GENERAL TERMS AND CONDITIONS
OF QUALIFIED ELECTRONIC SIGNATURE SERVICE

For the purposes of this Agreement, the following terms shall have the following meaning:

- **"Qualified Certificate**" or **"Certificate**": qualified electronic signature certificates issued by a qualified trust service provider in compliance with the requirements set out in annex I of EU Reg. 910/2014.
- **"Agreement**": the entire contractual documentation including the General Terms and Conditions, the Activation Application, the PKI Disclosure Statement, the Certificate Practice Statement and all documents referenced therein which govern relationships between the Parties.
- **"Domain**": the SP's web domain, where this document has been downloaded, or with any other web pages that the SP has used or will use in relationships with its clients, as described in the PKI Disclosure Statement and under section 4.5.3 "*Use restrictions and value limits*" of the CPS available on the website *www.infocert.it*.
- **"InfoCert" or "TSP" (Trust Service Provider):** InfoCert S.p.A. - a company managed and directed by TINEXTA S.p.A. - with registered office in Rome, Piazza Sallustio, 9 – 00187, Tax no. and VAT no. 07945211006, call center 199.500.130, Fax +39 06 83669634, Certified Mail address infocert@legalmail.it. InfoCert renders the Service as Qualified Trust Service Provider, pursuant to Regulation (EU) no. 910/2014 dated 23/07/2014, on the basis of a conformity assessment carried out by the Conformity Assessment Body CSQA Certificazioni S.r.l., pursuant to the aforementioned Regulation and to the Standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2, in accordance with the eIDAS assessment scheme defined by ACCREDIA in response to ETSI EN 319 403 and UNI CEI ISO/IEC 17065:2012. InfoCert's code of ethics is available on the website: https://www.tinexta.com/file/1790. The company is subject to the statutory supervision of AgID and operates as accredited certification body under the Italian Legislative Decree 82/2005 and subsequent amendments ("**Codice dell'Amministrazione Digitale**", or "**CAD**").
- "**PKI Disclosure Statement**" or "**PDS**": document named Public Key Infrastructure Disclosure Statement cod. ICERT-INDI-PDS (which fulfils the publication requirement provided for by the European standard ETSI EN 319 411-1), relating to the certification service offered by InfoCert S.p.A., and providing the technical information, applicable legislation, policies and standards relating to the use of the Service, as well as the best practices that the Applicant is required to adopt, attached to the Agreement and available on the website *www.infocert.it*.
- "**Certificate Practice Statement**" or "**CPS**": Certificate Practice Statement for the Remote Signature Subscription Certificates identified by the O.I.D.s 1.3.76.36.1.1.34 and 1.3.76.36.1.1.64, code ICERT-INDI-MO-ENT, filed by InfoCert S.p.A. with the Italian Agency for the Digital Agenda ("**AgID**") and available on the website *www.infocert.it*, on AgID's website or at its office or by means of a request to be filed with the Registration Offices or at the End User Information Contact, as defined in the CPS.
- "**Identification Procedure**": Owner identity verification procedure carried out according to the CPS.
- "**Applicant**" or "**Registration Office**" or "**Service Provider**" ("**SP**"): the entity applying for the issuance of Subscription Certificates in favour of the Owner/Owners and appointed by the TSP to perform, as Registration Office, the activities necessary for the issuance of the Certificate, as indicated in Section 1.3.5. of the CPS.
- "**Activation Application**": the QES Service activation form to be filled in by the Owner.
- **"Role"**: professional title and/or qualification held by the Owner, i.e. any power to represent natural persons or private or public law entities, or membership of such entities as well as the exercise of public functions.
- "**Qualified Electronic Signature Service**" or "**QES Service**": certificate activity carried out by InfoCert, consisting in an electronic public key procedure detectable by means of a validator which guarantees a two-way correspondence between the Public Key and its Owner and identifies the Owner and the validity period/expiry date of the certificate in accordance with the provisions of the Agreement.
- "**Interested Third Party**": the Applicant providing consent for inserting the Role in the certificate, where required.
- "**Owner**": the natural or legal person requesting activation of the QES service, identified on the basis of information provided in the Activation Application and issued with a Certificate containing their personal details.

*** *** ***

SECTION I - A
GENERAL PROVISIONS

1. Terms and Conditions of QES Service.

For the purposes of this Agreement, service performance and relationship with Applicant and Owner shall be governed by the eIDAS Regulation, InfoCert's local laws, the PDS, the CPS and the clauses of this Agreement.
The Applicant undertakes all obligations under this Agreement and agrees to pay the fees due for the delivery and management of digital certificates.
Applicant and Owner are required to read and approve the provisions of the CPS regarding the type of Certificate required and the present General Terms and Conditions, as well as to read the technical requirements related to the type of Certificate requested as described in the CPS.
Certificates issued under these Terms and Conditions may only be used for (i) the SP's web domain, corresponding with the SP's website or with any other website used by the SP in its relationship with its clients (the "**SP Domain**") and, if necessary, (ii) for signing electronic documents relating to products or services offered by the SP to its clients in its own name or as an agent for third party companies ("**Third Parties**") with or without powers of representation. For this reason, certificates shall be effective only if the Owner has entered into a contractual relationship with the SP concerning the services provided by the latter.
The Agreements and the forms signed by the Owner through a Qualified Certificate (including their contents) are outside the scope of the Qualified Electronic Signature Service. Therefore, it is the responsibility of the Owner to carefully check their contents.

2. Statement and Consent pursuant to EU Regulation no. 679/2016.

As data controller of the personal data provided by the Owner through the filling in the Activation Application form or during the term of the Agreement, InfoCert shall process such data, according to article 13 of EU Regulation no. 679/2016, with the help of paper files and computer tools to ensure maximum security and confidentiality, for the purposes and with the methods set out in the Privacy statement on processing of personal data submitted to the Owner upon signing this Agreement and available at the following link *https://www.infocert.digital/pdf/Information-Notice_customers-purchasing-from-the-website-and-end-customers.pdf*.

3. Owner's Liabilities.
The Owner shall be responsible for the accuracy of the data provided upon identification and in the Application Form. If during the identification the Owner conceals their identity or claims a false identity by providing untruthful personal documents or acts in such a way as to affect the identification process and its findings as stated in the Certificate, he or she shall be held liable for all damage incurred in by the TSP and/or third parties as a result of the incorrect information provided in the Certificate, and shall be obliged to indemnify and hold harmless the TSP in the event of any claims for damages.

4. Notifications.
Any written communication shall be sent by the Owner to the End Users Information Contact.
InfoCert shall send any written communication to the Applicant and/or Owner to the provided certified email address. If no certified email address has been provided, all correspondence shall be sent to the email address entered in the Application Form.

5. Execution of the Agreement/Termination.
Without prejudice of the provisions of Section 3, the Agreement shall be considered as executed when InfoCert receives the Activation Application duly and entirely filled in.
Without prejudice to the above, the validity of the Agreement is subject to the successful identification of the Owner. Therefore, in case the identification fails, the digital Certificate shall not be issued by the Trust Service Provider or, if issued, it shall be deemed null and void and the Agreement shall henceforth be deemed terminated by law.
The Certificate shall be issued upon successful identification of the Owner. In the event that the Application is filed by an unauthorized subject, is not complete or lacks the requested information, the Agreement shall not be considered as executed. If identification fails, no digital certificate shall be issued by the Trust Service Provider or, if issued, it shall be deemed null and void and the Agreement shall henceforth be deemed terminated by law.
Where the Owner is a consumer, the Owner requests immediate delivery of the Service by executing the Activation Application, and agrees to waive the right of withdrawal according to which the consumer waives its right of withdrawal in case the services are started and fully rendered with the execution of the contract upon request of the consumer and in this provision. Except as provided for in Article 16 of these General Terms and Conditions, the Owner acknowledges and agrees that this Agreement will be automatically terminated in case of termination of the Owner's contractual relationship with the SP under any reason and that this shall result in the revocation of the Digital Certificate and that the Owner will have no claims vis-à-vis InfoCert as a result of such termination.

6. Service Availability.
The request and/or verification of the Service are available as indicated in article 9.17 "Minimum Service Availability" of the CPS or from 00:00 to 24:00, 7 days a week. InfoCert undertakes to ensure compliance with the 95% of the aforementioned availability.

7. Applicable laws.
All matters related to the formation, perfection and signature of this Agreement is governed by the law of the country in which the Consumer has his/her [its – in case of Company] principal place of business or life.
The interpretation, performance and any other obligation that has become content of this Agreement after its perfection and signature shall be governed by Italian law, which rules the service that the Consumer has purchased according to the Regulation (EU) 910/2014 and the Regulation (EU) 679/2016 as well as to any further Italian implementing and technical regulations thereto.

8. Claims/Jurisdiction.
The Owner who intends to submit a formal complaint to InfoCert with reference to the provision of the Service may send a written communication, by Certified Electronic Mail (to the address: infocert@legalmail.it) or by registered mail with return receipt (to the address: InfoCert S.p.A., Piazza Luigi da Porto 3, 35131, Padova, Italy), or by fax (to +39 06 83669734). It should also be noted that, pursuant to the EU Regulation No. 524/2013, for the resolution of disputes relating to online contracts and services, it is possible to refer to the Online Dispute Resolution (ODR) procedure, provided by the European Commission and accessible at the following link: https://webgate.ec.europa.eu/odr/.
Any dispute arising between the Parties out of this Agreement, including those in relation to the validity, interpretation, execution and termination shall be exclusively assigned to the Court of Rome, with the exclusion of any other competent jurisdiction.
If the Owner is a consumer, pursuant to Art. 66-bis of the Consumer Code, civil disputes relating the Agreement executed by the consumer shall be assigned to the mandatory territorial jurisdiction of the court located in the consumer's place of residence or domicile.

*** *** ***

SECTION I - B
SIGNATURE CERTIFICATES WITH REMOTE SIGNATURE PROCEDURE

9. Scope.
In general, an Owner applying for a signature certificate is requesting the Trust Service Provider to issue a Qualified Certificate matched with the Owner's digital signature, as created through a secure device pursuant to the provisions of the regulations referred to in Article 1 (c) (I) of these General Terms and Conditions.
The Certificates use special IT procedures aimed at ensuring compliance with Italian applicable laws with respect to secure devices, procedures for signature generation and protection from the use by third parties.
The QES Service relates to the provision by the Trust Service Provider to the Owner of a software application residing on InfoCert's or the Applicant's systems, enabling the Owner to manage their remote signature procedure certificate available on the HSM (*Hardware Security Module*).

More specifically, it concerns the issuance of a Qualified Certificate associated with the Owner's public key and its publication together with the latter as detailed in the Practice Policy Statement.
Specifically, the QES Service allows the Owner, upon authentication by means of a dedicated tool and within 60 (sixty) minutes the issuance of a Qualified Certificate, to remotely manage their Qualified Certificate for the purpose of signing documents or document hashes made available to the Owner through a special electronic procedure set out by the Applicant.

10. Qualified Electronic Signature Service Application Form.
Pursuant to the provisions of the PDS, the Applicant undertakes to pay QES Service fees and to designate, through specific actions and procedures, the parties to whom the Certificates shall be issued.
The Owner must obtain from the TSP a duly issued and registered Certificate in the manner set out in the PDS and detailed in the CPS available on TSP's website, through the dedicated online Application Form. In case of a positive outcome of the necessary checks, a Certificate shall be issued to the Owner and published in the appropriate register in accordance with the CPS.
Such Certificate shall be effective only if the Owner has entered into a contractual relationship with the SP concerning the services provided or offered by the latter.
The Owner hereby grants its consent for the TSP to record and store for 20 (twenty) years the information collected with the registration, the information concerning the instruments provided, the revocations, the identity and the features inserted in the Certificate and grants its consent for the transfer of such information to third parties under the same conditions in case the TSP terminates its activity, as indicated in par. 5.8. of the CPS.

11. Activation and Operation of the QES Service.
The QES Service shall be activated following the identification and notification by the Applicant to the Trust Service Provider of the electronic procedure for submission of the documents to which the digital signature and the signature keys activation procedures shall be applied by the Owner.
If the Applicant has requested the insertion of the Role in the Certificate, this shall be done in accordance with the CPS, including the consent given by the Interested Third Party.

12. Owner's Obligations.
The Owners shall under their full responsibility state the type of selected authentication system through which the remote signature procedure shall be activated.
The Owner's obligations shall be as set by law and by the PDS and the CPS. In compliance with the Italian applicable laws with respect to the Owner's obligations, and specifically the safekeeping of the signature device and the obligation to personally use the signature device, the Owner is required to apply all appropriate measures aimed at preventing damages to third parties resulting from the use of qualified electronic signatures.
The Owner acknowledges that the use of qualified electronic signatures enables signing of legally enforceable deeds and documents which shall be solely attributable to the Owner and that the Owner is therefore bound to the utmost diligence with regards to specifying, using, storing and protecting the authentication tools which the TSP or the Registration Office shall provide to the Owner. Authentication tools for the activation of the remote signature procedure are strictly personal. Therefore, the Owner is required to protect the secrecy of such tools by not disclosing them to third parties in whole or in part and by storing them in a secure manner. The Owner shall upgrade their hardware and software systems to meet the safety requirements under applicable laws.
However, the Owner is obliged to carefully check the contents of the documents that they intend to sign via the remote signature procedure and to refrain from activating the signature procedure if such content is not consistent with the intention that the Owner intends to convey.

13. Obligations of the Trust Service Provider.
The obligations of the Trust Service Provider are as set out in the current legislation, in section 1.3.1. of the CPS and in these General Terms and Conditions.
The Owner recognition procedure, particularly as regards the identification of the Owner, may be performed in one of the manners provided in the CPS and agreed between InfoCert and the Applicant.
The TSP undertakes no obligations other than those provided for by these General Terms and Conditions, the PDS, the the CPS and the electronic certification legislation.
In particular, the TSP undertakes to:

- preserve all the Certificates issued in the manners provided for in the PDS and the CPS in a long-term preservation system for 20 (twenty) years;
- ensure digital preservation in the manners described above also of the logs of the Service.

In particular, the TSP does not offer any warranty regarding (i) the correct functioning and safety of hardware and software systems used by the Owner, (ii) any use of the Certificate other than that permitted by the Italian laws or covered in the PDS and the CPS, (iii) the regular and continued operation of national and international electric and telephone lines, (iv) the relevance and (evidential) effectiveness of the Certificate or of any message, record or document associated therewith or submitted through the relevant signing keys in respect of documents and records covered by the legislation of countries other than Italy, nor to the privacy and/or integrity of such documents (meaning that any privacy and integrity violations are normally detectable by the Owner through a specific verification procedure).
The TSP's warranty is limited to proper functioning of the remote signature procedure according to the service level mentioned to the Applicant and the Owner.
As described under the final subparagraph of Article 12, the Trust Service Provider is under no obligation to monitor the contents, the type or the electronic format of documents and hashes submitted via the electronic procedure specified by the Applicant or Owner and, except in cases of willful misconduct and gross negligence, shall not undertake any responsibility regarding their validity and their consistency with the actual intentions of the Owner.

14. Duration of the Agreement and validity of the Certificate.

The General Terms and Conditions shall enter into force on the date of issuance of the Certificate by the TSP and their duration shall be as stated in the "Validity" field of the same Certificate.

15. Fees.
The fees for the QES Service shall be payable to InfoCert under the agreements between the latter and the SP.

16. Revocation, Suspension and Renewal of the Certificate.
Since the duration of each Certificate shall be less than or equal to the minimum amount of time (60 minutes) before a Certificate invalidity warning is generated, the possibility of revoking and suspending does not apply to Certificates covered by these General Terms and Conditions.

17. Liability of the TSP.
Save as provided by Article 13 of these General Terms and Conditions, the liability of the TSP for QES Service shall be regulated by the PDS, by Section 4.1.2 of the CPS available on TSP's website, by these General Terms and Conditions and by applicable laws.
During the formation and performance of the Agreement, the TSP shall not be liable for any damage and/or delay due to system failure or system crash.

18. Termination of the Agreement.
The TSP has the right to terminate this Agreement in case of breach by the Owners of their obligations under these General Terms and Conditions as well as in the event of the Owner failing to pay the fees and in the other situations envisaged by these Terms and Conditions.
Any measures adopted pursuant to this Article shall be notified to the Applicant and the Owner as provided for by Article 4 above.
In all cases of termination not caused by TSP's default, the TSP shall have the right to withhold the amount paid by the Applicant under Article 15 above.