Luxembourg law

E-signatures in Luxembourg, practical aspects

Nicolas MARCHAND
Lawyer, Partner, AKD Luxembourg S.à r.l.[1]

TABLE OF CONTENT

1. Introduction

The recent Covid-19 pandemic showed the importance of remote working and demonstrated more than ever that the e-working environment is key to the reliability of businesses. In this redefined environment, organisations may be tempted or forced to move away from paper documents with wet ink signatures and replace them by e-signatures. In making such a change, it is important to pause and carefully consider the type of e-signatures[2] and their legal consequences. This article briefly describes the legal environment surrounding the e-signature and highlights practical aspects of the use of e-signatures in the corporate world and provides guidance on the legal requirements for electronic signatures in commercial transactions under Luxembourg law.

2. General overview of the legislative framework

This section summarizes the key regulations and legal framework surrounding the use of e-signatures in Luxembourg. While not exhaustive, it aims to provide the reader with a high-level summary of the legal environment, before entering into legal and practical considerations.

a. Directive 1999/93/EC of the European Parliament and the Council on a Community framework for electronic signatures (E-Signature Directive)

The purpose of this directive was to facilitate the use of electronic signatures and to contribute to their legal recognition by establishing a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.[3]

This E-Signature Directive did not, however, seek to harmonize national rules concerning contract law, particularly the formation and signature processes. The provisions of the E-Signature Directive concerning the legal effect of electronic signatures were thus, without prejudice to requirements regarding form, laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded.[4] In other words, although the E-Signature Directive specified the legal effect of an e-signature, it did not assure recognition in other EU member states.

1. The present work reflects the author's view solely
2. This article is dedicated to electronic signatures and does not cover, nor specifically address, the electronic seal as contemplated by the eIDAS Regulation (as defined below).
3. Directive (EC) No. 1999/93 of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ L*, No. 13, 19 January 2000, art. 1.
4. Directive (EC) No. 1999/93 of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ L*, No. 13, 19 January 2000, whereas 17.

b. Luxembourg law on electronic commerce dated 14th August 2000 (E-Commerce Act)

The E-Commerce Act constitutes the core of the Luxembourg e-commerce framework and sets out the main rules governing, amongst other things, the use of electronic signatures, the activity of the providers of e-signature solutions and their supervision.

This law was enacted immediately after the E-Signature Directive and Directive 2001/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. This shows Luxembourg's desire and appetite to be the best in class in terms of e-commerce in Europe. As is usually the case in Luxembourg, the E-Commerce Act faithfully transposed the terms of the E-Signature Directive.[5] The E-Commerce Act was subsequently amended.

c. Grand Ducal regulation dated the 1st of June 2001 relating to electronic signatures, to electronic payment and to the creation of an E-commerce committee (the 2001 Regulation)

Finally, this initial set of regulation cascading from the E-Signature Directive to the E-Commerce Act was completed by execution regulations. The 2001 Regulation sets forth in detail, with regard to the e-signature, the requirements applicable to:

- the qualified certificate applicable to the e-signature, which topic we will revert to later in this paper;
- the certifying service providers delivering the qualified certificates; and
- the technical system creating e-signatures.

d. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation)

Fifteen years after the E-Signature Directive, the eIDAS Regulation was introduced to harmonize the European framework for electronic signatures along with stricter obligations on trust service providers. It took effect on 1 July 2016 and replaced the E-Signature Directive. The legislative change from a directive to a regulation demonstrates that the level of harmonisation brought by the E-Signature Directive was far from perfect and lacked interoperability between the various systems used amongst the member states.[6]

The eIDAS Regulation includes the rules for trust services[7], which are key services contributing to the security and validity of transactions, such as the e-signature, the authenticity, the time stamping, etc.[8] The eIDAS Regulation also established the legal framework for e-signatures by distinguishing between standard electronic signatures, advanced electronic signatures and qualified electronic signatures. The eIDAS Regulation remains technologically neutral, however.[9] It is therefore a toolbox specifying the rules of the games of a hopefully level playing field.[10]

e. Luxembourg act of 17 July 2020 amending the E-Commerce Act

Following the pendulum movement initiated by the E-Signature Directive and the E-Commerce Act, the act of 17 July 2020 was a response to the eIDAS Regulation in Luxembourg.

The legislative process was initiated on 1 March 2019. The draft law intended to align the current Luxembourg regime on electronic signatures stemming from the e-Commerce Law with the eIDAS Regulation. Again, the responsiveness of the Luxembourg legislator is noteworthy and underlines the importance of e-commerce at large for the Grand Duchy of Luxembourg, this being part of the business-friendly environment that Luxembourg cherishes.

A coarser look shows this legislation to represent the last piece in the evolution of Luxembourg's legal framework on trust services (including e-signatures) and e-archiving. With regard to e-signing particularly, the act mainly aligns the Luxembourg legal framework with the eIDAS Regulation.

While the law provides for extensive amendments of the E-Commerce Act (notably with regard to recognising qualified trust service providers and by introducing administrative and criminal sanctions for breach of the E-Commerce Act and the eIDAS Regulation by trust service providers), the articles of the Luxembourg Civil Code (the **Code**) relating to e-signature (as inserted by the E-Commerce Act) remained untouched.

5. E. THIEL and A. HELVIG, "Le régime juridique des opérations bancaires en ligne à l'épreuve de la réalité" in *Droit bancaire et financier au Luxembourg*, Larcier-Anthemis, 2014, p. 1076.
6. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, whereas 9.
7. Pursuant to Article 3 of the Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, trust services "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".
8. M.F. GONZALEZ, "Le règlement eIDAS: l'identification électronique et les services de confiance au service du citoyen et du consommateur", *R.E.D.C.*, 2016, vol. 1, p. 36.
9. M.F. GONZALEZ, "Le règlement eIDAS: l'identification électronique et les services de confiance au service du citoyen et du consommateur", *R.E.D.C.*, 2016, vol. 1, p. 45.
10. D. GOBERT, "L'identification électronique et les services de confiance dans le règlement eIDAS", *JTDE* 2016/7, No. 231, p. 250.

3. Legal requirements applicable to e-signatures

Now that we have glanced at key legislative pieces applicable to the e-signature at large, it is time to address in more detail the different types of e-signatures and more in particular the various requirements applicable to each type. We have seen that the eIDAS Regulation distinguishes between three types of e-signature by the level of assurance they offer, i.e. the standard electronic signature, the advanced electronic signature and the qualified electronic signatures.

a. Standard electronic signature

The eIDAS Regulation defines an electronic signature as "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]

Under the first indent of Article 1322-1 of the Code, which addresses the requirements applicable to any signature (thus covering both wet ink and e-signatures), a signature must (i) identify the person signing and (ii) evidence the person's approval to the terms of the agreement.

Put simply, it means that any electronic tool identifying the signatory and capturing its intent to approve a document qualifies as an electronic signature as such. The form of a standard electronic signature is not defined, so it can take different shapes: from a typed name in an email to biometric data, for example.

One might even wonder whether acceptance could result from an email. As for the standard electronic signature, the burden of proof of meeting the legal requirements (as stated above) lies with the claimant in the event of a challenge.[12] If so, the rules of evidence come into play. Pursuant to Article 1108 of the Code, a contract is created as soon as there is an offer and an acceptance of the essential and lawful elements of that contract. It is, however, important to consider the difference between evidentiary regimes applicable to civil matters and commercial matters:

- In civil matters, Article 1341 of the Code requires that any agreement having a value of more than 2500 EUR needs to be evidenced in writing (either by public deed or under private seal). Leaving the public deed aside, Article 1322 of the Code solely requires that a private seal agreement be in writing and signed (either wet ink or electronically).
- In commercial matters, evidence between merchants[13] can be brought by any means as per Article 109 of the Luxembourg Commercial Code. Assuming that the parties are only corporate entities and acting in commercial matters, an email may therefore be used as evidence of the agreement to create a contract. This opinion is supported by first-instance Luxembourg case law, in which judgement the court sustained that an email was sufficient to express the consent and create the agreement, while no signature was affixed onto the agreement.[14] In Belgium, limited case law appears to suggest that an email could be used as a beginning of proof.[15]

Another common form of standard electronic signature is to use/affix a scanned signature on the agreement.[16] This technique has been subject to various litigation in Belgium, from which it emerges that its validity is tied to the ability to link the authentication method (i.e. the ability to link the signature to an identified or identifiable signatory).[17] This linkage offers a higher probative value and can be met technically by the use of login or passwords. While the basic method of authenticating a signatory is to use an email address, this may be considered insufficiently secure for most commercial transactions. A simple way of improving certainty is to opt for a two-factor authentication such as an SMS, one-time password or knowledge-based authentication to verify each signatory's identity. Such a service, which can be provided on an as-is basis by an external service provider, adds certainty to the signature process while remaining less cumbersome and significantly cheaper than obtaining an advanced or qualified electronic signature.

When it comes to commercial contracts, it is important to note that the evidentiary regimes applicable to the civil matters and commercial matters as set forth in the Code can, to a certain extent, be deviated from. It is thus possible for the contracting parties to agree on which means of proof are acceptable and/or which evidentiary value is attributed to certain documents. In other words, it is advisable to carefully cover those

11. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 3.
12. M. BRAUN, "Preuve et nouvelles technologies au Luxembourg", *Annales du droit luxembourgeois*, vol. 23, 2013, p. 104 *in limine*; Trib. arr. Luxembourg (civil), nr. 80/217, 7 avril 2017, p. 25.
13. In the event of a mixed contract (i.e. between a merchant and non-merchant), the non-merchant can use any evidentiary means against the merchant, while the merchant will have to comply with the Code in terms of acceptable evidence.
14. Trib. arr. Luxembourg (commercial), 2 avril 2014, *Pas. Lux.*, p. 392. Please, also refer to the case law quoted by M. BRAUN, "Preuve et nouvelles technologies au Luxembourg", *Annales du droit luxembourgeois*, vol. 23, 2013, p. 104.
15. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 24.
16. Please, refer to section 3a) with regard to handwritten documents being subsequently scanned.
17. J.B. HUBIN, "Signature scannée: quand une technologie simple confronte le juriste à des questions complexes", *RDTI* 2014/3, nr. 56, p. 125; see A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 131, p. 146; F. GEORGE, *et al.*, "Contrats de l'informatique et commerce électronique. Chronique de jurisprudence 2015-2017", *RDTI* 2017, p. 44.

elements in the contractual agreements by including specific clauses, such as in the banking environment.[18]

With regard to the legal effect of a standard electronic signature, the eIDAS Regulation creates a non-discrimination principle, meaning that an e-signature may not be denied legal effect and admissibility solely on the grounds that it is electronic or that it is not considered a qualified electronic signature.[19] A standard electronic signature is admissible in court as evidence and is capable of serving as *prima facie* evidence of an agreement.[20] In the event of a dispute, the signatory and/or party claiming the validity of this electronic signature would have to provide evidence to sustain its claim and demonstrate that the signature meets the conditions set forth by Article 1322 of the Code.[21] The main benefit of the non-discrimination principle is to allow and embrace the evolution of technologies but its drawback is an uncertain probative value, which is ultimately assessed by the courts.[22]

b. Advanced electronic signature

The advanced electronic signature needs to meet the following requirements[23]:

- uniquely linked to the signatory;
- capable of identifying the signatory;
- created using electronic signature creation data that the signatory can, with a high level of confidence, use under his/her sole control; and
- linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

In substance, an advanced electronic signature is a more sophisticated and secure form of electronic signature meeting certain criteria ensuring the authenticity of the signature and the integrity of the signed document (i.e. that the data was not altered).

As we have pointed out, the eIDAS Regulation is technologically neutral. However, based on current practice, advanced electronic signatures are based on the use of cryptography, meaning that the digital signature is created using public-key cryptography and inserted into the code of the electronic document. Basically, the advanced electronic signature securely associates the signature with a document in the form of a coded message. Please refer to section 4 below for further details on the most common technologies in use at the moment.

The eIDAS Regulation does not confer specific legal effects to advanced electronic signatures. It benefits from the same non-discrimination principle that applies to standard electronic signatures as detailed above and the burden of proof in the event of challenges remains with the claimant. However, the stronger the technical security is in the applied technology, the greater the chance that the advance signature would be considered valid in case its validity is challenged in court.[24] In other words, the eIDAS Regulation creates a toolbox for the parties to decide what level of security matches their needs.[25]

c. Qualified electronic signature

Finally, under the eIDAS Regulation, a qualified electronic signature has to meet the following criteria[26]:

- created by a qualified electronic signature creation device; and
- based on a qualified certificate for electronic signatures.

The first condition, as we have seen with the advanced electronic signature, implies that the software or hardware used to create the e-signature complies with the requirements on confidentiality and integrity of the data, as provided for a qualified electronic signature in Annex II of the eIDAS Regulation.

With regard to the second condition, a qualified certificate is an electronic certificate issued by a qualified trust service provider (**QTSP**) and containing the information required under Annex I of the eIDAS Regulation.[27] Thus, a qualified electronic signature must meet the requirements for an advanced electronic signatures and be supported by a qualified certificate issued by a QTSP whose credentials have been recorded in a trusted list published by a member state. Please refer to section 4.b below for further details.

18. E. THIEL and A. HELVIG, "Le régime juridique des opérations bancaires en ligne à l'épreuve de la réalité" in *Droit bancaire et financier au Luxembourg*, Larcier-Anthemis, 2014, p. 1082 *et seq*. In this article, the authors rightfully point out that the use of clauses relating to the means of proof and/or their evidentiary value is uncertain. To limit the uncertainty relating to their admissibility it is important that the clauses are not one-sided and/or arbitrary.
19. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 25.
20. D. GOBERT, "L'identification électronique et les services de confiance dans le règlement eIDAS", *JTDE* 2016/7, No. 231, p. 254.
21. In accordance with Article 1347 of the Code pertaining to the beginning of proof by writing.
22. J.B. HUBIN, "Signature scannée: quand une technologie simple confronte le juriste à des questions complexes", *RDTI* 2014/3, nr. 56, p. 125; E. MONTERO, "La signature électronique au banc de la jurisprudence", *DAOR* 2011/98, p. 236.
23. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 26.
24. In this regard, the E-Commerce Act introduced Article 292 of the *Nouveau Code de Procedure Civile;* see also P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 18.
25. M.F. GONZALEZ, "Le règlement eIDAS: l'identification électronique et les services de confiance au service du citoyen et du consommateur", *R.E.D.C.*, 2016, vol. 1, p. 41.
26. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 3.
27. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 28.

From a legal standpoint, a qualified electronic signature has a probative value that is equivalent to a hand-written signature.[28] This principle of equivalence is covered by the second indent of Article 25 of eIDAS. Consequently, in the event of a dispute, the authenticity of such electronic signature is presumed and the reverse burden of proof principle is applied, meaning that the person challenging the validity of a qualified electronic signature would have to provide evidence to that effect. It is also important to mention that the qualified electronic signature benefits from an EU-wide recognition based on eIDAS Regulation.[29]

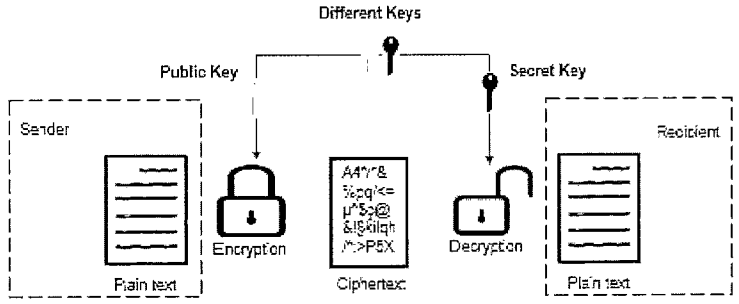
4. Technical aspects

a. Asymmetrical encryption

The general technical consensus regarding advanced and qualified electronic signatures is to use asymmetrical encryption, also known as public-key encryption.[30] Without entering into technical details that for the large part vastly exceed the author's knowledge and capabilities, it is nonetheless important to understand the basic principles.

Broadly speaking, encryption concerns the conversion by an algorithm of a plain text document into unintelligible ciphertext. In other words, the encryption transforms readable data into unreadable data, unless you have the "key" to turn them back into a readable form. More specifically, asymmetrical encryption uses not one but a pair of related keys – a public and a private key.[31] The public key, which can be shared with everyone, is used to encrypt the plaintext document into ciphertext.[32] This step secures the document towards unrelated parties. There are several types of digital signature algorithms, each with its own particular mechanism, but essentially, the data will be signed with a private key, and the receiver of the message can then check its validity by using the corresponding public key provided by the signatory.[33] Private keys must remain confidential to their respective owners and can be stored on the computer, a smart card, a token, etc. Contrary to handwritten signatures, which are constant, digital signatures are directly linked to each document.[34]

While both the public and the private keys are mathematically related, the private key cannot be derived from knowing the public key. Technically, both the public and private keys are computed together at the same time, in the same mathematical process, using "trapdoor" functions. The main characteristic of "trapdoor" functions is that they are easy to compute one way, yet difficult to compute in the opposite direction (finding its inverse) without special information.[35]



The asymmetrical encryption offers a high level of security as compared to notably the symmetric encryption, in which the very same key is used for both encrypting and decrypting messages. In this latter technique, the entire mechanism is dependent on keeping the key a shared secret.

b. Trust service providers (TSPs) and QTSPs

The asymmetrical encryption does not suffice to fulfil the requirements of an advanced or qualified signature under the eIDAS Regulation. Under the eIDAS Regulation, another important element is the linkage with the signatory, i.e. the ability to establish the identity of the signatory. To that effect, TSPs and QTSPs are used. For example, QTSPs must verify the identity of

28. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 20.
29. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 25.3.
30. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 127, p. 141; P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 13.
31. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 128, p. 142.
32. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 13.
33. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 11.
34. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 130, p. 144.
35. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 128, p. 142.

the person to whom a qualified certificate is provided based on official identification documents.[36] To simplify, an electronic certificate is the electronic ID of the signatory.[37] The service providers aim at demonstrating that the use of a specific public key belongs to a specific person.[38]

The eIDAS Regulation defines a set of minimum requirements to be met by all TSPs and requires stricter requirements for QTSPs. This ensures the highest level of security and consolidates the legal recognition and acceptance of the e-signing process across EU member states while ensuring a level playing field for all competitors.

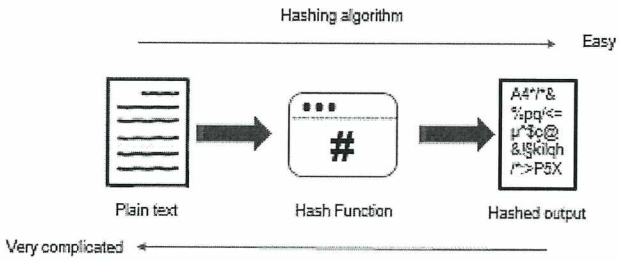
Using a QTSP is the only way of having a qualified electronic signature. This higher level of security is to be used for transactions that require a high level of legal certainty. Conversely, the use of TSPs might be more suitable for transactions where the risk of challenge is remote, such as e.g. group restructurings.[39]

In accordance with the eIDAS Regulation, each member state must draw up a list of QTSPs. In Luxembourg, this list is maintained by the Luxembourg Institute for Standardisation, Accreditation, Safety and Quality of Products and Services. This list, as per the date of this article, includes only two QTSPs (LuxTrust S.A. and BE INVEST International S.A.). The European Commission holds a centralised trust services browser for all member states (https://webgate.ec.europa.eu/tl-browser/#/). This is a helpful tool to verify the qualification status of the trust service providers. In fact, it should be remembered that as per the eIDAS Regulation a qualified electronic signature based on a qualified certificate issued in any EU member state must be recognised as a qualified electronic signature in all other EU member states. In that regard, the leading worldwide actor (i.e. Docusign) is a QTSP registered in France and benefits from this passporting provision to operate EU wide.

c. Hashing

Lastly, for an e-signature to qualify as an advanced or qualified electronic signature under the eIDAS Regulation, it is still necessary to ensure the document integrity, i.e. that no changes have been made to its content. This last issue is generally solved by "hashing" the data.[40] We have seen that encryption is a two-way function. The keys enable encryption and decryption, depending on the method used. Hashing, however, is a one-way function. The algorithm scrambles plaintext to produce a unique message digest, which is why hash functions are widely used for verifying the authenticity of digital data.[41] There is no way to invert the hashing process to reveal the original password.

The hashing, it follows, comes in addition to the encryption to ensure that no alteration of the data occurred while transferred or stored. This provides protection against malicious or unintentional modification of the data.



d. Digital e-signature

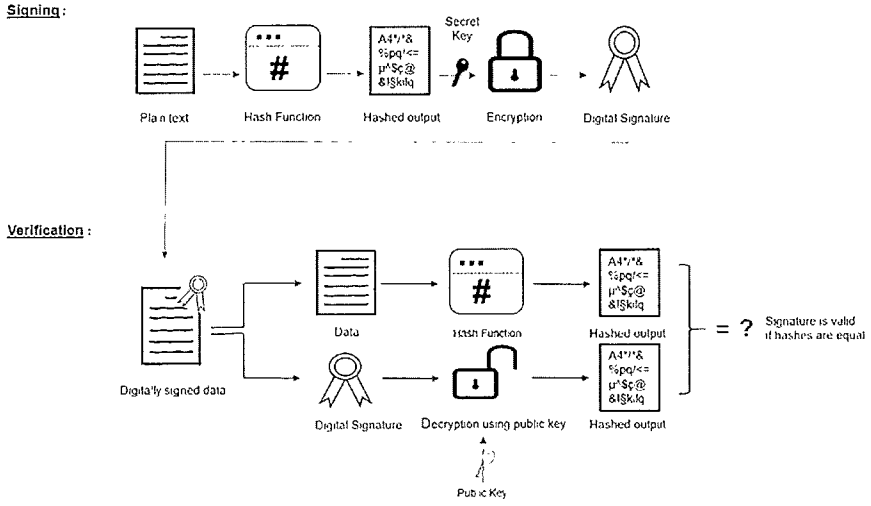
The digital signature process ensures that the cryptographic goals of authentication, integrity, and non-repudiation are met.

When combined with asymmetrical encryption, the so-called cryptographic hash function can be used to generate a digest that acts as a digital fingerprint. This means that any change in the input data (message) would result in a completely different output (digest). Now that the basic technical elements are clear, it is time to summarise the use of a qualified electronically signed document between two parties[42]:

- The plain text document (e.g. a Word draft agreement) is hashed to create a unique message digest guaranteeing its integrity.
- The digest is encrypted with the signatory's private key resulting in the digital signature, which is added to the digest.

36. Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité commerce électronique, *Mémorial*, 22 juin 2001, art. 3 (1), 4°.
37. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 133, p. 148.
38. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 11.
39. D. GOBERT, "L'identification électronique et les services de confiance dans le règlement eIDAS", *JTDE* 2016/7, No. 231, p. 254.
40. P. VAN EECKE, "De elektronische handtekening in het recht", *RDC* 2009/4, p. 13.
41. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 129, p. 142.
42. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 129, p. 142.

- Once the encrypted document is received, the counterparty decrypts it with the signatory's public key.
- The counterparty also hashes the decrypted document, resulting in a message digest again.
- If the document digests match, then the counterparty can be sure that the sender signed the document and that the content of the message is unaltered. Any difference in the hash values would reveal tampering of the message.
- The identity of the signatory is confirmed by the QTSP.



5. Scope of e-signature and e-contracts

While the scope of the E-Commerce Act (as amended) is to cover all B2B and B2C contracts, Article 50 excludes certain contracts, which cannot be concluded electronically. These contracts mainly are:

- contracts creating or transferring rights on real estate (except rental rights);
- contracts for which the law requires the involvement of courts, public authorities or professions exercising a public authority (such as notaries);
- security agreements and guarantees given by persons acting outside the scope of their professional or commercial activities; and
- contracts relating to inheritance and family law.

Additionally, Article 2 of the E-Commerce Act excludes certain activities (taxation, agreement and practices subject to cartel rules and gambling activity) from its scope of application.

Subject to very specific exceptions, contracts can be entered either in electronic or paper version. Once the formalist question relating to the acceptability of the electronic format for a contract is solved, it must still be considered how such an agreement can be enforced. In that regard, it should be recalled that the Code makes a distinction between B2B and B2C disputes over evidentiary rules applicable to any such disputes, as further detailed above under section 3, point a).

6. Practical aspects relating to e-signature

a. PDF copies of wet ink documents

It is very common practice to exchange PDF copies of signature pages in commercial matters. It should in that regard be noted that where a document is physically signed and then exchanged electronically, the wet ink copy will constitute the original version of the agreement. The fully compiled PDF version will only be an electronic copy of that wet ink document.[43]

Where agreements are signed in counterparts with wet ink signatures and subsequently compiled as is often the case in transactions, it will thus be important to ensure that each party effectively receives a properly compiled original set of the agreements. It should be noted that in accordance with Article 1325 of the Code, the formality of having as many copies of an agreement as there are parties with a distinct interest does not apply to electronically signed

43. O. POELMANS, *Le droit des obligations au Luxembourg*, Larcier, 2013, p. 526, E. MONTERO, "La signature électronique au banc de la jurisprudence", *DAOR* 2011/98, p. 232.

agreements, which eases the process when having multiparty agreements.

b. Mixed signing

To our knowledge, there is no Luxembourg case law relating to mixed signing, i.e. where one party to a deed signs a counterpart in wet ink and another signs a counterpart electronically. Whilst we think such a signed document is likely to be valid, provided the documentation authorises counterparts and each party uses a valid signature method.[44] From an evidentiary point of view, mixed signings should, however, not be preferred as the audit trail is more complex to establish.

c. Tax implications

One of the main advantages of the e-signature is its flexibility in terms of the location of the signatories. A contract can be signed by different signatories located in various jurisdictions. While this is obviously welcome, it is also important to carefully assess the possible tax impact as neither the eIDAS Regulation nor the E-Commerce Act addresses the place of execution of electronically signed documents.

From a tax standpoint, this may notably raise questions as to substance. If the e-signatories are not present in Luxembourg when executing corporate documents, such as board minutes, or contractual documents, this may indeed affect the assessment of facts relating to the company's place of effective management, central administration and control. It should also be taken into account that the place of execution may have particular legal consequences (e.g. stamp duty). It is worthwhile to consider those elements in advance and properly document those aspects in the agreement.

d. Timing of execution

Another point worth noting is that the eIDAS Regulation implements the concept of electronic time stamping.[45] [46] While exceeding the scope of this article, the concept nonetheless needs introducing. If the electronic time stamp is a qualified electronic time stamp within the meaning of Article 42 of the eIDAS Regulation, it carries a presumption of accuracy as to the date and time indicated. In practice, time and date stamping can also be made without being considered a qualified electronic time stamp under the eIDAS Regulation. In both cases, the electronic stamp should be admissible as evidence in legal proceedings but their evidentiary value will be subject to the same discussions as for the electronic signature.[47]

What happens if no stamp is attached to the electronic document and the agreement makes no mention of these points? There is no default rule setting the time of execution of an electronic signature. By default, certain scholars[48] refer to the civil rule under which a contract is deemed to be concluded at the place and time where the offering party has or could have had knowledge of the acceptance of its offer.

e. Financial collateral arrangements

Article 2.2 of the act on financial collateral arrangements dated 5 August 2005 expressly states that the written agreement evidencing the provision of collateral can be in an electronic format. Since the Covid-19 outbreak, market participants have been increasingly relying on electronic signatures to sign financial collateral arrangements in order to ease the signing process. Perfection formalities, such as notifications, can also be signed electronically. Certain formalities may nevertheless still require wet ink signatures in practice; this will, for instance, typically be the case for the purpose of registering a pledge on financial instruments in registered form, which will require an entry into the register of such financial instruments, usually countersigned by a member of the management of the company.

f. E-archiving and obsolescence

As we have seen, there is one major difference between a wet ink and electronic agreement, which is that the latter needs to come with reliable warranties that its integrity has not been altered since its execution. For certain authors, the integrity of an electronically signed contract is ensured by the qualified electronic signature itself as one of its elements is, as we have seen, to be a set of data inseparably linked to the act, which guarantees its integrity.[49]

While the purpose of this article is limited to the e-signature, it should be added that the electronic contracts are to be correctly stored in readable format for the applicable legal retention periods. The eIDAS Regulation[50] only sets forth the minimal principle of

44. See Practice note of The Law Society, "Execution of a document using an electronic signature", 2016, nr. 4.5.
45. With regard to the competence of the court, in contractual matters, parties should refer to the courts of the place of performance of the obligation in question. See Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, art. 7, (1), (a); and also Nouveau Code de procédure civile, art. 28.
46. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 33(3).
47. D. GOBERT, "L'identification électronique et les services de confiance dans le règlement eIDAS", *JTDE* 2016/7, No. 231.
48. See *inter alia* P. ANCEL, *Contrats et obligations conventionnelles en droit luxembourgeois*, Bruxelles, Larcier, 2015, p. 197.
49. See *inter alia* S. LE GOUEFF, *Internet et e-commerce en droit Luxembourgeois*, Ed. Portalis, 2003, p. 107.
50. Regulation (EU) No. 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, *OJ L*, No. 257, 28 August 2014, art. 46.

non-decimation. Luxembourg went further by implementing an e-archiving act.[51] The key principle is to ensure the integrity and fidelity of the original document.[52]

One of the key issues of e-archiving is the evolution of technology. Let's consider, for example, the needs to ensure the readability and integrity of a document for a period of 30 years. Today, the only way to ensure the archiving for long periods of time is to migrate documents from one carrier medium to another but doing so is creating obvious risks in terms of integrity and tampering.[53]

g. E-signature and GDPR

While not directly affecting the e-signing process, the EU General Data Protection Regulation (**GDPR**) should nonetheless, be taken into account, when considering electronic signature solutions as the risk and burden of complying with the GDPR is borne entirely by the customer as the data controller. Under GDPR, a customer may not contractually transfer its obligations or liability as a data controller to the platform provider, which is acting as a data processor.

While the interplays of the GDPR with the use of external service providers within an e-signing process are outside of the scope of this article, it should be considered that the digital audit trail can help data controllers strengthen their regulatory compliance, particularly in relation to data privacy and security. Under Article 5(2) of GDPR, the data controller is responsible for complying with the data protection principles as set forth in GDPR and must be able to demonstrate that their data processing activities comply with those principles. In this regard, using e-signing documents creates a digital audit trail evidencing what was signed when, and by whom. Moreover, a data controller must have appropriate security measures when handling personal data. Electronically signed documents through a reputable platform are encrypted, helping the data controller to comply with the accountability principle and satisfy other statutory duties under GDPR.

7. Conclusion

While not fully integrated into our daily practice yet, the footprint of the e-signature will continue to increase. The variety of technologies in use and the evolution of the software used may blur the lines, but it is very important to carefully assess your needs in terms of efficiency and security before opting for a specific system. If properly implemented, the use of e-signatures may result in streamlining repetitive administrative tasks (such as collecting, verifying, compiling and archiving signed documents), enhance legal compliance and security, while allowing increased mobility. The potential uplifts for businesses are major, but careful planning should not be dispensed with.

51. Act dated 25 July 2015 on electronic archiving (as supplemented by two Grand Ducal regulations of the same date relating to the implementation of its Article 4(1) and the digitalization and archiving of documents, respectively), signed on 25 July 2015, *J.O.*, 8 October 2015.
52. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 150, p. 167.
53. A. AYEWOUADAN, *Les droits du contrat à travers l'Internet*, Larcier, 2013, No. 152, p. 169.