

General terms and conditions WEB sites Authentication Certificates

InfoCert S.p.A. (hereinafter, "**InfoCert**"), a Company under the direction and coordination of Tecnoinvestimenti S.p.A., with registered office in Rome, Piazza Sallustio n. 9 - 00187, VAT Reg. No. 07945211006, Call Centre 199.500.130, Email firma.digitale@legalmail.it, Fax +39 049 0978914, Certified Electronic Email infocert@legalmail.it, subject to the supervision of the Agenzia per l'Italia Digitale (Digital Agency for Italy) (hereinafter, "**AgID**") for the activities provided for by law. InfoCert adheres to the Code of Ethics which is accessible on the website through the following link: <https://www.infocert.it/pdf/all3codetico12.pdf>. and acts as an accredited certifier, pursuant to Art. 29 of Legislative Decree 82/2005 and subsequent amendments and integrations. ("**Digital Administration Code**", hereinafter the "**D.A.C.**").

In this capacity, InfoCert ("**Certifier**") issues, among other services, web sites certification services, by means of the issuance of Web Server Organization Validation type Authentication Certificates (with validation by the Organization as defined below), Extended Validation (with validation extended to the Organization as defined below) and qualified Organization Validation.

Such activity consists of the electronic procedure, applied to the public key and detectable by the validation systems, by means of which the bi-univocal correspondence between the public key, the legal entity and the Internet domain to which it belongs is guaranteed and the period of validity of said key and the expiration term of the relevant certificate is attested ("**Service**").

InfoCert renders the Service as qualified trust service provider, pursuant to Regulation (EU) no. 910/2014 dated 23/07/2014 ("**Regulation**"), 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.

*** **

SECTION I GENERAL PROVISIONS

1. Terms and conditions of the Services.

1.1. Discipline and definitions.

Under these General Terms and Conditions, the terms used have the meaning indicated in the Certificate Policy

and Practice Statement ICERT-INDI-MOWS hereinafter better described or in the legislation listed below according to the following clarifications.

The Applicant is the subject filing the request for the issuance of the SSL certificate with InfoCert and who pays the fees.

The Subject is the internet domain, the device or the system for which the certification service is requested.

The Organization is the owner of the domain indicated above as Subject.

The Applicant usually coincides with the Organization and will therefore be indicated hereinbelow as Applicant/Organization.

However, these two subjects may also be distinguished (by way of example and not limited to, in case the Applicant is a company affiliated to or controlled by the or is mandated by the Organization).

The contractual relationship between the Certifier on the one hand and the Organization/applicant on the other hand is ruled by the following contractual documentation (hereinafter, jointly defined as the "**Contract**"):

- these general terms and conditions,
- the Order and the Registration and Certification request,
- the "**Certificate Policy**" or Operating Manual for the qualified Certificates, cod. ICERT-INDI-MOWS, filed by InfoCert with AgID (the "**Certificate Policy and Practice Statement ICERT-INDI-MOWS**"), that the Applicant represents to have previously read and to fully approve.

The above mentioned Certificate Policy and Practice Statement s are available:

- in electronic format on the Certifier's web site (<http://www.firma.infocert.it>);
- in electronic and hardcopy format at AgID;
- in hardcopy format, by prior request to the Registration Offices or to the Certifier's "Contact for end users" specified in the aforementioned Certificate Policy and Practice Statement .

The Applicant is required to carefully read and approve of all the provisions referred to in the Contract. In particular, the Applicant undertakes the obligation to pay the fees due for the issuance and management of digital certificates and for the delivery and/or provision of secure seal devices.

If the Applicant is other than the Organization, the Applicant undertakes to submit the Contract to the Organization and to ensure the compliance, by the Organization, with the provisions contained therein. Therefore, the Applicant guarantees against InfoCert,



General terms and conditions WEB sites Authentication Certificates

also pursuant to art. 1381 Civil Code, the full compliance with the Contract by the Organization.

It is understood that all the obligations hereto to be borne by the Applicant are also charged jointly to the Organization.

Any use of the Service contrary to the terms of the Contract is prohibited.

1.2. Execution of the Contract. Pursuant to the Consumer Code and other relevant and applicable laws, if the services are requested online, the computerised procedure for the execution of the Contract provides that the parties accept InfoCert's proposal and request the services only after having acknowledged the documentation and then follow the computerised procedure for the storage of documents and the provision of consent. Before submitting the request, any data entry errors can be detected and corrected by exiting and restarting the procedure from the original website. The Contract is executed when the request, as acceptance of the proposal, is received by InfoCert. Subsequently, the execution shall be confirmed on a durable device with the delivery of a copy of all the contractual documentation. The Contract shall be stored with the Certifier by law.

When the services are not requested online, the Contract is executed when InfoCert receives the Registration and Activation Request properly completed in all its parts. The Contract shall not be deemed to be executed if the Request comes from an unauthorised subject, is not completed in all its parts or lacks the requested information.

2. Processing of personal data (EU Regulation no. 679/2016).

2.1. InfoCert, as data controller of the data provided by the Applicant through filling in the Order or Registration and Certification Request or in the course of the relationship, undertakes to process the aforesaid personal data, including the personal data of any delegated parties who act in the name and on behalf of the Applicant during the relationship, pursuant to Art. 13 of EU Regulation no. 679/2016, by means of hardcopy archives and IT and electronic devices suitable to guarantee their security and confidentiality for the purposes and according to the modalities described in the "Privacy Policy – InfoCert Services Activation" available on the "Documentation" page on the website www.infocert.it, which the Applicant represents to acknowledge.

3. The Organization's and the Applicant's liability.

3.1. The Applicant and the Organization are jointly liable for the truthfulness of the data reported in the Registration and Certification Request. If upon identification, the Applicant has hidden, also by means of false personal documents, their actual identity or falsely declared to be another subject or, in any case, acted in such a way as to jeopardise the identification process and related results indicated in the certificate, he/she shall be held liable for all damages caused to the Certifier and/or to third parties due to the inaccuracy of the information contained in the certificate, with the obligation to guarantee and hold the Certifier harmless from any possible claims for compensation for damages. The Applicant and the Organization are also liable for damages to the Certifier and/or third parties in the event of omission (even partial) or in case they delay the activation of the procedures provided for by the Certificate Policy and Practice Statement for the revocation and/or the suspension of the Certificates. More in general, the Applicant and the Organization shall have to jointly compensate InfoCert for all the damages the latter may suffer as a (direct or indirect) consequence of the Applicant or the Organization failing to comply with their obligations under this Contract or with the laws applicable from time to time; they shall also jointly compensate and hold InfoCert harmless from any amount owed by InfoCert to third parties, or to pay any monetary or administrative fine, as a consequence of failing (even partially) of the above mentioned Applicant's and Organization's obligations.

4. Miscellaneous.

4.1. Communications. Any written communication, including any complaints regarding the provision of the Service, shall be sent by the Applicant and/or by the Organization to the addresses indicated in the Certificate Policy and Practice Statement under the Article "*Contact for end users and communications*".

InfoCert shall send any possible communications to the Applicant/Organization to the certified email address ("**PEC**") or, in default, to the email address indicated in the Order and/or the Request Form.

4.2. Changes to contractual terms. The provision of the services is ruled and governed by the Contract. Save as provided for in the next paragraph, InfoCert is entitled to make changes to the contractual terms of the services. In such case, and at least thirty (30) days prior to the application of these changes, the new contractual terms applicable to the service shall be notified to the parties by means of PEC or other device chosen by InfoCert. In case the Applicant/Organization does not accept the



General terms and conditions WEB sites Authentication Certificates

new terms, he/she shall properly inform about the cancellation by PEC or by registered letter with return receipt prior to, under penalty of decadence, these changes entering into force. Lacking said cancellation, or in case the cancellation is not prompt, the Contract shall remain in force under the new terms.

The aforesaid provisions on changes in contractual terms and conditions do not apply to the amendments and changes made over time to the Certificate Policy and Practice Statement . In fact, the Certificate Policy and Practice Statement are drawn up by InfoCert in accordance with legal provisions and are published by AgID only after the latter's positive assessment in relation to the certification report (CAR - Conformity Assessment Report) produced by an accredited Conformity Assessment Body (CAB). The Manuals are published on InfoCert website following AgID's approval and publication. The aforesaid Certificate Policy and Practice Statement are subject to changes over time that are not due to InfoCert's mere discretion, but to the need to ensure their adaptation to changes in the applicable law. Therefore, it is the sole responsibility of the Organization and of the Applicant to know and to adapt their behaviour to the applicable Certificate Policy and Practice Statement ratione temporis available for consultation at any time on AgID website. Furthermore, changes to the Certificate Policy and Practice Statement , even if not communicated to the parties are, in any case, always valid, effective and binding for the parties since the publication of the Certificate Policy and Practice Statement containing these changes on AgID website.

4.3. Jurisdiction. Any dispute arising between the parties in relation to this Contract, including those related to its validity, interpretation, execution and termination shall be exclusively assigned to the Court of Rome, with the exclusion of any other competent jurisdiction. Additionally, pursuant to EU Regulation no. 524/2013, in order to solve any controversies relating online contracts, it is possible to file for the Online Dispute Resolution (ODR) proceedings set forth by the European Commission and available at the following link: <https://webgate.ec.europa.eu/odr/>.

4.4. Applicable law. This Contract is governed by the Italian law. For anything that is not expressly provided herein, reference shall be made to the provisions of the Civil Code and other applicable laws.

4.5. Severability. Each provision of the Contract shall be deemed as approved in the sense that i) it constitutes an autonomous part of the Contract, ii) it produces, in any case, its effects regardless of the effectiveness or nullity of other contractual provisions and (iii) its possible

invalidity shall not affect in any case the validity and effectiveness of the Contract.

4.6. Service availability.

The request service is available on business days from 9 until 17. The request of audit over the state of the certificate is available according to what indicated in the Certificate Policy and Practice Statement under art. 9.17 "Service minimum availability" or from 00:00 until 24:00, 7 days out of 7. InfoCert undertakes to ensure the compliance with 99% of the aforementioned availability.

5. Intellectual property.

5.1. All intellectual and industrial property rights and any and all other rights on the service and its software and any other technological solution included therein and/or connected thereto are and shall remain the property of InfoCert, unless third party's ownership is expressly indicated. All rights for the use of the service and the software and technological solutions included therein are reserved to InfoCert. The Applicant and the Organization are granted with the use of the service solely within the limits and the terms provided in the Contract. They cannot use the service, software and technological solutions included therein in any other way. By way of example but not limited to, copying, modifying, decompiling, disassembling, distributing, also online, and granting third parties with the use of the service, software and technological solutions is prohibited.

*** **

SECTION II WEB SITES AUTHENTICATION CERTIFICATES

6. Scope.

6.1. the web sites authentication certificates allow the visitor of a site, that is to say the User as to par. 1.3.4 of the Certificate Policy and Practice Statement , to ascertain that behind that web site there is an actual and legal entity. The service request of web sites authentication certificate is aimed at the issuance by the Certifier of a **qualified or unqualified Certificate** for a domain with validation of the organization (OV Certificate or qualified OV Certificate) or for a domain with organization's extended validation, (EV certificate). Such certificate is compliant with the requirements of the certification/browser Forum Authorities (CA/B Forum) and to what is provided under the Certificate Policy and Practice Statement ICERT-INDI-MOWS.



General terms and conditions WEB sites Authentication Certificates

The qualified certificate is compliant with the requirements as to annex IV of the Regulation.

The issuance occurs according to the modalities indicated in the ICERT-INDI-MOWS Certificate Policy and Practice Statement .

7. Request of registration and certification.

7.1. If indicated, the Applicant is obliged to pay fees and to indicate, by separate deeds, the persons to whom the digital certificates should be issued.

The Applicant shall request the registration and the issuance of the web sites authentication certificate according to the modalities provided for in the ICERT-INDI-MOWS Certificate Policy and Practice Statement , by using the proper Registration and Certification Request Template made available to him.

7.2. In case of positive outcome of the controls necessary to the issuance of the certificate, the latter is issued and released to the Applicant/Organization based on what provided for by the ICERT-INDI-MOWS Certificate Policy. The Applicant and the Organization hereby give their consent for the Certifier to register and retain for 20 (twenty) years the information collected through the registration, those information relating the provided devices, the revocations, the identity and features inserted in the certificate. The termination of the Service and the AC or the RA is ruled by Art. 5.8 of the Certificate Policy and Practice Statement . The Applicant/Organization hereby give their consent to the possible transfer of the aforesaid information to third parties, under the same terms and conditions, in the event that the Certifier shuts down its business.

8. The Applicant's/Organization's obligations.

8.1. The Organization's obligations are those set forth in the applicable legislation, the Contract and the Certificate Policy and Practice Statement . The Organization/Applicant shall ensure the custody of the keys and adopt all the suitable organization and technical measures to avoid damages to third parties.

8.2. The Organization/Applicants shall also apply the utmost diligence in the indication, usage, storing and protection of the authentication tools also including the private key. Moreover, the Applicant and the Organization, shall also provide the adaptation of their *hardware* and *software* to the security measures provided by the current laws.

More in general, the Organization/Applicant guarantees the absolute security and reliability of the site on which the certificate is used.

8.3. Prior to installing the certificate on its server, the Applicant/Organization shall verify the correctness of the same certificate and of all the contents contained therein.

The Applicant/Organization shall also install said certificate exclusively on servers accessible through the domain to which the same certificate refers to, and to use the relevant keys only for the domain contained in the same certificate.

8.4. The Applicant and the Organization shall immediately inform in writing InfoCert about any circumstance that may reasonably and precautionally suspect about any threat (by way of example: theft, loss, damage, ...) of the private key or of the certificate.

8.5. The Applicant and the Organization shall in no way use the certificate or the relating key after its expiration, or revocation or suspension.

8.6. The Applicant and the Organization shall in no way use the certificate or the relating key to certify or anyway let other subjects obtain the typical effects of certification.

8.7. The Applicant and the Organization cannot use the certificate, even indirectly, to:

- deposit, send, publish, transfer and/or share IT applications or documents in contrast or in violation of intellectual property rights, commercial secrets, trademarks, patents or other third parties' intellectual property rights or that may damage, breach or try to breach the secrecy of correspondence and the right to confidentiality;

- publish and/or share material that, by way of example: breaches or infringe intellectual property rights, commercial secrets, trademarks, patents or other rights, contents against morality and the public order, contains pedopornographic, pornographic obscene contents or that are anyway contrary to the public morality, is suitable to breach or try to breach the confidentiality or personal or other sensitive data protection, or is aimed at damaging the integrity of third parties' resources or to provoke a direct or indirect damage to anyone (bootlegged software, cracks, key generators, serials, virus, worm, trojan horse or other harmful components), may represent an abuse, menace, libel, harassment, spamming, or may incite violence, racial hate, terrorism, etc.

8.8. The Applicant and the Organization undertake to strictly comply with the Model pursuant to legislative Decree 231/2001 and InfoCert's Code of Ethics, in the version that will be available from time to time on the site www.infocert.it and that the Applicant and the Organization undertake to periodically monitor.



General terms and conditions WEB sites Authentication Certificates

Any failure to comply with such obligation shall entitle InfoCert to terminate the Contract pursuant to art. 1456, Civil Code.

8.9. More in general, the Applicant and the Organization undertake to hold InfoCert harmless from any liability in relation to the contents and all information published through the certificate, in relation to the use of the same certificate and in case of charges, legal actions, judiciary or administrative actions, losses or damages (including legal costs and expenses) arisen out of the illegal use of the services or anyway contrary to the Contract by the Applicant or the Organization.

9. Certifier's obligations.

9.1. The Certifier's obligations are those set out in the applicable legislation and in the Certificate Policy and Practice Statement ICERT-INDI-MOWS. In particular, InfoCert undertakes to:

- store all the certificates issued according to the modalities provided for by the Certificate Policy and Practice Statement for 20 (twenty) years in a suitable non-editable digital database;
- ensure the storage also for Service logs, according to the above described modalities.

The Certifier undertakes no additional obligations other than those provided for by these General Terms and Conditions, the Certificate Policy and Practice Statement ICERT-INDI-MOWS and the applicable laws on certification activities.

9.2. In particular, the Certifier provides no guarantee on the proper functioning and security of the hardware and software equipment used by the Applicant and/or Organization, on different uses of the Certificate with respect to the ones provided herein and by the Certificate Policy and Practice Statement, on the regular and continuous operativity of the national and/or international electric and telephone lines, on the validity and relevance, even probationary, of the Certificate.

9.3. In consideration of what provided herein, the Certifier shall not undertake any surveillance obligation with respect to the contents of the sites, the transmission protocol indicated by the Applicant, thus not undertaking any liability save the case of fraud and gross negligence in relation to their validity.

10. Duration of the Contract and validity of the Certificate. No assignment or transfer abroad.

10.1. The Contract has the same duration as that of the signature certificate indicated in the latter's "validity" field.

10.2. Before the date of expiry, the Applicant may request a renewal of the certificate according to the procedure provided in the Certificate Policy and Practice Statement ICERT-INDI-MOWS. The renewal entails the extension of the certification Contract until the expiration or revocation of the renewed certificate and the payment of the fees established for this service. An expired or revoked certificate cannot be renewed.

10.3. The certificate shall in no way be assigned or transferred, by the Applicant or the Organization, to third parties (neither as a consequence of transfer or rent of business), without InfoCert's prior written consent. The certificate shall neither be transferred or exported in other countries in breach of laws or regulations of other jurisdictions.

10.4. Once the certificate is expired or revoked, or in any case they are no more in its possession, the Applicant and the Organization shall be obliged to immediately, and permanently, remove the same certificate from the servers.

11. Fees.

11.1. The fees for the issuance of the Certificate are available at the registration offices and anyway known by the Applicant before the service request.

The Applicant is obliged to pay said fees according to the amount, timescale and modalities indicated in the Order or the Registration Request.

12. Revocation and suspension of the certificate.

12.1. The requirements, procedures and timeframes for the revocation or suspension of the signature certificate are set out in the Certificate Policy and Practice Statement ICERT-INDI-MOWS in compliance with the law in force.

12.2. The Applicant/Organization and the End User using the Certificate are obliged to verify the validity, suspension and revocation of the Certificate in use according to the modalities provided by the Certificate Policy and Practice Statement.

The Applicant/Organization undertakes to prevent the access to the sites any time the certificate is revoked or threatened.

13. Certifier's liability.

13.1. Without prejudice to the provisions of these General Terms and Conditions, the Certifier's liability for the Service is ruled by the Certificate Policy and Practice Statement.

Except in the case of fraud or gross negligence, the Certifier undertakes no liability for the direct and indirect



General terms and conditions WEB sites Authentication Certificates

damages suffered from the Owners and/or third parties as a result of the use or non-use of the WEB authentication certificates issued in accordance with the provisions of these General Terms and Conditions and the Certificate Policy and Practice Statement ICERT-INDI-MOWS.

InfoCert is not liable for any direct and/or indirect damages also arising alternatively out of the i) loss, ii) improper storage, iii) improper use by the Applicant/Organization of the identification and authentication device and/or his/her non-compliance with the above.

Furthermore, the Certifier, since the Contract formation and also during its execution, shall not be liable for any damages and/or delays due to the malfunction or failure of the computer system and the Internet network.

Save the case of fraud or gross negligence, InfoCert shall not bear any burdens or liabilities for direct or indirect damages of any nature and extent that the Applicant and/or third parties may incur into, due to alterations or interventions on the Service or on the devices carried out by third parties that have not been authorized by InfoCert.

13.2. Save the cases of exemption from liability as to art. 13.1, in any event of failing to comply with its obligations by the Certifier, the Applicant or the Organization shall be entitled to obtain, as compensation for all the damages possibly suffered, exclusively the reimbursement of the fees paid for the service connected with the service missed availability.

The reimbursement may not be requested if the missed availability is attributable to the telecommunications manager or to fortuitous event, force majeure or causes anyway not attributable to InfoCert, such as, by way of example, strikes, riots, earthquakes, acts of terrorism, turmoils, deliberate sabotage, chemical and/or bacteriological accidents, war, floods, measures of the competent authorities or the inadequacy of facilities and hardware and/or software equipment used by the Applicant.

14. Termination of the relationship.

14.1. Pursuant to Art. 1456 Civil Code, the Contract shall terminate by law with the simultaneous interruption of the Service and revocation of the issued certificate, in case the Applicant and/or the Organization fail to comply with the provisions contained in the clauses referred to in art. 3 (Organization's and Applicant's liability); art. 4.6 (Intellectual Property); art. 8 (Applicant's/Organization's obligations), art. 11 (Fees); as well as what provided in the ICERT-INDI-MOWS

Certificate Policy and Practice Statement . Termination shall occur by law when the concerned party informs the other party by means of PEC or registered letter with return receipt about its intention to make use of this clause.

14.2. The Certifier is entitled to withdraw from this Contract at any time pursuant to Art. 1373 of the Civil Code with a 30 day notice, and, consequently, to revoke the certificate.

In any case of revocation of the contract, the Service shall no longer be provided and the Contract shall terminate its effects.

Pursuant to art. 1373, para. 2, Civil Code, it is unprejudiced he right to the fees accrued until the date the withdrawal takes effect.

14.3. In all cases where the Applicant or the organization fail (even partially) to comply with whatever obligation they have undertaken, the Certifier may suspend the provision of the Service, also through the suspension of the Certificate. In particular, in case of non-payment of Service fees, InfoCert shall in any case be entitled to terminate the Contract with the Applicant and/or the Organization and the Holder at any time, without notice and burden and shall consequently revoke any issued certificate.

14.4. In the event of withdrawal by the Applicant or the Organization, to be exercised with at least a 30 (thirty) day notice, the fees are anyway due and, if already paid, it is entirely withheld by InfoCert also as compensation for withdrawal. or of revocation of the certificate, the fees shall anyway be due and, if already paid, said fees shall be fully retained by InfoCert also as compensation for withdrawal.

14.5. In all cases of termination of the Contract, the effects of the Contract until termination shall be maintained. The Applicant and the Organization acknowledge that they shall no longer be able to make use of the Service should the Contract terminate for any cause whatsoever.

14.6. In any case of termination of the contractual relationship between InfoCert and the Applicant, also the contractual relationship between InfoCert and the Organization shall terminate, and viceversa.

*** **

