Electronic Signature

Certificate Practice Statement (CPS)

Document code ICERT-INDI-FD

Ver 3.1

Date 28/09/2021

This page was intentionally left in white

1 Summary

Sommario

1.1 Introduction to the Document

1.1.1 Updates to previous version:

Release n°:	3.1	Data Release: 28/09/2021
Modification Description:	Change of contact information	
Motivation:		

Release n°:	3.0	**Data Release**:	27/09/2019
Modification Description:	Periodic review CodeSign feature Server Authentication feature Application ports feature		
Motivation:	New feature		

Release n°:	2.0	**Data Release**:	15/02/2016
Modification Description:	Complete review of the manual		
Motivation:			

Release n°:	1.0	**Data Release**:	11/07/2008
Modification description:	First issue		
Motivation:			

The present document has the aim to describe the operative procedure chosen for the digitalized certification structure of InfoCert ‘s to the supply of the certification service of the public key of a copy of asymmetric key, used:

- to authenticate the application in the web scope (client, server, application ports)
- to sign and encipher e-mail
- to sign the code

Il Certificatore si riserva di apportare variazioni al presente documento per esigenze tecniche o

per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.

Each new version of the manual cancels and replaces the previous versions, which however remains applicable to the certificates issued during their validity and until their first expiry.

The present document is called "*Certificati Firma Elettronica- Manuale Operativo"* characterised of document code: ICERT-INDI-FD.

The Object Identifiers (OIDs) of this documents are:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Certificate practice statement for "Electronic Signature"	1.3.76.36.1.1.8
Certificate practice statement for "Code signing"	1.3.76.36.1.1.8.7
Certificate practice statement for "Web Authentication"	1.3.76.36.1.1.8.8

The manual is published in electronic format in the Certifier Web, in the web address https://www.firma.InfoCert.it/documentation/

1.2 Terms and Definitions

- **Certifier:** Is the entity that provides the Certification Service. In order to comply with this document, Infocert S.p.A.
- **Client:** Is a Software app, for example a browser Web, used by the user which connects to the website server certified, which whom he wants to have a secure and protect communcation.
- **Applicant subject:** Entity, organization or person who apply to the service.
- **Private and Public Key:** numb. (1)
- **CSR:** Certificate Signing Request. Watch PKCS#10.
- **Data for the creation of a signature-**numb. (1)
- **Data for the verification of the signature-** numb. (1)
- **Digest:** fingerprint of the message after the application of the cryptographic algorithm.
- **Distinguished Name:** attribute of the certificate that identifies it.
- **Electronic Signature:** numb. (1)
- **Digital Signature:** numb. (1)
- **PEM:** acronym of Privacy Enhanced Mail, a standard that ruled the transmission of the secure post over the internet which are based on criptographyc technics and digital signature for the protection of the exchanged data.
- **PKS#10:** PKCS, acronim of Privacy Enhanced Mail, is a standard for the design of the criptography of the public key developed from the RSA Lab: define the syntax of the digital certificate and the cryptographic message, in particular the PKCS#10 define the structure of the request for the certification of the public key and the copy of an asymmetric key.
- **PKCS#12:** Public Key Cryptograhy Standards number 12. The PKCS#12 is the standard for the syntax of the transfer of personal data. Creates the structure of enveloping able to contain the private key or the public key.
- **RSA:** Asymmetric Cryptography Algorithm.

- **Requesting Subject or Client:** Entity, organization or person which requires the services.
- **SHA256:** the Acronym SHA for the Secure Hash Algorithm, is a cryptographic function used for calculating hash or digest. 256 is the number of bit of the resulting message.
- **SSL:** The Acronym to Secure Sockets Layer, is the protocol that consents to established a communication authenticated and reserved between the communicating parts, the client and server.
- **TSL:** Acronym of Transport Sockets Layer, it is the protocol that consents to establish a authenticated communication and reserved between the communicating parts, client and server. Successor of the protocol SSL.
- **Holder:** the subject/entity, holder of the certificate.
- **User:** Anyone that verifies the Certificate.
- **Web server:** is the software that allows the distribution of information over the Internet and receives the request from the browser Web returning the requested data.
- **X.509**: Standard for the definition of the digital certificate's format estructure for the Public Key. Defines, furthermore, the features of an infrastructure of Public Key (PKI).

1.3 References

References

1. Italian law: *Decreto legislativo 7 marzo 2005, n.82 (G.U. n112 del 16 maggio 2005)- Codice dell'amministrazione digitale (AD).*

1.3.1 Technical Reference

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 Responsible for this CPS

InfoCert is liable for the draft, publication and updating of this document.
Questions, complaints, comments and requests for clarification regarding this Certficate Practice Statement must be addressed to the address and person indicated below:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telefono: 06 836691
Fax: 06 23328861
Call Center: see the link https://help.infocert.it/contatti/

Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

2 Service Features

2.1 Supplier of the Services

The Electronic Signature certification service (hereinafter abbreviated as FD) is provided by the Certification Authority InfoCert S.p.A. according to the procedures and conditions established in this document.

InfoCert complete data in the table below

Company Name	InfoCert – Società per azioni Società soggetta a direzione e coordinamento di Tinexta S.p.A.
Registered Office	Piazza Sallustio n.9, 00187, Roma (RM)
Head Office	Via Marco e Marcelliano n.45, 00147, Roma (RM)
Legal Representative	Danilo Cattaneo In qualità di Amministratore Delegato
Phone	06 836691
National Trade Register Number	Codice Fiscale 07945211006
VAT	07945211006
Web Site	https://www.infocert.it

2.2 Description of the Services

The service described concerns to the certification of the public key belonging to the copy of the asymmetrical (Private key and public key) of the owner, whose use are:

- Web Server and Client authentication no trusted
- Application to application authentication
- Signature and encryption of e-mail
- Code Authentication
- Application ports authentication

2.3 Service Recipients

The certification service can be required by any Entity or Organization or Person (denominated **Client or Customer**) that undersigned an agreement with InfoCert for the supply of this service

2.4 Service Manager

The supplier of the service and the responsible is InfoCert. The information of the responsible is included in the point 1.4.

3 Description of the Certificates

3.1 Format and validity of the certificates

The certificate issued by InfoCert is compliant to the format standard X.509 v3 (4).

The duration is established via agreement between InfoCert and the Client: can be between 1 and 5 years.

The obligations and rights of the Certifying Body and of the holders that arise from this CPS are intended to refer to the validity period of the certificate issued.

4 Operational Procedures

The procedure for certifying a holder consists of the following steps:

1. Request to InfoCert by the customer to issue the certificate(s)
2. InfoCert audit and validation of request data
3. InfoCert logging of data
4. Certificate issuance
5. Delivery to the applicant

4.1 Issuance of the certificates

4.1.1 Method of transfer of the request

The request of certification, depending on the type of certificates requested and their number, has to be forwarded to the CA through various channels to the disposition of the certifier entity.

The principals are:

- Clause of e-mail certificati.P12@InfoCert.it
- Clause of e-mail dedicated to the client certificate.
- Application web based with credential released to the applicant.
- Request application based on the integration of specific service.
- Special issuance follows through dedicated operator.

The request must be authenticated by means of an advanced electronic signature, which is issued to the subjects that the Customer will have indicated as their referents. Other forms of authentication are agreed upon with the customer according to the certificates requested, the relative number and the channel used.

The key pair can also be generated at the customer who must send a CSR (Certificate Signing

Request) in the format previously agreed with the certifier.

In the case of the multiple request, the certifier supply indicating the obligatory fields respect to the typology of the request treated. Once complied through the layout, the file has to be sign with an Advance Electronic Signature, which is previously released to the subject that the client has indicated as own refer to and send to InfoCert.

4.1.2 Features of the public key subject of certification

For the compatibility with the CAB Forum, the Digest algorithm must be SHA256 and the length of the key it is not inferior to 2048 bit.

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, detection, modification or unauthorised use of the private key.

In the event that the key pair is generated by the user, the operation must be done in such a way as to prevent any compromise, loss, detection, modification or unauthorised use of the private key.

The certifier excludes any responsibility for non-compliance with the safety conditions set out above.

4.2 Control and validation of the request

The request is checked by the InfoCert office. The origin, integrity, authorisations of the sender and the existence of the contractual conditions are verified. If the necessary information to issue the certificate are missing, the office in charge will contact the applicant for clarification and additional information.

InfoCert will not proceed with the issuance of the certificate if the documents and information received is not correct or complete based on the findings deriving from the verifications.

During the verification, the InfoCert appointee may call the applicant back to verify the truthfulness of the information.

4.3 Issuance of the certificate

InfoCert issues the certificate(s) against the consistency of the request.

The Customer who signed the contract has the right to make available on his website the public key certificate correspondent to the private key with which the InfoCert Certification Body signs the electronic signature certificates.

This certificate can also be downloaded from the Certifier website under "Products and Services", following the procedures indicated on the site. The collection and subsequent insertion of this certificate in the list of "trusted" CA certificates managed by users' clients and servers will allow validation of the entire certification chain (application certificate and CA certificate), thus allowing

to verify the identity of the communicating application.

4.4 Delivery to the applicant

Once the certificate has been issued, the applicant is informed and receives what is requested by e-mail to the address provided. It will receive two separate messages.

The first message, signed by the issuer, contains a zip file with the generated PKCS#12 file and the whole certification chain for its correct validation.

The second message contains the passwords for using the PKCS#12 file. Alternatively, if you have communicated a phone number, the password is sent via SMS.

It remains the responsibility of the end user to provide the correct settings of their workstation or services for the use of these certificates.

In the event that the request is made by integrating application services, the certificate or PKCS# 12 is delivered through the same channel.

5 Life cycle of the certificates

The life cycle of this type of certificates in part always depends on the intended end use and the commercial agreements made during the issue phase. The general rules are described in this chapter.

The revocation of a certificate invalidates all uses of the corresponding private key made after the time of revocation.

Withdrawn certificates are entered in a revocation list (CRL) signed by the Certifier. The withdrawal of a certificate is effective from the moment the list is published.

5.1 Withdrawal

The Certification Authority can withdraw the certificate on its own initiative, at the customer's request or at the certification holder's request. The withdraw must be requested if the following conditions are met:

- the private key has been compromised, that is, the secrecy of the same has disappeared, or any event has occurred that has compromised the level of reliability of the private key itself;
- the certificate holder is no longer able to use the certificate in his possession;
- the data and information in the certificate have changed;
- the relationship between the owner and the Certifier has ended;
- a condition of non-compliance with this document has been ascertained;
- a measure has been issued by the Judicial Authority.

5.1.1 Withdrawal under request of the certifier

The Certifier activates a request for revocation in the following way:

1. the Certifier informs the customer of the intention to withdraw the certificate, providing the reason for the withdrawal and the effective date;

2. the certificate withdrawal procedure is completed with the insertion of the same in the list of revoked or suspended certificates.

5.1.2 Withdrawal under request of the customer

The customer forwards the withdrawal request by email, signed with an advanced electronic signature of an authorised contact person, providing the reason for the withdrawal request, attaching the relevant documentation, if any, and specifying the "serial number" and "distinctive name" of the certificate.

The Certifier, having verified the authenticity of the request, proceeds with the withdraw

5.1.3 Withdrawal under request of the certificate holder

The certificate holder/owner forwards the request for withdrawal by email, possibly signed with an advanced electronic signature of an authorised contact person, providing the reason for the request, attaching the relevant documentation, if any, and specifying the "serial number" and "distinctive name" of the certificate.

The Certifier, having verified the authenticity of the request, proceeds with the withdraw

5.2 Publication and issuance frequency of the CRL

The revoked or suspended certificates are included in a revocation list (CRL), signed by the Certification Authority, entered and published in the certificate register (LDAP Directory) at the address indicated in the "CRL Distribution Point" extension that are present in the certificate.

The CRL is published on a scheduled basis every day.

The acquisition and consultation of the CRL is the responsibility of the users, or owners. The CRL is always issued complete. Each element of the CRL list contains the date and time of the request for revocation in the appropriate extension.

5.3 Validity and Renewal

The certificate contains the indication of the 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-hour-minute-second-time zone in the UTC Time representation required by the reference standard.

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

For electronic signature certificates, the renewal consists of a new issue. The Certifier will inform the customer via e-mail, with at least 30 days' notice, of the imminent expiry of the certificate and the need to request a new one to guarantee the continuity of the service, in the manner indicated in the communication itself. other methods can be agreed with the customer.

The new request will be made in the same way as the first request.

The Certifier will proceed to the generation of a new certificate in the manner foreseen for the first certification issued, without prejudice to the verification of the existence of the contractual conditions.

The private signature key whose certificate of the relevant public key has expired, must no longer be used.

6 Rates and Conditions

The rates for the first issue and for the renewal of the certificates are established by the contract between InfoCert and the customer.

The withdrawal of the services is not charged.