

## Covid-19: Doing Business As Usual in a Paperless World – Legal Considerations on Digitally Compliant Documents



The distancing measures imposed to address the spread of Covid-19 are not only affecting our social relations but are also disrupting the way we are used to doing business. For instance, given that physical meetings can no longer be held to execute transaction documents, electronic signatures are widely being used instead.

Of course, for some time now, practitioners and the parties to transactions have already used digital methods to execute transactions when it was impossible to hold physical meetings to do so. However, although it is already a well-established practice, the current situation will undoubtedly contribute to generalize doing business remotely, as it is now, more than ever, vitally important to keep deals and transactions ongoing.

Notwithstanding the common practice of electronic signatures, many questions have been raised on how to legally execute documents by electronic means and whether electronic copies of documents (namely pdf versions) have the same value as the original ones. These questions have been frequently ignored and are usually raised only when disputes are triggered.

This article provides for a brief summary of the key legal aspects on these matters.

### 1. Electronic Signatures

In Luxembourg electronic signatures are governed by the Luxembourg Civil Code (the “**Civil Code**”), the Luxembourg law

dated 14 August 2000 on e-Commerce, as amended (the “**Luxembourg e-Commerce Law**”), and the directly applicable European Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “**eIDAS Regulation**”) which provide similar regimes in substance, even if some definitions and criteria differ. The provisions of the latter only cover part of what are usually named “electronic signatures”.

### Under Luxembourg Law

Since the implementation of the Luxembourg e-Commerce Law, article 1322-1 of the Civil Code recognizes that any signature may be either handwritten or electronic and defines the latter as a set of data, inseparably associated with the deed, which guarantees its integrity, identifies the signatory and expresses his consent to the deed.

Thus, an electronic signature is deemed to have the same probative value in court as a handwritten signature<sup>1</sup> once it is created by using a device that shall be:

- (i) **a secured signature creation device** (i.e. a software or hardware device configured to implement signature creation data complying with the requirements set out in article 4 of the Grand-Ducal Regulation dated 1 June 2001 on electronic signatures (the “**e-Commerce Grand-Ducal Regulation**”) maintained under the sole control of the signatory, and
- (ii) **based on a qualified certificate** (i.e. an electronic certificate that links signature verification data to a person and confirms that person’s identity complying with the requirements of the e-Commerce Grand-Ducal Regulation and provided by a certification service provider).<sup>2</sup>

Such presumption may only be challenged by way of a burdensome signature verification procedure.

Consequently, any electronic signature which does not meet the abovementioned conditions will not benefit from the presumption of equivalence before a court.

<sup>1</sup> Article 18 of the e-Commerce Law

<sup>2</sup> A list of the certification service providers accredited in Luxembourg is available on the website of the *Institut Luxembourgeois de la Normalisation, de l’Accréditation, de la Sécurité et qualité des produits et services* (ILNAS) at <https://portail-qualite.public.lu/fr/confiance-numerique/pres-tataires-services-confiance/liste-confiance.html>

<sup>3</sup> Draft law n°4641/00 on electronic commerce

However, the non-compliant e-signature will still be admitted to Court according to a non-discrimination principle that foresees that an electronic signature may not be rejected by a judge solely on the grounds that it is in electronic form or it does not meet the equivalence legal conditions.

In practice, the signatory of a non-qualified electronic signature must prove that his/her signature meets the criteria of integrity and authenticity required by the Civil Code. The deed on which the signature is affixed could be used as a beginning of written proof (*commencement de preuve par écrit*) which must be then supported by other means of evidence (eg, testimony, presumptions).<sup>3</sup>

### Under European Regulation

The eIDAS Regulation, directly applicable across the European Union, provides for three types of electronic signatures:

- (i) **Simple electronic signature (“SES”)**: defined 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”,
- (ii) **Advanced electronic signature (“AES”)**: defined as “an electronic signature that is (a) uniquely linked to the signatory, b) capable of identifying the signatory, c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, and d) linked to the data signed therewith in such a way that any subsequent change in the data is detectable”,
- (iii) **Qualified electronic signature (“QES”)**: defined as “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”.

The eIDAS Regulation gives a QES the same legal effect as a handwritten signature and ensures that when it is recognized in one EU Member State EU is also recognized in other Member States.

The difference between “advanced” or “simple” electronic signatures may have a certain theoretical interest, but little practical interest.

The eIDAS Regulation and Luxembourg law share the following two features:

- (i) the QES is the only signature that is vested with a presumption of authenticity and validity,
- (ii) there is no discrimination between the QES, the SES, and the AES as all of them will not be denied legal effect and will be admissible as evidence in legal proceedings.

- email signing: signature page or whole document printed, hand-signed, scanned and then sent back by email,
- pictured signature: picture of a signatory’s handwritten signature pasted on an electronic/Word document,
- finger signature by using a signature pad,
- qualified electronic signatures.

## 2. Most Commonly Used Electronic Signing Methods

Here below is a table setting out these methods, their qualification under both the Luxembourg and European law, their main characteristics and their legal value.

Several types of signing methods are commonly considered as an alternative to handwritten signature:

Type of signature under eIDAS Regulation	Simple electronic signature (SES)	Advanced electronic signature (AES)	Qualified electronic signature (QES)
Type of signature under Luxembourg Law	Non-qualified electronic signature		Qualified electronic signature
Requirements to be met	No requirements: all forms of signatures made by using some sort of electronic means.	Electronic signature that is: <ul style="list-style-type: none"> <li>(a) uniquely linked to the signator,</li> <li>(b) capable of identifying the signatory;</li> <li>(c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, and</li> <li>(d) linked to the data signed therewith in such a way that any subsequent change in the data is detectable.</li> </ul>	Advanced electronic signature that is: <ul style="list-style-type: none"> <li>(a) created by a qualified signature creation device, and</li> <li>(b) based on a qualified certificate for electronic signatures.</li> </ul>
Hardware/software to be used	None	Secured Signature Creation Device (SSCD)	Qualified Signature Creation Device (QSCD) relying on a qualified certificate issued by a Qualified Certification Service Provider listed in the EU/Luxembourg Trusted List.
Legal admissibility	yes		
Legal authenticity	to be proved by the signatory		Presumed authenticity (may be challenged by the opposing party)
Signature methods	Email signing pictured signature signature on tablet.	Simple electronic signature or signature created based on the use of a signature creation device (smart cards, usb-token, etc.) that meets the requirements set out above.	Signature created by using a qualified signature creation device (smart cards, usb-token, etc.) and relying on a qualified certificate for electronic signatures provided by a qualified trust service provider (in Luxembourg: LuxTrust and Be Invest International).

The electronic signing method to be used should be chosen on a case-by-case basis mainly depending on the level of authenticity (shall the signature link to its signatory?), identity (shall the signatory be absolutely identified?), integrity (shall any changes be detected in the document after the signature?), and authentication (is the signature created 100% under the sole control of the signatory?) that is wished or required in the context of the transaction and/or the document at stake.

The chosen signing method, will obviously rely on the nature of the contract (whether highly important or not) and the trustworthiness between signatories as well as the additional assurances they have given to each other. The most secure and enforceable solution will always be the usage of a qualified signature but a simple one might be sufficient when what is at stake is less important.

Moreover, the above mentioned signature issues affect the way agreements are drafted and negotiated:

- provisions may be included in the agreement to provide for a mechanism in accordance to which it (and any amendments thereto or any other documents or agreements in relation therewith) shall be signed,
- in order to speed up and facilitate the electronic signing of the agreement, the latter may be signed in counterpart. Including a counterpart clause, although not essential, would reduce the risk of one of the parties arguing that the document is not binding,
- the legal requirement pursuant to which the contract shall be executed in as many originals as the number of parties to the contract is not applicable to private deeds signed electronically,<sup>4</sup>
- where an electronic private deed includes a party's unilateral undertaking, it is not mandatory to mention in handwriting its sum or quantity, but it should be mentioned in print along with an electronic signature.<sup>5</sup> Two electronic signatures shall therefore be needed: the first one will cover the mention of the sum or quantity undertaken by the party and the second one will cover the act itself in its entirety.

<sup>4</sup> Article 1325 al. 5 of the Civil Code

<sup>5</sup> According to article 1326 of the Civil Code

If the above point seems quite complex, it is important to note that, subject to certain exceptions, legal provisions relating to the proof of private deeds are neither mandatory nor of public policy. Therefore, the parties may freely agree on the rules that shall apply with respect to its burden, object or way of proof as well as the probative value of the electronic signature. A clause could, therefore, be included in the deed to define the electronic signature's usage (whatever form it shall take) by the parties and that it should be given the same legal force and effect as a handwritten signature. In view of any dispute on the electronic signature's conformity, the parties may also establish a presumption that would reverse its burden of proof. In our opinion, however, such presumption shall not be irrefutable, as the counterparty shall always be in a position to challenge it.

Finally, it is worthwhile to mention that in March 2019 a [draft law](#) has been submitted to the Luxembourg Chamber of Deputies to amend the Luxembourg e-Commerce Law to align the definitions and criteria of electronic signatures with the ones provided for in the eIDAS Regulation. It is currently under discussion.

### 3. Electronic Copies

In addition to the legal recognition of electronic signatures, the use of remote information and business has been further developed by the Luxembourg law dated 25 July 2015 on electronic archiving, as amended (the “**Luxembourg e-Archiving Law**”) which aimed, among others, at defining the conditions under which electronic copies may benefit from a legal presumption of conformity with respect to the original document of any private deeds (as opposed to authentic ones).

Prior to the implementation of the Luxembourg e-Archiving Law, article 1333 of the Civil Code provided that the probative value of electronic copies depended on the existence or not of the original document and insofar as if the latter still existed, it could always be requested by a judge. A copy was therefore granted lesser probative value as compared to the existing original document.

However, article 1334 of the Civil Code provided that where the original document did not exist, the electronic copy could have the same probative value as the original, only if the holder of the copy proved that the latter complied with certain criteria set out by the law.

Since the implementation of the Luxembourg e-Archiving Law, the probative value of electronic copies no longer depends on the existence or not of the original deed.

Article 1333 of the Civil Code now provides that such article “does not apply to digitized copies that are probative value copies as defined by law” (probative value copy being defined by the Luxembourg e-Archiving Law as “a faithful and durable reproduction in a digital or micrographic form of an original document”).

If the probative value of a copy no longer depends on the existence of the original deed, it depends on the conditions under which the copy has been digitized instead. The Luxembourg e-Archiving Law introduced article 1334-1 in the Civil Code providing that “*digitized copies that are created by a Digitization and E-Archiving service provider have, unless the contrary is proved, the same probative value as the original or as the document deemed equivalent to the original document*”. Therefore, a legal presumption of conformity to the original document for the electronic copy exists only where it has been created by a Digitization and E-Archiving service provider.

Digitization and E-Archiving service providers are those certified as such in compliance with the requirements set out in the Luxembourg e-Archiving Law.<sup>6</sup>

An electronic copy that has not been created by the aforementioned service providers is, however, still admissible in court as article 1334-1 of the Civil Code provides for a non-discrimination principle, similar to the one applicable for electronic signatures. Documents cannot be rejected by a judge solely on the ground of being an electronic copy that has not been created by a Digitization and E-Archiving service provider. The holder of

these documents shall however prove that the electronic copy has the same probative value as the original document.

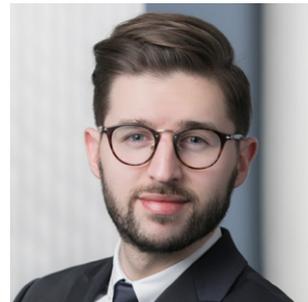
Should you need assistance on the issues discussed above, do not hesitate to contact us.

## Your Contacts at Luther



### Selim Souissi

Avocat, Partner  
Luther S.A. Luxembourg  
P +352 27484 683  
selim.souissi@  
luther-lawfirm.com



### Jeremy Da Silva Reis

Avocat, Managing Associate  
Luther S.A. Luxembourg  
P +352 27484 654  
jeremy.da.silva.reis@  
luther-lawfirm.com

<sup>6</sup> A list of Digitization and E-Archiving service providers accredited in Luxembourg is available on the website of the *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services* (ILNAS) at <https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/liste-psdc.html>

