Policy and Practice Statement

Electronic Signature

Certificate Practice Statement

DOCUMENT CODE ICERT-INDI-FD

VERSION 3.2

DATE 18/07/2023

INFOCERT

TINEXTA GROUP

This page has been left
blank intentionally

1 Contents

1.1 Introduction to this document

1.1.1 Changes introduced since the previous edition:

Version/Release No.:	3.2	**Version/Release date:**	18 July 2023
Description of changes:	New InfoCert logo		
Reasons:	Rebranding		

Version/Release No.:	3.1	**Release Date:**	28/09/2021
Description of changes:	Contact update		
Reasons:			

Version/Release No.:	3.0	**Release Date:**	27/09/2019
Description of changes:	Complete revision of the manual. CodeSign references added Added references to Server Authentication and Application Ports		
Reasons:			

Version/Release No.:	2.0	**Version/Release date:**	15/02/2016
Description of changes:	Complete revision of the manual		
Reasons:			

Version/Release No.:	1.0	**Version/Release date:**	11 July 2008
Description of changes:	First release		
Reasons:			

The purpose of this manual is to describe the rules and operational procedures adopted by InfoCert's digital certification authority for the provision of the public key certification service for an asymmetric key pair, used for

- authentication in web-based applications (Client, Non-Trusted Server, Application Ports)
- signing and encrypting email
- code signing

The Certification Authority reserves the right to amend this document for technical reasons or due to changes in procedures arising either from statutory requirements or regulations, or to optimise the workflow.

Each new version of the manual supersedes and replaces previous versions, which nevertheless remain applicable to certificates issued during their period of validity and until their first expiry date.

This document is entitled "Electronic Signature Certificates –
Policy and Practice Statement' and is identified by the document code: ICERT-INDI-FD.

The document is associated with the Object Identifiers (OIDs) described below, which are referenced in the CertificatePolicy extension of the certificates, according to their intended use. The meaning of the OIDs is as follows:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Service-Policy and Practice Statement for "Electronic Signature" Certification	1.3.76.36.1.1.8
Policy and Practice Statement – Service for 'Code Signature' Certification	1.3.76.36.1.1.8.7
Policy and Practice Statement – Certification Certification "Authentication NoTrust Server"	1.3.76.36.1.1.8.8

The manual is published in electronic format on the Certification Authority's website at https://www.firma.InfoCert.it/documentazione/

1.2 Terms and definitions

- **Certification Authority:** the body that provides the Certification Service. For the purposes of this document, the Certification Authority is InfoCert S.p.A.
- **Client:** the software application, such as a web browser, used by the user connecting to a certified web server site, with which they wish to establish secure and protected communication.

- **Client or subscriber:** an entity, organisation or individual requesting the service
- **Private Key and Public Key – see [1]**
- **CSR:** Certificate Signing Request. See PKCS#10
- **Data for creating a signature – see [1]**
- **Data for verifying the signature – see [1]**
- **Digest:** the message's fingerprint following application of the SHA cryptographic algorithm.
- **Distinguished Name:** attributes of the certificate that identify it.
- **Electronic signature – see [1]**
- **Qualified electronic signature – see [1]**
- ***Digital signature* – see [1]**
- **PEM:** an acronym for Privacy Enhanced Mail, it is a standard for the secure transmission of email over the Internet, based on cryptographic techniques and digital signatures to protect the data being transmitted.
- **PKCS#10:** PKCS, which stands for Public Key Cryptography Standards, is a set of standards for public-key cryptography developed by RSA Laboratories: they define the syntax of digital certificates and encrypted messages; in particular, PKCS#10 defines the structure of the request for the certification of the public key of an asymmetric key pair.
- **PKCS#12:** Public Key Cryptography Standards number 12. PKCS#12 is the standard for the syntax of the exchange of personal information. It defines the encapsulation structure capable of containing both the private key and the certificate associated with it.
- **RSA:** Asymmetric encryption algorithm
- **Subscriber or Client:** An entity, organisation or individual requesting the service
- **SHA256:** the acronym SHA stands for Secure Hash Algorithm; it is a cryptographic function used to calculate a hash or digest. 256 refers to the number of bits in the resulting message
- **SSL:** Acronym for Secure Sockets Layer; this is the protocol that enables the establishment of authenticated and confidential communication between the communicating parties, the client and the server.
- **TLS:** An acronym for Transport Layer Security; this is the protocol that enables the establishment of authenticated and confidential communication between the communicating parties, the client and the server. It is the successor to the SSL protocol.
- **Certificate Subject:** the individual or entity that holds the Certificate.
- **User:** anyone who verifies the certificate.
- **Web server:** the software that enables information to be distributed over the Internet and receives requests from a web browser, returning the requested data.
- **X.509:** a standard defining the structure and format of public-key digital certificates. It also defines the characteristics of a Public Key Infrastructure (PKI).

1.3 References

Technical references

[1] Legislative Decree No. 82 of 7 March 2005 (*Official Gazette* No. 112 of 16 May 2005) – Digital Administration Code (hereinafter referred to as CAD)

1.3.1 Technical references

2. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

3. RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
4. Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (2012) | ISO/IEC 9594-8:2014

1.4 Person Responsible for the Policy and Practice Statement

InfoCert is responsible for the definition, publication and updating of this document. Any questions, complaints, comments or requests for clarification regarding this policy and practice statement should be addressed to the address and contact person indicated below:

InfoCert S.p.A.
Head of the Digital Certification Service
Piazza Luigi da Porto No. 3,
35131 Padua
Telephone: 06 836691
Fax: 06 23328861
Call Centre: see the link https://help.infocert.it/contatti/ Website:
https://www.firma.infocert.it
Email: firma.digitale@legalmail.it

2 Service features

2.1 Service Provider

The Electronic Signature certification service (hereinafter abbreviated to FD) is provided by the Certification Authority InfoCert S.p.A. in accordance with the procedures and conditions set out in this policy and practice statement.

The full details of the organisation acting as the Certification Authority (CA) are as follows:

Table 2

Company name	**InfoCert – Public Limited Company** **Company subject to management and coordination** **by Tinexta S.p.A.**
Registered office	Piazza Sallustio 9, 00187, Rome (RM)
Operational headquarters	45 Via Marco e Marcelliano, 00147, Rome (RM)
Legal representative	Danilo Cattaneo In his capacity as Managing Director
Telephone number	06 836691
Company Registration No.	Tax Code 07945211006

VAT number	07945211006
Website	https://www.infocert.it

2.2 Service description

The service described relates to the certification of the public key belonging to the asymmetric key pair (private key and public key) of the certificate, the purpose of which is:

- authentication to a web server,
- authentication to other applications,
- signing and encrypting emails,
- code authentication
- authentication of 'no trust' servers.
- application port authentication

2.3 Target users of the service

The certification service may be requested by any body, organisation or individual (referred to as the 'Client') that has entered into a contract with InfoCert for the provision of this service.
InfoCert will carry out the necessary checks in this regard when the service is requested and may refuse to issue the certificate in the event of falsehoods, inconsistencies or discrepancies in the information provided.

2.4 Service provider

The Certification Authority InfoCert is responsible for the service provided. The contact details for the person to contact regarding matters relating to the service are set out in paragraph 1.4.

3 Description of certificates

3.1 Certificate format and validity

Certificates issued by the Certification Authority comply with the X.509 v3 standard format [4].

The duration of the certificates is contractually agreed between InfoCert and the Customer: it may be for a period of between 1 and 5 years.

The obligations and rights of the Certification Authority and subjects arising from this policy and practice statement are understood to refer to the period of validity of the certificate issued.

4 Operational procedures

The procedure for certifying a subject consists of the following stages:

1. Request by the customer to InfoCert for the issue of the certificate(s)
2. Checking and validation of the application data by InfoCert
3. Registration of the data by InfoCert
4. Issue of the certificate
5. Delivery to the subscriber

4.1 Request for issuance

4.1.1 How to submit the application

Depending on the type and number of certificates requested, the certification application must be submitted to the CA via the various channels made available by the certification authority.

The main channels are:

- email address certificati.P12@InfoCert.it
- email address dedicated to the customer/type of certificate
- web-based application using credentials issued to the subscriber
- application requests based on the integration of specific services
- special issuances handled by a dedicated operator

The request must be authenticated by means of an advanced electronic signature, which is issued to the individuals designated by the Customer as their authorised representatives.
Other forms of authentication may be agreed with the client depending on the certificates requested, their number and the channel used.

The key pair may also be generated by the client, who must submit a CSR (Certificate Signing Request) in the format previously agreed with the certification authority.

In the case of multiple requests, the certification authority provides the templates to be used, specifying the mandatory fields according to the type of request being processed. Once completed in accordance with the aforementioned template, the files must be signed using an advanced electronic signature – which is issued in advance to the individuals designated by the Client as their authorised representatives – and sent to InfoCert.

4.1.2 Characteristics of the public key to be certified

For compatibility with CAB-Forum, the digest algorithm must be at least SHA256 and the key length must not be less than 2048 bits.
The asymmetric encryption algorithm to be used is RSA.

The key pair must be used in such a way as to prevent any compromise, loss, discovery, alteration or unauthorised use of the private key.

If the key pair is generated by the user, this must be done in such a way as to prevent any compromise, loss, discovery, alteration or unauthorised use of the private key.

The Certification Authority accepts no liability for failure to comply with the security conditions set out above.

4.2 Verification and validation of the application

The request is checked either by the relevant application services or by the designated InfoCert office. The origin, integrity and authorisations of the sender, as well as compliance with the contractual conditions, are verified. Should any information required to issue the certificate be missing, the designated officer will contact the subscriber for clarification.

InfoCert will not proceed with issuing the certificate if the data provided is found to be incorrect or incomplete based on the findings of the checks

During the verification process, the InfoCert representative may contact the subscriber to verify the accuracy of the information.

4.3 Issue of the certificate

Subject to the validity of the application, InfoCert will issue the certificate(s).

The Customer who has signed the contract is entitled to make available on their website the public key certificate corresponding to the private key with which the InfoCert Certification Authority signs electronic signature certificates. This certificate can also be downloaded from the Certification Authority's website under the heading 'Products and Services', by following the procedures indicated on the website itself. Downloading and subsequently adding this certificate to the list of 'trusted' CA certificates managed by users' clients and servers will enable the entire certification chain (application certificate and CA certificate) to be validated correctly, thereby allowing the identity of the communicating application to be verified.

4.4 Delivery to the subscriber

Once the certificate has been issued, the subscriber is notified and receives the requested documents via email at the address provided. They will receive two separate messages.

The first message, signed by the issuing authority, contains a ZIP file containing the generated PKCS#12 file and the entire certificate chain required for its correct validation.

The second message contains the passwords required to use the PKCS#12 file. Alternatively, if a telephone number has been provided, the password will be sent via SMS.

It is the end user's responsibility to ensure that their system or services are correctly configured for the use of these certificates.

If the request is made via the integration of application services, the certificate or the PKCS#12 file is delivered via the same channel.

5 Certificate lifecycle

The lifecycle of this type of certificate always depends in part on the intended end use and on the commercial agreements made at the time of issue. This chapter describes the general rules.

The revocation of a certificate renders all uses of the corresponding private key made after the time of revocation **invalid**.

Revoked certificates are included in a revocation list (CRL) signed by the Certification Authority. The revocation of a certificate takes effect from the time the list is published.

5.1 Revocation

The Certification Authority may revoke a certificate on its own initiative, at the customer's request or at the subject's request. Revocation must be requested if any of the following conditions arise:

- the private key has been compromised, or its confidentiality has been breached, or any event has occurred that has compromised the reliability of the private key itself;
- the subject is no longer able to use the certificate in their possession;
- the data contained in the certificate has changed;
- the relationship between the subject and the Certification Authority has ended;
- a breach of this policy and practice statement has been established;
- a court order has been issued.

5.1.1 Revocation at the Certificate Authority's initiative

The Certification Authority initiates a revocation request as follows:

1. the Certification Authority notifies the customer of its intention to revoke the certificate, stating the reason for revocation and the effective date;
2. the certificate revocation procedure is completed by adding the certificate to the list of revoked or suspended certificates.

5.1.2 Revocation at the Customer's initiative

The Customer submits the revocation request by email, signed with an advanced electronic signature by an authorised representative, stating the reason for the request, attaching the relevant documentation (if any), and specifying the 'serial number' and 'distinctive name' of the certificate.

Once the Certification Authority has verified the authenticity of the request, it proceeds with the revocation

5.1.3 Revocation at the subject's request

The subject must submit the revocation request by email, signed where applicable with an advanced electronic signature by an authorised representative, stating the reason for the request, attaching any relevant documentation, if available, and specifying the 'serial number' and 'distinctive name' of the certificate.

Once the Certification Authority has verified the authenticity of the request, it proceeds with the revocation

5.2 Publication and frequency of CRL issuance

Revoked or suspended certificates are included in a revocation list (CRL), signed by the Certification Authority, entered and published in the certificate directory (LDAP Directory) at the address specified in the 'CRL Distribution Point' extension contained within the certificate.
The CRL is published on a scheduled basis every day.
Users, i.e. subjects, are responsible for obtaining and consulting the CRL. The CRL is always issued in its entirety. Each entry in the CRL contains, in the relevant extension, the date and time of the revocation request.

5.3 Validity and Renewal

The certificate contains details of its validity period in *the* 'validity' field, with the attributes 'valid from' (*not before*) and 'valid *until' (not after).*

5.4 NOTE

The dates indicated in the above attributes are expressed in the format

year-month-day-hours-minutes-seconds-timezone
{YYYYMMDDHHMMSSZ}

in the UTCTime format specified by the reference standard.

Outside this date range, including hours, minutes and seconds, the certificate is to be considered invalid.

For electronic signature certificates, renewal consists of a new issue. The Certification Authority will inform the customer by email, with at least 30 days' notice, of the imminent expiry of the certificate and the need to apply for a new one to ensure continuity of service, in accordance with the procedures set out in the notification itself. Other procedures may be agreed with the customer

The new application will be made in the same way as the first.
The Certification Authority will proceed to generate a new certificate in the manner prescribed for the initial issue, subject to verification that the contractual conditions are met.

A private signature key for which the corresponding public key certificate has expired must no longer be used.

6 Fees and terms

The fees for the initial issue and renewal of certificates are set out in the service contract between InfoCert and the Customer.

Certificate revocations are free of charge.