

I. Introduction

The Regulation (EU) No 910/2014, of 23 July 2014 (known as eIDAS – Electronic Identification Authentication and Signature) was published in the Official Journal of the European Union on 28-8-2014, entered into force on the 1-07-2016 and created the nominated Digital Single Market. In order to evaluate the existing regulation, the Commission has launched a public consultation on the revision of the rules of eIDAS Regulation, “to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans and create a secure and interoperable European Digital Identity which gives citizens control”¹.

At present, from the recitals, we can infer its main objectives:

- Enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities [see Recital (2)].
- To promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication [see Recital (5)].
- To create appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, which will provide secure electronic interaction between citizens, businesses and public authorities in the European Union, [see Recitals (6) and (14)].

However, from Recital (21), last part, it is expressly clear that the Regulation shouldn't “[...] cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union

¹ As Executive Vice-President Margrethe Vestager said. *Vide* <https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation>.

law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.”

Consequently, Article 2(3) (*Scope*) determines that the Regulation does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form. Therefore, the Regulation does not aim to harmonise national legislation on contracts, in particular as regards their perfection and effectiveness, nor as regards other formalities relating to signatures², as in the case of requirements for land registers. In Recital 49 it says explicitly that “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.”

The European legislator has set up a system whereby the legal value of the electronic document depends on the typology of electronic signatures on the document: *simple electronic signature*; *advanced electronic signature*; or *qualified electronic signature*.

There are different degrees of electronic signature: At a higher level, it establishes the document with a qualified electronic signature (Article 25(2) of the Regulation); And at a lower level, simple electronic signature (Article 25(1) of the Regulation). In any case, as we shall see, qualified electronic signature still have some weaknesses.

Regarding the *electronic document*, which is defined by reference to the content, in Article 3(35) of Regulation No 910/2014, as “any content stored in electronic form, in particular text or sound, visual or audio-visual recording”, the Academy has not concluded on whether to adopt a strict or broad concept of electronic document. The electronic document in a strict or proper sense is that which is only visible by man through computer and software. The electronic document in a broad or improper sense (or computer document) is the one that is written with a computer on paper support or another and which, in most cases, is printed.

In this presentation we will use the concept of electronic document in a strict sense, that is, when the original is only visible through the computer and whose *qualified electronic signature* is only verifiable through the computer³.

² LUÍS FILIPE PIRES DE SOUSA, *O Valor Probatório do Documento Eletrónico no Processo Civil*, 2.^a Ed., 2017, pp. 34, and foll., E-book edition, that we will follow.

³ LUÍS FILIPE PIRES DE SOUSA, *cit.*, p. 39.

Since the “decline of paper civilisation” is expected and the consequent growth of electronic subscriptions, knowing the importance of the use of an electronic signature that provides the integrity of the documents accepted in Land Registry, in particular to promote legal certainty, the present paper will address some issues related to the use of electronic signatures, interconnecting it with the principles of Land Registry.

II. Electronic signature

Over time, the signature had as paradigm the traditional written documents in paper with a handwritten signature. The signature always implies the association of its author with the content of the document where the signature is attached⁴. By signing, the author of the document reveals his/her personal identity; Expresses their willingness to generate the document and to issue certain declarations; And intends to preserve the integrity of the document⁵.

The traditional formula has therefore been the handwritten signature, which usually consists of a manual inscription by the author, in the document, of their own full or abbreviated name, of their known pseudonym or nickname, or of any other identifying sign and assigned to them.

As defined by Regulation [Article 3, 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.”

The electronic signature is thus the broad species of the various forms of authentication of an electronic document, so we can divide it into two species: Non-advanced or simple electronic signature and advanced electronic signature.

The *simple electronic signature* consists in any method of imputation of the authorship of an electronic document. It can be a name at the end of an email (typed expressly or as a result of previous programming), a numeric code or a digitalised signature. Identifies

⁴ AFONSO PATRÃO, “Assinaturas eletrónicas, Documentos Eletrónicos e Garantias Reais. Reflexões sobre a viabilidade de constituição de garantias imobiliárias por meios eletrónicos à luz da lei portuguesa”, *RevCEDOUA*, 2012, pp. 51-52 e 55; and LUÍS FILIPE PIRES DE SOUSA, *O Valor Probatório do Documento Eletrónico no Processo Civil*, *cit.*, p. 134.

⁵ Cf. MANUEL LOPES ROCHA [et. al], *Leis da sociedade da informação: comércio electrónico*, Coimbra: Coimbra Editora, 2008, p. 33.

the subscriber but does not absolutely ensure that only the subscriber has access to the document, not ensuring that the document was not modified after its creation. Therefore, it does not securely provide the authenticity and integrity of the subscription⁶.

Pursuant Articles 3, 11) and 26 of Regulation No 910/2014, the *advanced electronic signature* is, different, the signature which must meet certain requirements, knowing: 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 (*principle of document integrity*). An example of this type of signature is the one that is certified by a qualified trusted service provider whose certificate is not valid at the time of certification [see Article 32.1.b) of the Regulation].

The *qualified electronic signature* will be a subspecies of *advanced electronic signature*. Pursuant Article 3, 12) of Regulation No 910/2014 “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” In turn, the qualified certificate for electronic signature means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets certain requirements, those set out in points (a) to (j) of Annex I to the Regulation [Articles 3, 15) and 28]. Thus, its level of security is higher, as in addition to meeting the requirements of the advanced electronic signature it has two additional requirements: Creation by a qualified device and its attestation by a qualified certificate.

In any case, the qualified electronic signature has some weaknesses, because it is subject to a time limit, since the certificate has an expiration date. This result can be mitigated by the use of a *qualified electronic time stamp* [see Articles 3, 34) and 42 of the Regulation].

As regards the legal effects of electronic signatures, Article 25 of Regulation No 910/2014 provides that the qualified electronic signature has the equivalent legal effect of a handwritten signature (paragraph 2 and Recital 49).

⁶ LUÍS FILIPE PIRES DE SOUSA, *O Valor Probatório do Documento Eletrónico no Processo Civil*, cit., pp. 83.

As is clear from all legislation, electronic signature is intrinsically linked to an electronic document. Thus, the qualified electronic signature may be the successor of the handwritten signature since the document to which it is attached is electronic⁷.

In addition, a qualified electronic signature attached to an original document can only be subject to a confirmation with a computer and confronted with the original document in electronic format. It is impossible to confirm the electronic signature, for example, on a printed copy. Thus, when an electronic document with a qualified electronic signature is printed on paper, the electronic signature is no longer verifiable in such a way that we can say that, once printed, the electronic document is no longer signed.

Whereas the registries are made with documents, this means that applications and documents will have to be submitted to the registry services electronically, so that the Registrar can verify their legality and validate the qualified electronic signature. In order to do a qualified electronic signature, the document or application must be electronic; And to be able to verify the signature attached to the requirements or documents, this can only be done through a computer. Therefore, land registry services should be prepared to receive and analyse electronic documents with qualified electronic signatures in such a way as to ensure security and legal certainty.

In Portugal, for example, recently, due to the COVID-19 pandemic, Decree-Law No 16/2020 of 15 April came in to effect to enable certain applications for land registration (that couldn't be made online via the IRN's website, like procedures for justification and rectification, and contestation of the Registrars' decision) to be sent to the e-mail address of the registry service, but the requirement has to have a qualified electronic signature. All other registration requests may be submitted online, through www.predialonline.pt, but in order to access the website, authentication is required through the use of a qualified certificate or a certificate proving the professional quality of the user (in the case of lawyers, notaries and solicitors), but, either in the case of submitting via the e-mail address or in the case of the use of the website, as a rule, the documents delivered will not have a qualified electronic signature⁸.

⁷ LUÍS FILIPE PIRES DE SOUSA, *O Valor Probatório do Documento Eletrónico no Processo Civil*, cit., pp. 44-45.

⁸ Normally they are scanned documents. The authentication is prior.

That is, they will not be electronic documents in the strict sense, but scanned images of the original documents on paper with a handwritten signature (e.g. public deeds or requirements). In the case of use of the IRN's website, only if the documents are sent by legitimate interested parties other than lawyers, solicitors or notaries, qualified electronic signatures should be associated to them. But these cases are rare or almost non-existent.

III – The use of electronic signature by Land Registry services

The Land Registry has the function of publicising the legal situation of the immovables for the security of legal transactions. To this end, for example, in Portugal, the Land Registry ensures that validly acquired rights are opposable to third parties (Article 5(1) of the Land Registry Code) and, consequently, the rights publicised contain a presumption of truth and exactness (Article 7 of the Land Registry Code).

In view of the mentioned security of legal transactions, there are legal and organisational rules in all land registry systems, that is, structuring principles, relating to the operation of registries, their viability, their purposes and their effects, whose adherence by the Registrar will ultimately ensure that the legal situation of the immovable is properly publicised.

These principles are intended: or to ensure that only facts which are in accordance with the law and which are based on formal and substantially valid titles can be recorded (principle of legality); Or to ensure that the person that submits the registry is entitled to that effect (principle of legitimacy); Or ensure that the first registered right prevails over what is subsequently registered (principle of priority); Or ensure that the content resulting from the Land Registry, concerning the immovables and their legal situation is correctly publicized (principle of publicity).

Therefore, with the decline of the use of paper and handwritten signatures and with the rise of electronic documents, it is urgent to reflect on the form of requirements pertaining to public registers and land registers, in particular to applications and documents. If the Regulation, in Article 25(2), says that “A qualified electronic signature shall have the equivalent legal effect of a handwritten signature”, that is to say, if the qualified electronic

signature is the one that is substitutable to the handwritten signature, that must be the minimum requirement, either for the signature by the interested parties to electronic applications or documents, or for the subscription of the Registrar, when the document is electronic.

The studies refers to many and different technical procedures for signature – *signature in a broad sense* – such as (i) the secret code or PIN, (ii) the digitalised signature; (iii) the biometric key⁹; (iv) the biometric or graphometric signature; (v) the digital or cryptographic signature (with single key or public key); (vi) and the digital mobile key¹⁰. But these various technical procedures of signatures are not similar in guarantees of safety, reliability, and inalterability. That is why the Regulation provided for the *qualified trust service* [Article 3, 17)] and the *qualified trust service provider* [Article 3, 20)], that validate the qualified electronic signatures (Articles 33 and 34).

On the other hand, knowing that the qualified electronic signature attached to the original document can only be conferred with a computer, and that its printing on paper (analogic copy of an electronic document, a ‘document of a document’) prevents verification of the signature – it can also be stated that the paper document is not signed, since the signature after printing is not verifiable – it will be necessary to define rules for the secure electronic transmission of documents (namely using qualified electronic registered delivery service, laid down in Article 44) and acceptance of their visualisation on a computer and their electronic files.

In this context, a secure and interoperable system of information transmission similar to that regulated in the E-Codex Regulation (*e-Justice Communication via On-line Data Exchange*), in which the negotiation is taking place at the European Commission, could be a way forward. The Regulation E-Codex was launched under the multiannual e-Justice action plan 2009-2013, mainly to promote the digitalisation of cross-border judicial proceedings and to facilitate the communication between Member States’ judicial authorities. As is said in the explanatory memorandum proposal, “e-CODEX has the potential to become the main digital solution for a secure transmission of electronic data in cross-border civil and criminal proceedings in the Union”.

⁹ For example, a fingerprint scanner.

¹⁰ Law 37/2014, of 26 June 2014.

In the context of the Land Registry, we may already consider, for example, whether judicial decisions issued in one Member-State and which have to be registered in another Member-State, cannot use this secure transmission provided in the Regulation E-Codex, directly from a authorized E-Codex access point, representative of a Civil Court, of a Member-State to an authorized E-Codex central access-point, representative of the registry services, in another Member-State, pursuant the Regulation Brussels I Recast¹¹ or the Succession Regulation, since they are in the Annex I of the proposal as legal instruments falling within the scope the Regulation E-Codex. Regarding the signatures, a connector software will provide functions *such as verification of electronic signatures via a security library and proof of delivery*.

Blandina Soares, Conservadora dos Registo Civil,
Predial e Comercial de Portugal.

¹¹ 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 judgments in civil and commercial matters.