TERMS AND CONDITIONS OF USE OF THE NATURAL PERSON CERTIFICATE

PRIVACY POLICY

PARTIES

SIGNATURIT SOLUTIONS S.L.U. (hereinafter "SIGNATURIT") is a Qualified Trust Service Provider (hereinafter the "QTSP"), of Spanish nationality with its registered office in Barcelona, carrer d'Avila, no 29 (08005 Barcelona) and NIF B-66024167, telephone 960031203 and contact email info@signaturit.com, whose activity is supervised by the Ministry of Economic Affairs and Digital Transformation. In providing the service, SIGNATURIT acts as a Certification Authority (hereinafter the CA) linking a specific public key to a specific person through the issuance of a digital Certificate. SIGNATURIT belongs to the "Signaturit Group".

The REGISTRATION AUTHORITY (hereinafter, the RA) is the entity responsible, among other functions, for delivering the Certificate issued in the name of the APPLICANT and verifying the identity of the APPLICANT and, if applicable, the other circumstances associated with the certificate called "ATTRIBUTES" (if they are incorporated in the list of Certificates subject to these Terms and Conditions). All or part of the RA functions may be assumed either directly by SIGNATURIT, or by a third entity that will be constituted, depending on the case, as an External Registration Authority (External RA), and that will act in any case by delegation of the CA. In some cases, the SIGNATURIT RA or the External RA may rely on PRESENT VERIFICATION POINTS (PVP) to carry out the face-to-face identity checks.

The APPLICANT is a natural person who makes the certificate issuance request for him/herself (SUBSCRIBER) and who may be linked to an ENTITY (with or without legal personality) by a legal or voluntary representation relationship, corporate membership or by some type of business relationship. Once the certificate has been issued, it assumes the status of HOLDER and SIGNATURE responsible for the custody and use of the private key within the meaning of the LEGAL FRAMEWORK applicable to the provision of the service. When it is the ENTITY that contracts the service for natural persons with whom it has a relationship (e.g. employees, representatives or proxies), it must assume the status of **SUBSCRIBER** within the meaning of the LEGAL FRAMEWORK and must accept these Terms and Conditions.

CERTIFICATES SUBJECT TO THESE TERMS AND CONDITIONS

These Terms and Conditions apply to all qualified electronic certificates of natural persons with or without attributes, issued by the **SIGNATURIT GLOBAL CA** Certification Authority, which belongs to **IvSign Root CA** Hierarchy owned by IVNOSYS SOLUCIONES, S.L.U. (Signaturit Group). Specifically the following under version 1 of this T&C:

- **Citizen**: Identifies a natural person without establishing any kind of linkage.
  SIGNATURIT OID: 1.3.6.1.4.1.50646.5.16.1.1.2 (SW)

1. OBJECT

The issuance by the CA in favour of the APPLICANT of a natural person's Digital Certificate (with or without ATTRIBUTES), the conditions of use of the Certificate by the APPLICANT and the obligations of the parties involved applicable to the Digital Certification Service, in accordance with the terms set out in these Terms and Conditions and in the corresponding CPs and CPS.

2. LEGAL FRAMEWORK FOR SERVICE PROVISION

The digital certificate issuance service is regulated by the APPLICABLE REGULATIONS, specifically Regulation (EU) No. 910/2014 European Parliament and Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation), and in Spain by Law 6/2020 of 11 November, regulating certain aspects of electronic trust services (Law 6/2020). Based on these regulations and the technical standards applicable to the service, the QTSP prepares a Certification Practices Statement of the SIGNATURIT GLOBAL CA Certification Authority (hereinafter "CPS") with O.I.D. 1.3.6.1.4.1.50646.5.1 and Certification Policies (hereinafter "CP") attached to the CPS, which contains detailed information on the intervening parties, the life cycle of the certificates, the security and support systems, as well as the rules and uses applicable to each type of certificate.

The APPLICANT (and the SUBSCRIBER if different) declares that he/she is aware of and accepts the SIGNATURIT PCs and the SIGNATURIT CPS, available at the address https://policy.signaturit.com/ , and applicable to the type of certificate he/she has contracted.

The Contract between the PARTIES constituted by these Terms and Conditions, the CPS and the CPs mentioned above and the APPLICABLE REGULATIONS, constitute the LEGAL FRAMEWORK that will regulate the relationship between the parties, internally and vis-à-vis third parties, without prejudice to the provisions of the legislation in force. This document therefore constitutes a summary of the most relevant rights and obligations.

3. CONCLUSION OF THE CONTRACT - VALIDATION OF THE CERTIFICATE

The present Contract, which includes the privacy policy, will be made available to the APPLICANT and to the SUBSCRIBER, if different, for their express acceptance prior to the execution of the service. Acceptance, even by

electronic means, shall constitute a valid conclusion of the contract. The conclusion of the contract shall be documented on a durable medium, with a copy delivered to the APPLICANT and, where applicable, to the SUBSCRIBER, and kept by the QTSP in the manner and within the periods required by the APPLICABLE REGULATIONS.

In case of a positive result of the checks necessary for the issuance of the certificate, the certificate is issued and delivered to the APPLICANT, in accordance with the provisions of the applicable CPS/PC.

4. DURATION OF THE CONTRACT

This Agreement shall come into force and terminate on the issue and expiry dates indicated in the Certificate without prejudice to the grounds for revocation provided for in the LEGAL FRAMEWORK.
The Certificate may be renewed in accordance with the terms set out in the CPs and CPS, in which case the Contract will be extended until the new expiry or revocation date.

5. CONSIDERATION

The price of the Certificate, which will include the consideration for the SIGNATURIT services associated with it, is defined in the offer subscribed by the APPLICANT (or the SUBSCRIBER) when making the request for the Certificate and in the corresponding invoice.
This price must be paid by the APPLICANT or the SUBSCRIBER ENTITY to the CA or RA prior to delivery of the Certificate and signature creation devices, unless otherwise agreed in the commercial offer.

6. ACCEPTANCE OF THE CERTIFICATE

Once the APPLICANT has been notified of the issuance of the certificate, it has a period of 7 calendar days to verify its correct issuance (correction of the data). Once this time has elapsed, the issued certificate will be considered expressly accepted, and the APPLICANT/HOLDER therefore assumes the veracity of its content and the obligations arising from it with regard to the CA, the RA, the ENTITY or any third party that relies on the content of the certificate by virtue of the CPS/CPS and the APPLICABLE REGULATIONS.
If the certificate has not been issued correctly for technical reasons, the certificate will be revoked and a new one will be issued free of charge, once the incident has been detected or communicated to the RA by the HOLDER or the ENTITY.

If there is any difference between the data supplied to the CA and the content of the Certificate, or if a defect is detected, this must be communicated immediately to the CA by the HOLDER or by the ENTITY, so that it can proceed with its revocation. Any damage and prejudice caused by the delay in communicating these differences and the request for revocation of the certificate, must be assumed by the HOLDER and, if applicable, by the ENTITY.

7. THE OBLIGATIONS OF THE

a) Notify the APPLICANT of the revocation or suspension of its Certificate when this occurs, explaining the reasons, the date and time when the certificate will cease to have effect. The QTSP shall replace the certificate free of charge with another valid certificate of the same type and for the remaining period of validity, unless the revocation is based on any of the reasons set out in the CPS/CP, and shall not entitle the APPLICANT to any compensation whatsoever.
b) Maintain the database of valid Certificates, suspended Certificates and revoked Certificates up to date.
c) Process requests for suspension/revocation of Certificates as soon as possible.
d) Retain the information relating to the certificates issued and event logs for 15 years following their expiry or revocation. This logging activity may be carried out electronically.
e) Comply with the Certification Practice Statement and the relevant Certification Policies.

8. OBLIGATIONS OF THE RA (and where applicable of the PVP)

a) Correctly identify the APPLICANT in accordance with the procedures set out in the APPLICABLE REGULATIONS, the CPS and the applicable CPs.
b) Check the data relating to the constitution and legal personality of the ENTITY and the relationship of representation or corporate membership of the APPLICANT with it, in accordance with the procedures established in the APPLICABLE REGULATIONS, the CPS and the specific CPs for this type of Certificate.
c) Archive and keep the information relating to the issuance of certificates for 15 years following their expiry or revocation. This registration activity may be carried out by electronic means.
d) Proceed with the delivery of the Certificate to the APPLICANT in accordance with the conditions defined in the CPS/PC, once the above checks have been carried out.
e) Submit to periodic audits carried out by the CA.
f) Comply with the Certification Practice Statement and the relevant Certification Policies.

9. OBLIGATIONS OF THE APPLICANT/HOLDER

a) Diligently safeguard the secret keys, passwords or activation pins, taking reasonable precautions to prevent their loss, disclosure, modification or unauthorised use, in order to maintain exclusive control over the use of the certificate. In this regard, the HOLDER is aware that the certificate is personal and entails the possibility of identifying, authenticating and signing documents with full legal effects attributable to his/her person or to the ENTITY he/she represents.
b) Request the suspension/revocation of the Certificate when any of the cases of suspension and revocation of certificates foreseen in the CPs and in the APPLICABLE REGULATIONS are fulfilled.

c) Provide all the information and documentation required by the CA/RA in order to carry out a correct identification, taking responsibility for its veracity and correctness.
d) Immediately notify the CA or RA in the event that it detects that any incorrect or inaccurate information has been included or in the event that, unexpectedly, the information in the Certificate does not correspond to reality.
e) Immediately inform the CA or RA of any situation that may affect the validity of the Certificate, or the security of the keys, and cease its use.
f) Ensure that the use of the Certificate is in accordance with the APPLICABLE REGULATIONS and the limits set by the CPs and the Certificate itself according to its type.
g) Any other that derives from the content of the specific CPs for each type of Certificate.

10. OBLIGATIONS OF THE ENTITY AND THE SUBSCRIBER

Obligations (b), (c), (d), (e), (f) and (g) of the APPLICANT shall also apply to the ENTITY/SUBSCRIBER, which may be exercised through its legal representative.

11. INFORMATION FOR RELYING PARTIES

a) The QTSP does not keep revoked certificates in the CRLs after their expiry. To consult expired certificates, RELYING PARTIES must use the OCSP consultation service.
The PSCS will issue the last CRL at the moment that all certificates issued under the CA of this certificate are expired or revoked, due to any of the possible circumstances (expiry or revocation of the CA).
CRLs shall remain published for a minimum period of 5 years from the expiry or revocation of the CA.
b) In order to trust a qualified certificate issued by a QTSP, the RELYING PARTY must validate the certificate via the TSL trust anchor.

12. LIMITATIONS ON THE USE OF THE CERTIFICATE - PROHIBITION ON TRADING WITH THE CERTIFICATE

The different types of certificates issued under the SIGNATURIT CA (or "profiles") respond to certain uses and functions that are defined in the CPS and its corresponding CP and that the APPLICANT, and if applicable the ENTITY, must be aware of and respect. It is the responsibility of the APPLICANT and, where applicable, of the ENTITY, to use the certificate issued in accordance with these uses and functions, and in particular to use it in accordance with the legal or voluntary powers of representation granted to the APPLICANT by the ENTITY. It is also the responsibility of the RELYING PARTIES to verify the purpose of the certificate and any limitations on its use.

The contracting of the QTSP digital certification service only admits the use of the certificate within the scope of activity of the APPLICANT or the ENTITY to which it is linked, in accordance with the purpose of the type of certificate requested. Failure to comply with this clause shall entitle the CA to revoke the certificate and to claim compensation for damages caused by the breach, including loss of profit and indirect damages.

13. RESPONSIBILITIES

The CA and the RA (and if applicable the PVP), will be responsible for their functions under the CPS and the CPs and, in particular, will assume full responsibility for the correct verification of the identity of the APPLICANT and, if applicable, of the ENTITY and other relevant circumstances.

The CA and the RA shall not be liable for damages arising from or related to the non-execution or defective execution of the obligations of the APPLICANT and/or the ENTITY, nor for the incorrect use of the Certificates and the signature activation PIN, nor for any indirect damage that may result from the use of the Certificate or the information provided by the CA, in particular, loss of profits, loss of income or orders or loss of data, not giving rise to any right to compensation. In particular, neither the CA nor the RA shall be liable in the following cases:

- In the event of any inaccuracies in the data provided and/or to be included in the Certificate resulting from the information provided by the APPLICANT or the SUBSCRIBER, or when their inaccuracy has been accredited by means of a public or official document, registered in a public register if required, provided that the CA or RA has always acted with the maximum diligence required. In the event that the HOLDER or the ENTITY has not communicated without undue delay any change in the circumstances that affect the provision of the service, in particular, those reflected in the Digital Certificate.
- In the event of negligence on the part of the HOLDER in ensuring the confidentiality of the signature creation data and in protecting any access or disclosure thereof or, as the case may be, of the means giving access thereto.
- In the event of not requesting the revocation of the certificate if there are doubts as to the maintenance of the confidentiality of the signature creation data or, where applicable, of the means giving access to them.
- In case of use of the signature creation data when the validity period of the electronic certificate has expired or the QTSP notifies it of the expiry of its validity.
- In case of negligence on the part of the addressee for not taking into account the loss of validity of the certificate or when not verifying the signature.

Neither the CA nor the RA shall be liable for failure or delay in the performance of any of the obligations under the PSC and the CPs if such failure or delay results from or is the consequence of natural disasters, war, state of siege, state of alarm or health emergency or any other force majeure.

Neither the CA nor the RA shall be responsible for the content of digitally signed or encrypted documents. They do not assume any obligation to monitor the content, type or electronic format of the documents or hashes transmitted by any electronic procedure used by the HOLDER.

The CA and the RA shall not be liable for the correct operation with non-approved applications, and for damages resulting from the impossibility of use with such applications.
Neither shall they be liable for damage or breakdowns in computer equipment or data for reasons not directly attributable to the use of the Certificates or the installation of the certificate, and provided that the APPLICANT does not act with the necessary diligence.

14. MODIFICATIONS

The CA may modify this Contract, as well as the CPS and the CPs or any of their clauses under the terms set out in the same, by notifying the HOLDER or SUBSCRIBER, when the change directly affects their rights and obligations, 15 days in advance, explaining, in any case, the reasons for such a decision (the reasons must have a legal, technical, operational basis). The HOLDER or SUBSCRIBER may choose between terminating the Contract or novating it in accordance with the new terms. The HOLDER or SUBSCRIBER shall have a maximum of 15 days from the date of such communication to inform the CA of the acceptance of the subrogation or of the modifications made. However, if the CA has not received any written communication to the contrary from the HOLDER or SUBSCRIBER after this period, the subrogation and the modifications made shall be deemed to have been accepted.

The above shall not apply to changes and variations made over time to the CPS/CP that are due to the need to ensure compliance with relevant legal changes, to improve processes and to incorporate new services. Successive versions of the CPS/CP are published at https://policy.signaturit.com/, and it is therefore the sole responsibility of the parties involved (APPLICANT, HOLDER, ENTITY, SUBSCRIBER, RELYING PARTIES) to be aware of and adapt their behaviour to the CPS/CP in force ratione temporis. Therefore, changes to the CPS/CP, even if not communicated to the parties, are always valid, effective and binding on the parties from the time of their publication at the address indicated.

15. SERVICE AVAILABILITY

The request and/or consultation of the status of the certificate is available 24 hours a day, 7 days a week as indicated in the CPS/CP. RELYING PARTIES are reminded of their obligation to check this status by consulting the CRL and/or OSCP lists made available by SIGNATURIT on its website.

16. INFORMATION ON DATA PROTECTION

SIGNATURIT (whose details are reflected in the section on the PARTIES of this document) is responsible for the processing of the personal data provided for the provision of the digital certificate issuance service and in this capacity guarantees full compliance with the obligations set out in the regulations in force, both national and European, in accordance with the principles of Article 5 of EU Regulation 2016/679 of 27 April 2016 General Data Protection Regulation (GDPR). In accordance with the RGPD and the Organic Law 3/2018 of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDDA), we inform that, during the application process, the APPLICANT must agree and expressly consent to the terms in which we will treat their personal data in order to continue the process.

We will now provide information on the processing that the data controller will carry out on the personal data provided:

Purpose of processing: In application of the provisions of the CPS and CP, the service of issuing digital certificates to a natural person requires the processing of the personal data of that person (the APPLICANT and future certificate HOLDER) for the issuance and management of digital certificates. In effect, personal identification and contact data such as name, surname, DNI/NIE/Passport, e-mail address, will be included in all natural person certificates, and if the certificate contains ATTRIBUTES of representation or corporate link to an ENTITY, other identification data such as employee number, position, functions, department, etc. and data relating to the ENTITY may also be included. In order to provide the service, the data controller may additionally require the processing of your telephone number, postal address, date and place of birth.

These personal data, as well as the serial number of the certificate, will be included in public key directories necessary to check the validity of the certificates and their non-revocation, in such a way that they will be processed automatically in order to be accessible for consultation by the users of the system (intervening parties).

Furthermore, such data will be processed in order to comply with the legal obligations applicable to the respective services, in particular: their incorporation in IT security and compliance products, the sending of reminders about service expiry dates, their retention for the required legal period and their use in the event of defence in legal proceedings.

In the event that the identity verification process of the APPLICANT has been requested by means of a video identification system, with the prior informed consent of the user, the biometric data of images and video of the face, as well as the recording of the identity document and the sending of the OTP code to the mobile phone will also be processed.

Target group:
It is important to bear in mind that the very operation of a digital certification system means that when using the certificate to sign documents or authenticate, any third party can access the data contained in its certificate (personal data including the certificate serial number) from anywhere in the world, through the public key directories to check the validity of the same (OSCP/CRL services). These accesses shall at all times be in accordance with the provisions of the QTSP CPS, but the QTSP cannot control the use that third parties make of the data contained in the certificate and shall not be responsible for this in any case.

Personal data will be stored on servers owned by SIGNATURIT's provider (the entity IVNOSYS SOLUCIONES, S.L.U.) within the European Union. Beyond the data communications necessary for the provision of digital certification services and beyond the data communications authorised and required by law, SIGNATURIT will not communicate your data to third parties or transfer them to third countries other than the EU or international organisations.

In the process of issuing the certificate, SIGNATURIT can count on the collaboration of third parties or entities for the registration tasks (Registration Authorities (RA) and On-Site Verification Points (PVP) dependent on the RA), as well as for the maintenance and custody tasks of databases and the tasks of support and assistance to clients, which contain and manage personal data (technological and functional suppliers). These entities shall in any case act as data processors for SIGNATURIT for the sole and exclusive performance of the obligations and instructions given by SIGNATURIT or for the performance of the services contracted. The complete list of external data processors shall be made available to the Clients upon written request sent via the means indicated for the exercise of rights.

In the event of termination of the QTSP's activity, the information supplied for the issuance of the certificate may be disclosed to third parties, under the same terms and conditions, in order to comply with the custody obligations required by the APPLICABLE REGULATIONS.

Legitimation of the processing: The legal basis for the processing of personal data is to be found both in the contractual relationship established by virtue of the services contracted from SIGNATURIT and in the very purpose of the service that requires linking signature validation data with a natural person, and in the legal obligation imposed on QTSPs to verify the identity and other attributes of the natural person to whom they issue a digital certificate and to record and keep accessible such data for the stipulated legal period. The contracting of our services obliges the customer to provide personal data, even in the case of the use of a pseudonym, and therefore, if the customer does not consent to the processing of his personal data, the service cannot be provided.

Retention periods: SIGNATURIT will process your data for the duration of the provision of services and, subsequently, for the time necessary for the management of suspended or revoked certificates and for the periods of time legally established for the purging of its own and third party responsibilities. In this regard, the APPLICABLE REGULATIONS require your identification data and other information relating to the service provided to be kept for 15 years from the expiry or revocation of the certificate or from the end of the service provided. During this period, your data will only be used for the fulfilment of SIGNATURIT's legal obligations in its capacity as PSC.
Once the period referred to in the previous paragraph has expired, SIGNATURIT will erase the data and therefore cease any processing activity, without prejudice to the requirements of the authorities or under current or future legislation.

Rights of data subjects: Data subjects as subjects of the processing of their personal data may exercise the following rights granted to them by applicable privacy laws: access, rectification, erasure, deletion, restriction of processing, portability and objection.
It is hereby informed that the exercise of the rights of rectification or deletion of personal data that have been used for the issuance of a digital certificate will entail the revocation of said certificate and that without prejudice to adopting technical and organisational measures for the effectiveness of the request, SIGNATURIT shall keep the identification data and other data associated with the certificate in order to comply with the legal obligations imposed on it as a QTSP and for the exercise or defence of claims.

To exercise your rights, you can contact our Data Protection Delegate by sending an email to dpo@signaturit.com or via the email address soporte@signaturit.com or by sending a letter to the attention of SIGNATURIT SOLUTIONS, S.L.U., Carrer d'Avila no29, piso 1, (08005 Barcelona). In the event that your request is not satisfied, you may file a complaint either with our Data Protection Officer, through these means, or directly with the Spanish Data Protection Agency.

It is reminded that the APPLICANT or SUBSCRIBER cannot provide us with third party data beyond the data strictly necessary for the execution of the service, such as those of the ENTITY to which the certificate is linked or those of the persons benefiting from the service (and always with their prior consent) and that they are responsible for the veracity of the data they provide us with.

17. TERMINATION OF THE CONTRACT

Failure by either PARTY to comply with the provisions contained in this Contract and/or the CPS or the CPs shall be grounds for termination of this Contract. In such a case, the non-breaching party shall be entitled to terminate the Contract with immediate effect. Failure by the APPLICANT/HOLDER, the ENTITY or the SUBSCRIBER shall entitle the CA to revoke the Certificate, irrespective of any damages that may be claimed.

The CA shall have the right to revoke and not renew the Certificate prior to the expiration date in the cases foreseen in the corresponding CPS and CP or for causes based on possible regulatory requirements including the applicable technical standards. When the revocation is unjustified, the CA may compensate those APPLICANTS and SUBSCRIRIBERS who request it in writing within three months from the date of revocation. This compensation shall not exceed the amount paid by the APPLICANT for obtaining the Certificate.

The APPLICANT or the SUBSCRIBER may freely terminate this contract at any time by giving 30 days' written notice. In any case, such termination shall not entitle the right to a refund of the amounts paid for obtaining the Certificate.

If the exercise of the rights of objection or cancellation of the data set out in this document would hinder the provision of the services covered by this contract, SIGNATURIT shall be entitled to terminate this contract.

18. LEGISLATION AND JURISDICTION

This contract, the CPs applicable to the type of certificate requested and the CPS shall be governed by the Spanish and European law on certification and electronic signatures applicable at any given time, in accordance with which its content must be interpreted.
For the resolution of any dispute that may arise in relation to this contract or the CPS and the CPs, the parties, waiving any other jurisdiction that may correspond to them, submit to the Spanish Court of Arbitration. If the HOLDER is a consumer, the Court or Tribunal of their place of residence shall have jurisdiction.

19. SOLE AGREEMENT

This agreement, and the documents to which it refers, constitute the entire agreement between SIGNATURIT, the Registration Authority and the APPLICANT on the subject matter hereof, and supersedes, cancels and renders null and void any other oral or written agreement on the same subject matter reached by the parties prior to the date of signature of this agreement.

_____

SIGNATURIT SOLUTIONS SLU (and the external Registration Authority where applicable) being in agreement with the above, the APPLICANT (and where applicable the SUBSCRIBER) reads the whole of the present document and declares that he/she fully adheres to its contents.