Signaturit Solutions
by Signaturit Group

Legal Department

Legal validity of Signaturit's e-Signature process

Index

01. Introduction and scope.

The purpose of this report is to establish the legal validity of the trust services provided by Signaturit, with special attention to electronic signature services and certified electronic delivery.

It should be noted that this paper is not intended to determine the assessment that may subsequently be made by a competent court or any authority with the capacity to do so.

02. Legal validity of the Electronic Signature and the Certified Electronic Delivery

02.1. Legal Framework

At the European level, the validity and legal effects of electronic signatures are regulated by Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, repealing the previous Directive No 1999/93/EC (eIDAS Regulation).

In this regard, it should be borne in mind that the main difference between Regulations and Directives in the EU is that, while the Directive must first be transposed into the national legal system of each Member State in order to be applied, the Regulation is directly applicable to all States.

Each country has developed regulations to implement the provisions of the eIDAS Regulation. This document will analyse the Spanish regulation in detail, although what is indicated at European level is common to all member states.

02.1.1. Regulation (EU) 910/2014

The eIDAS Regulation seeks to enhance trust in electronic transactions within the internal market by establishing a secure common basis for electronic interaction between citizens, businesses and public entities, thereby increasing the effectiveness of European public and private online services, e-business and e-commerce. The eIDAS Regulation, which is directly applicable in Spain and throughout the EU, establishes the minimum requirements for considering an electronic signature or a certified electronic delivery to be valid, as well as its legal effects.

ELECTRONIC SIGNATURE

The main criterion to be taken into account is that reflected in **Article 25**:

> *"An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is an electronic signature or that it does not meet the requirements of a qualified electronic signature.*

According to the eIDAS Regulation there are three types of electronic signatures, each with a different level of protection:

a) **Simple electronic signature**: this is the simplest form of electronic signature. As a mere example, a simple electronic signature can be a simple acceptance or a "checkbox".

b) **Advanced electronic signature**: this is an electronic signature with higher requirements than a simple electronic signature and therefore enjoys a higher degree of protection.

These requirements are:

- It is unique and exclusive to each signatory;
- It is possible to identify the signatory through the data provided by the signatory;
- It is created using data for the creation of electronic signatures, which the signatory can use, with a high degree of confidence, under his own control; and
- It is connected in such a way to the data in the signed document that any subsequent changes to the document are detectable.

c) **Qualified electronic signature**: This is the type of electronic signature that offers greater protection since, in order to be considered as such, it must meet the requirements established in Annex I of Regulation (EU) 910/2014. This type of electronic signature has been attributed the same legal effects as those granted to handwritten signatures.

The main difference between advanced electronic signatures and qualified electronic signatures is that the latter:

- It needs to be created through a qualified electronic signature creation device, i.e. a device that guarantees that the created signature is secure and protected against fraud;
- It must be registered in a certified electronic signature system offered by a reliable and certified provider, namely a Qualified Trust Service Provider.

CERTIFIED ELECTRONIC DELIVERY

Certified electronic delivery is "a service that enables data to be transmitted between third parties by electronic means and provides evidence related to the handling of the transmitted data, including proof of sending and receipt of the data, and that protects the transmitted data against the risks of loss, theft, damage or unauthorised alteration" (definition of Art. 3(36) eIDAS).

This service is recognised by Regulation (EU) 910/2014, giving it the following legal effects, based on the provisions of its Article 43:

> *"Data sent and received through a certified electronic delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or does not meet the requirements of a qualified certified electronic delivery service".*

02.1.2. Trust Services Act, LSSI and LEC in Spain.

Law 6/2020 of 11 November aims to determine certain aspects related to Trust Services, as a complement to the provisions of the eIDAS Regulation.

Among other issues, the Trusted Services Act has amended **Article 326.3 of the Civil Procedure Act** (LEC) as follows:

> *"Where the party in whose interest the effectiveness of an electronic document is sought or the authenticity, integrity, date and time accuracy or other characteristics of the electronic document that a non-qualified electronic trust service as provided for in Regulation (EU) 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 enables to prove, is challenged, the procedure shall be as set out in paragraph 2 of this Article and in Regulation (EU) No 910/2014."*

Another of the modifications that the Trusted Services Act has brought about is the burden of proof for those electronic documents that have been issued on the basis of a qualified trust service. Specifically, the Second Final Provision of the Trusted Services Act modifies **Article 326.4 of the LEC by** granting a presumption of validity to qualified trust services as follows:

> *"If any qualified trust service provided for in the Regulation referred to in the previous paragraph has been used, the document shall be presumed to have the disputed characteristic and the trust service shall be presumed to have been properly provided if it was, at the relevant time for the purposes of the discrepancy, on the trusted list of qualified providers and services".*

For its part, **Article 299.2 of the LEC** stipulates that:

> *"Means of reproduction of speech, sound and image, as well as instruments for recording and knowing or reproducing words, data, figures and mathematical operations carried out for accounting or other purposes, relevant to the proceedings, shall also be admissible in accordance with the provisions of this Act".*

Likewise, **Article 23** of Law 34/2002 of 11 July 2002 on information society services and electronic commerce (LSSI) establishes that:

> *"1. Contracts concluded by electronic means shall produce all the effects provided for by law **when consent** and the other requirements necessary for their validity **are met.***
> *Electronic contracts shall be governed by the provisions of this Title, by the Civil and Commercial Codes and by the other civil or commercial rules on contracts, in particular, the rules on consumer and user protection and on the organisation of commercial activity.*
> *2. For the conclusion of contracts by electronic means to be valid, it **is not necessary for the parties to have previously agreed on the use of electronic means**.*

*3. **Where the law requires the contract or any information relating to the contract to be in writing, this requirement is satisfied if the contract or the information is contained in an electronic medium.***

They are therefore valid as long as the parties freely consent to the conclusion of contracts for a lawful purpose and cause.

Finally, it is important to quote in full **Article 24 of the LSSI** on 'Proof of contracts concluded electronically', which stipulates the following:

"1. Proof of the conclusion of a contract by electronic means and of the obligations arising therefrom shall be subject to the general rules of the law.
*When contracts concluded electronically are **signed electronically**, the provisions of Article 3 of Law 59/2003 of 19 December 2003 on electronic signatures shall apply.*[1]
2. In any event, the electronic medium on which a contract concluded by electronic means is recorded shall be admissible in court as documentary evidence".

02.1.3. Spanish Civil Code

As stipulated in the previous paragraph, the parties may use any form of electronic signature to conclude contracts and documents of any kind, provided that there is no legal requirement or formality to the contrary.

Articles 1258 and 1262 of the Civil Code, and Article 23.1 of the LSSI, do not require contracts to be concluded by handwritten means, accepting that these are in electronic format, and that their ratification can also be carried out by means of an electronic instrument.

However, in order for an electronic contract, signed by means of an electronic signature, to be effective, and to ensure respect for the contractual will and consent of the parties, it will be necessary:

- There must be the will or consent of the parties (arts. 1262-1270, CC).
- There must be an object or a contractual purpose (arts. 1271-1273, CC).
- The object must be based on a lawful cause (arts. 1274-1277, CC).

02.1.4. Conclusion

[1] Law 59/2003 was repealed by Law 6/2020 and replaced by the eIDAS Regulation and Law 6/2020.

On the basis of the above, in Spain, electronically signed documents have full legal effect and are legally valid as documentary evidence in legal proceedings.

Therefore, Signaturit's electronic signature (or the certified electronic delivery service) may be used to sign (or send) all types of documents that are not subject to specific form requirements. In particular, electronic signatures may be used on documents in the field of citizens' relations with the Administration and, especially, in relations between companies or between companies and customers (all types of contracts that do not require specific formal requirements or that need to be established "in writing", i.e. contracts for the provision of services, contracts of deposit, sales mandates, etc.), and between these and consumers (i.e. in the field of so-called e-commerce).

03. Signaturit as a Trusted Service Provider.

03.1. Definition and monitoring

Regulation (EU) 910/2014 defines a Trusted Electronic Service Provider as "*a natural or legal person who provides one or more trusted electronic services, either as a qualified provider or as an unqualified provider of trusted electronic services*".

The trust services referred to are the following:
"the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps; certified electronic delivery services and certificates relating to these services; or the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates relating to these services".

Trust Service Providers may be either unqualified or qualified, the latter being those providers that have been qualified by the supervisory body on the basis of the eIDAS Regulation. To this end, one of the functions of the supervisory bodies is to supervise Qualified Trust Service Providers established in the Member State, in order to ensure, through ex-ante and ex-post supervisory activities, that these qualified providers and the qualified trust services provided by them comply with the requirements established in the Regulation. In Spain, the supervisory body is the Ministry of Economic Affairs and Digital Transformation.

The eIDAS Regulation establishes a series of security requirements that apply to Trust Service Providers, whether qualified or not. They must adopt appropriate technical and organisational measures to manage the security risks of the trust services they provide. These measures **shall ensure a level of security** proportionate to the degree of risk, and in particular measures shall be taken to prevent and minimise the impact of security incidents and to inform stakeholders of the negative effects of such incidents.

The Ministry of Economic Affairs and Digital Transformation, on its website, registers and publishes both Qualified Trust Service Providers and non-qualified Trust Service Providers. In this regard, Signaturit is registered as a Qualified Trusted Service Provider for the following categories of services, having therefore complied with the duty of communication provided for in the regulations:

"Service for issuing qualified electronic certificates for electronic signatures".

On the other hand, Signaturit is registered as a Trusted Service Provider for several non-qualified services:

- In the category of "Other services in relation to the electronic signature of documents": Service consisting of the provision of the necessary telematic means (web integration, mobile signature) so that Signaturit's customers and their third parties of interest can sign and manage electronic documents (e.g.: contracts) with full legal validity.
- In the category of "Certified electronic delivery service". Service consisting of sending certified communications (e.g. email and SMS) to send contracts and notifications with acknowledgement of receipt.
- In the category of "Certified electronic delivery service": Service consisting of the provision (notification) of the necessary telematic means (web integration, mobile signature) for Signaturit customers and their third parties of interest to sign and manage electronic notifications.

Signaturit's status as a Trusted Service Provider can be verified with:
A) The Secretary of State for Digitalisation and Artificial Intelligence integrated in the Ministry for Digital Transformation and the Civil Service, through the following link: https://avancedigital.mineco.gob.es/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

B) The list of EU Trusted Service Providers by country published by the Commission of the European Union via the following link:
https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

03.2. Guarantees offered by a Trusted Service Provider

Framed within a specific regulation and controlled by a state body, a Trusted Service Provider offers the security guarantees required for any IT process and compliance with the legal and technical requirements necessary to give legal validity to the act or document that is processed electronically.

Thus, as we shall see below, several factors come into play in an electronic signature process that will make it possible to consolidate the authenticity of the document, the identity of the signatory or

signatories and, in general, of each step in the process of sending and receiving the electronic document.

It is important to point out that a Trusted Service Provider is a third party outside the legal relationship that may be established between the parties that use its services, and therefore offers guarantees of neutrality in the face of the claims of one or the other in the event of a conflict, being able to certify the integrity and authenticity of the electronic events produced and recorded in its systems with impartiality and therefore providing legal security and evidential validity in legal proceedings.

It is precisely this role of the Trusted Service Provider (formerly also called "Trusted Third Party" under the LSSI) that creates a climate of trust that enables and strengthens e-commerce and digital transactions in the EU, as promoted by the eIDAS Regulation.

04. Operation of the Signaturit e-Signature Platform

04.1. Overview of an e-signature process with Signaturit

The Signaturit Platform works as follows: from their user account, the customer (sender) generates a signature process or circuit by choosing the desired signature level (simple signature, advanced signature with biometrics, with OTP signature or signature with digital certificate) and uploads one (or several) document previously prepared by them that they wish to send for signature to the interested parties (recipients or signatories).

The sender can then configure the place where he/she wants the signatory's signature to appear on the document and add additional actions (widgets) to be performed by the recipient, such as setting the date, the place, filling in a checkbox to accept a specific text or even including a text.

Finally, the sender must inform the recipient of his identity with his name and surname as well as his personal e-mail address. In addition, he can add his telephone number for sending an OTP code to reinforce the effectiveness of the electronic signature by means of an additional authentication factor.

Once the process is launched, an email is sent to the recipient, who must open a link that will allow them to enter the Signaturit Provider's controlled environment and follow the steps indicated until the signature process is complete. Each action performed by the recipient will be recorded in Signaturit's systems, generating as many evidences as the number of events produced.

All the evidence of the transaction generated during the signing process is collected in the evidentiary document (**Audit Trail**) generated by the Provider for each process, through which the parties will be able to assert the evidence generated in an easily understandable way.

This evidentiary document containing the evidence generated during the entire signature process is electronically signed and, together with the subsequent application of the encryption algorithm, ensures the integrity of the data and its legal validity as proof of to whom a document has been sent, when and where it has been received, etc....

The encryption algorithms used are highly secure and are based on cryptographic keys that guarantee the confidentiality of the data. This means that only authorised recipients can access the information contained in the document sent.

We therefore use encryption and authentication techniques to guarantee the integrity of the document and avoid subsequent modifications that would not be evident without the use of these techniques. This integrity implies that the electronic evidence generated during the process of sending certified email through Signaturit existed and cannot be altered from a specific moment in time.

04.2. Signaturit's advanced signature process

Article 26 of eIDAS establishes the requirements that an advanced electronic signature must meet in order to be valid. Signaturit complies with the requirements of the aforementioned article 26 in the following way:

1. In order to ensure that the signature is associated with a single signatory, the document is sent to the e-mail address of the signatory in question;
2. In order to identify the signatory, we obtain the geolocation at the time of the signature, the IP addresses of origin and destination of the request, the date/time of the signature and the biometric data of the signatory's graph (pressure, speed and acceleration); additionally, the identification of the signatory is reinforced by means of the second authentication factor that constitutes the OTP Code sent to the signatory's mobile phone.
3. Full control of the signature is ensured by the possibility we give the signatory to sign the document in question using any device with internet access (computer, tablet, mobile phone); and
4. We prevent any further changes to the signature by guaranteeing the integrity of the document. To guarantee absolute integrity, we encrypt the document and include a qualified time stamp that ensures that the data in the document has not been altered since the time of signing.

All the electronic evidence generated by Signaturit in the signature process will be reflected in an evidentiary document or audit trail. The audit trail gathers all the relevant information gathered in the signature process and may be presented as legal evidence in any court.

The supporting document contains the following information:

- **Unique transaction identifier**

This is recorded and indicated both in the Audit Trail and in the signed document itself in order to correlate the documents. In addition, it should be remembered that both documents (signed document and Audit Trail) are automatically and simultaneously received in the sender's mailbox, so there is a double correlation factor between documents.

The signatory is linked through the generation of hashes identifying the document, the private identifier, the signature identification process and the biometric references of the signature for each signatory.

- **Name of the signatory and his/her e-mail address**

There is a precise and unique linkage in that the signatory receives an e-mail to the e-mail address of which he/she is the owner.

There are other measures to reinforce this linkage which would include, in addition to this e-mail, the application of OTP (One Time Password) measures in order to be able to sign the document in question or the validation of IDs, passports, etc., by means of our OCR technology.

- **Evidence of the process**

The signatory can be identified by recording all evidence relating to IP address, time, geolocation and device type. The document can also be traced by recording the time it was sent, the number of times it was opened, the time of acceptance of the terms and conditions, as well as when it was signed.

    - IP address
    - Geolocation
    - Authentication history
    - Chain of custody (e.g. sent, viewed, signed, etc.)
    - Status completed

- **Official time stamping**

The use of time-stamping guarantees the integrity of the set of electronic data that make up the electronic signature. In other words, the time stamp guarantees that a signature was made at a specific time, making it impossible to modify it later, since the document is encrypted and sealed once the signing process has been completed.

- **Biometric data**

The biometric information we capture comes from information about the graph, consisting of the points that make up the graph and their position, velocity, acceleration and finally, in devices that allow it, the pressure with which it is performed.

It should be noted that pressure is an additional piece of biometric signature data, which is defined as unique features of each person. In cases where the device does not allow the collection of pressure data, computer algorithms are used to collect the pseudo-pressure that allows to adapt the thickness of the stroke to the speed of the signature. Consequently, an approved device is required to meet the requirements defined in ISO/IEC 19795-7 to be fully valid.

It should be noted that Signaturit's activity is covered by article 9.2 of the GDPR since, in order to collect biometric data, it requests prior express consent from the owners of said data, so that it can process them for the sole purpose of identifying those who sign documents through its platform, as part of a general electronic signature process.

04.3. The certified electronic delivery process

The certified electronic delivery process offered by the Signaturit Platform has two delivery modes:

- By sms
- By e-mail

Each of these modalities in turn allows for two types of electronic deliveries:

- Certified electronic communication: the content of a message sent by sms or email is certified.
- Certified electronic notification: the content of a message sent by sms or email is certified, but especially the delivery and opening of attached documents.

The following evidence is recorded for each shipment:

- Delivery of the message to the addressee with date and time stamp
- Opening and reading of attachments
- Content of the documents

All evidence is collected in the evidentiary document similar to the one generated in electronic signature processes (see previous point)).

05. Legal validity of electronic signatures and deliveries made with Signaturit

05.1. Validity of the electronic signature with digital trace and collection of biometric data

As indicated above, in order to meet the requirements necessary to provide an advanced electronic signature service in compliance with article 26 of eIDAS, Signaturit must be able to identify the signatory. The biometric data of the signatory's signature collected by Signaturit allows us to provide security to our customers, since, in the event that any of the signatories denies their authorship, we can use the information collected to prove the identity of the signatory in question.

In any case, it is important to clarify that the biometric data obtained by Signaturit remain encrypted: as a general rule, no one will be able to access the data and they will remain blocked until, for some exceptional circumstance, they must be presented for analysis, especially in court due to the occurrence of a conflict that may have arisen around the signature of the document in question.

At the privacy level, according to the GDPR, biometric data means personal data obtained through specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person that allow or confirm the unique identification of that person, such as facial images or fingerprint data.

Consequently, biometric data will be considered to be data that allow a person to be identified and/or to confirm who he/she is by means of technical processing that collects data relating to physical appearance, body or behaviour.
The GDPR also identifies biometric data as a special category of personal data. Article 9(2) of the GDPR allows the processing of biometric data provided that the data subject has given his or her consent. Specifically, Article 9(2)(a) states that: [the prohibition does not apply where] '*the data subject for such processing has given his or her explicit consent to such processing for one or more of the specified purposes, unless there is a legal prohibition at European or State level on this*'.

In this sense, Signaturit's activity is covered by this article: Signaturit is authorised to collect biometric data as, in order to do so, it requests prior and express consent from the owners of said data. Specifically, Signaturit requests consent from the owners of the biometric data in order to process them for the sole purpose of being able to identify those who sign documents through its platform, within a general electronic signature process.

05.2. Validity of the electronic signature with OTP key

At present, a large number of countries require, by law, that in order to obtain a mobile phone number, a process of verification of the user's identity is necessary. In Spain, the issuing of a mobile SIM requires this identification by, as well as the signing of a contract. Therefore, a mobile line is necessarily linked to a natural or legal person.

Therefore, the aforementioned requirements for an electronic signature to be considered advanced in accordance with Article 26 of the eIDAS Regulation are met. These are analysed below with the SMS OTP signature solution:

1. Be uniquely linked to the signatory. The signatory owns a mobile phone with a telephone number
2. It allows the signatory to be identified. The telephone number is personal and belongs exclusively to you.
3. The signature must have been created using signature creation means that the signatory can use with a high level of confidence and under his exclusive control. Both access to the signature request and the SMS code remain under the signatory's exclusive control (sent to the signatory's email and mobile phone, respectively).
4. It is linked to the signed data so that any subsequent alterations can be detected. The document is linked to the Audit Trail and is also stamped with a qualified time stamp so that any changes to the document can be detected.

On the other hand, it should be borne in mind that this correspondence would not occur in countries where SIM cards can be obtained anonymously. In the OTP signature process the phone number is linked to the signing operation with the signatory and the content is also linked to the created OTP and additional evidence and traceability of the message is obtained in the Audit Trail document.

05.3. Validity of certified electronic delivery

As indicated in section 2.1.1, the electronic certified delivery service is a service recognised by the eIDAS Regulation and therefore legally valid, even if it is not qualified, on the basis of Article 43:

In order to obtain this recognition, it is necessary that the delivery process, either by sms or by email, meets a series of requirements:

- Transmission of data between third parties by electronic means
  - Identification of the issuer
  - Identification of the recipient (email or mobile phone)
- Generation of evidence:
  - On the forwarding of transmitted data
  - Reception
  - From the content of the message
  - Of the accompanying documents
- Protects data from the risk of loss, theft, damage or unauthorised alteration.
  - Provider's electronic seal
  - Time stamping

As eIDAS is a trusted service provided by a Trusted Service Provider, national rules of evidence -such as art. 326.3 of the Spanish LEC-, recognise its legal effectiveness in the same way as evidence provided in paper format, depending on the public or private nature of the document.

In short, with Signaturit's services, you can provide security to your digitisation processes by having all the evidence to convince any party, judge or court of the authenticity of the electronic evidence provided, and thus protect yourself against the hypothetical challenge of the opposing party. And

if you still need our intervention in the event of litigation or challenge, you can count on the help of our teams to advise you and of our legal team in the event that you need to prepare reports or intervene in court*.

(*consult applicable rates)

Signaturit Group Legal Department.