Certificate policy
&
Certificate Practice Statement

DOCUMENT CODE	ICERT-INDI-FEA
VERSION	1.5
DATE	20/05/2022

CONTENTS

FIGURES

1 INTRODUCTION

1.1 Overview

A certificate links the public key with a set of information identifying the holder of the private key: this legal entity or natural person is the certificate's **Subject**. Other people use the certificate to find the public key that is distributed with the certificate, and to verify the electronic signature that is affixed or linked to a document. The certificate guarantees the link between the public key and the Subject. This link's reliability depends on a number of factors: the means used by the Certification Authority to issue the certificate, the security measures adopted, the obligations assumed by the Subject to protect the private key and the guarantees provided.

This Certificate Practice Statement is issued by InfoCert, a **Trust Service Provider** that provides advanced electronic signature and advanced electronic seal services in addition to trust services. This manual contains the policies and practices applied in the certificate identification and issue process, the security measures adopted, the obligations, guarantees and responsibilities, and generally, everything that makes a certificate reliable, in accordance with the legislation in force applicable to trust services, advanced electronic signatures and advanced electronic seals.

By publishing this Certificate Practice Statement and inserting references to it in the certificates, we can ensure users are able to assess the characteristics and reliability of the certification service and therefore the link between the key and the Subject.
This Certificate Practice Statement's content is based on the legislation in force on the date of its issue and transposes the recommendations of the "Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003.

1.2 Document title and identifier

This document is titled "InfoCert Trust Service Provider – Certificate Practice Statement" and is identified by the document code **ICERT-INDI-FEA**. Its version and release are indicated in the footer on each page.

The Object Identifiers (OID) described below are linked to the document, and are referenced in the certificates' CertificatePolicy extension, depending on their intended use. The OID identify:

The Object IDentifier (OID) identifying InfoCert is 1.3.76.36

Description	OID

Certificate policy statement for certificates issued to natural person	1.3.76.36.1.1.8.1 in accordance with NCP 0.4.0.2042.1.1
Certificate policy statement for certificates issued to natural person and keys on device (SSCD)	1.3.76.36.1.1.8.3 in accordance with NCP+ 0.4.0.2042.1.2
Certificate policy statement for certificates issued to natural person for automatic remote signature on device	1.3.76.36.1.1.8.5 in accordance with NCP+ 0.4.0.2042.1.2
Certificate policy statement for certificates issued to legal entity	1.3.76.36.1.1.8.2 in accordance with NCP 0.4.0.2042.1.1
Certificate policy statement for certificates issued to legal entity and keys on device (SSCD)	1.3.76.36.1.1.8.4 in accordance with NCP+ 0.4.0.2042.1.2
Certificate policy statement for certificates issued to legal entity for automatic remote signature on device	1.3.76.36.1.1.8.6 in accordance with NCP+ 0.4.0.2042.1.2
Certificate policy statement for certificates issued for testing purposes only	1.3.76.36.1.1.8.9 in accordance with NCP+ 0.4.0.2042.1.2

The certificate may include additional OIDs to indicate limitations of use. These OIDs are listed in section 4.5.3. The existence of limitations of use in no way modifies the rules established in the rest of the Certificate Practice Statement.

This document is published in electronic format in the Documentation section of the Trust Service Provider's website at http://www.firma.infocert.it.

1.3 Participants and responsibilities

1.3.1 Certification Authority (CA)

The **Certification Authority** is the trusted third party that issues the signature certificates, signing them with its own private key, which is called the CA key or the root key.

InfoCert is the Certification Authority (**CA**) that issues, publishes and revokes certificates, in accordance with the technical rules issued by the Supervisory Authority,

with the eIDAS Regulation [1] and with the Digital Administration Code [2].

Complete information regarding the CA is as follows:

Company name	InfoCert S.p.A. Company managed and coordinated by Tinexta S.p.A.
Registered office	Piazza Sallustio 9, 00187 Rome (RM)
Operating headquarters	Via Marco e Marcelliano 45, 00147 Rome (RM)
Legal representative	Danilo Cattaneo In his capacity as Chief Executive Officer
Phone number	+39 06836691
Corporate register number	Tax number 07945211006
VAT number	07945211006
Website	https://www.infocert.it

1.3.2 Registration Authority (RA)

Registration Authorities are subjects to which the CA has assigned a specific mandate to perform one or more of its registration processes, such as:

- identification of the Subject or Applicant
- registration of the Subject's data
- forwarding of the Subject's data to the CA's systems
- collection of the certification request
- distribution and/or initialisation of the signature device, where applicable
- activation of the certification procedure for the public key
- support for the Subject, Applicant and CA for certificate renewals, revocations or suspensions

In short, the Registration Authority serves as an interface between the Certification Authority and the Subject or Applicant, in accordance with the agreements between

them.

1.3.2.1 Registration Officer (RO)

The Registration Authority can appoint natural persons or legal entities to perform Subject identification procedures. **Registration Officers** follow the instructions provided by the RA, to which they report, and are responsible for ensuring the procedures are followed correctly.

1.3.3 Subject

The Subject is the natural person or legal entity who holds the certificate containing essential identifying data.

1.3.4 User

The User is the subject who receives an electronic document that is signed using the Subject's digital certificate, and who relies on the validity of the certificate (and/or on the advanced signature on it) to determine whether the document is accurate and valid in the contexts in which it is used.

1.3.5 Applicant

The Applicant is the natural person or legal entity who asks the CA to issue digital certificates for a Subject. The Applicant may sometimes bear the costs of the digital certificate and may have the power to suspend or revoke the certificates. When present, the RA may also assume this role.

The following cases are possible:

- The Applicant can be the Subject if the Subject is a natural person.
- The Applicant can be the natural person having the authority to request a certificate for a legal entity.
- The Applicant can be the legal entity requesting the certificate for natural persons connected to it through commercial relationships or within organisations.

If not stated otherwise in contractual documents, the Applicant is considered to be the Subject.

1.3.6 Authorities

1.3.6.1 Agenzia per l'Italia Digitale (AgID)

The Agenzia per l'Italia Digitale is the Italian supervisory body for trust service providers, pursuant to Article 17 of the eIDAS Regulation. The AgID oversees both qualified and unqualified certification trust service providers established in Italy, ensuring they comply with the requirements laid down in the Regulation

1.3.6.2 Conformity Assessment Body (CAB)

The conformity assessment body is accredited under the eIDAS Regulation and is authorised to verify qualified trust service provider compliance with applicable legislation and standards for the qualified and unqualified services it provides.

1.4 Certificate use

1.4.1 Authorised uses

The certificates issued by the CA InfoCert, as explained in this Certificate Practice Statement, are certificates for advanced electronic signatures or advanced electronic seals pursuant to the Digital Administration Code and Article 26 or Article 36 of the eIDAS Regulation.

The certificate issued by the CA is used to verify the advanced electronic signature or electronic seal of the Subject to whom the certificate belongs.

1.4.2 Unauthorised uses

The certificate may not be used outside of the limits and contexts specified in the Certificate Practice Statement and in the contracts, in violation of the limitations of use and value (key usage, extended key usage, user notice) indicated in the certificate.

1.5 Administration of the Certificate Practice Statement

1.5.1 Administrator of the Certificate Practice Statement

1.5.2 Contacts

InfoCert is responsible for defining, publishing and updating this document. Any questions, complaints, comments and requests for clarification regarding this Certificate Practice Statement must be sent to:

Infocert S.p.A.
Digital Certification Department Manager
Piazza Luigi da Porto 3
35131 Padua, Italy
Telephone: +39 06836691
Fax: +39 062 332 8861
Digital Signature Call Centre: https://help.infocert.it/contatti/
Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

The Subject or the Applicant may request a copy of the documentation related to them by completing and sending the form available at www.firma.infocert.it as indicated on the website. The documentation will be sent in electronic format to the email address

provided in the form.

1.5.3 Persons responsible for approving the Certificate Practice Statement

This Certificate Practice Statement is verified by the Security and Policies Manager, Privacy Manager, Certification Service Manager, Legal Office and the Consultancy Area, and is approved by company management.

1.5.4 Approval procedure

This manual is drafted and approved in accordance with the procedures required by the Company's ISO 9001:2015 Quality Management System.

At least once each year, the Trust Service Provider verifies that the Certificate Practice Statement conforms to the company's certification delivery service process.

1.6 Definitions and acronyms

1.6.1 Definitions

The following definitions are used in this document. For terms defined by the eIDAS Regulation [1] and by the Digital Administration Code [2], please see the definitions set out therein.

Term	Definition
Self certification	Declaration to the CA that is made by the subject who will become the Subject of the digital certificate, certifying the truthfulness of their personal conditions, facts and qualities, and assuming all responsibilities required by law.
Conformity Assessment Body (CAB)	Body accredited under the eIDAS Regulation as being competent to assess the conformity of the qualified trust service provider and of the qualified trust services it provides. The CAB drafts the CAR.
Conformity Assessment Report (CAR)	The report by which the CAB confirms that the qualified trust service provider and its trust services comply with the Regulation (see eIDAS [1]).
Card Management System (CMS)	Tool used to authenticate, identify, collect and store the Subjects' or Applicants' data.
Electronic signature certificate	An electronic certificate linking an electronic signature's validation data to a natural person and

	confirming at least that person's name or pseudonym (see eIDAS [1])
Qualified electronic signature certificate	An electronic signature certificate issued by a qualified trust service provider and complying with the requirements set out in Annex I of the eIDAS Regulation (see eIDAS [1])
Certification key or root key	Pair of encryption keys used by the CA to sign certificates and certificate revocation lists.
Private key	The key in the pair of asymmetric keys that is used by the Subject to affix the electronic signature on the electronic document.
Public key	The key in the pair of asymmetric keys that is intended to be made public to verify the electronic signature that the Subject affixes on the electronic document.
Emergency request code (ERC)	Security code delivered to the Subject to request suspension of a certificate on the TSP's portals.
Validation	The signature validity verification and confirmation process (see eIDAS [1])
Validation data	Data used to validate an electronic signature (see eIDAS [1])
Personal identification data	A set of data establishing the identity of a natural person or legal entity, or of a natural person representing a legal entity (see eIDAS [1])
Electronic signature creation data	The unique data used by the Signatory to create an electronic signature (see eIDAS [1])
Electronic signature creation device	Configured software or hardware used to create an electronic signature (see eIDAS [1])
Qualified electronic signature creation device (SSCD – Secure System Creation Device or QSCD)	An electronic signature creation device that meets the requirements of Annex II of the eIDAS Regulation (see eIDAS [1]). The letter Q indicates that the device is qualified.
Electronic document	Any content stored in electronic format, particularly text or sound, visual or audiovisual recordings (see eIDAS [1])

Automatic signature	A specific electronic signature process performed with the authorisation of the signatory who retains exclusive control over their signature keys, in the absence of their strict and continuous supervision.
Digital signature	A specific type of advanced electronic signature based on a qualified certificate and a system of encryption keys, one public and one private, that are connected to each other, in which the Subject uses the private key and the recipient uses the public key to indicate and verify the origin and integrity of an electronic document or a set of electronic documents (see CAD [2])
Electronic signature	Data in electronic format that are connected or linked by a logical association with other electronic data that the signatory uses for signing (see eIDAS [1])
Advanced electronic signature	An electronic signature that meets the requirements of Article 26 of the eIDAS Regulation (see eIDAS [1])
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device and that is based on a qualified electronic signature certificate (see eIDAS [1])
Signatory	A natural person who creates an electronic signature (see eIDAS [1])
Control log	The control log contains all automatically or manually saved events required by the Technical Rules [5].
Electronic identification	The process using electronic personal identification data representing a single natural person or legal entity, or a single natural person representing a legal entity (see eIDAS [1])
Certificate revocation list (CRL)	A list of certificates that have been “invalidated” before their normal expiry. The operation is called “revocation” if it is permanent, and suspension if it is temporary. When a certificate is revoked or suspended, its serial number is added to the CRL,

	which is then published in the directory.
Certificate Practice Statement	The Certificate Practice Statement defines the procedures that the CA applies in providing the service. The Manual is drafted in accordance with the guidelines issued by the Supervisory Authority and the international literature.
Means of electronic identification	Hardware and/or software containing personal identification data and used to authenticate an on-line service (see eIDAS [1])
Online Certificate Status Protocol (OCSP)	Protocol defined by the IETF in RFC 6960 that allows applications to verify the certificate's validity more quickly and precisely than the CRL, with which it shares data.
One-Time Password (OTP)	A One-Time Password is a password that is valid for one transaction only. The OTP is generated and sent to the Subject immediately before the Subject affixes the electronic signature. It can be based on hardware devices or software processes.
Party relying on certification	A natural person or legal entity that relies on electronic identification or a trust service (see eIDAS [1])
Trust service provider	A natural person or legal entity providing one or more trust services, either as a qualified trust service provider or as an unqualified trust provider (see eIDAS [1])
Qualified trust service provider	A trust service provider providing one or more qualified trust services and to which the supervisory body assigns the status of qualified trust service provider (see eIDAS [1])
Product	Hardware or software or their components used to provide trust services (see eIDAS [1])
Public officer	Subject who is authorised under the law to certify the identity of natural persons in the performance of their duties.
Directory	The Directory is an archive that contains: all certificates issued by the CA for which the

	Subject has requested publication the Certificate Revocation List (CRL)
Certificate revocation or suspension	The operation by which the CA cancels the certificate prior to its normal expiry.
Role	Generally, the Subject's professional title and/or authorisation, or any proxy to represent natural persons or private or public entities, or membership in said entities and the exercise of public office.
Trust service	An electronic service generally provided in exchange for payment and consisting in the: creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery service and certificates for such services; or creation, verification and validation of certificates for website authentication; or Storage of signatures, seals or electronic certificates for such services (see eIDAS [1])
Qualified trust service	A trust service that meets the requirements set out in the eIDAS Regulation (see eIDAS [1])
Coordinated Universal Time	Keeps time to within one second as defined in ITU-R Recommendation TF.460-5.
Electronic time stamp	Data in electronic format that link other data in electronic format to a specific date and time to prove that the latter data existed at that time (see eIDAS [1])
Qualified electronic time stamp	An electronic time stamp that meets the requirements of Article 42 of the eIDAS Regulation (see eIDAS [1])
Webcam	Small video camera used to transmit images in streaming via Internet and to take photographs. It may be connected to a PC or integrated in mobile devices and used for video chats or video conferences.

1.6.2 Acronyms and abbreviations

Acronym	
AgID	Agenzia per l'Italia Digitale: Italy's supervisory authority for trust service providers
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Digital Administration Code
CAR	Conformity Assessment Report
CC	Common Criteria
CIE	Electronic identity card
CMS	Card Management System
CNS – TS-CNS	National Services Card Health Card-National Services Card
CRL	Certificate Revocation List;
DMZ	Demilitarized Zone
DN	Distinguished Name
EAL	Evaluation Assurance Level
eID	Electronic IDentity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: a secure device for creating signatures, with functions similar to those of a smart card but with superior memory and

	performance
http	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
RO	Registration Officer
ISO	International Organization for Standardization: founded in 1946, ISO is an international organisation composed of representatives from national standards organisations
ITU	International Telecommunication Union: founded in 1865, the ITU is the international organisation responsible for defining telecommunications standards
IUT	Holder unique identifier: a code associated with the Subject that identifies them uniquely to the CA; the Subject has a different code for each certificate
LDAP	Lightweight Directory Access Protocol: protocol used to access the certificates directory
LoA	Level of Assurance
NTR Code	National Trade Register Code
OID	Object IDentifier: a number sequence registered under the procedure indicated in standard ISO/IEC 6523 that identifies a specific object within a hierarchy
OTP	One-Time Password
Certified email	Certified E-mail
PIN	Personal Identification Number: code linked to a secure signature device used by the Subject to access the device's functions
PKCS	Public-Key Cryptography Standards

PKI	Public Key Infrastructure: set of technological resources, processes and means allowing trusted third parties to verify and/or guarantee the Subject's identity, and to link a public key to a subject
RA	Registration Authority
RFC	Request for Comments: document containing information or specifications regarding new computer research, innovations and methods, submitted by the writers for evaluation by the community
RSA	Derives from the initials of the algorithm's inventors: River, Shamir, Adleman
SGSI	Information security management system
SPID	Public digital identity system
SSCD – QSSCD	Secure Signature Creation Device: a device used to create an electronic signature Qualified Secure Signature Creation Device: a qualified device used to create an electronic signature
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value-Added Tax Code
X509	Standard ITU-T for PKI
X500	ITU-T standard for LDAP and directory services

2 PUBLICATION AND ARCHIVING

2.1 Archiving

Published certificates, CRL and Certificate Practice Statements are available 24/7.

2.2 Publication of certification information

2.2.1 Publication of the Certificate Practice Statement

This Certificate Practice Statement is available in electronic format on the Certification Authority's website (see § 1.5.2).

2.2.2 Publication of certificates

Certificates issued under this Certificate Practice Statement cannot be made public.

2.2.3 Publication of certificate revocation lists

Certificate revocation lists (CRLs) are published in the certificates directory that can be accessed using the LDAP protocol or the http protocol at the address indicated in the certificate's CRL Distribution Points attribute. They can be accessed via software provided by the CA and/or functions present in products available on the market that interpret the LDAP and/or HTTP protocol.

The CA may provide other means in addition to that indicated to consult the list of published certificates and their validity.

2.3 Publication period or frequency

2.3.1 Certificate Practice Statement publication frequency

The Certificate Practice Statement is published on the certification body's website each time significant modifications are made.

2.3.2 Certificate revocation list publication frequency

CRLs are published every hour.

2.4 Public archive access control

Information regarding published certificates, CRLs and the Certificate Practice Statements are published. The CA has not established any restriction to access for

queries and has updated all countermeasures to prevent unauthorised modifications/deletions.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Name

3.1.1 Name types

The subject in the certificate is identified by the Distinguished Name (DN) that must be entered and must comply with standard X500. Certificates are issued in accordance with ETSI standards and with the Prime Ministerial Decree.

3.1.2 The name must have a meaning

The attribute of the Distinguished Name (DN) certificate uniquely identifies the subject to whom the certificate is issued.

3.1.3 Applicant anonymity or pseudonym

Only for identification according to method 1_LiveID (see 3.2.3.1), the Subject may ask permission from the CA to use a pseudonym on the certificate instead of the Subject's real name. The CA keeps information on the Subject's true name for a certain number of years following the certificate's issue as established contractually.

3.1.4 Name type interpretation rules

InfoCert follows standard X500.

3.1.5 Name uniqueness

For a natural person, to guarantee unique identification of the Subject, the certificate must indicate the Subject's first and last name and a unique identifier:

- The tax code for Italian citizens
- TIN – Tax Identification Number for citizens of foreign countries; the TIN may be assigned by the authorities of the Subject's country of origin or of the country in which the organisation for which they work is established.

If no tax code or TIN is provided, an identification code taken from a valid identification document used for the identification procedures may be used.
For a legal entity, to guarantee unique identification of the subject, the certificate must indicate the organisation's name and a unique identifier:

- VAT number or corporate register number for Italian legal entities
- VAT codes (Value-Added Tax Code) or NTR (National Trade Register) for legal entities

3.1.6 Identification, authentication and role of trademarks

When a Subject and Applicant request a certificate from the CA, they guarantee that they will comply fully with national and international intellectual property laws.

The CA does not verify the use of trademarks, and can refuse to generate a certificate or may request the revocation of an existing certificate if it is involved in a dispute.

3.2 Initial identity validation

This chapter describes the procedures used to identify the Subject or Applicant when they request issuance of a certificate.

The identification procedure requires that the CA identify the Subject, including via the RA or one of its Officers, who verifies the Subject's identity using one of the procedures indicated in the Certificate Practice Statement.

3.2.1 Method for demonstrating possession of the private key

InfoCert establishes that the applicant controls or is in possession of the private key corresponding to the public key to be certified, verifying signature of the certificate request using the private key corresponding to the public key to be certified.

3.2.2 Authentication of the identity of organisations

N/A

3.2.3 Identification of natural persons

Without prejudice to the CA's responsibility, the Subject's identity may be ascertained by subjects authorised to perform identification, as follows:

Method	Subjects authorised to perform identification	Authentication tools used for identification
1 LiveID	• Certification Authority (CA) • Registration Authority (RA) • Registration Officer • Public officer • Employer identifying its own employees, contract staff, agents	N/A
2 AMLID	• Subjects with anti-money laundering obligations pursuant to laws transposing Directive 2005/60/EC of the	N/A

	European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and subsequent community implementing legislation •	
3 SignID	• Certification Authority (CA) • Registration Authority (RA) • Registration Officer	Qualified electronic signature issued by a Qualified Trust Service Provider
4 AutID	Certification Authority (CA) Registration Authority (RA) • Registration Officer	• Valid CNS or TS-CNS device • Valid CIE device • Valid SPID issued by a SPIC Digital Identity Manager • Valid eID issued by a Qualified Trust Service Provider • ID from other compliant electronic identification systems • Biometric data system
5 VideoID	Certification Authority (CA) Registration Authority (RA) • Registration Officer	N/A
6 SelfID	Certification Authority (CA) Registration Authority (RA) Registration Officer	N/A

3.2.3.1 Identification using method 1 – LiveID

Method 1 – **LiveID** requires an in-person meeting between the Subject, who must be of age of majority, and one of the subjects authorised to perform identification, who identifies the Subject via presentation of one or more original valid pieces of

identification[1]. The Subject must have their Tax Code, which may be requested by the subject authorised to perform identification. Subjects not having an Italian tax code must present the document containing their TIN[2] or a similar identification code, such as a social security number or general identification code. If the Subject has no identification code, the passport number may be used.

The CA considers as valid identification already performed by the employer for signature of the employment contract in accordance with the following methods of identification:

- identification by the employer to activate the agent's duties
- identification by the employer of retired former employees who continue to access company portals and/or premises for recreational purposes or to use goods and services under company agreements

The CA stores the registration data for LiveID identification in analogue or electronic format.

3.2.3.2 Identification using method 2 – AMLID

In **method 2 – AMLID**, the CA uses identification performed by one of the subjects responsible for Identification and Appropriate Verification, pursuant to the laws in force transposing EU Directive 2015/849, on prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and subsequent Member State implementing legislation.

With regard to the Italian context, the data used for identification are presented by the Subject pursuant to Legislative Decree 90/2017 as amended [6], under which clients are required to provide—under their sole responsibility—all necessary and up-to-date information allowing the Subjects bearing the responsibilities listed in the aforementioned law to perform their client identification duties. The subjects bearing these responsibilities obtain the data using autonomously defined procedures while respecting obligations under Legislative Decree 90/2017 as amended, i.e. procedures adopted under the anti-money laundering laws in force at the identification date (including prior to the date of this Manual).

This identification method requires a mandate from the CA to represent the subject bearing the responsibilities, who thereby acts as RA. The Subject's identifying data

[1] For Italy, these are the documents required by Presidential Decree 445/2000 as amended (Administrative Documentation Consolidation Act). For identification, subjects who are citizens of a country other than Italy must present the original of one of the following pieces of identification:

- passport
- Italian identity card (European citizens)

The CA reserves the right to accept identification documents issued by authorities of European Union Member States, based on objective analysis of the identity and security features used in the issue process by the issuing authorities.

[2] The Tax Identification Number is the national identification number assigned by European Union Member States to their citizens for identification in the national taxation system.

collected for identification are stored electronically or in analogue mode by the CA as required by law.

3.2.3.3 Identification using method 3 – SignID

In **method 3 – SignID**, InfoCert's CA uses identification performed by another CA who issues qualified certificates**.** The Subject already holds a valid certificate and uses it with InfoCert. In this case, registration data are stored only in electronic format.

3.2.3.4 Identification using method 4 – AUTID

In **method 4 – AutID**, the CA uses identification already performed by a public or private authority to issue:

- CNS (National Services Card), TS-CNS (Health Card-National Services Card) or CIE (Electronic Identity Card) in Italy
- Electronic Identity Card in a European country
- SPID Digital Identity Manager or another eID or eIDAS Identity Provider
- an existing electronic identification method that has not been notified and that has been issued by a public authority or private subject, provided it offers a guarantee of reliability equivalent to physical presence
- biometric identification system

The Subject must hold a secure device with a valid certificate, or an eIDAS digital identity, with which they sign in to the systems of the CA or RA who thereby ascertain their identity.
An identity from other compliant electronic identification systems whose use is regulated through the contract between the CA and the Applicant is considered consistent with this identification method.
Any biometric methods provided by the Applicant or the RA are considered valid authentication methods. These allow identification using biometric elements such as a handwritten signature, fingerprints, voice authentication, etc.
In these cases, registration data are stored only in electronic format.

3.2.3.5 Identification using method 5 – VideoID

In **method 5 – VideoID**, the Subject is required to have a device able to connect to the Internet (computer, smart phone, tablet, etc.), a web cam and a functioning audio system.
The Registration Officer verifies the Subject or Applicant's identity by comparing one or more valid pieces of identification bearing recent and recognisable photographs.
For security and fraud prevention reasons, the only documents accepted for this method are common identity documents (e.g. identity card, driving license or

passport)[3]. The Registration Officer may refuse to accept a document presented by the Subject or Applicant if its characteristics are insufficient to verify the document's validity. Registration data, composed of audio and video files, and electronic metadata, are stored in protected form.
The CA or RA may also use asynchronous video to identify clients, allowing the Subject or Applicant to send identification first, and then upload a video that the CA or RA verifies. For the video, the Subject is asked to follow instructions provided, not by an operator, but by a script or other computer tool. Then, CA or RA personnel verify the validity of the video and the congruity of the documents provided electronically.

3.2.3.6 Unattended asynchronous identification

In **method 6 – SelfID**, identification is done without the Registration Officer and Subject or Applicant actually being present during an audio-video session. In this method, the Subject performs the identification session alone, uploading their piece of identification and following the instructions to take a "video selfie", during which they perform a few movements as instructed by the procedure established by the CA. The CA uses a technology that provides a compatibility score between the Subject and the documents presented: if the compatibility score is insufficient, the process will not complete and the Subject will have to repeat identification. Optionally, a back-office may perform asynchronous verification and collect additional evidence to complete identification.

For security and fraud prevention reasons, the only documents accepted for this method are common identity documents (e.g. identity card, driving license or passport)[4].

3.2.4 Identification of legal entities

A certificate for a legal entity must be requested by a natural person who is identified using one of the methods above (see § 3.2.3).

The person must also present up-to-date documentation identifying the legal entity and documentation certifying the natural person's authority to make the request on the legal entity's behalf.

3.2.5 Unverified Subject or Applicant information

The Subject may have information about their position and/or authority added to the certificate.

[3] The CA reserves the right to accept other types of identification documents, i.e. documents issued by authorities of European Union Member States, based on analysis of the identity and security features used in the issue process by the issuing authorities.

[4] The CA reserves the right to accept other types of identification documents, i.e. documents issued by authorities of European Union Member States, based on analysis of the identity and security features used in the issue process by the issuing authorities.

If used in the SPID circuit, this information must be communicated by the Attribute Provider authorised for this type of certification.

3.2.6 Authority validation

The CA or RA verifies the requested information defined in section 4.2.1 for identification, and validates the request.

3.3 Identification and authentication for key and certificate renewal

3.3.1 Identification and authentication for key and certificate renewal

This section describes the procedures used to authenticate and identify the Subject for signature certificate renewal.

The certificate indicates the validity period in the “validity” field, with the attributes “not before” and “not after”. The certificate is considered invalid outside this period, including hours, minutes and seconds.

However, the Subject can renew the certificate before its expiry using the tools provided by the CA. The renewal request is signed using the private key corresponding to the public key contained in the certificate to be renewed. A certificate cannot be renewed once it has expired or been revoked; instead, a new one must be issued.

3.4 Identification and authentication for revocation or suspension requests

A certificate can be suspended or revoked on request from the Subject or Applicant (concerned third party if they have consented to being included in the Role) or on the CA’s initiative.

3.4.1 Request by the Subject

The Subject can request revocation or suspension by filling out and signing (including electronically) the form available on the CA’s website.

The suspension request can be made by filling out the online form; in this case, the Subject is authenticated using the emergency request code provided when the certificate was issued, or using another authentication system described in the contractual documentation provided at the time of registration.

If the request is made to the Registration Authority, the Subject signs in using the identification methods.

If the Subject is a legal entity, a legal representative or a proxy must make the suspension or revocation request.

3.4.2 Request by the Applicant

An Applicant requesting revocation or suspension of the Subject's certificate authenticates by signing the revocation or suspension request form provided by the CA. The request must be sent using one of the methods indicated in section 4.9.3.2 or 4.9.15.2. The CA reserves the right to require other means for forwarding the revocation or suspension request by the Applicant or the Concerned Third Party in specific agreements with them.

4 OPERATIONS

4.1 Requesting a certificate

4.1.1 Who can request a certificate

A certificate for a natural person can be requested by:

- the Subject, by
  - contacting the CA directly at www.firma.infocert.it or www.infocert.digital
  - contacting a Registration Authority
- The Applicant on behalf of the Subject, by
  - contacting the CA directly at www.firma.infocert.it or www.infocert.digital signing a commercial agreement with the CA
  - contacting a Registration Authority

A certificate for a legal entity can be requested by:

- The Applicant who represents the legal entity, by
  - contacting the CA directly at www.firma.infocert.it or www.infocert.digital or signing a commercial agreement with the CA
  - contacting a Registration Authority specifically authorised to issue these types of certificate.

4.1.2 Registration procedure and responsibilities

The registration process includes the Subject's request, generation of the pair of keys, certification request for the public key and contract signature, not necessarily in that order. During the process, the people involved have different responsibilities all of whom are required for success.

- The Subject is responsible for providing correct and true information on their identity, for reading carefully the materials provided by the CA, including via the RA, and for following the CA and/or RA's instructions in the certificate request process. When the Subject is a legal entity, these responsibilities fall on the legal representative or proxy requesting the certificate.
- When present, the Applicant is responsible for informing the Subject (on whose behalf they are requesting the certificate) of the obligations deriving from the certificate, for providing correct and true information on the Subject's identity, and for following the CA and/or RA's instructions.
- When present, the Registration Authority (including via the Registration Officer)

is responsible for clearly identifying the Subject and the Applicant, for informing the subjects of their obligations deriving from the certificate and for carefully following the processes established by the CA.
- The Certification Authority is responsible for the proper functioning of the entire signature system, for correctly managing the PKI and for properly storing the certificates unless otherwise agreed between the parties.

If the keys are generated by the Subject's device, the Applicant must also send the request in PKCS#10 format signed by the Applicant.

4.2 Making the request

To receive a signature certificate, the Subject and/or the Applicant must:

- read this Certificate Practice Statement, the contract documentation and any additional information
- follow the identification procedures adopted by the Certification Authority as described in section 3
- provide all information necessary for the purposes of identification, accompanied by appropriate documentation, where required
- in signing the request for registration and certification, accept the contractual conditions regulating the provision of the service, as stated in analogue or electronic forms prepared by the CA

4.2.1 Information to be provided by the Subject

4.2.1.1 Natural person

To request a signature certificate, the Subject or the Applicant requesting the natural person's certificate must provide the following information:

- last and first name
- date and place of birth
- tax code or similar identification code (TIN)
- residential address
- details of the identity document presented for identification, i.e., type, number, issuing authority and date of issue
- e-mail address for communications sent by the CA to the Subject
- cell phone number to which the OTP will be sent when OTP technology is used

Optionally, the Subject (or Applicant) can provide a different name by which they are commonly known, which will be entered in the SubjectDN commonName field in the certificate. If the Subject or Applicant does not provide another name, the Subject's first and last name will be entered in the commonName field.
If the natural person wants to certify their pair of keys, the applicant must also provide the request file in PKCS#10 format signed by the Applicant.

4.2.1.2 Legal entity

When requesting a certificate for a legal entity, the Applicant, who is the entity's legal representative or proxy, must provide the following information:

- Applicant's first and last name
- Applicant's tax code or similar identification code (TIN)
- 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 by the CA to the Applicant
- name of the legal entity that is the Subject
- VAT number or corporate register number for Italian Subjects, or VAT code or NTR for foreign Subjects

Optionally, the Applicant can provide a different name by which the legal entity is commonly known, which will be entered in the SubjectDN commonName field in the certificate.
If the legal entity wants to certify its pair of keys, the applicant must also provide the request file in PKCS#10 format signed by the Applicant.
The information is saved in the CA's archives (during the registration phase) and will be used to generate the certificate.

4.2.2 Identification and authentication functions

During the initial registration and receipt of the registration and certification request, the Subject or Applicant (the legal entity's legal representative) is given the security codes to activate the signature device or signature procedure (if remote), and to request certificate suspension (ERC or similar code, if provided by the contract). The security codes are provided in an unmarked envelope; electronic codes are transmitted inside encrypted files, or may already be in the Subject's possession.
The CA may ask the Subject or Applicant (the legal entity's legal representative) to choose their own signature PIN; in this case, the Subject or Applicant is responsible for remembering the PIN.

4.2.3 Certificate request approval or refusal

Following initial registration, the CA or RA can refuse to issue the signature certificate in the event of missing or incomplete information, based on the coherence and consistency of information provided, anti-fraud verifications, doubts regarding the Subject or Applicant's identity, etc.

4.2.4 Time permitted to prepare the certificate request

The time between the registration request and certificate issue depends on the request method chosen by the Subject (or Applicant) and on whether any more information is required or if the device needs to be physically delivered.

4.3 Issuing a certificate

4.3.1 CA's duties during certificate issue

4.3.1.1 Issuing the certificate on a signature device (smartcard or token)

The pair of encryption keys are generated by the RA directly on the secure signature devices, using the applications provided by the CA, following secure authentication.

The RA sends the public key certification request to the Certification Authority in PKCS#10 format signed electronically using the signature certificate for this purpose.

After verifying the validity of the signature on the PKCS#10 and the subject's right to make the request, the Certification Authority generates the certificate, which is sent to the device on a secure channel.

4.3.1.2 Issuing the certificate on a remote signature device (HSM)

The Subject or Applicant signs in to the services or applications provided by the RA.

The pair of encryption keys are generated on the HSM at the TSP's site; then the RA sends the public key certification request to the Certification Authority via a secure channel.

After verifying the validity of the signature on the PKCS#10 and the subject's right to make the request, the Certification Authority generates the certificate, which is saved on the HSM.

4.3.1.3 Issuing the certificate using a Card Management System

The pair of encryption keys are generated by the RA directly on the devices using an authenticated Card Management System. The system manages the encryption device's entire lifespan, sending the electronically signed public key certification request in PKCS#10 format on a secure channel.

After verifying the validity of the signature on the PKCS#10 and the subject's right to make the request, the Certification Authority generates the certificate, which is sent to the device on a secure channel.

4.3.1.4 Issuing the certificate to a legal entity

The pair of encryption keys are generated by the RA directly on the HSM. The RA sends the public key certification request in PKCS#10 format to the Certification Authority where the request is signed electronically using the signature certificate via an automated procedure specifically authorised for this purpose.

After verifying the validity of the signature on the PKCS#10 and the subject's right to make the request, the Certification Authority generates the certificate, which is saved on the HSM.

If the pair of keys are generated in the Subject's HSM, the Subject must send the signed

PKCS#10. After verifying the validity of the signature on the PKCS#10 and the subject's right to make the request, the Certification Authority generates the certificate, which is saved on the HSM.

4.3.2 Notifying Applicants of certificate issuance

When the certificate is issued on an encryption device, the Subject (or Applicant) requires no notification because the certificate is already present on the device given to them. In other cases, the Subject (or Applicant) will be notified at the email address they provided at the time of registration.

4.3.3 Activation

4.3.3.1 Activating the signature device (smartcard or token)

After receiving the device, the Subject uses the confidential activation codes and the software provided by the CA to activate the device. The Subject also chooses a signature PIN and is responsible for keeping it secure and confidential.

4.3.3.2 Activating the remote signature device (HSM)

To activate the remote signature device, the Subject (or Applicant for a legal entity) chooses the signature PIN and is responsible for keeping it secure and confidential. The PIN is confirmed by entry of the One-Time Password received via SMS or generated on the token or token app linked to the certificate.
In some cases, the remote signature can be activated using one or more components of an authentication system managed by the RA. In this case, the CA first verifies that the system's security requirements have been met, ensuring that the system guarantees only knowledge of the datum for the Subject to create the signature, including through regular audits. Responsibilities are defined contractually.

4.4 Accepting a certificate

4.4.1 Conduct implying certificate acceptance

N/A

4.4.2 Publication of the certificate by the Certification Authority

Upon completion of the certification procedure, the certificate is entered in the certificates directory and will not be made public.

4.4.3 Notifying other subjects of certificate publication

N/A

4.5 Using the keys and the certificate

4.5.1 Use of the private key and certificate by the Subject

The Subject must protect the signature device, if present, or the authentication tools for remote signature. The Subject must store authorisation information for the private key separate from the device. The Subject must guarantee protection of the confidentiality and storage of any emergency request codes required to suspend the certificate. The Subject must use the certificate only for the uses stipulated in the Certificate Practice Statement and in compliance with the national and international laws in force.

The Subject must not affix electronic signatures using private keys whose certificate has been revoked or suspended and must not affix electronic signatures using a certificate issued by a revoked CA.

4.5.2 Use of the public key and certificate by End Users

The End User must know the cases in which the certificate may be used as indicated in the Certificate Practice Statement and in the certificate itself. The End User must verify the certificate's validity before using the public key contained in it and must ensure that the certificate has not been suspended or revoked, by consulting the lists in the certificates directory. The End User must also verify the existence and the content of any limitations of use for the pair of keys, powers of representation and professional qualifications.

4.5.3 Limitations of use and value

The Subject or Applicant may ask the Certification Authority to add personalised limitations of use to the certificate. The CA will consider requests for other specific limitations of use based on their legality, technical nature and interoperability.

Advanced electronic signature certificates and advanced electronic seal certificates can be issued for testing purposes, with the following limitation of use:

- Use of the certificate is limited to signing documents for testing purposes. use of the certificate is limited to the signature of documents for testing purposes

4.6 Renewing a certificate

4.6.1 Reasons for renewal

Upon renewal, a new certificate is issued.

4.6.2 Who can request renewal

The Subject can request renewal of the certificate before its expiry only if it has not been revoked. The certificate cannot be renewed after the expiry date; instead, a new certificate must be requested.
The renewal procedure applies exclusively to certificates issued by InfoCert.
Certificates for automatic signature cannot be renewed; instead, a new one must be issued.
Certificates issued to a legal entity cannot be renewed; instead, a new one must be issued.

4.6.3 Certificate renewal request

Certificates are renewed via a service provided by the CA within the framework of the commercial and contractual relations established with the Subject and with the RA, if applicable.

4.7 Reissuing a certificate

N/A

4.8 Modifying a certificate

N/A

4.9 Revoking or suspending a certificate

When a certificate is revoked or suspended, it is rendered invalid before its normal expiry and any signatures affixed after publication of the revocation will not be valid. Revoked or suspended certificates are entered in a Certificate Revocation List (CRL) signed by the CA having issued them, which is published in the certificate directory on a regular basis. The CA may force entry in the CRL in specific circumstances. Revocation and suspension take effect when the list is published as attested by the registration date in the Certification Authority's control log.

4.9.1 Reasons for revocation

Revocation must be requested for the following reasons:

1. the private key has been compromised, or
    - the secure signature device containing the key has been lost
    - the key or its activation code (PIN) has been revealed, or, for remote signature certificates, the OTP device has been compromised or lost
    - an event compromising the key's reliability has occurred

2. the Subject can no longer use the secure signature device in their possession, e.g., due to device failure
3. the Subject's data contained in the certificate have changed, including those relating to the Role, which would render the data incorrect and/or untrue
4. the relationship between the Subject and the CA, or between the Applicant and the CA has been terminated
5. this Certificate Practice Statement has not been followed in a substantial way

4.9.2 Who can request revocation

The Subject can request revocation at any time and for any reason. The Applicant can also request certificate revocation for the reasons and in the manners stated in this Certificate Practice Statement. The CA can also revoke the certificate as a matter of right.

4.9.3 Revocation procedures

Revocation can be requested in different ways depending on the person requesting it.

4.9.3.1 Revocation requested by the Subject

The Subject is required to sign the revocation request using the form available on InfoCert's website, deliver it to the RA or send it directly to the CA by registered mail, certified e-mail or fax, attaching a copy of a valid identity document.

The CA verifies the request's authenticity, revokes the certificate and immediately notifies the Subject.

If the certificate being revoked contains information regarding the Subject's Role, the CA will report the revocation to any Concerned Third Party with whom specific agreements are in force. If the certificate being revoked indicates the Organisation, the CA will inform the Organisation of the revocation.

4.9.3.2 Revocation requested by the Applicant or the Concerned Third Party

The Applicant may request revocation of the Subject's certificate by completing the revocation form available on the CA's website and from the RA, providing the reason for the request, attaching any necessary documentation, and indicating the Subject's data included in the certificate that were communicated to the CA when the certificate was issued.

The CA verifies the request's authenticity, notifies the Subject via the method of communication established in the certificate request and revokes the certificate.

Agreements with the CA may include additional methods of revocation by the Applicant or Concerned Third Party.

4.9.3.3 Revocation by the Certification Authority

If necessary, the CA can revoke the certificate, informing the Subject in advance, providing the reason, date and time of the revocation.

If the certificate being revoked contains information regarding the Subject's Role, the CA will report the revocation to any Concerned Third Party with whom specific agreements are in force. If the certificate being revoked indicates the Organisation, the CA will inform the Organisation of the revocation.

4.9.4 Grace period for the revocation request

The CRL grace period is the time at which the current CRL expires and when the CA publishes the next CRL. To avoid inconveniences, this period is longer than the time needed by the CA to generate and publish a new CRL. In this way, the current CRL will remain valid at least until it is replaced by the new CRL.

4.9.5 Time permitted to prepare the revocation request

The request is processed within one hour, unless additional authenticity checks are required. The request is processed immediately if it is correctly authenticated, otherwise the certificate is suspended until additional authenticity checks can be done.

4.9.6 Requirements for revocation checks

N/A

4.9.7 CRL publication frequency

Revoked or suspended certificates are entered in a Certificate Revocation List (CRL) signed by the CA and published in the certificates directory. The CRL is published every hour (ordinary issue). In special circumstances, the CA can force an unscheduled issue of the CRL (immediate extraordinary issue) if a certificate is being revoked or suspended due to suspected compromised confidentiality of the private key (immediate revocation or suspension). The CRL is always issued in full. The CRL publication time is certified using the date provided by the InfoCert Time Stamping Authority and recorded in the control log. Every element in the CRL includes the revocation or suspension date and time in its extension. The CA reserves the right to publish other CRL or CRL subsets separately to lighten network loads. Users are responsible for acquiring and consulting the CRL. The CRL to be consulted for a specific certificate is indicated in the certificate in accordance with the laws in force.

4.9.8 CRL maximum latency

The waiting period between the revocation or suspension request and its completion through publication of the CRL is no more than one hour.

4.9.9 Online verification of certificate revocation status

In addition to publication of the CRL in LDAP and http directories, InfoCert also provides an OCSP service for certificate status verification. The service's URL is indicated in the certificate. This service is available 24/7.

4.9.10 Online verification service requirements

N/A

4.9.11 Other revocation forms

N/A

4.9.12 Specific rekey requirements in case of compromise

N/A

4.9.13 Reasons for suspensions

Suspension must be requested under the following conditions:

1. a revocation request has been made without it being possible to verify the authenticity of the request in a timely manner
2. the Subject, Applicant or Concerned Third Party, RA or CA have doubts regarding the certificate's validity
3. there are doubts regarding the OTP device's security
4. a temporary interruption of certificate validity is required

In these cases, suspension will be requested for the certificate, stating the duration. Upon expiry of that time period, the certificate will either be revoked or become valid again.

4.9.14 Who can request a suspension

The Subject can request a suspension at any time and for any reason. The Applicant can also request a suspension for the reasons and in the manners stated in this Certificate Practice Statement. The CA can also suspend the certificate as a matter of right.

4.9.15 How to request suspension

Suspension can be requested in different ways depending on the person requesting it. Suspensions are always limited in time. Suspension ends at 00:00:00 on the last day of the requested period.

4.9.15.1 Suspension requested by the Subject

The Subject must request suspension using one of the following methods:

1. using the suspension function available on the CA's website, providing the required data and using the emergency request code provided when the certificate was issued
2. using (where available) the suspension with OTP function on the website indicated in the contract documentation provided at Registration
3. calling the CA's call centre and providing the required information. If the Subject does not have an emergency request code and only if the suspension is requested for key compromise, the Call Centre will verify the number of the call received and then immediately suspend the certificate for ten calendar days until the Subject's written request can be received. If the CA does not receive the signed request by that time, it will reactivate the certificate through the Registration Authority, which requests the data necessary for necessary verifications and then asks the CA to suspend the certificate. The Subject is required to sign the suspension request and deliver it to the RA or send it directly to the CA by ordinary post, certified e-mail or fax, attaching a copy of a valid identity document.

4.9.15.2 Suspension requested by the Applicant or the Concerned Third Party

The Applicant may request suspension of the Subject's certificate by completing the revocation form available on the CA's website and from the RA, providing the reason for the request, attaching any necessary documentation, and indicating the Subject's data that were communicated to the CA when the certificate was issued.

The CA verifies the request's authenticity, notifies the Subject via the methods of communication established in the certificate request and suspends the certificate. Agreements with the CA may include additional methods of suspension by the Applicant or Concerned Third Party.

4.9.15.3 Suspension by the Certification Authority

Except in cases of emergency, the CA informs the Subject in advance that the certificate is to be suspended, providing the reason for the suspension and the start and end dates. In any case, the Subject is informed of these dates as soon as possible.
If the certificate being suspended contains information regarding the Subject's Role, the CA will report the suspension to any Concerned Third Party with whom specific agreements are in force. If the certificate being suspended indicates the Organisation, the CA will inform the organisation of the suspension.

4.9.16 Limitations to the suspension period

Upon expiry of the requested suspension period, the certificate's validity is restored

through removal of the certificate from the certificate revocation list (CRL). It is reactivated within 24 hours of the end of the suspension period. If the suspension end date coincides with the certificate's expiry date or follows it, suspension becomes revocation and takes effect on the first day of suspension.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status information is available via the CRL and the OCSP service. A revoked certificate's serial number remains in the CRL even after the end of the certificate's validity and at least until expiry of the CA certificate.
Certificate information provided by the OCSP service is updated according to the most recently published CRL.

4.10.2 Service availability

The OCSP service and the CRLs are available 24/7.

4.10.3 Optional characteristics

4.11 Cancellation of the CA's services

The Subject and/or the Applicant's relationship with the Certification Authority ends once the certificate expires or is revoked, except in specific cases defined contractually.

4.12 Filing with third parties and recovery of the key

N/A

5 SECURITY AND CONTROL MEASURES

InfoCert TSP has created a security system for its digital certification service computer system. The security system has three levels:

- a physical level guaranteeing the security of the environments in which the CA manages the service
- a procedural level, with strictly organisational aspects
- a logical level, with hardware and software technological measures addressing the problems and risks related to the type of service and the infrastructure used

This security system was created to avoid risks deriving from system, network and application malfunctions, hacking and data modification.

To request an excerpt from InfoCert's security policy, please write to infocert@legalmail.it.

5.1 Physical security

The measures adopted provide adequate security guarantees with regard to:

- building and construction characteristics
- active and passive intrusion detection systems
- physical access controls
- electric power and air conditioning
- fire protection
- flood protection
- magnetic media archiving
- magnetic media archiving sites

5.1.1 Structure location and construction

InfoCert's Data Centre is located at its operating headquarters in Padua. The Disaster Recovery site is located in Modena and is connected to the Data Centre via a dedicated connection with redundancy on two different 40 Gbit/s MPLS circuits that can be upgraded to 100 Gbit/s.

Both sites have rooms, protected with the highest levels of both physical and logical security, hosting the computer hardware constituting the core of the digital certification, time stamping, remote signature and automatic signature services.

For continuous services with RTO/RPO values close to zero, some components of the CA's services related to the publication of the CRL and the OCSP are hosted on AWS clouds, located in the Europe (Frankfurt) Region and the Europe (Ireland) Region,

respectively. To guarantee operational continuity for the CA "InfoCert Advanced Electronic Signature CA 4", an encrypted copy of the data is stored on AWS clouds in the Europe (Milan) Region.

AWS holds certificates of compliance under the following standards: ISO/IEC 27001:2013, 27017:2015, 27018:2019 and ISO/IEC 9001:2015.

Figure 1 - Location of the InfoCert Data Centre and of the Disaster Recovery site

5.1.2 Physical access

Access to the Data Centre is regulated by InfoCert's security procedures. Inside the Data Centre is a bunker area hosting the CA's system for which an additional security factor is required.

5.1.3 Electric and air conditioning system

Although it is not certified, InfoCert's Data Centre in Padua has the characteristics of a tier 3 Data Centre.

Its technical rooms have an electric power system designed to prevent failures and especially interruptions. The systems' power source uses the most modern technologies to increase reliability and guarantee redundancy of the functions most critical to the services.

The power supply infrastructure includes:

- uninterrupted power supply (UPS), with alternating current accumulators
- availability of alternating current (220-380V AC)
- cabinets with redundant power source and protected lines, sized for the agreed power draw
- emergency generators
- automatic system and generator, network and battery switching and synchronisation (STS)

Each technological cabinet installed at the Data Centre is equipped with two electric lines guaranteeing HA in the event of interruption of one of the two lines.

The technological cabinet is monitored remotely with constant power line status (on/off) and absorbed power checks (each line must not exceed 50% of the load).

The technical area is generally kept at a temperature of between 20° and 27° with relative humidity of between 30% and 60%. The systems are equipped with condenser coils with collection system and sealed condensate drain monitored by flood probes. The entire A/C system is slaved to emergency generators in case of power failure. Guaranteed cooling capacity per cabinet with maximum load of 10 kW and maximum 15 kW per pair of side-by-side cabinets.

5.1.4 Flood prevention and protection

The building is located in an area not subject to environmental risks due to proximity to “dangerous” installations. During building design, appropriate steps were taken to isolate potentially dangerous areas, such as those containing the generator and the central heating plant.
The area hosting the hardware is located on the ground floor above road level.

5.1.5 Fire prevention and protection

The Data Centre has a smoke detection system with NOTIFIER analogue system with optical sensors located in the environment and in the false ceiling, and air sampling sensors installed in the subfloor and in the air ducts.
The automatic fire detection system is connected to environmentally friendly NAFS125 and PF23 automatic gaseous fire suppression systems and, in certain rooms, with aerosol fire suppression systems.
In the event two detectors in the same area are triggered simultaneously, the extinction system is triggered for the affected area.
Each fire-prevention area is equipped with a dedicated extinction system.

Portable extinction means are also present, in accordance with the laws and regulations in force.
Primary air ducts slaved to the hardware rooms are equipped with fire dampers located at intersections of fire areas triggered by the automatic fire detection system.

5.1.6 Storage media

The solution used for the storage platform is NetApp systems (FAS 8060) for the NAS part. For the SAN part, an infrastructure is used for the data centre part based on Infinidat technologies with two F4000 and F6000 generation InfiniBox enclosures. For the CA, the infrastructure is based on Pure Storage technology.

5.1.7 Waste disposal

InfoCert is ISO 14001 certified for sustainable environmental management of its production cycle, including waste sorting and sustainable disposal. With regard to electronic waste, all media are erased using specific procedures or using certified sanitisation companies prior to disposal.

5.1.8 Off-site backup

Off-site data backup is done on the Disaster Recovery site, using an EMC Data Domain 4200, on which the primary Data Domain is the Padua site.

5.2 Procedural controls

5.2.1 Key roles

Key roles are played by persons having the necessary requisites of experience, professionalism and technical and legal skills, which are verified regularly at annual reviews.
The list of names of people in key roles was filed with the AgID at the time of first accreditation and is kept up to date with company organisational changes.

5.3 Personnel controls

5.3.1 Required qualifications, experience and authorisations

Once annual human resource planning has been completed, the Department/Organisational Structure Manager identifies the job profiles required. Then the search and selection process is initiated in collaboration with the selection manager.

5.3.2 Experience control procedures

Job candidates undergo the selection process with an initial background and motivation interview with the selection manager, followed by a second technical interview with the Department/Organisational Structure Manager to verify the skills claimed by the candidate. Other verification tools include exercises and tests.

5.3.3 Training requisites

In order to prevent any single person from compromising or altering overall system security or from performing unauthorised activities, system operational management is assigned to different people having separate and clearly defined duties. The person responsible for designing and providing the certification service is an InfoCert employee who was selected for their computer system design, creation and operational experience, and for their reliability and discretion. Regular training is provided to develop knowledge of the duties assigned. In particular, employees receive training to guarantee their necessary technical, organisational and procedural skills prior to assuming their duties.

5.3.4 Frequency of refresher courses

Training needs are assessed at the beginning of each year in order to define the training plan for the year. The analysis includes:

- meeting with Management to collect data regarding training needs required to meet company objectives
- interview with Managers to identify specific training needs in their area
- presentation of the collected data to Company Management for approval of the Training Plan

The Training Plan is shared and made public in February.

5.3.5 Frequency of shift rotations

On-site or smart working shifts are between 8:00 AM and 7:00 PM from Monday to Friday.

Production areas are monitored at night and on holidays via an on-call rotation scheduled by the manager on a monthly basis with at least ten days' notice. Intervention can be provided remotely or on site, as required.

The Company ensures as many employees possessing the necessary technical and professional skills are included in the on-call system, with priority given to employees requesting inclusion.

5.3.6 Sanctions for unauthorised activities

Please see the metalworkers and private industrial systems national labour collective agreement (*CCNL Metalmeccanici e installazione impianti industria privata*) for information on sanctions procedures.

5.3.7 Non-employee controls

N/A

5.3.8 Documentation to be provided by personnel

When they are hired, employees must provide a copy of a valid identity document, a copy of a valid health card and a passport-sized photo for their access badge. They must complete and sign the personal data processing consent form and agree not to disclose confidential information and/or documents. They must read InfoCert's Code of Ethics and Netiquette.

5.4 Control log management

All events related to CA management and the certificate are recorded in the control log as required by the regulations and the technical rules [5].

5.4.1 Types of events recorded

Security events, start-ups and shut-downs, system crashes and hardware failures, firewall and router activities, and PKI system access attempts are recorded.
All data and documents used in the applicant's identification and acceptance phase are stored: copy of the identity card, contracts, certificate of incorporation, etc.
Events related to certification registration and life cycle are recorded: certificate requests and renewals, certificate registrations, generation, diffusion and revocation/suspension.
All events regarding the personal nature of the signature device are recorded.
All events are recorded with the system date and time of the event.

5.4.2 Frequency of control log processing and registration

Data processing, grouping and recording on InfoCert's compliant archiving system is done monthly.

5.4.3 Control log storage period

The CA keeps the control log for a number of years defined contractually.

5.4.4 Control log protection

The control log is protected by InfoCert's electronic document archiving system, which is accredited with the AgID in accordance with the legislation in force.

5.4.5 Control log backup procedure

The electronic document archiving system applies a backup policy and procedure in accordance with the system's manual.

5.4.6 Control log recording system

Event logs are collected by ad-hoc automatic procedures. They are recorded by procedures in accordance with InfoCert's archiving system's manual.

5.4.7 System vulnerability notification

N/A

5.4.8 Vulnerability assessments

InfoCert regularly performs system vulnerability assessments and penetration tests. Based on the results, it applies all necessary countermeasures to protect application security.

5.5 Report archiving

5.5.1 Types of report archived

All reports related to a Certification Authority's events are drafted and archived. The Certification Authority archives the reports for 20 years in InfoCert's documentation archiving system.

5.5.2 Protecting the reports

Protection is guaranteed by InfoCert's document archiving system, which is accredited with the AgID.

5.5.3 Report backup procedures

The standardised archiving system applies a backup policy and procedure as required by the system's manual

5.5.4 Report time stamping requirements

N/A

5.5.5 Archive storage system

Reports are collected by ad-hoc automatic procedures. They are recorded by the procedures as described in the manual of InfoCert's archiving system.

5.5.6 Archive information access and verification procedures

Automatic procedures and systems have been established to monitor the status of the certification system and the CA's entire technical infrastructure.

5.6 Replacement of the CA private key

The CA regularly replaces its certificate private key used to sign certificates in a manner that ensures the Subject can use their certificate right up to the time of renewal. Each replacement will be indicated in this manual and reported to the CAB.

5.7 Compromise of the CA private key and disaster recovery

5.7.1 Incident management procedures

The CA has described the incident management procedures for the SGSI certificate under ISO 27000. Every incident is analysed as soon as it is detected, corrective countermeasures are identified and the service manager drafts a report. The report is signed electronically and sent to the InfoCert archiving system. A copy of it is also sent to the AgID, along with the report on the actions taken to eliminate the causes of the incident if they were under InfoCert's control.

5.7.2 Hardware, software or data corruption

In the event of failure of the HSM security signature device containing the certification keys, the backup copy of the certification keys is used and the CA's certificate does not need to be revoked.

Software and data are backed up on a regular basis in accordance with internal procedures.

5.7.3 Procedures in the event of compromise of the CA private key

Compromise of the certification key is considered particularly critical because it would invalidate the certificates issued and signed using that key. Therefore, special care must be taken to protect certification keys and with regard to system development and maintenance that can impact that protection.
InfoCert has described the procedure to be followed in the event of key compromise in the ISO 27000 SGSI certificate, providing proof of it to the CAB.

5.7.4 Provision of CA services in the event of disaster

InfoCert has adopted the procedures necessary to guarantee continuity of service even in highly critical situations or in disasters.

5.8 Cessation of the CA or RA's services

In the event of cessation of the certification activity, InfoCert will give the supervisory

authority (AgID) at least 60 days' advance notice, indicating the replacement certification body, the depositary of the certificate directory and related documentation, if available. InfoCert will also notify all holders of certificates issued by it of the cessation of activity with the same notice period. If no replacement certification body is indicated in the notice, it will be clearly stated that all certificates not yet expired at the time of the CA's cessation of activity will be revoked.

6 TECHNOLOGICAL SECURITY CONTROLS

6.1 Installation and generation of the pair of certification keys

To perform its activity, the Certification Authority needs to generate the pair of certification keys for the signature of Subject's certificates.

The keys are generated only by people specifically assigned this duty. The keys and the signature are generated in dedicated and certified encrypted modules in accordance with the legislation in force.

The CA private keys are protected by the key generation and use encryption module. The private key can be generated in the presence of two operators responsible for generation. Keys are generated in the presence of the service manager.

The CA private keys are duplicated only for recovery following breakage of the secure signature device, in a controlled procedure that separates the key and the context on several devices as required by the HSM device's security criteria.

The encryption module used to generate the keys and signature has requisites that ensure:

- compliance of the pair of keys with the requisites set by the generation and verification algorithms used
- equal possibility of generating all possible pairs
- identification of the subject activating the generation procedure
- that signature generation is done inside the device to prevent interception of the value of the private key used

6.1.1 Generation of the Subject's pair of keys

The asymmetrical keys are generated inside an SSCD or QSCD Secure Device for the Signature Creation using the devices' native functions.
If the CA did not provide the device, the applicant must ensure the device complies with the legislation in force, presenting appropriate documentation and being subject to regular audits.

6.1.2 Delivery of the private key to the Applicant

The private key is contained in the SSCD or QSCD encryption device. When the Subject is given the encryption device, they enter into full possession of the private key, which can be used only with the PIN, which is known only to the Subject.

If registration is done in the Subject's presence, the device is delivered when the keys are generated.
If the Subject is not present during registration, the device is delivered according to methods defined in the contract, ensuring that the device and the information for its use travel via different channels or are delivered to the Subject at different times.

6.1.3 Delivery of the public key to the CA

N/A

6.1.4 Delivery of the public key to users

The public key is contained in the certificate issued only to the applying subject. If the Applicant requests it, it is also published in the certificates directory, where it can be retrieved by the User.

6.1.5 Key algorithm and length

The pair of asymmetrical certification keys is generated in a hardware encryption device as explained above. The RSA asymmetrical algorithm is used and the key length is at least 4096 bits.
For the subject's keys, the asymmetrical RSA encryption algorithm is used and the key length is at least 2048 bits.

6.1.6 Quality controls and public key generation

The devices used are certified in accordance with high standards of security (see § 6.2.1) and guarantee that the key is both correct and random. Before issuing the certificate, the CA verifies that the public key has not already been used.

6.1.7 Purpose of key use

6.1.7.1 Use of the CA key

The CA key is used only to sign Owner's certificates, Revocation Lists and OCSP certificates. The CA certificate's KeyUsage extension contains the certified signature (keyCertSign) and CRL signature (cRLSign).

OCSP responses are signed using specific certificates with extKeyUsage valued with ocspSigning.

6.1.7.1 Use of the Owner's key

The private key's use is determined by the KeyUsage extension as defined by standard X509. For the certificates described in this Certificate Practice Statement, the only permitted use is "non-repudiation", that is, certificates can be used only for signing.

6.2 Private key protection and engineering controls of the encryption module

6.2.1 Encryption module controls and standards

The encryption modules used by InfoCert for the certification keys (CA) and for the OCSP responder are FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) validated in Europe.
The smartcards used by InfoCert are validated Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) or EAL5 Augmented by ALC_DVS.2, AVA_VAN.5.
The encryption modules used by InfoCert for the Subject's remote and automatic certification keys are validated FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4.

6.2.2 Controls of the CA private key by more than one person

Only two simultaneously authenticated people can access the devices containing the certification keys.

6.2.3 Filing of the CA private key with third parties

N/A

6.2.4 Backup of the CA private key

The key backup is stored in a vault that can be opened only by personnel who do not have access to the HSM devices. Therefore, recovery requires the presence of both the person having access to the devices and the person having access to the vault.

6.2.5 Archiving of the CA private key

N/A

6.2.6 Transfer of the private key from a module or to an encryption module

N/A

6.2.7 Storage of the private on an encryption module

The certification key is generated and stored in a protected area of the encryption device that prevents it from being exported. In the event the protection is forced, the device's operating system blocks the device or makes it illegible.

6.2.8 Private key activation method

The certification private key is activated by the CA's software in dual control, that is, by two people having specific roles and in the presence of the service manager.
The Subject or Applicant who is the legal representative of the legal entity is responsible for protecting the private key with a strong password to prevent unauthorised use. The Subject must sign in to activate the private key.

6.2.9 Private key deactivation method

N/A

6.2.10 Destruction method for the CA private key

The InfoCert staff member responsible for this destroys the private key when the certificate has expired or been revoked using security procedures established by the security policies and the device manufacturer's instructions.

6.2.11 Classification of the encryption modules

N/A

6.3 Other aspects of key management

N/A

6.3.1 Archiving of the public key

N/A

6.3.2 Certificate and pair of keys validity period

The certificate's validity period is determined by:

- the state of the technology
- the state of encryption knowledge
- the planned use of the certificate

The certificate's validity period is expressed inside it as explained in section 3.3.1.

Currently, the CA's certificate is valid for 16 years, while certificates issued to natural persons or legal entities are valid for a maximum of 3 years.

6.4 Private key activation data

See sections 4.2 and 6.3.

6.5 IT security controls

6.5.1 Specific computer security requirements

The operating system of the computers used to generate keys in certification activities, generate certificates and manage the certificates directory are hardened, which means that they are configured in a way that minimises the impact of any vulnerability by eliminating all functions that are not necessary for the CA's operation and management.

System administrators, who are appointed in accordance with the legislation in force, access the system via an on-demand root application that allows root user privileges only with individual authentication. Accesses are tracked and logged, and archived for 12 months.

6.6 Operations on control systems

InfoCert assigns strategic importance to the secure processing of information and recognises the need to develop, maintain, control and constantly improve an information security management system (SGSI) in accordance with ISO/IEC 27001.
InfoCert is ISO/IEC 27001:2005 certified since March 2011, for the operating headquarters in Padua, the Disaster Recovery site in Modena and for the Rome and Milan sites for EA:33-35 activities. In March 2015, InfoCert was certified under the new version of standard ISO/IEC 27001:2013.
The SGSI includes procedures and controls for:

- asset management
- access control
- physical and environmental security
- operating activity security
- communications security
- systems acquisition, development and maintenance
- incident management
- business continuity

All procedures are approved by their managers and shared within the InfoCert document management system.

6.7 Network security controls

For the certification service, InfoCert has created a network security infrastructure based on the use of firewalls and the SSL protocol in order to create a secure channel between the registration offices and the certification system, and between it and the administrators/operators.

InfoCert's systems and networks are connected to the Internet behind firewall systems able to split the connection into areas with progressively higher security levels: Internet, DMZ (Demilitarized Zone) or Perimeter networks and Internal Networks. All traffic flowing between the different areas is subject to acceptance by the firewall, on the basis of a set of established rules. The rules defined for firewalls are designed in accordance with the principles of "*default deny*" (anything not expressly permitted is forbidden by default, that is, the rules allow only whatever is strictly essential for correct operation of the application) and "*defence in depth*" (successive levels of defence, first at the network level, by means of successive firewalls, and then through hardening at the system level).

6.1 Network security controls

For information on time stamping, see the ICERT-INDI-TSA Certificate Practice Statement on the InfoCert website.

7 CERTIFICATE, CRL AND OCSP FORMAT

7.1 Certificate format

The certificate contains the information indicated on the certification request.
The certificate format conforms with the eIDAS Regulation and the CNIPA Deliberation [9] to guarantee complete legibility and verifiability with respect to European law and certificates.
InfoCert uses standard ITU X.509, version 3 for the entire PKI structure.
In 0 the format of the root certificates and of the subjects, whether natural persons or legal entities.

7.1.1 Version number

All certificates issued by InfoCert are X.509 version 3.

7.1.2 Certificate extensions

N/A

7.1.3 Signature algorithm OID

Certificates are signed using the following algorithm:
sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Name forms

Each certificate has a serial number unique to the CA having issued it.

7.1.5 Naming constraints

See section 3.1.

7.1.6 Certificate OID

See section 1.2.

7.2 CRL format

To form certificate revocation lists (CRL), InfoCert uses the RFC5280 “Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)” profile and adds the extensions defined by RFC 5280 to the base format: “Authority Key Identifier”, “CRL Number”, “Issuing Distribution Point” and “expiredCertsOnCRL”

7.2.1 Version number

All CRL issued by InfoCert are X.509 version 2.

7.2.2 CRL extensions

For CRL extensions, see ANNEX A.

7.3 OCSP format

In order to determine a certificate's revocation status without requesting it from the CRL, InfoCert provides OCSP services conforming to the RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" profile. The protocol specifies the data that must be exchanged between an application wanting to verify the certificate's status and the OCSP service.

7.3.1 Version number

The OCSP protocol used by InfoCert complies with RFC6960 version 1.

7.3.2 OCSP extensions

For OCSP extensions, see ANNEX A.

8 CONFORMITY CONTROLS AND ASSESSMENTS

In accordance with the Regulation, InfoCert has requested a Conformity Assessment Report (CAR) from an assessment body accredited by the Conformity Assessment Body (CAB); in Italy, this is Accredia.
InfoCert provides the Service as a qualified trust service provider pursuant to Regulation (EU) No 910/2014 of 23 July 2014, on the basis of a conformity assessment performed by the Conformity Assessment Body CSQA Certificazioni S.r.l., pursuant to the Regulation referred to above and Standard ETSI EN 319 401, in accordance with the eIDAS system of assessment established by ACCREDIA on the basis of ETSI EN 319_403 and UNI CEI EN ISO/IEC 17065:2012.

8.1 Conformity assessment frequency or circumstances

The conformity assessment is repeated every two years, although the CAB conducts a surveillance audit every year.

8.2 Auditor identity and qualifications

The assessment is performed by

Company name	CSQA Certification S.r.l.
Registered office	Via S. Gaetano 74, 36016 Thiene (VI)
Phone number	+39 044 531 3011
Corporate register number	Tax number 02603680246 Vicenza corporate register: 02603680246 / Economic and administrative index: 258305
VAT number	02603680246
Website	http://www.csqa.it

8.3 Relations between InfoCert and the CAB

InfoCert and CSQA have no financial interests or business relations.
They have no current commercial or partnership relationship that could prejudice CSQA for or against InfoCert in the objective assessment.

8.4 Objective assessment aspects

The CAB assesses conformity of the procedures adopted, the CA's organisation, the organisation of the roles, personnel training and contractual documentation with respect to the Certificate Practice Statement, the Regulation and the applicable legislation.

8.5 Consequences of nonconformity

The CAB informs InfoCert of any instance of nonconformity, requesting it guarantee correction. The CAB may decide to repeat the audit once the nonconformity has been corrected.
InfoCert undertakes to resolve all nonconformities in a timely manner, making all necessary improvements and adjustments.

9 OTHER LEGAL BUSINESS ASPECTS

9.1 Rates

9.1.1 Certificate issue and renewal rates

Rates are available on www.infocert.it, or from the Registration Authority. The CA may sign commercial agreements and establish special rates with the RA and/or the Applicants.

9.1.2 Certificate access fees

N/A

9.1.3 Fees for access to certificate revocation and suspension status information

Access to the certificate revocation list (CRL) is free of charge.

9.1.4 Fees for other services

Rates are available on www.infocert.it, or from the Registration Authority.

The CA may sign commercial agreements and establish special rates with the RA and/or the Applicants.

9.1.5 Refund policies

If the service is purchased by a consumer, the Subject has the right to withdraw from the contract within 14 days of contract signature, and the price paid is refunded. Instructions to exercise the right of withdrawal and request a refund are available in the customer service section at www.infocert.it or from the RA.

9.2 Financial liability

9.2.1 Insurance coverage

The TSP InfoCert has insurance coverage for business risks and for damage to third parties. The text has been processed and accepted by the AgID. Its maximum coverage is:

- €3,000,000 per claim
- €6,000,000 per year

9.2.2 Other activities

N/A

9.2.3 Guarantee or insurance coverage for end users

See section 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No confidential information is managed for the activity that is the subject matter of this Manual.

9.3.2 Information not included in the scope of confidential information

N/A

9.3.3 Duty to protect confidential information

N/A

9.4 Privacy

Unless expressly agreed otherwise, information concerning the Subject and the Applicant that comes into the CA's possession in the course of its typical activities is deemed confidential and not publishable, except where explicitly intended for public use (public key, certificate (if requested by the Subject), certificate revocation and suspension dates). In particular, InfoCert processes personal data in accordance with Legislative Decree 196 of 30 June 2003 [4], as amended by Legislative Decree 101 of 10 August 2018, containing measures for the compliance of national law with Regulation (EU) No 2016/679 of the European Parliament and of the Council of 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal 205 of 4 September 2018).

9.4.1 Privacy program

InfoCert adopts a set of policies by which it implements and integrates personal data protection in its information security management system certified under ISO 27001, sharing its continuous improvement process with this system.

9.4.2 Data considered to be personal

Any data meeting the definition of personal data under the legislation in force [4] is considered personal. Therefore, personal data is any information regarding a natural person that is identified or identifiable, including indirectly, through reference to any other information, including a personal identification number.

9.4.3 Data not considered personal

Data that are to be made public by the CA's technical management, i.e. public key, certificate (if requested by the Subject), certificate revocation and suspension dates are not considered personal data.

9.4.4 Data Controller

Infocert S.p.A.

Operating headquarters

Via Marco e Marcelliano 45

00147 Rome

richieste.privacy@legalmail.it

9.4.5 Privacy notice and consent to personal data processing

The privacy notice is available at www.infocert.it.
Before processing any personal data, InfoCert collects consent to processing using the methods and in the forms required by law [4].

9.4.6 Data disclosure following a request from the authority

Data must be disclosed following a request from the Authority and is done in the manner established by the Authority on a case-by-case basis.

9.4.7 Other reasons for disclosure

N/A

9.5 Intellectual property

9.6 Representation and guarantees

See the contract between CA, RA, Applicants and Subjects for information on the guarantees and responsibilities of each party.

9.7 Limitation of warranty

See the contract governing the service for this aspect.

9.8 Limitations of liability

See the contract governing the service for this aspect.

9.9 Indemnification

See the contract governing the service for this aspect.

9.10 Term and termination

9.10.1 Term

The certificate is revoked upon expiry of the relationship between the CA and the Subject, between the CA and the RA, and between the CA and the Applicant.

9.10.2 Termination

See the contract governing the service for information on contract termination.

9.10.3 Effects of termination

Termination triggers immediate revocation of the certificate.

9.11 Official communication channels

See the contact channels indicated in section 1.5.2.

9.12 Revision the Certificate Practice Statement

The CA reserves the right to modify this document for technical reasons or due to procedural modifications as required by law or regulations, or to optimise the working cycle. Each new version of the Certificate Practice Statement cancels and replaces the previous versions, which remain applicable to certificates issued when they were in force and until their first expiry date.

Variations not having a significant impact on users will be indicated by an increase in the document's release number, while variations having a significant impact on users (e.g., modifications to operating procedures) will be indicated by an increase in the document's version number. In any case, the Manual will be published promptly and made available following the usual procedures. Each technical or procedural modification to this Certificate Practice Statement will be promptly reported to the RA.

9.12.1 Revision history

Version/Release no:	**1.5**
Version/Release date:	20/05/2022
Description of changes:	Correction of typos Accessible formatting
Reasons:	Periodic document revision

Version/Release no:	**1.4**
Version/Release date:	24/03/2022
Description of changes:	update of identification methods § 3.2.3.4 e 3.2.3.6
Reasons:	New process and flow needs

Version/Release no:	**1.3**
Version/Release date:	08/06/2021
Description of changes:	correction of misprints revision and policy addition § 1.2 update of group name § 1.3.1 update of contacts § 1.5.2 revision of description § 4.3.1.2, addition of limitation of use for testing purposes § 4.5.3 technological update and references to services hosted on the AWS cloud § 5.1.1 technological update § 5.1.6 update of description §§ 2.2.3, 5.3.5, 6.1.7 addition of new CA root § Appendix A
Reasons:	periodic document revision

Version/Release no:	**1.2**
Version/Release date:	25/07/2019
Description of changes:	correction of misprints change of company logo update of anti-money laundering legislation § 3.23.2 update of privacy notice § 9.4
Reasons:	document revision for change of legislative and business context, and correction of misprints

Version/Release no:	**1.1**
Version/Release date:	12/07/2017
Description of changes:	§ 1.3.1.1 simplification of IR appointment procedure; § 1.3.3 correction of misprints; § 1.4.2 correction of misprints; § 1.6 alignment of definitions; § 2.2.1 correction of misprints; § 2.2.2 definition of non-possibility to publish certificates; § 3.2. and § 3.2.3.2 elimination of redundant reference to Legislative Decree 231/2007 for Italy; § 3.2.1 section rewritten; § 3.2.3.4 section rewritten without altering its meaning; § 3.4.1 correction of misprint; § 4.1.1 modification of website; § 4.1.2 replacement of “inscription” with “registration”; § 4.3.3.2 modification of remote signature device activation procedure; § 4.4.2 definition of non-possibility to publish certificates; § 4.5.1 correction of misprints;

	§ 4.9.3.2 simplification of the revocation request procedure; § 4.9.6 correction of misprint in document structure; § 4.9.10, § 4.9.11, § 4.9.12 correction of misprint in document structure; § 4.10.1 section rewritten; § 5.6 section rewritten; § 6.1 insertion of reference to CSP ICERT-INDI-TSA; § 7.3 section rewritten; § 8 and § 8.5 correction of misprints; § 9.1.1 and § 9.1.4 and § 9.1.5 modification of website; § 9.1.2 correction of misprint; § 9.12 correction of misprint; § 9.12.3 simplification of Certificate Practice Statement retrieval; Appendix A – correction of misprints
Reasons:	document revision for change of business context, and correction of misprints

Version/Release no:	**1.0**
Version/Release date:	12/12/2016
Description of changes:	First release
Reasons:	First document release

9.12.2 Revision procedures

Certificate Practice Statement revision procedures are similar to drafting procedures. Revisions are made jointly by the Certification Service Manager, Security Manager, Privacy Manager, Legal Department and the Consultancy Area, and are approved by management.

9.12.3 Notification period and mechanism

The Certificate Practice Statement is published in electronic format in the documentation section of the InfoCert website (www.infocert.it).

9.12.4 Cases in which the OID must be changed

N/A

9.13 Dispute settlement

See the contract governing the service for information on dispute settlement.

9.14 Court of jurisdiction

For consumers, the court of jurisdiction is the court in the consumer's city of residence. For other subjects, the court of jurisdiction is that of the city of Rome. In agreements between the CA and the RA, between the CA and the Applicant, and between CA the and the Subject, a different court of jurisdiction may be defined.

9.15 Applicable law

This Certificate Practice Statement is governed by Italian law.

Below is a partial list of major applicable legislation:

[1] Regulation (EU) No 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 (also called *eIDAS Regulation*)

[2] Legislative Decree 82 of 7 March 2005 (Official Journal 112 of 16 May 2005) – Digital Administration Code (also called *CAD*) as amended and supplemented

[3] Presidential Decree 445 of 28 December 2000 (Official Journal 42 of 20/2/2001) as amended and supplemented

[4] Legislative Decree 196 of 30 June 2003 (Official Journal 174 of 29 July 2003) – Privacy Code – and Regulation (EU) No 2016/679 of the European Parliament and of the Council of 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 (in force since 25 May 2018) as amended and supplemented

[5] Prime Ministerial Decree of 22 February 2013 (Official Journal 117 of 21 May 2013) – Technical rules on the generation, affixing and verification of advanced, qualified and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3),

32(3b), 35(2), 36(2), and (71)

[6] Legislative Decree 90 of 25 May 2017 implementing Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending 2005/60/EC and 2006/70/EC and implementing Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, rewriting in its entirely, among others, Italian Legislative Decree 231/2007 on the prevention of money laundering and the financing of terrorism, implementing Directive (EU) 2015/849 (so-called IV Anti-money laundering Directive) as amended and supplemented

[7] Legislative Decree 206 of 6 September 2005, as amended and supplemented – Consumer Code

[8] Not used

[9] CNIPA deliberation 45 of 21 May 2009, as amended by subsequent decisions.

The implementation documents required under the eIDAS Regulation [1] also apply.

9.16 Miscellaneous

See the contract governing the service for any provision not included in this Manual.

9.17 Other provisions

The service is available during the following hours (unless otherwise agreed contractually):

Service	Hours
Access to the public certificates archive (including certificates and CRL)	24 hours per day 7 days per week
Certificate revocation or suspension	24 hours per day 7 days per week
Other activities: registration, generation, publication, renewal[5]	9:00 AM to 5:00 PM Monday to Friday, excluding holidays 9:00 AM to 1:00 PM Saturday

[5] Registration is done at the Registration Offices that may have different office hours. In any case, InfoCert guarantees its services during the hours indicated above.

Time stamp request and/or verification	24hx7gg (minimum 95% availability)

ANNEX A

ROOT Certificate: InfoCert Advanced Electronic Signature CA 3

```
  0 1848: SEQUENCE {
  4 1312:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
       :     }
 13    1:     INTEGER 1
 16   13:     SEQUENCE {
 18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29    0:       NULL
       :     }
 31  154:     SEQUENCE {
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'IT'
       :         }
       :       }
 47   24:       SET {
 49   22:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56   15:           UTF8String 'InfoCert S.p.A.'
       :         }
       :       }
 73   31:       SET {
 75   29:         SEQUENCE {
 77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   22:           UTF8String 'Trust Service Provider'
       :         }
       :       }
106   26:       SET {
108   24:         SEQUENCE {
110    3:           OBJECT IDENTIFIER '2 5 4 97'
115   17:           UTF8String 'VATIT-07945211006'
```

```
    :        }
    :       }
134  52:     SET {
136  50:      SEQUENCE {
138   3:       OBJECT IDENTIFIER commonName (2 5 4 3)
143  43:       UTF8String
    :         'InfoCert Advanced Electronic Signature CA 3'
    :        }
    :       }
    :     }
188  30:   SEQUENCE {
190  13:     UTCTime 12/12/2016 16:45:37 GMT
205  13:     UTCTime 12/12/2032 17:45:37 GMT
    :     }
220 154:   SEQUENCE {
223  11:     SET {
225   9:      SEQUENCE {
227   3:       OBJECT IDENTIFIER countryName (2 5 4 6)
232   2:       PrintableString 'IT'
    :        }
    :       }
236  24:     SET {
238  22:      SEQUENCE {
240   3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
245  15:       UTF8String 'InfoCert S.p.A.'
    :        }
    :       }
262  31:     SET {
264  29:      SEQUENCE {
266   3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
271  22:       UTF8String 'Trust Service Provider'
    :        }
    :       }
295  26:     SET {
297  24:      SEQUENCE {
299   3:       OBJECT IDENTIFIER '2 5 4 97'
304  17:       UTF8String 'VATIT-07945211006'
    :        }
    :       }
323  52:     SET {
325  50:      SEQUENCE {
```

```
327   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
332  43:         UTF8String
     :           'InfoCert Advanced Electronic Signature CA 3'
     :         }
     :       }
     :     }
377 546:    SEQUENCE {
381  13:      SEQUENCE {
383   9:       OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
394   0:       NULL
     :       }
396 527:      BIT STRING, encapsulates {
401 522:       SEQUENCE {
405 513:        INTEGER
     :          00 D9 F0 76 FE E9 14 07 07 DD 31 2B 48 E1 1A 93
     :          DC 42 43 C1 ED 3D 96 36 DF 49 F6 A7 E9 58 BB A0
     :          34 E2 8D 77 77 1F 73 CD 17 37 28 50 F6 4D 18 C9
     :          0E 78 81 DA 15 77 02 8D 1F DA C5 1F 28 E9 5D B2
     :          3F 07 3A 8F 4D 00 DB 76 40 6A CA D3 87 BA AA 43
     :          7C AE C5 E6 2B 60 B8 7E 65 64 F3 F1 06 B2 94 95
     :          6F C5 1E 3E 39 39 41 17 44 A9 87 E2 D6 EB 08 35
     :          5E 2E 7E 3B E8 6A E0 6E DB 57 F6 32 34 76 36 55
     :                [ Another 385 bytes skipped ]
922   3:        INTEGER 65537
     :       }
     :     }
     :   }
927 389:    [3] {
931 385:     SEQUENCE {
935  15:      SEQUENCE {
937   3:       OBJECT IDENTIFIER basicConstraints (2 5 29 19)
942   1:       BOOLEAN TRUE
945   5:       OCTET STRING, encapsulates {
947   3:         SEQUENCE {
949   1:           BOOLEAN TRUE
     :         }
     :       }
     :     }
952  88:      SEQUENCE {
954   3:       OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
959  81:       OCTET STRING, encapsulates {
```

```
 961  79:          SEQUENCE {
 963  77:           SEQUENCE {
 965   4:            OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 971  69:            SEQUENCE {
 973  67:             SEQUENCE {
 975   8:              OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
 985  55:              IA5String
      :             'http://www.firma.infocert.it/documentazione/manu'
      :             'ali.php'
      :              }
      :             }
      :            }
      :           }
      :          }
      :         }
1042 228:       SEQUENCE {
1045   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1050 220:        OCTET STRING, encapsulates {
1053 217:         SEQUENCE {
1056 214:          SEQUENCE {
1059 211:           [0] {
1062 208:            [0] {
1065  39:             [6] 'http://crl.infocert.it/ca3/ades/ARL.crl'
1106 164:              [6]
      :             'ldap://ldap.infocert.it/cn%3DInfoCert%20Advanced'
      :             '%20Electronic%20Signature%20CA%203,ou%3DTrust%20'
      :             'Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?aut'
      :             'horityRevocationList'
      :              }
      :             }
      :            }
      :           }
      :          }
      :         }
1273  14:       SEQUENCE {
1275   3:        OBJECT IDENTIFIER keyUsage (2 5 29 15)
1280   1:        BOOLEAN TRUE
1283   4:        OCTET STRING, encapsulates {
1285   2:         BIT STRING 1 unused bit
      :          '1100000'B
      :         }
```

```
      :        }
1289   29:       SEQUENCE {
1291    3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1296   22:         OCTET STRING, encapsulates {
1298   20:           OCTET STRING
      :             2E B8 32 31 EF 4F 33 13 70 04 23 1D BE 8B 48 9D
      :             B1 5F E0 51
      :           }
      :         }
      :       }
      :     }
      :   }
1320   13:   SEQUENCE {
1322    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1333    0:     NULL
      :     }
1335  513:   BIT STRING
      :     42 9D E2 BD 74 54 70 30 5F 57 6E 3C 6A 5D 27 94
      :     07 85 3E 80 D5 DC DE 56 73 91 34 A2 59 3D 5C 23
      :     AC 3B 55 52 E3 1F BC 9A CE 44 FA 72 CE 7A 50 46
      :     FB 9E AB 21 B5 57 B7 89 7E 1B 2B 66 E9 5D F4 AE
      :     5A 05 EC E3 D3 11 4B D5 39 A7 B3 1B 8C 78 C2 9F
      :     BF A2 BE 32 EA 59 0F 7B DA DC 3F EA 53 EA 36 A0
      :     A6 72 C6 1C 61 C0 A2 F0 B7 2E 9D 61 BE 89 45 B4
      :     F2 C7 3A B1 99 A8 13 BE 68 33 49 35 A0 1A 1B 3A
      :           [ Another 384 bytes skipped ]
      :   }
```

ROOT Certificate: InfoCert Advanced Electronic Signature CA 4

```
  0 1673: SEQUENCE {
  4 1137:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
      :     }
```

```
13   1:    INTEGER 1
16  13:    SEQUENCE {
18   9:     OBJECT IDENTIFIER
     :      sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29   0:     NULL
     :     }
31 154:    SEQUENCE {
34  11:     SET {
36   9:      SEQUENCE {
38   3:       OBJECT IDENTIFIER countryName (2 5 4 6)
43   2:       PrintableString 'IT'
     :      }
     :     }
47  24:     SET {
49  22:      SEQUENCE {
51   3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
56  15:       UTF8String 'InfoCert S.p.A.'
     :      }
     :     }
73  31:     SET {
75  29:      SEQUENCE {
77   3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
82  22:       UTF8String 'Trust Service Provider'
     :      }
     :     }
106  26:    SET {
108  24:     SEQUENCE {
110   3:      OBJECT IDENTIFIER '2 5 4 97'
115  17:      UTF8String 'VATIT-07945211006'
     :      }
```

```
    :       }
134  52:     SET {
136  50:       SEQUENCE {
138   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
143  43:         UTF8String
    :           'InfoCert Advanced Electronic Signature CA 4'
    :         }
    :       }
    :     }
188  30:   SEQUENCE {
190  13:     UTCTime 07/06/2021 08:35:29 GMT
205  13:     UTCTime 07/06/2036 09:35:29 GMT
    :     }
220 154:   SEQUENCE {
223  11:     SET {
225   9:       SEQUENCE {
227   3:         OBJECT IDENTIFIER countryName (2 5 4 6)
232   2:         PrintableString 'IT'
    :         }
    :       }
236  24:     SET {
238  22:       SEQUENCE {
240   3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
245  15:         UTF8String 'InfoCert S.p.A.'
    :         }
    :       }
262  31:     SET {
264  29:       SEQUENCE {
266   3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
271  22:         UTF8String 'Trust Service Provider'
```

```
    :         }
    :       }
295  26:      SET {
297  24:       SEQUENCE {
299   3:        OBJECT IDENTIFIER '2 5 4 97'
304  17:        UTF8String 'VATIT-07945211006'
    :         }
    :       }
323  52:      SET {
325  50:       SEQUENCE {
327   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
332  43:        UTF8String
    :          'InfoCert Advanced Electronic Signature CA 4'
    :         }
    :       }
    :     }
377 546:    SEQUENCE {
381  13:     SEQUENCE {
383   9:      OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
394   0:      NULL
    :       }
396 527:     BIT STRING, encapsulates {
401 522:      SEQUENCE {
405 513:       INTEGER
    :          00 C3 BB 3C 19 5E B2 5E A6 81 0D 21 31 82 12 32
    :          31 D6 D6 BD 78 97 7C 39 CA 15 C0 37 AA 1D 9B ED
    :          45 34 02 77 EE 95 8C AE 26 CF 87 E4 82 81 E1 D2
    :          34 6A 14 1C 21 B9 EA C9 76 E3 78 4F 79 B4 94 2B
    :          40 D8 F8 A7 F5 EA 86 20 58 8F 69 43 75 9D 21 F3
    :          4C B9 E2 67 86 B9 1C 11 49 A4 1E A1 4C 59 6D 6F
```

```
    :          3B 98 E4 EE F4 A1 0F FD 08 9D 5D 8F 01 58 62 0C
    :          9E 57 24 64 AA FF EF AB CD 01 BC 9C A1 BB 7A B6
    :          6C F1 48 0A BC 67 25 CB 3B AA DF 3B F5 37 28 FD
    :          F7 1F B8 CB 33 50 94 C4 D1 6A D8 0D 6F 8E 19 B1
    :          4F 7E 8A 52 EC 38 5A E2 EC BF C8 B5 DC 10 BB A7
    :          2B 13 C7 18 63 EF 52 08 73 71 71 9B D0 14 BB E4
    :          E2 22 55 7D 33 FC 41 D0 D9 55 45 4D A9 B1 8F 0F
    :          BD 24 18 9F 55 74 80 C6 31 56 3B C8 93 E1 00 FD
    :          CC E1 9A A4 6E AC D5 91 9C BF A4 65 DB 4F 4D CF
    :          ED 49 CF 82 CB A1 A4 BC B0 B8 24 0B 2E EE F2 CD
    :          AD 19 96 2C 0F D1 82 AC 14 7F 0A E4 E4 FA 76 30
    :          EF 47 92 70 6C 8C 9B 56 DA EF 05 CF 59 74 55 9D
    :          31 5F DE FD A4 83 6B 12 77 AE BB 7C 46 36 9D CB
    :          77 CB 9B ED 93 16 8C 6F 88 F7 0F 91 4A F8 C7 5F
    :          68 FB AB A1 63 E0 0B 1D AE 16 CE 3D FC 57 CA 04
    :          1F 99 51 EC 43 90 A5 46 D9 EF 29 90 D0 B9 AE 14
    :          77 5D D2 67 2A 01 CE 0E 6A EF 12 78 AD C4 7F CD
    :          57 8F 1E 81 06 07 4B D8 88 14 43 30 50 80 3F 31
    :          C0 1E 61 ED AA B8 49 30 33 9C 9E 40 17 E4 2D C7
    :          61 AC EB E9 5E 3F 16 54 9B F5 74 06 49 BF 48 C2
    :          71 29 D2 D8 D4 DE EF 8F A4 E9 52 F5 4D D9 77 44
    :          28 5A D9 A5 7C B3 E7 5F 39 E5 58 46 B0 C7 2C AC
    :          2F 0A 27 58 1A 17 DD A6 7D F8 78 00 2D 0F 51 D1
    :          5A 37 8C 10 AF D3 28 09 60 97 DF 79 D4 37 50 5E
    :          E0 F3 82 3E 4C 69 BC 60 E3 AC 54 E0 13 B8 A9 9E
    :          91 FA 9C 85 39 D4 18 DA B6 CB 74 99 44 82 9E 3C
    :          43
922   3:        INTEGER 65537
    :       }
    :     }
```

```
    :     }
927  215:    [3] {
930  212:      SEQUENCE {
933   15:       SEQUENCE {
935    3:        OBJECT IDENTIFIER basicConstraints (2 5 29 19)
940    1:        BOOLEAN TRUE
943    5:        OCTET STRING, encapsulates {
945    3:          SEQUENCE {
947    1:            BOOLEAN TRUE
    :           }
    :         }
    :       }
950   88:       SEQUENCE {
952    3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
957   81:        OCTET STRING, encapsulates {
959   79:          SEQUENCE {
961   77:            SEQUENCE {
963    4:              OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
969   69:              SEQUENCE {
971   67:                SEQUENCE {
973    8:                  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
983   55:                  IA5String
    :                  'http://www.firma.infocert.it/documentazione/manu'
    :                  'ali.php'
    :                }
    :              }
    :            }
    :          }
    :        }
    :      }
```

```
1040  56:       SEQUENCE {
1042   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1047  49:        OCTET STRING, encapsulates {
1049  47:         SEQUENCE {
1051  45:          SEQUENCE {
1053  43:           [0] {
1055  41:            [0] {
1057  39:             [6] 'http://crl.ca4.infocert.it/ades/ARL.crl'
      :            }
      :           }
      :          }
      :         }
      :        }
1098  14:       SEQUENCE {
1100   3:        OBJECT IDENTIFIER keyUsage (2 5 29 15)
1105   1:        BOOLEAN TRUE
1108   4:        OCTET STRING, encapsulates {
1110   2:         BIT STRING 1 unused bit
      :          '1100000'B
      :         }
      :        }
1114  29:       SEQUENCE {
1116   3:        OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1121  22:        OCTET STRING, encapsulates {
1123  20:         OCTET STRING
      :          84 B0 C8 E9 41 16 7C 8F B2 96 8E 70 2D 13 DD 14
      :          58 96 87 A2
      :         }
      :        }
```

```
    :       }
    :     }
    :   }
1145  13:   SEQUENCE {
1147   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1158   0:     NULL
    :   }
1160 513:   BIT STRING
    :     09 B7 20 4A 06 28 B6 50 70 6E 46 63 36 0E A1 BF
    :     64 2C 60 F3 A9 23 2A A1 D3 DA 86 E7 0D 4F 99 CD
    :     E0 8B 1E 76 F3 7C 63 DE F0 A8 51 C3 97 B8 17 BA
    :     E2 9D 87 CC A6 24 BE C1 D2 6C D7 3A 76 36 D4 5B
    :     0F 71 19 DC 61 53 9F F4 0B EE B7 8A 6F B3 AE 2B
    :     4C 4B 11 92 2F ED B9 0F 25 4D A1 30 1F 5E EF 7F
    :     05 43 5F 56 5D 16 2A E4 F8 9C D6 1E DC CB A8 9A
    :     71 37 FF FA 47 BB 3B 98 50 4D 7C A0 F1 A1 38 DB
    :     7D C4 B9 50 E6 46 2E 66 09 2B 9B C4 35 C4 6B A3
    :     2D 86 24 9B 29 28 A8 52 3B 09 92 99 F2 4E 9C 05
    :     BE 33 D7 11 6C CB 86 3D 52 97 40 C5 FA 6C E2 13
    :     DD B3 1B 30 E4 D0 4F 08 AF C0 B9 27 4D A8 05 7D
    :     BE 73 AE 97 F5 BA CB D5 A7 6A DB 19 00 C4 F0 E7
    :     42 51 F3 EB 4A 94 F5 78 2A B1 F1 29 8A D1 71 46
    :     D2 90 B0 A8 A0 39 37 4E 74 C6 95 05 41 56 BF 22
    :     C0 13 96 05 F5 BA 50 60 93 84 44 A0 D2 91 77 51
    :     52 B9 25 32 A3 E9 13 76 5E 5A BF 08 76 C0 30 3F
    :     8B 1B D1 0B 04 5C 0D 4F 2B 1F FC 3B D4 F4 DF FE
    :     6A 40 30 1B 1D 4C 73 DA 7F 46 B5 58 CE C1 14 21
    :     94 42 82 39 01 6A D2 BB 04 60 D5 95 15 96 DA 4F
    :     3C DA 7C A5 66 19 0E E6 DC C9 70 AE B0 F7 D5 7E
    :     60 92 90 26 FD 23 5E 0C F1 98 DD 92 8B 82 89 F5
```

: 4B C1 30 0C BF 10 F5 A2 81 E2 84 2E 85 8E 13 CE

: 31 D9 10 74 34 48 86 95 10 8C 2E F3 31 40 77 B5

: 0D A4 01 2A 58 AA A2 90 15 06 07 A6 B0 7E 8F 96

: 57 62 15 84 89 FB 73 27 F2 78 CD 60 C8 52 51 ED

: D9 15 BA 2C 50 E0 F2 C6 9F 14 0A 33 ED 5D 98 5C

: C1 D9 11 49 DB 64 1E 62 B0 F1 B9 CC 33 93 BE 49

: 9E 71 E5 CA B4 3A ED 67 9A 92 FD 73 48 83 40 A4

: B3 A7 0A 1F 88 08 0A C8 21 F4 FD 39 34 28 90 F8

: D8 25 71 FC 75 12 A0 E9 FD 72 2D E1 EA 1C 02 7B

: 55 EC 0B 5F 7C 5B BA D6 E7 BA 1B AB AE 69 80 05

: }

CRL and OCSP format

Extension	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCert
thisUpdate	Date in UTC format
nextUpdate	Date of next CRL in GeneralizedTime format
Revoked Certificates List	List of revoked certificates, with serial number revocation/suspension date
Issuer's Signature	CA signature

CRL and OCSP values and extensions

The CRL have the following extensions

Extension	**Value**
Authority Key Identifier	issuerPublicKey 160-bit SHA-1 hash value
CRL number	Unique CRL number assigned by the CA
ExpiredCertsOnCRL	Date in GeneralizedTime format starting on which expired certificates are kept in the CRL. The value is set equal to the CA issue date.

Issuing Distribution Point	Identifies the CRL distribution point and the purpose: indicates whether the CRL is generated only for CA certificates, or subject certificates (end-entity)
Invalidity Date	Date in UTC format indicating the date starting on which the certificate is considered invalid

The OCSP request contains the following fields:

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash of the issuer's DN
Issuer Key Hash	Hash of the issuer's public key
Serial Number	Certificate serial number

The OCSP response contains the following fields:

Field	Value
Response Status	OCSP response status
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN of the OCSP response certificate
Produced at	Date in GeneralizedTime format on which the response was generated
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash of the issuer's Distinguishedname
Issuer Key Hash	Hash of the issuer's public key
Serial Number	Certificate serial number
thisUpdate	Date in GeneralizedTime format on which the certificate status was verified
nextUpdate	Date on which the certificate status could be updated
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

OCSP Extensions

The OCSP request can contain the following extensions:

Extension	Value
nonce	A random number that can be used only once. It cryptographically links a request to its response to prevent replication attempts. It is contained in a requestExtensions for the request and can be contained in a responseExtensions for the response.

The OCSP response can contain the following extensions:

Extension	Value
nonce	A random number that can be used only once. It cryptographically links a request to its response to prevent replication attempts. It is contained in a requestExtensions for the request, and can be contained in a responseExtensions for the response.