PDS

PKI Disclosure Statement

DOCUMENT CODE	ICERT-INDI-PDS
VERSION	3.2
DATE	21.09.2021

InfoCert
TINEXTA GROUP

CONTENTS

1. Introduction

This PKI-Disclosure-Statement (PDS) fulfils the publication requirement specified under European standard ETSI EN 319 411-1, regarding the certification service offered by Qualified Trust Service Provider InfoCert S.p.A., ("**InfoCert",** "**QTSP**" or "**CA**" hereinafter), and is intended to provide applicants for the service with technical information necessary for its use.

Regulation (EU) n° 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 and repealing Directive 1999/93/EC, is referred to hereinafter as the "**eIDAS Regulation**".

The present document accompanies the Terms and Conditions of service and constitutes an integral part of the InfoCert contract documentation.

The publication of this PDS does not replace the publication of the Certification Practice Statement (CPS), which provides more detailed information and is available on the InfoCert website at the following link:
https://www.firma.infocert.it/documentazione/.

2. Contacts

InfoCert S.p.A. – VAT reg n° 07945211006
Qualified Trust Service Provider
Piazza Sallustio, 9
00187 - Roma, Italy

Business offices
Piazza Luigi da Porto 3
35131 Padova, Italy

Phone: +39 06 836691 - Fax: +39 06 23328861
Digital Signature Call Center: see the link https://help.infocert.it/contatti/
Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it

Revocation of a digital signature certificate can be requested using the relative form published on the InfoCert website and sending it via certified e-mail (PEC), registered letter or fax, accompanied by a photocopy of a valid identity document. Revocation can also be requested at the competent registration office, in accordance with the procedure indicated in the Terms and Conditions of service. InfoCert reserves the right to carry out additional checks on the identity of the applicant.

Suspension of a digital signature certificate can be requested directly online, on the InfoCert website, using the secret code assigned during the registration procedure.

3. Types of certificate, validation and use

InfoCert issues qualified certificates responding to Euro standard **ETSI EN 319 411** and other related standards, offered to the public (private businesses, public bodies, professionals, individuals, etc.) under the conditions published on the website of the QTSP or other Registration Authorities (RA).

The algorithm used for signing certificates can be chosen from the following:

• sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]

• ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]

• ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]

• ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

Signatures and certificates can be verified using the **Dike GoSign** App, downloadable free from the InfoCert website.

4. Reliance limits

InfoCert issues:

- **qualified certificates to natural persons** for advanced or qualified electronic signature;
- **qualified certificates to legal persons for electronic seal**, including for PSD2 compliance

InfoCert also provides remote electronic signature services on Qualified Electronic Signature Creation Devices (QSCDs), generating and managing keys and certificates for the signatory.

Details and policy statements are given in the Certificate Practice Statements, available at *https://www.firma.infocert.it/documentazione*.

The validity period of every certificate is stated in the selfsame certificate and can vary from one hour minimum to three years and three months maximum.

It is forbidden to use the certificate outside of the limits and settings specified in the CPS and in contracts, and at all events in breach of the limits of usage and value (*key usage*, *extended key usage*, *user notice*) indicated in the certificate.

Event logs connected with the issue of certificates are preserved for at least 20 (twenty) years in the InfoCert data storage system, as required under current statutory regulations in Italy.

5. Obligations of the Subject

The **Subject** must abide by the clauses in the CPS and the Terms and Conditions of service, and in particular, must:

- read and understand the contract documentation and any additional informative documentation;
- follow the identification procedures adopted by the Certification Authority as described in the CPS;

- provide all information necessary for the purposes of identification, accompanied, where required, by the appropriate documentation;
- utilize the assigned pair of keys only for the purposes and in the ways allowed by the CPS;
- in signing the request for registration and certification, accept the contractual conditions regulating the provision of the service, as stated in analog or electronic forms prepared by the CA;
- inform the CA or RA promptly, as long as the certificate remains valid, up to the expiry date, of the following circumstances:
    - the Subject's signature device has been lost, stolen or damaged;
    - the Subject has lost sole control of his/her private key, for example as a result of the activation data (e.g. PIN) of the signature device being compromised;
    - certain items of information in the Subject's certificate are inexact or no longer valid;
- safeguard the secrecy of credentials necessary for the use of signature devices or services, neither communicating nor disclosing them to third parties, and maintaining sole control of them;
- desist immediately and definitively from using the key that has been compromised, except for the purpose of deciphering the selfsame key;
- ensure that the subject makes no further use of the private key in the event of the applicant being informed that the certificate of the subject has been revoked or that the CA has been compromised.

Responsibility for the procurement and utilization of an internet connection and of all the requisite tools (hardware and software) lies with the applicant.

6. Obligations of the Applicant if other than the Subject

The **Applicant**, if other than the Subject, must abide by the clauses in the CPS and the Terms and Conditions of service, and in particular, must:

- read and understand the contract documentation and any additional informative documentation;
- follow the identification procedures adopted by the QTSP;

- provide all information necessary for the purposes of identification, accompanied, where required, by the appropriate documentation;
- in signing the request for registration and certification, accept the contractual conditions regulating the provision of the service, as stated in analog or electronic forms prepared by the CA;
- identify and inform the TSP of the information technology procedure that will be used to send documents for submission to the remote signature procedure and to the activation of signature keys by the Subject;
- meet the costs of the remote signature service and, by way of specific deeds and procedures, indicate the Subjects to whom the certificates must be issued;
- indicate the preferred type of authentication system to be used for activation of the remote signature procedure;
- in the event of a decision to revoke or suspend the certificate of the Subject, sign the relative form provided by the QTSP for the purpose of requesting revocation or suspension;
- inform the Subject of obligations deriving from the certificate, provide correct and truthful information as to the identity of the Subject, and abide by the processes and indications of the QTSP and/or RA;
- in the event that the Subject is a legal person, provide the QTSP with the following information:
    - Surname and first name of the Applicant;
    - TIN or similar code or number identifying the Applicant (in Italy, 'codice fiscale');
    - Details of the identity document presented for the purpose of identifying the Applicant, namely type, number, issuing authority and date of issue;
    - e-mail address for communications sent from QTSP to Applicant;
    - name of the Subject as legal person;
    - VAT code or NTR (VAT reg. number or Company Register number for Italian Subjects);
- when keys are generated in a device belonging to the Subject, the Applicant must forward a specific request in PKCS #10 format, signed by the selfsame Applicant. In the event that the signature device is not provided by the QTSP, the Applicant must make certain that the device is in compliance with current regulations, presenting the appropriate documentation and remaining subject to periodic audits conducted by the QTSP.

7. Validity status of certificates

All parties relying on information contained in certificates must check that the certificates are not suspended or revoked.

Information on the status of certificates is available by consulting the list of revoked certificates (CRL) published by the CA at the URL indicated on the certificate or through the OCSP service. Certificate validity checks can be performed using the Dike GoSign product, which can be downloaded free of charge from the InfoCert website.

8. Limited guarantee and absence/limitation of liability

Qualified certificates are provided in accordance with this document and with the Terms and Conditions of service. All necessary technical details are specified in the CPS.

InfoCert assumes liability for damages that may be caused directly to any natural or legal person, wilfully or through negligence, as a result of failure to fulfil the obligations set out in Regulation (EU) n° 910/2014 of the European Parliament and of the Council of 23 July 2014 and of failure on the part of InfoCert to adopt all appropriate measures for the avoidance of such damages.

In a situation as described in the foregoing paragraph, the Applicant or the Subject will be entitled to claim a sum by way of compensation for damages suffered as a direct result of the above noted wilful or negligent conduct, which cannot at all events exceed the maximum amounts prescribed, per single loss and in any one year, under article 3 section 7 of the Regulation attached to AgID Resolution n° 185/2017.

A reimbursement cannot be claimed in the event that the loss is attributable to improper use of the certification service or to the telecommunications network operator, or to a situation deriving from a chance event, from force majeure or from causes not in any way attributable to InfoCert.

9. Applicable agreements, policies and Certificate Practice Statements

Agreements and conditions applicable to the QTSP service, and Certification Practice Statements, are published on the InfoCert website at the following link https://firma.infocert.it/documentazione.

10. Privacy policy

Unless expressly agreed otherwise, information concerning the Subject and the Applicant that comes into the possession of the CA in the course of its typical activities is deemed confidential and not publishable, except where intended explicitly for public disclosure: *public key, certificate (if requested by the Subject), dates of revocation and suspension of the certificate*.

In particular, items of personal data are processed by InfoCert in accordance with Legislative Decree (Italy) n° 196 dated 30 June 2003 and with Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data, binding in its entirety since 25 May 2018.

11. Refund policies

Should a decision be taken to withdraw from the contract, the Subject is required to inform the QTSP, before the expiry of the withdrawal period, in an explicit statement sent by certified e-mail (PEC) to *richieste.rimborso@legalmail.it* or by registered letter with advice of receipt to InfoCert S.p.A. - Direzione Generale e Amministrativa - Via Marco e Marcelliano, 45 00147 Roma. To this end, in the interests of convenience, the Subject can use the standard withdrawal form available on the InfoCert website at the following link: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

Whilst the costs of returning the signature device, if any, shall be borne by the Subject and/or the Applicant, the QTSP will duly refund payments that have already been remitted. The refund in question will be paid into the current account used for the initial transaction, unless the Subject has expressly indicated different bank details for the

payment; whichever the case, the payment of the refund will be ordered and remitted at no cost to the Subject.

12. Applicable law governing complaints and resolution of disputes

The provision of certification and time stamp services is regulated by the current laws of Italy. For matters not expressly covered in the present document, reference is made to the Italian Civil Code and to other applicable laws.
All disputes deriving from or connected with the interpretation and performance of the present agreement shall be submitted to the exclusive jurisdiction of the competent law courts in Rome, unless stated otherwise in the Terms and Conditions of this same agreement.

Should the client be a consumer, any disputes relating to the agreement concluded by the consumer shall be submitted to the mandatory local jurisdiction of the judge officiating in the district where the consumer resides or is domiciled.

13. Archives, licences and trademarks, audits

The CA does not check on the use of registered trademarks, but can refuse to generate a certificate or may seek the revocation of an existing certificate if involved in a dispute.

Verification of compliance with Regulation (EU) n° 910/2014 of 23/07/2014 in standards ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, has been carried out by CSQA Certificazioni S.r.l, employing the eIDAS evaluation method defined by ACCREDIA according to standards ETSI EN 319 403 and ISO/IEC 17065: 2012.

The compliance report was presented by InfoCert to Agenzia per l'Italia Digitale - AgID, which confirmed the inclusion of InfoCert in the Trusted List of Qualified Trust Service Providers as required by Regulation (EU) n° 910/2014 of 23/07/2014.

The Trusted List of Certification Authorities in Italy can be found on the AGID website at *https://eidas.agid.gov.it/TL/TSL-IT.xml*