. 1ère ch., 30 septembre 2010, n° 09-68.555, Publié au bulletin (overruling lower court's recognition of electronic messages sent by landlord to tenant without verification that the conditions in art. 1316-4 (the predecessor to art. 1367) were satisfied); Cass. Civ. 1ère ch., 6 avril 2016, n° 15-10.732 (upholding lower court's recognition of electronic contract for complementary health insurance, based on court's findings that the electronic request for insurance coverage was created and preserved under conditions guaranteeing its integrity, that the signatory was identified through a reliable process guaranteeing the link of the electronic signature with the contract to which it is associated, and that the request for coverage produced in court mentions the delivery of this document by online contracting platform, allowing for a precise identification and authentication of the signatories).

[22] C. proc. civ., art. 287.

[23] REGULATION (EU) N°910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[24] Regulation (EU) n° 910/2014, art.46.

[25] Cass. 1re civ., 28 oct. 2015, n° 14-23.110, F P+B : Comm. Com. Elec.n°3, mars 2016, comm.30, note Eric A. Caprioli.

[26] Civ. 1re, 1er juill. 2015, n° 14-19.781 ; Ph. Le Tourneau, Contrats du numérique, Dalloz référence, 10ème édition 2018-2019 (« Le Tourneau »), n°412.42.

IV. Qualified electronic signature

Article 1 of French regulation issued in 2017[27] specified requirements for a reliable signature process, referring to the concept of "qualified" or "advanced" electronic signature as defined in the Regulation (EU) n° 910/2014:

"The reliability of a process of electronic signature is presumed, absent contrary proof, where this process implements a *qualified electronic signature*.

A qualified electronic signature is an advanced electronic signature, in conformity with article 26 of [Regulation (EU) n° 910/2014] and created through a mechanism of creation of qualified electronic signature fulfilling the requirements of article 29 of said regulation, which is based on a qualified certificate of electronic signature fulfilling the requirements of article 28 of this regulation."

The presumption of reliability of the signature process can be rebutted by "contrary proof". As stated by article 288-1 of the code of civil procedure, it is up to the judge to say whether the elements at his disposal justify the rebuttal of this presumption.

A qualified electronic signature has the equivalent legal effect of a handwritten signature.[28]

The Regulation (EU) n° 910/2014 defines "qualified electronic signature" and related terms as follows:

"(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

(12)'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;"

But a "qualified" electronic signature is not indispensable to an enforceable electronic contract. As stated in whereas 49 of the Regulation (EU) n° 910/2014:

« (49)This Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature.[29] However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature."

[27] Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique
[28] Regulation (EU) n° 910/2014, art. 25.
[29] This principle is implemented in Regulation (EU) n° 910/2014, art. 25.

Indeed, case law has upheld the validity of "simple" (i.e. not qualified) electronic signatures where the party relying on them proved that the process of their creation was reliable.[30] As stated by the court of appeals of Nîmes: "the principle is not that the signature is without value if it does not respect the requirements of regulation, but only that the reliability of the process is not presumed".[31]

Scanned signatures have been treated in different ways by courts. In some cases, courts have refused to recognize them for the reason that they were not created through a reliable process assuring the identity of the signatory[32]. In other cases, however, courts have been more open to recognition of scanned signatures, if they were corroborated by other evidence of identity of the signatory.[33]

We turn to study each of the criteria of a qualified electronic signature.

1) Advanced electronic signatures

To be qualified, an electronic signature must be an "advanced" electronic signature, meeting the following requirements set out in Article 26 of Regulation (EU) n° 910/2014:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

[30] Cour d'appel Aix en Provence, 26 juin 2014, Comm. Com. Electr. n° 11, Novembre 2014, comm. 90, note E. Caprioli (power of attorney which was electronically signed was held valid, as the online process of creation of the power was determined by an expert ("huissier de justice") to be reliable, as it described in great detail the different steps of validation in the process, through screen shots with voice instructions, under real-world conditions applying to a real user, and as it was based on a certificate issued by the party giving the power containing an acknowledgment by such party that it signed the request for the electronic power for the benefit of the debt collection company); see also Cour d'Appel Caen, 5 mars 2015. RG n°13/03009, commentaire E. Caprioli, dans Comm. Com. Electr. n° 5, Mai 2015.

[31] Cour d'Appel Nîmes, 1er octobre 2015, Comm. Com. Electr n°2, février 2016, comm.20, note E. Caprioli. See also Cour d'Appel Toulouse, 3e ch., 9 décembre 2015, n°15/01828, SA TKB c/ SARL Chevalier Diffusion.

[32] Cour d'appel de Fort-de-France, 14 décembre 2012, N° de RG: 12/00311 (refusing to recognize scanned signature of trademark application sent by applicant to National institute of industrial property, as "the mere scanned signature of [applicant] is insufficient to ensure the authenticity of his legal commitment as not allowing for a perfect identification of the signatory").

[33] Cass. Civ. 2ème ch., 28 mai 2020, n° de pourvoi 19-11.744, Publié au bulletin (overruling lower court's refusal to recognize scanned signature of payment demand document issued by interprofessional retirement fund to defendant, and stating that "the affixing on the payment demand document of the digital image of a handwritten signature does not allow, in and of itself, the conclusion that its signatory lacked the authority required to sign this document").

2) Qualified electronic signature creation device

Another requirement for being qualified, is that the electronic signature be created by a "qualified electronic signature creation device". The term "qualified electronic signature creation device" is defined as follows:

"(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;

(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;"

According to Annex II of Regulation (EU) n° 910/2014, qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

(b) the electronic signature creation data used for electronic signature creation can practically occur only once;

(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology.

Interpreting this requirement, the European Commission has noted that to ensure that the electronic signatures generated by a qualified signature creation device are reliably protected against forgery, suitable cryptographic algorithms, key lengths and hash functions are the prerequisite for the security of the certified product. Since this matter has not been harmonised at European level, Member States should cooperate to agree on cryptographic algorithms, key lengths and hash functions to be used in the field of electronic signatures.[34]

(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

Annex II further requires that, qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

Annex II also provides that, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes. This back-up must be performed in a manner so as to ensure the security of the duplicated

[34] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Whereas 8.

datasets is at the same level as for the original datasets. The number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.[35] Member States are required to notify to the European Commission the names and addresses of the public or private body responsible for such certification. The European Commission makes that information available to Member States.

This certification is based on a security evaluation process carried out in accordance with standards for the security assessment of information technology products. A part of such standards has been developed by the European Committee for Standardisation (CEN), for situations where the electronic signature creation data is held in an user-managed environment, and such developed standards are listed in the Annex to Commission implementing decision (EU) 2016/650 of 25 April 2016.[36]

For situations where the electronic signature creation data is managed by a qualified trust service provider on behalf of a signatory, standards will be developed. Until such development, the certification of signature creation devices shall be based on a process that uses comparable security levels and that is notified to the Commission by the certifying body.[37]

Member States notify the European Commission of a list of qualified electronic signature creation devices that have been certified.[38] The European Commission publishes such lists.

3) Qualified certificate for electronic signature and trust service providers

The third requirement for an electronic signature being qualified, is that it is based on a "qualified certificate for electronic signatures". This is where the key concept of "trust service providers" comes into play.

a) Qualified certificate

A "qualified certificate for electronic signature" is defined in Regulation (EU) n° 910/2014, as follows:

« (15)'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;"

To be qualified, a certificate for electronic signature has to meet the requirements laid down in Annex I of Regulation (EU) n° 910/2014, as follows:

[35] Regulation (EU) n° 910/2014, art. 30.
[36] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, art.1(1) and Whereas 4.
[37] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, art.1(2).
[38] Regulation (EU) n° 910/2014, art. 31.

Qualified certificates for electronic signatures shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

— for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

These requirements for qualified electronic signature certificates are an area where the EU regulation was careful to reserve to itself, and restrict the possibility for national law imposing additional requirements, which could have undermined the recognition of qualified electronic signatures across member states. As stated in article 28 of Regulation (EU) n° 910/2014: "Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I".

National law may only prescribe "non-mandatory additional specific attributes" for qualified certificates for electronic signatures. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

b) Qualified trust service provider

In addition to the Annex I requirements, qualified certificates for electronic signature must be issued by a "qualified trust service provider".

Regulation (EU) n° 910/2014 defines "qualified trust service provider" and related terms as follows:

"(16) 'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;

(19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body."

Member States must supervise (through designated bodies) qualified trust service providers established in their territory to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation (EU) n° 910/2014.[39]

i. Identity verification

When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.[40] This verification of identity is a fundamental function performed by the qualified trust service provider, allowing the provider to certify that the signer is the person he or she claims to be.

As verification of identity can take some time, it can be done as a first step as part of creating the qualified certificate. Once this certificate is created, electronic transactions can be performed quickly through the use of the certificate, without the need to verify identity for each transaction.

Identity shall be verified by the qualified trust service provider in the following manner:

[39] COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Annex 1, page 5.
[40] Regulation (EU) n° 910/2014, art. 24.

(a) by the physical presence of the natural person or of an authorised representative of the legal person; or

(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 of Regulation (EU) n° 910/2014 with regard to the assurance levels 'substantial' or 'high'; or

(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

(d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

ii. Expert staff

Qualified trust service providers must employ staff and subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards.

iii. Financial resources and insurance

Qualified trust service providers must maintain sufficient financial resources and obtain appropriate liability insurance, in accordance with national law.

iv. Terms of use of service

Qualified trust service providers must inform, in a clear and comprehensive manner, any potential customer of the precise terms and conditions regarding the use of their service, including any limitations on its use.

v. Security measures

Trust service providers are required to implement security measures:

"Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is

commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents."[41]

Qualified trust service providers must use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.[42]

Qualified trust service providers must use trustworthy systems to store data provided to them, in a verifiable form so that:

(i) the data are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity.

Qualified trust service providers must take appropriate measures against forgery and theft of data.

vi. Record-keeping

Qualified trust service providers must record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically.

This record-keeping requirement ensures that the qualified trust service provider (or a third party acting on its behalf, after the qualified trust service provider's dissolution) will be available, in the event of disputes involving electronic signatures certified by it, to provide relevant evidence to the court or authorities.

vii. Security breaches

Trust service providers must promptly report significant security breaches to their supervisory body and (in case personal data is affected) data protection authorities. Trust service providers must also inform any affected customers promptly of security breaches.[43]

viii. Conformity assessments

Qualified trust service providers must undergo conformity assessments every 24 months by conformity assessment bodies, to confirm compliance with the EU regulation.[44] The conformity assessment report

[41] Regulation (EU) n° 910/2014, art. 19.
[42] Regulation (EU) n° 910/2014, art. 24.
[43] Regulation (EU) n° 910/2014, art. 19.2.
[44] Regulation (EU) n° 910/2014, art. 20.

is promptly provided to the supervisory body. Any shortcomings revealed by an assessment must be remedied. Failure to do so may cause the trust service provider to lose its qualified status.

ix. Trusted lists

Each Member State publishes trusted lists, containing information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.[45] The French trusted list is available at the EU trusted list browser at https://webgate.ec.europa.eu/tl-browser/#/.

These trusted lists are a handy, free, reliable reference for anyone in need to determine the qualified status of a trust service provider at a given time.

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. The list shall clearly indicate which trust service providers are not qualified.[46]

For help in understanding signs and acronyms used in trusted lists, readers can refer to Annex I of COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015, which laid down technical specifications and conventions for trusted lists.

x. Trust mark

After being included in the trusted list, qualified trust service providers can use an EU "trust mark" to indicate in a simple, recognisable and clear manner the qualified trust services they provide.[47] This EU trust mark was created to enhance confidence and convenience by users in online services and to allow qualified trust service providers to distinguish themselves in the market, thus contributing to transparency.[48]

The EU trust mark for qualified trust services was established through a competition of art and design students organized by the European commission, and is as follows:[49]

[45] Regulation (EU) n° 910/2014, art. 22.
[46] COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015, art. 2.
[47] Regulation (EU) n° 910/2014, art. 23.
[48] Regulation (EU) n° 910/2014, Whereas 47.
[49] COMMISSION IMPLEMENTING REGULATION (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services, Annex 1.

EU trust mark for qualified trust services in colour

xi. Liability

The EU regulation provided for the liability of trust service providers "for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation"[50]. Being critical players in the qualified electronic signature process, trust service providers were thus made accountable for their shortcomings.

Trust service providers can limit their liability, however, by limiting the use of their services. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.[51]

For example, a trust service provider might limit its services to a particular type of transaction, or might exclude certain types of transactions (e.g. real estate transactions). Or a trust service provider might set a monetary cap on the value of transactions for which it provides trust services.

xii. Providers outside EU

If the trust service provider is in a third country outside the European Union, its trust services will be granted the same legal effect as EU-originated trust services if they are recognized as equivalent by a treaty between the EU and the third country.[52] These equivalence treaties provide for EU requirements to apply to the non-EU trust services, and for reciprocal recognition of EU trust services in the third country.

4) Validation of qualified electronic signatures

[50] Regulation (EU) n° 910/2014, art. 13.
[51] Regulation (EU) n° 910/2014, art. 13.2.
[52] Regulation (EU) n° 910/2014, art. 14.

Trust service providers perform validation of qualified electronic signatures. As part of this validation, the trust service provider performs a series of checks, to ensure that all the various elements of a qualified electronic signature are present in a specific signature:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of Regulation (EU) n° 910/2014;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the electronic signature was created by a qualified electronic signature creation device;

(g) the integrity of the signed data has not been compromised;

(h) the requirements provided for "advanced electronic signatures" were met at the time of signing.

The system used for validating the qualified electronic signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security issues.

V. Integrity of contract

In addition to identification of the signatory, the other key requirement for validity of electronic contracts is that, their integrity be preserved during creation and conservation (art. 1366).

Here are a few takeaways and lessons from how cases have interpreted this integrity requirement:

a. Archived copy should be *identical* to the original

Although this may seem obvious and easy to achieve with modern software, it is important to make sure the archived copy does not display any differences from the original, which could call into question the integrity of the archiving process. In one case, a court refused to recognize an archived copy of a letter (whose existence was challenged by the recipient) because the archived copy showed a newer logo of the sender, instead of the logo existing at the time the letter had been sent.[53]

[53] Cass. civ. 2ème, 4 décembre 2008, SNC Continent France c/ CPAM de la Marne, pourvoi n° 07-17.622, Note Eric Caprioli, Comm., Com. Electr. (Lexisnexis), février 2009, n°19, p. 44 et s.

b. Archiving process should conform to standards, as confirmed by audits.

The archiving process used by a company (or its supplier) should conform to industry standards. It is also important that this conformity be confirmed by independent audits, as courts have relied on audit findings in determining whether an archived copy is reliable.[54]

VI. Questionnaire and review of electronic signature service providers

Companies using electronic signature service providers have good reason to verify the compliance of their providers with the EU and French requirements.

A company needs to begin by determining how important the enforceability of electronic contracts really is, in light of the company's contracting parties and the availability of alternative items of evidence.

As seen above, commercial transactions (where a company is doing business with other commercial companies) can be proved under French law by any type of evidence. Thus, in these commercial transactions, even if an electronic contract is not enforceable (such as because of a non-complying signature process), the company will still be able to prove the transaction by other means, such as correspondence, which will be available and substantial if the transaction involves significant negotiation between the parties.

These commercial scenarios may justify a simpler approach to electronic contracting, with lighter identification and signature processes, which are cheaper and faster. The risk of non-enforceability of electronic contracts may be outweighed by considerations of speed and simplicity in the signature process.

By contrast, if a company is transacting with consumers or small non-commercial companies (like doctors, accountants, lawyers, or other professionals performing "civil" acts), it will be important to ensure enforceability of electronic contracts, as here a "writing" will be necessary at least for transactions above 1500 euros.

Another consideration in determining the importance of enforceability will be the type of transaction involved. Highly sensitive transactions, such as financial ones, will require a high level of identification assurance and impose strict signature processes.

Aware of its real needs and the level of assurance needed for enforceability of its electronic contracts, a company will be able to adapt the review and questionnaire used with its service providers.

1) Questionnaire to service providers

[54] Cour d'appel de Paris, 9e ch., 11 février 2016, Comm. com. électr. mai 2016, n°5, comm. 47, note E. Caprioli.

Although representations and warranties can be negotiated in contracts, companies can go one step further and conduct reviews of compliance through questionnaires, containing the following questions:

1. Are the electronic signatures issued by the provider, "qualified" electronic signatures as defined by the Regulation (EU) n° 910/2014?

    a. If yes, please confirm the electronic signatures issued are "advanced electronic signatures" which meet the requirements set out in Article 26 of Regulation (EU) n° 910/2014.

    b. If yes, please confirm the electronic signatures are created by 'qualified electronic signature creation device' that meets the requirements laid down in Annex II of Regulation (EU) n° 910/2014.

    c. If yes, please confirm that the conformity of the qualified electronic signature creation device used with the requirements laid down in Annex II has been certified by appropriate public or private body designated by relevant Member State. Please indicate the name of the certifying body and provide copy of certification.

    d. If yes, please provide copy of the certificate from supervisory body attesting to qualified status of the trust service provider used.

    Please provide name of trust service provider used.

    e. If yes, please confirm that the certificate for electronic signatures meets the requirements laid down in Annex I of Regulation (EU) n° 910/2014.

    f. If yes, please provide copy of the latest conformity assessment report issued for the qualified trust service provider.

2. Are there any "limitations" identified by the trust service provider used (who may be either the electronic contract service provider itself, or a third party subcontractor) on the use of the trust services?

    If yes, are electronic signatures being issued in a manner exceeding such limitations?

3. Is the trust service provider established in a third country outside the EU? If yes, is there an equivalence treaty between the EU and the third country, providing for recognition by the EU of the trust services originating in the third country?

4. Does the archiving process conform to industry standards? If yes, please identify standards.

5. Do independent audits confirm the conformity of the archiving process to industry standards? How frequently? When was the last such audit, and what was the audit finding?

2) Reviews

In addition to questionnaires and analysis of answers, companies can assess the compliance of their electronic signature providers by reviews, including the following:

a) A search of public announcements by the relevant supervisory body (overseeing the trust service provider used) can be performed, to look for any breaches of security or loss of integrity committed by the trust service provider.

b) The relevant national trusted list should be checked, to confirm the qualified status of the trust service provider.