Certificate policy
&
Certificate Practice Statement

Document code: **ICERT-INDI-MO***

Version: **4.10**

Date: **20/09/2023**

* starting from version 4.0, ICERT-INDI-MO and ICERT-INDI-MO-ENT are both included in this document

Contents

INDEX FIGURES

1 INTRODUCTION

1.1. Overview

A certificate binds a public key to a set of information that identifies the entity associated with the corresponding private key: this entity is known as the **Subject** of the certificate. A certificate is used by other persons to recover the public key distributed with the certificate and verify a qualified electronic signature affixed to or associated with a document. A certificate guarantees consistency between the public key and the Subject. The degree of reliability of the binding depends on several factors, such as the practices followed by the certification authority in issuing the certificate, the used security measures, the Subject's responsibilities in protecting the private key and any warranties given.
This document is the Certificate Practice Statement of the **Trust Service Provider InfoCert**, which provides qualified electronic signature services as part of its trust services. This Certificate Practice Statement describes the policies and procedures applied to the identification and issuance process of the qualified certificate, as well as security measures, obligations, warranties, responsibilities and, more broadly, any measures taken to ensure reliability of a qualified certificate in accordance with existing legislation on trust services, electronic signature, qualified seal and digital signature.
By issuing this Certificate Practice Statement and incorporating it by reference in certificates, the Certification Authority enables relying parties to assess the characteristics and reliability of the certification service and thus the binding between the keys and the Subject.
The contents are based on applicable regulations as of the date of issue and on the recommendations contained in “Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” © Internet Society 2003.

This Certificate Practice Statement also describes the policies and practices followed by InfoCert in the process of checking the requests, identifying the applicants and issuing certificates for the authentication of websites pursuant to Article 34 Delegated Regulation (EU) 2018/389 [12], supplementing Directive (EU) 2015/2366 (PSD2) [11], in accordance with the requirements defined in the ETSI TS 119 495 standard (referenced below as "PSD2 Certificates").

1.2. Document name and identification

This document is entitled “Trust Service Provider InfoCert – Certificate Practice Statement” and has the following document ID: ICERT-INDI-MO. For version and release level information, please see the page header.

Version 4.0 of this document is consistent with the following previous Certificate

Practice Statements and replaces them:

- ICERT-INDI-MO, version 3.5 of 30/11/2018 on the issuance of qualified certificates to natural and legal person using a CMS system
- ICERT-INDI-MO-ENT, version .3.5 of 30/11/2018 on the issuance of qualified certificates to individuals through LongTerm and OneShot signature

The document describes policies and procedures set out to manage qualified certificates in compliance with eIDAS Regulation [1].
This document is associated with the Object Identifiers (OID) described below, which are referenced in the CertificatePolicy extension of each certificate according to its intended use. The meaning of OIDs is given below.

The *Object Identifier* (OID) which identifies InfoCert is 1.3.76.36.

The following policies apply to qualified certificates:

Description	**OID**
Certificate policy statement for qualified certificates issued to natural persons	1.3.76.36.1.1.48.1 compliant with QCP policy No. 0.4.0.194112.1.0
Certificate policy statement for qualified certificates issued to natural persons and device-based keys (SSCD)	1.3.76.36.1.1.48.2 compliant with QCP policy No. 0.4.0.194112.1.0
Certificate policy statement for qualified certificates issued to legal persons, including device-based keys (SSCD) Also available for PSD2 (QSealC)	1.3.76.36.1.1.47 compliant with QCP-l policy No. 0.4.0.194112.1.1

The following policies apply to device-based qualified certificates:

Description	**OID**
Certificate policy statement for qualified certificates issued to natural persons and qualified device-based keys (QSCD)	1.3.76.36.1.1.1/1.3.76.36.1.1.61 compliant with QCP-n policy No. 0.4.0.194112.1.2
Certificate policy statement for qualified certificates issued to natural persons for qualified device-based automatic remote signature (QSCD)	1.3.76.36.1.1.2/1.3.76.36.1.1.62 compliant with QCP-n policy No. 0.4.0.194112.1.2
Certificate policy statement for qualified certificates issued to natural persons for qualified device-based remote signature (QSCD)	1.3.76.36.1.1.22/1.3.76.36.1.1.63 compliant with QCP-n policy No. 0.4.0.194112.1.2
Certificate policy statement for qualified	1.3.76.36.1.1.32/1.3.76.36.1.1.66

certificates issued to natural persons through a qualified device (QSCD)-based CMS system	compliant with QCP-n policy No. 0.4.0.194112.1.2
Certificate policy statement for qualified device-based qualified certificates issued to legal persons (QSCD) Also available for PSD2 (QSealC)	1.3.76.36.1.1.46 compliant with policy QCP-l-qscd 0.4.0.194112.1.3
Certificate policy statement for qualified certificates issued to natural persons for qualified device-based remote signature	1.3.76.36.1.1.35/1.3.76.36.1.1.65 Compliant with policy QCP-n-qscd 0.4.0.194112.1.2
Certificate policy statement for qualified certificates issued to natural persons for qualified device-based remote OneShot signature	1.3.76.36.1.1.34/1.3.76.36.1.1.64 Compliant with policy QCP-n-qscd 0.4.0.194112.1.2
Certificate policy statement of the "Spanish Citizen" issued to natural persons and qualified device-based keys (QSCD)	1.3.76.36.1.1.10.16.1.1.1 Compliant with policy QCP-n-qscd 0.4.0.194112.1.2

Below there is a list of policies for qualified certificates on qualified devices defined with type B or F key usage settings, as indicated in section 4.3.2 of the standard ETSI EN 319 412-2. Since combining the non-repudiation bit with the digital signature and key encipherment bits can have security impacts, the use of these OIDs is limited and each request is assessed individually.

Description	OID
Qualified certificate-operating-manual issued to natural person and keys on qualified device (QSCD) and key usage settings Type B or F	1.3.76.36.1.1.61.1 in accordance with QCP-n-qscd 0.4.0.194112.1.2
Qualified certificate-operating-manual issued to natural person for remote signature on qualified device (QSCD) and key usage settings Type B or F	1.3.76.36.1.1.63.1 in accordance with QCP-n-qscd 0.4.0.194112.1.2
Qualified certificate-operating-manual issued to natural person for LongTerm	1.3.76.36.1.1.65.1 in accordance with

type remote signature on qualified device (QSCD) and key usage settings Type B or F	QCP-n-qscd 0.4.0.194112.1.2
Qualified certificate-operating-manual issued to natural person for OneShot type remote signature on qualified device (QSCD) and key usage settings Type B or F	1.3.76.36.1.1.64.1 in accordance with QCP-n-qscd 0.4.0.194112.1.2

Additional OIDs may be used in the certificate to specify existing use restrictions. A list of these OIDs is included in § 4.5.3. Such use restrictions do not alter in any way the rules set out in the rest of this Certificate Practice Statement.
Furthermore, from 5 July 2019, all certificates complying with the recommendations of AgID determination no. 121/2019 with the corrections of subsequent AgID determination no. 147/2019 [13] will contain an additional PolicyIdentifier element with AgIDcert value (OID 1.3.76.16.6) in the CertificatePolicies field (OID 2.5.29.32)[1]. This document is available in electronic format from the Trust Service Provider's website at: http://www.firma.infocert.it, “Documentation” section.

1.3. Participants and responsibilities

1.3.1. Certification Authority

A **Certification Authority** is a trusted third party that issues electronic signature qualified certificates and signs them with its own private key, known as the "CA key" or "root key".
InfoCert is the Certification Authority (**CA**) responsible for issuing, publishing in the directory and revoking Qualified Certificates in accordance with the technical requirements issued by the Supervisory Authority and as prescribed by the eIDAS Regulation [1] and by the CAD [2].

Full details of the organisation acting as Certification Authority are as follows:

Company name	InfoCert – Società per azioni Company managed and coordinated by Tinexta S.p.A.

[1] The absence of this OID may lead to the inadequacy of online services offered in the specific Italian context. An example, in this sense, is the absence of the obligation to indicate in the qualified certificate for the generation of the signature the Tax Identification Number of the holder, an essential element for several Italian public administrations.

Registered office	Piazza Sallustio n.9, 00187, Rome, Italy
Head Office	Via Marco e Marcelliano n. 45 - 00147 Rome, Italy
Legal Representative	Danilo Cattaneo As Managing Director
Telephone number	06 836691
Companies Register Registration No.	Tax Identification Number 07945211006
VAT No.	07945211006
Website	https://www.infocert.it

1.3.2. Registration Authority

Registration Authorities are entities to whom the CA has issued a special representation mandate to perform one or more of the activities associated with the registration process, such as:

- Subject or Subscriber identification,
- registration of Subject data,
- forwarding of Subject data to the CA systems,
- collecting qualified certificate applications,
- distributing and/or initializing OTP code generation devices, where required by the process and according to contractual terms,
- activation of the public key certification procedure,
- providing support to Subject, Subscriber and CA during certificate renewal, revocation and suspension of the certificate.

A Registration Authority essentially performs all interface activities between the Certification Authority and the Subject / Subscriber based on applicable agreements. The representation mandate, known as "RAO Agreement", regulates the type of activities entrusted by the CA to the RA and the relevant operating procedures.
RAs are activated by the CA following adequate staff training. The CA verifies that the procedures used are compliant with the provisions of this Certificate Policy Statement.

1.3.2.1. Registration appointee

By completing the relevant forms provided by the CA, RAs may appoint natural or legal persons entrusted with performing Subject identification. Registration Appointees shall act in accordance with instructions received from the RA, to which they shall report and which shall supervise compliance of implemented procedures.

1.3.3. Subject

A Subject is a natural or legal person who holds a qualified certificate and whose basic identification data are included in the certificate. In some parts of this Certificate Policy Statement and in some use restrictions, he may be referred to as Holder.

1.3.4. Relying Party

A natural or legal person that receives an electronic document signed by means of the Subject's digital certificate and relies on the validity of such certificate (and/or on the digital signature affixed on it) to assess the accuracy and validity of the document in relation to the context in which the document itself is used.

1.3.5. Subscriber

A natural or legal person applying to the CA for issuance of a digital certificate to a Subject and that may, where appropriate, bear the costs of issuance and acquire the power to suspend or revoke the certificate. This role can be taken by the RA, where present.
Specifically, the following cases are possible:

- The Subscriber is the Subject itself, if the latter is a natural person;
- The Subscriber is a natural person requesting the certificate for a legal person on the base of adequate representation powers;
- The Subscriber is a legal person requesting the certificate on behalf of a natural person with whom it has business dealing or who is part of its organization.
- It can be the parent or the tutor in the case of minor over the age of 14 years.

The Subscriber may be the natural or legal person from whom derives the power of signature or the Subject's role. In this case, where the Subscriber is defined C*oncerned Third Party*, the Organization to which the Subscriber is connected and/or the role are mentioned in the certificate.
Unless otherwise specified in the contract, the Subscriber is the Subject itself.

1.3.6. Authority

1.3.6.1. Agenzia per l'Italia Digitale –Agency for Digital Italy AGID

Agenzia per l'Italia Digitale (AgID) is the supervisory board for trust service providers pursuant to Article 17 of the eIDAS Regulation. As such, AgID supervises qualified trust service providers established in the Italian territory to ensure that they meet the requirements laid down in the Regulation.

1.3.6.2. Conformity Assessment Body

The Conformity Assessment Body (CAB) is an accredited body under the eIDAS Regulation which is competent to assess the conformity of a qualified trust service provider and of the qualified trust services it provides with applicable regulations and standards.

1.3.6.3. National Competent Authority (NCA)

According to PSD2 [11], the national supervisory authority for financial intermediaries

is the body responsible for authorizing the PSPs of each Member State. If authorization is granted, the NCA issues an authorization number and publishes this information in its public registers.

1.3.6.4. European Banking Authority (EBA)

The European Banking Authority (EBA) works to ensure a uniform level of regulation and supervision in the European banking sector. According to PSD2 [11], it supervises and guarantees the transparency of the work of payment service providers (PSPs) authorized by the NCAs responsible for each Member State. It is responsible for the development and maintenance of the "Electronic Central Register", in which each NCA must publish the list of names and information related to authorized subjects.

1.4. Certificate usage

1.4.1. Permitted uses

Certificates issued by InfoCert according to the procedures set down in this Certificate Practice Statement are Qualified Certificates within the meaning of the CAD and of the eIDAS Regulation.
Certificates issued by the CA shall be used to verify the qualified signature or electronic seal of the Subject who owns the certificate.
For the signature verification, InfoCert provides some products available on the InfoCert website. Other verification software may be available on the market with features and limitations as specified by their manufacturer.

1.4.2. Prohibited uses

A certificate shall not be used outside the limitations and contexts set out in the Certificate Practice Statement and in the contracts and it shall not, in any case, be used in violation of mandatory use and value restrictions (such as key usage, extended key usage, user notice) reported in the certificate itself.

1.5. Management of the Certificate Practice Statement

1.5.1. Contacts

InfoCert is responsible for defining, updating and publishing this document. For questions, complaints, comments and requests for clarification regarding this Certificate Practice Statement, please contact:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telephone number: +39 06 836691

Fax: + 39 049 0978914
Digital signature call center: + 39 06 54641489
Web: https://www.firma.infocert.it

e-mail: firma.digitale@legalmail.it

Subjects and Subscribers may request a copy of their personal documentation by filling in and sending the form available on www.firma.infocert.it and following the given procedure. Documentation will be sent electronically to the email address indicated on the form.

1.5.2. Parties responsible for approving the Certificate Practice Statement

This Certificate Practice Statement has been approved by the Company's management following a review by the Head of Security and Policy, the Privacy Manager, the Head of Certification Services, the Legal Office and the Consultancy department.

1.5.3. Approval procedures

Drafting and approval of this Certificate Practice Statement are carried out in accordance with the procedures described in the Company's Quality Management System ISO 9001:2015.
At least once a year, the Trust Service Provider checks the compliance of this Certificate Practice Statement with its certification service process.

1.6. Definitions and acronyms

1.6.1. Definitions

For the purposes of this document, the following definitions apply. For terms defined by the eIDAS Regulation [1] and the CAD [2], please see the relevant definitions laid down therein.

TERM	DEFINITION
Self-certification	A signed statement personally submitted to the CA by the future Subject of the Digital Certificate, in which he confirms the existence of mandatory statuses, facts and capacities and accepts the responsibilities established by law.
CAB – Conformity Assessment Body	Body accredited under the eIDAS Regulation as competent to assess the conformity of a qualified trust service provider and of the qualified trust services he provides. It is

	responsible for drafting the CAR
CAR – Conformity Assessment Report	Report in which the Conformity Assessment Body confirms that the qualified trust service provider and its trust services comply with the requirements of the Regulation (see eIDAS [1]).
Card Management System (CMS)	Tool for authentication, identification, collection and storage of data relating to Subjects or Subscriber
Electronic Signature Certificate	Electronic certificate that links the validation data of an electronic signature to a natural person and confirms at least its name or pseudonym (see eIDAS [1])
Electronic Seal Certificate	Electronic certificate that links the validation data of an electronic seal to a legal person and confirms the name of that person (see eIDAS [1])
Qualified Electronic Signature Certificate	Electronic signature certificate that is issued by a qualified trust service provider and meets the requirements of the Annex I of eIDAS Regulation (see eIDAS [1])
Qualified Electronic Seal Certificate (QSealC)	Certificate for an electronic seal that is issued by a qualified trust service provider and meets the requirements of the Annex III of eIDAS Regulation (see eIDAS [1])
Qualified Electronic Seal Certificate for PSD2 (QSealC PSD2)	QSealC referred to in Article 34 Delegated Regulation (EU) 2018/389 [12], supplementing Directive (EU) 2015/2366 (PSD2) [11], in accordance with the requirements defined in the standard ETSI TS 119 495 (hereinafter as "QSealC PSD2")
LongTerm Certificate	Qualified certificate for qualified electronic signature for remote procedure. The use of this certificate is limited exclusively to an IT domain for which it was issued.
OneShot Certificate	Qualified certificate for a qualified electronic signature for remote procedure as defined by this Certificate Practice Statement whose keys, once generated, are available only in the context of an IT domain and exclusively for the signature transaction for which it was issued. Immediately after its use the private key is destroyed.

	This category also includes certificates named "short-term" pursuant to ETSI 319 411-1, whose validity period is shorter than the maximum time to process a revocation request as described in this CPS.
Certification key or root key	Cryptographic key pair used by the CA to sign certificates and lists of revoked or suspended certificates
Private Key	The asymmetric key pair element used by the Subject to place his Qualified Electronic signature on an electronic document (see CAD [2])
Public Key	The asymmetric key pair element intended to be made public. It is used to verify the Qualified Electronic signature applied to the electronic document by the Subject (see CAD [2])
Emergency Code (ERC)	Security code delivered to the Subject to submit a certificate suspension request through a TSP portal
Validation	The process by which signature validity is verified and confirmed (see eIDAS [1])
Validation data	Data used to validate an electronic signature (see eIDAS [1])
Personal identification data	Set of data used to determine the identity of a natural and/or legal person or of a natural person representing a legal person (see eIDAS [1])
Electronic signature creation data	Unique data used by the signatory to create an electronic signature (see eIDAS [1])
Electronic signature creation device (SSCD-secure system creation device)	Configured software or hardware used to create an electronic signature (see eIDAS [1])
Qualified electronic signature creation device (QSCD)	Device used to create an electronic signature that meets the requirements of Annex II of the eIDAS Regulation (see eIDAS [1]).
Electronic document	Any content stored in electronic form, especially text or sound, visual or audio-visual recording (see eIDAS [1])
Informatic Domain	It is identified with the applications through which the qualified certificate is issued to

	the Subject and within which the Subject can use the certificate to sign electronic documents. Applications can be managed directly by the Certifier or by the Subscriber and may also contain additional special provisions depending on the identification procedure adopted for the issue of the qualified certificate
Automatic signature	Special electronic signature procedure that is subject to authorization by the Subscriber. It enables the Subject to retain exclusive Control over its signature keys without requiring timely and continuous supervision from him
Digital signature	Special type of qualified electronic signature based on a qualified certificate and on a system of correlated cryptographic keys that consist of a public key and a private key and through which the Subject (by means of the private key) and the recipient (by means of the public key) can view and verify the origin and integrity of an electronic document or a set of electronic documents (see CAD [2])
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and is used by the signatory to sign a document (see eIDAS [1])
Advanced electronic signature	An electronic signature which meets the requirements set out in Article 26 of the eIDAS Regulation (see eIDAS [1])
Qualified electronic signature	An advanced electronic signature which is created by a qualified electronic signature creation device, and that is based on a qualified electronic signature certificate (see eIDAS [1])
Remote signature	A special, HSM-generated qualified electronic signature or digital signature procedure which ensures exclusive control of private keys by their owners
Signatory	A natural person who creates an electronic signature (see eIDAS [1])
Audit log	The set of automatic or manual entries of

	events provided for in the Technical Requirements [9]
Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person (see eIDAS [1])
Certificate Revocation List (CRL)	List of certificates that have been made "invalid" before their natural expiry. Revocation is permanent, whereas suspension is temporary. When a certificate is revoked or suspended, its serial number is added to the CRL, which is then published in the public register
Certificate Practice Statement	The Certificate practice statement sets out the procedures applied by the CA in carrying out its service. In drafting it, consideration has been given to the Supervisory Authority guidelines and international literature.
Electronic identification means	A material and/or immaterial unit containing personal identification data, and which is used to access online services (see eIDAS [1])
Online Certificate Status Protocol (OCSP)	Protocol defined by IETF in RFC 6960. It enables applications to verify a certificate's validity in a faster and more accurate manner than CRL, which it shares data with
One-time Password (OTP)	A One-Time Password is a password which can only be used for a single transaction. OTPs are generated and made available to the Subject immediately before he places his Qualified Electronic Signature. OTPs can be based on hardware devices or software procedures
Relying Party	A natural or legal person relying on an electronic identification or a trust service (see eIDAS [1])
Trust service provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider (see eIDAS [1])
Qualified trust service provider	A trust service provider who provides one or more qualified trust services. Its qualified

	status is granted by the supervisory body (see eIDAS [1])
Product	Hardware or software or their relevant components which are intended to be used for provisioning of trust service (see eIDAS [1])
Public Official	A person who, as part of his or her duties, is authorized under applicable laws to certify the identity of natural persons
Directory	A directory is a file containing: ▪ all certificates issued by the CA for which the Subject has requested publication; ▪ the list of revoked and suspended certificates (CRL)
Certificate revocation or suspension	Action by which the CA invalidates a certificate before its natural expiry
Role	'Role' generically refers to a professional title and/or qualification held by the Subject or to the power to represent natural persons or private or public law entities, or to the membership of said entities as well as the exercise of public functions
Trust service	An electronic service normally provided for remuneration which consists of: a) the creation, verification and validation of electronic signatures, seals or time stamps, certified electronic delivery services and related certificates, or b) the creation, verification and validation of certificates for Website authentication, or c) the preservation of electronic signatures, seals or certificates related to those services (see eIDAS [1])
Qualified trust service	A trust service that meets the applicable requirements laid down in the Regulation (see eIDAS [1])
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity (see eIDAS [1]).
Advanced electronic seal	An electronic seal, which meets the requirements set out in Article 36 of eIDAS

	Regulation (see eIDAS [1]).
Qualified electronic seal	An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal (see eIDAS [1]).
Member State	Member State of the European Union
Coordinated Universal Time	Time scale with second precision as per ITU-R Recommendation TF.460-5
Electronic time stamp	Data in electronic form which binds other data in electronic form to a particular time and date establishing evidence that the latter data existed at that time (see eIDAS [1])
Qualified electronic time Stamp	An electronic time stamp which meets the requirements laid down in Article 42 of eIDAS Regulation (see eIDAS [1])
Webcam	Small-sized camcorder designed to stream images through the Internet and to capture pictures. If connected to a PC or embedded in a mobile device, it can be used for video chats or videoconferencing.

1.6.2. Acronyms and abbreviations

ACRONYM	MEANING
AgID	Agenzia per l'Italia Digitale: Supervisory Authority for Trust Service Providers
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale (Digital Administration Code)
CAR	Conformity Assessment Report
CC	Common Criteria
EIC	Electronic Identity Card
CMS	Card Management System
CNS - TS-CNS	National Service Card Health Card – National Service Card
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguished Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority

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: secure signature creation device with similar features to those of a smart card, but with superior memory and performance features
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Registration Appointee
ISO	International Organization for Standardization: Established in 1946, the ISO is an international organisation made up of national standardisation bodies
ITU	International Telecommunication Union: established in 1865, it is the international organisation that deals with defining telecommunications standards
IUT	Subject Unique Identifier: a code associated with the Subject, which identifies him unambiguously in CA systems. A Subject will have different codes for each certificate held
LDAP	Lightweight Directory Access Protocol: the protocol used to access the Certificates Registry
LoA	Level of Assurance
NCA	National Competent Authority
NTR Code	National Trade Register Code
OID	Object Identifier: a sequence of numbers registered according to the procedure given in ISO/IEC 6523, and which references a specific object within a hierarchy
OTP	OneTime Password
PEC	Posta Elettronica Certificata (Certified e-mail)
PIN	Personal Identification Number: code associated with a secure signature device and used by the Subject to access the

	functions of such device
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure: a set of resources, processes and technologies enabling trusted third parties to verify and/or guarantee a Subject's identity and to bind a public key to a Subject
PSD2	Payment Services Directive 2
PSP	Service Payment Provider
QSealC	Qualified electronic Seal Certificate
RA	Registration Authority
RFC	Request for Comment: Document containing specific information concerning new IT research, innovation and methodologies, and which is submitted for peer review by its drafters
RSA	An algorithm named after the initials of its authors, i.e. River, Shamir, Adleman
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni (Information security management system)
SPID	Sistema Pubblico di Identità Digitale (Public Digital Identity System)
SSCD – QSSCD	Secure Signature Creation Device: electronic signature creation device; Qualified Secure Signature Creation Device: qualified electronic signature creation device
TIN	Tax Identification Number
UUID	Universally unique identifier
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X500	ITU-T standard for LDAP and directory services
X509	ITU-T standard for PKIs

2 PUBLICATION AND REPOSITORY

2.1. Repository

Issued certificates, CRLs and Certificate Practice Statements are published and available 24 hours a day, 7 days a week.

2.2. Publication of certification information

2.2.1. Publication of the Certificate Practice Statement

This Certificate Practice Statement, the list of certificates of the certification keys and other information about the CA provided by law are published in the certification authorities list (at https://eidas.agid.gov.it/TL/TSL-IT.xml)and at the Certification Authority website (see § 1.5.1).

2.2.2. Certificate Publication

A Subject – or a Subscriber acting as the legal representative of a legal person – who wishes to publish his or her certificate may apply for certificate publication through the dedicated form available at www.firma.infocert.it. This form shall be digitally compiled and signed with the key matching the certificate to be published and submitted by e-mail to richiesta.pubblicazione@cert.legalmail.it following the procedure described on the site. This procedure is not provided for the LongTerm and OneShot Certificates.

2.2.3. Publication of revocation/suspension lists

Revocation and suspension lists are published in the certificate public registry, accessible via the LDAP protocol or via HTTP protocol as indicated in the “CRL Distribution Points” of the certificate. Lists can be accessed through the software provided by the CA and/or through compliant products available on the market that can interpret LDAP and/or HTTP protocols.
The CA may provide additional access options to consult the list of published certificates and their validity.

2.3. Period or frequency of publication

2.3.1. Frequency of publication of the Certificate Practice Statement

Frequency of publication of the Certificate Practice Statement varies to reflect any changes that have occurred. For major changes, the CA must undergo an audit by an accredited CAB, submit the certification report (*CAR—Conformity Assessment Report*) and the Certificate Practice Statement to the Supervisory Authority (AgID) and wait for a publication permission to be granted.

2.3.2. Frequency of publication of revocation/suspension lists

CRLs are published every hour.

2.4. Controlling access to public archives

Information on issued certificates, CRL and Certificate Practice Statements are public. The CA has not restricted read access and has implemented all necessary countermeasures to avoid unauthorised changes/cancellations.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The Subject is identified in the certificate through a Distinguished Name (DN), an attribute which must contain a value and comply with the X500 standard. Certificates are issued according to the RFC-5280 specification, ETSI EN 319 412 from 1 to 5.
However, ETSI standards EN 319 412-2 section 4.2.4 and 319 412-3 section 4.2.1 allow for both natural person and legal entity certificates to be longer than laid down in RFC specification 5280 for the givenName, surname, commonName fields.
In accordance with this derogation, the following maximum limits have been set: 40 characters for givenName and surname, 81 characters for commonName.
Depending on the context, the provisions of AgID Determination 147/2019 [13] or those of other countries apply as long as they do not conflict with the eIDAS Regulation [1].

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity and pseudonymity of Subscribers

Only in case of identification performed through Method 1_LiveID (see § 3.2.3.1) the Subject can request to the CA that a pseudonym is shown on his or her certificate instead of his or her actual name. This possibility is not expected in the LongTerm and OneShot Certificates.

As the certificate is qualified, the CA will retain all information regarding the Subject's real identity for twenty (20) years after certificate issuance.

3.1.4 Rules for interpreting various name forms

InfoCert adheres to the X500 standard.

3.1.5 Uniqueness of names

Natural Person Subject:

To ensure unambiguity of the Subject, the certificate shall include the name and surname of the Subject and a unique identifier, such as: normally the TIN (Tax Identification Number) is used. TIN code is either assigned by the authorities of the country of which the Subject is a citizen or by those of the country where the Subject's organisation has its registered office. For Italian citizens, the unique identifier code is the Tax Code (Codice Fiscale).

In absence of a TIN or Tax Code, the certificate may display:

- an identifier code taken from a valid identity document, which has been used in identification procedures. The format is provided by the std ETSI 319 412-1
- a unique identifier determined by the CA. The format used in this case is UUID (Universal Unique Identifier) of type 4 described in RFC4122.
- a unique identifier as described in EIDAS eID profile within the EIDAS cooperation network. The reference document is "eIDAS SAML AttributeProfileVersion" ver 1.2. (Https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile)

  However, since the TIN is used by all Italian public administrations as identification of the citizen and of the taxpayer, the failure to indicate it within the signature certificate entails the inadequacy of the same towards the Italian Public Administration.

Legal Person Subject:

In the case of a legal person, to ensure unambiguity of identity data, the certificate shall include the name of the organisation and a unique identifier, such as:

- VAT number (Value Added Tax Number)
- NTR (National Trade Register)
- LEI (Legal Entity Identifier)

In the case of Italian legal entities, the identification code uses the VAT number or the Business Register Number. If the organization does not have a VAT number or NTR, but only a Tax Code, it is possible to use the two characters "CF" followed by ": IT-" (example: CF:IT-97735020584), as required by AgID determination no. 147/2019 [13].

3.1.6 Recognition, authentication and role of trademarks

When requesting a certificate to the CA, the Subject and the Subscriber shall ensure that they fully comply with national and international intellectual property laws.
The CA shall not verify the use of trademarks and may refuse to generate or may request to revoke any certificates involved in a dispute.

3.2 Initial identity validation

This chapter describes the procedures used to identify the Subject and the Subscriber upon submission of a request for qualified certificate issuance.
An identification procedure entails Subject recognition by the CA, including through the RA or its appointees, who shall verify the identity of the Subject according to one of the methods set out in the Certificate Practice Statement.

3.2.1 Method to prove possession of private key

InfoCert determines that a Subscriber has possession or control of the private key corresponding to the public key which has to be certified, by verifying the signature of the certificate request through the private key corresponding to the public key which has to be certified.

3.2.2 Authentication of organisation identity

See § 3.2.4.

3.2.3 Authentication of a natural person

Without prejudice to the CA's responsibility, the identity of the Subject can be verified by entities authorised to perform recognition according to the following methods pursuant to eIDAS article 24:

Method	Entities authorised to perform identification	Authentication tools supporting the identification phase
1-LiveID	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee • Public Official • Employer (for identification of its employees, contractors, agents)	N/A
2-AMLID	Entities subject to the obligations under Anti-Money Laundering laws transposing Directive 2005/60/EC of the 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 EU implementing legislation.	N/A
3-SignID	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee	Use of a qualified electronic signature issued by a qualified Trust Service Provider
4-AutID	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee	Use of a pre-existing means of electronic identification
5.1 Attended VideoID	• Certification Authority (CA) • Registration Authority (RA)	N/A

	• Registration Appointee	
5.2 Unattended VideoID	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee	N/A
5.3 Semi-automatic VideoID (SelfQ)	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee	N/A
6 eDocId	• Certification Authority (CA) • Registration Authority (RA) • Registration Appointee	Use of a pre-existing means of electronic identification
7 ContoID	• Certification Authority (CA)	Strong Customer Authentication for bank account access

The Addendum [14] includes a list of Italian and foreign identity documents that are considered acceptable for the correct identification of the Subject within the qualified electronic signature certificates issuing processes.

3.2.3.1 Recognition through Method 1 – LiveID

The **LiveID** identification method requires an in-person meeting between the Subject and one of the subjects entitled to perform the recognition.
Identity verification involves production by the Subject of one or more valid identity documents in original version, as mentioned in the list of accepted documents available on the CA website[2].
To ensure the uniqueness of the Subject and its name, the latter must also be in possession of the unique identifier as per § 3.1.5. The person authorized to perform the recognition can request the presentation of documentation proving the possession of this unique identifier, if they find inconsistencies compared to the applicant's statement.
The Certification Authority (InfoCert) may authorise Registration Authorities operating abroad or that are otherwise responsible for identifying Subjects residing abroad to accept identity documents issued by EU Member States authorities, as mentioned in the list of accepted documents available on the CA website.
Identification may also be performed by a Public Official as provided for in applicable laws. The Subject fills out the request for certification and signs it in front of a Public Official. The Subject's signature is then authenticated by the Public Official according to existing regulations. The application is then submitted to the CA or to an enabled

[2] The list of accepted recognition documents is drawn up by the CA after analysing the documents and their objective characteristics of identity certainty and security in the issuing process by the Issuing Authority. The list is notified to AgID and updated every time a modification occurs.

Registration Authority.
Identification previously performed by an employer for the definition of an employment contract shall be considered a valid LiveID identification by the CA (Employee_ID) after verification of the identification and authentication procedures applied. Similarly, identification performed according to the recognition methods described below by an employer as part of the activation of agency relationships shall be considered a valid LiveID identification after verification of the identification and authentication procedures applied.
Under this identification method, the employer acts as a Registration Authority appointed by the Certification Authority with a specific mandate[3]. Certificates issued under this identification method may only be used for the employment purposes for which they were released and are subject to specific use restrictions.
Registration data gathered in LiveID mode are stored by the Certification Authority in analogical or electronic format.

3.2.3.2 Recognition through Method 2 – AMLID

Under the **AMLID method**, the Certification Authority draws on identification performed by an Entity subject to Identification and Adequate Verification obligations under applicable laws implementing Directive 2005/60/EC of the European Parliament and of the Council on the prevention of use of the financial system for the purpose of money laundering and terrorist financing, and subsequent additional Community implementing legislation.
Specifically, in the Italian context, data used for recognition is provided by the Subject according to Legislative Decree No. 231/2007, as amended, which requires Subjects to provide – on their own responsibility – all necessary and updated information to enable the parties, subject to the obligations set out in the aforementioned Decree, to perform their client identification duties.
Under this identification method, the parties subject to the above-mentioned obligations act as Registration Authorities appointed by the Certification Authority with a specific mandate. Subject identification data collected upon recognition are stored by the Certification Authority, typically in electronic form or optionally in analogical form.

3.2.3.3 Recognition through Method 3 – SignID

With **Method 3 SignID**, the CA relies on recognition previously carried out by another CA that issues qualified certificates (QTSP). The Subject already has a valid qualified certificate which he uses in his relationships with InfoCert. In this case, registration data

[3] Prior to issuing the mandate, the CA carries out a careful security assessment of employee identification procedures and of the way in which personal identification tools are managed and assigned to the employee in order to allow the latter (and/or agent or retired employee) to access the computer systems through which the digital signature certificate application is submitted to the CA. The cases concerned shall be notified to the Supervisory Authority.

are stored solely in electronic format.
A request for a certificate may only be made in SignID mode if the qualified certificate used to sign such a request has not been issued in SignID mode.

3.2.3.4 Recognition through Method 4 – AUTID

Under the **AutID method 4**, the recognition is based on a pre-existing means of identification:

- Notified by the Member State pursuant to Article 9 of the eIDAS Regulation, level high;
- Notified by the Member State pursuant to Article 9 of the eIDAS Regulation, level substantial, as long as it gives an equivalent guarantee of reliability in terms of physical presence;
- Not notified and issued by a public authority or by a private entity, as long as it gives a guarantee equivalent to physical presence in terms of reliability and this is confirmed by a conformity assessment body.
- issued by a public authority or a private entity, further confirmed by the Holder by authentication to its payment account performed by means of Strong Customer Authentication (SCA) through a Payment Service Provider (PSP), in accordance with EU Directive 2015/2366 (PSD2).

With specific reference to the interoperability framework defined by article 12 of the eIDAS Regulation, the message returned by the EIDAS node upon use of a notified national identification system, of at least substantial level, is considered sufficient for the issuance of a qualified certificate. The message is of SAML type, as provided for by CEF (Connecting Europe Facility) specifications within the CEF eID programme[4], and is sent to the CA by the subject managing the national node, or by one of the subjects authorised to use the node itself. The CA verifies the integrity of the received SAML message and considers the subject identified on the basis of the data contained in the message itself.

With specific reference to the Italian context, the CNS card (National Service Card) or TS-CNS (Health Card - National Service Card), the EIC (Electronic Identity Card), the electronic residence permit and the identities released by the SPID system are electronic identification means.

The means of electronic identification that can be used by the CA and the RAs are listed

[4] These specifications are available at the following link https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile

and published on the CA website, and notified to AgID.

InfoCert will evaluate the possibility of making use of identifications made by subjects in possession of a certification issued by a CAB which certifies that the identification method used complies with the Art. 24 letter d) eIDAS.

3.2.3.5 Recognition through Method 5 – VideoID

The **VideoID method** requires Subjects to be equipped with an internet-enabled device (such as a PC, smartphone, tablet, etc.), a webcam and a working sound system.

The VideoID method can be configured alternatively:

5.1. with the simultaneous presence of the Registration Appointee and the Subject or Subscriber within the same audio-video session (attended VideoID). The Registration Appointee, properly trained, shall verify the identity of the Subject or of the Subscriber by comparison with one or more valid ID documents showing a recent and recognisable photograph of the Subject. For reasons of security and fraud prevention, only conventional ID documents (such as ID cards, driving licences and passports) can be accepted under this recognition method, as mentioned in the list of accepted documents available on the CA website[5].

5.2. without the simultaneous presence of the Registration Appointee and the Subject or Subscriber within the same audio-video session. Under this scenario, the Subject autonomously carries out the audio-video session and, as a confirmation of his/her identity, makes a bank transaction from a bank account in his/her name or co-owned by him/her, indicating in the reason for payment the specific correlation code provided by the CA or RA. In a subsequent backoffice phase, the Registration Appointee checks the audio-video session, the coincidence between the account holder of the bank transfer and the Subject's data, and the correctness of the correlation code, and, in the event of successful checks, proceeds to validate the identity (unattended VideoID).

5.3. without the simultaneous presence of the Registration Appointee and the Subject or Applicant within the audio-visual session, with automated validation tools (SelfQ). Under this configuration, the Subject is guided through a procedure of collecting a copy of the identity document and a face capture automated

[5] The list of accepted identification documents is drawn up by the CA after analyzing the documents and their objective characteristics of identity certainty and security in the issuing process by the Issuing Authority. The list is notified to AgID and updated with each change. For security reasons and anti-fraud procedures, the type of documents accepted by this mode is limited to the most common identity documents.

procedure (so-called "video-selfie"), where he/she performs some random reinforcement actions. CA applies document validation technologies to verify the authenticity of the presented identity document, extracts its data and face photo, and finds that it really belongs to the Subject by using one or more biometric technologies to compare the extracted face photo and the collected video-selfie. If the index of compatibility (so-called "scoring") does not yield a sufficient result, a Registration Appointee performs a further manual review.

Additionally, video identification can take place following the operating and process methods approved by a different Supervisory Body notified to the Commission in accordance with Article 17 of the eIDAS Regulation in compliance with the corresponding applicable national law pursuant to article 24 of the eIDAS Regulation, and provided that they do not violate Italian law[6].

The Certification Authority may authorise Registration Authorities operating abroad or which are otherwise responsible for identifying Subjects residing abroad, to accept identity documents issued by EU Member States authorities, after reviewing the objective characteristics of such documents in terms of certainty of identification, security of the Issuing Authority's issuance process and specific training[7].
ID documents used by the Subscriber that are not compliant with the above requirements may be rejected by the RA or the Registration Appointee. Registration data – namely audio and video files and structured metadata in electronic format – are stored in protected form.

3.2.3.6 Recognition through Method 6 – eDocID

In eDocID method 6, the Subject is in possession of an Internet-connected device, equipped with a webcam and a proximity reader, and shows a machine readable identity document for biometric identification[8].By framing the document with the camera and placing it close to the proximity reader, the Subject allows access to the electronic memory of the chip, from which the identification data and photo contained therein are extracted; the Subject is also guided through an automatic video-selfie procedure, during which he performs some random additional actions, following the instructions of the procedure provided by the CA.
The CA checks the authenticity of the technical signature on the data and photo extracted from the identity document, and checks that they really correspond to the

[6] Said cases will be notified to the Supervisory Body.

[7] The cases concerned will be notified to the Supervisory Authority.

[8] These are documents complying with ICAO standards with MRZ, or otherwise having compatible security features.

Subject by using one or more biometric technologies to compare the extracted photo with the collected video-selfie. If the scoring is insufficient, a Registration Appointee will carry out a subsequent back-office identity check.
The registration data, consisting of audio-video files and electronic structured metadata, are securely stored.

3.2.3.7 Recognition through Method 7 – ContoID

In Method 7 ContoID, the Subject is in possession of an Internet-connected device equipped with a webcam and presents a valid identity document for identification.
By framing the document with the camera, the Subject is guided through a procedure for collecting a copy of the identity document so that the relevant identification data and photo can be extracted. The Subject is also guided in an automatic procedure of filming his/her face (so-called "video-selfie"), during which he performs some random reinforcement actions, following the instructions of the procedure set up by the CA.
CA checks that the document really belongs to the Subject by using one or more biometric technologies to compare the extracted photo and the collected video-selfie; it also verifies that the account header data correspond to the Subject's own data.
The Subject confirms its data by authentication to its payment account performed by means of Strong Customer Authentication (SCA) by a Payment Service Provider (PSP), in accordance with EU Directive 2015/2366 (PSD2).
The registration data, which consist of video files and structured metadata in electronic format, are stored in a secure form.

3.2.4 Non-verified Subject or Subscriber information

The Subject may – either directly or with the consent of any Concerned Third Party - obtain the inclusion of the following information in the certificate:

- Titles and/or professional qualifications;
- Representation powers of natural persons;
- Representation powers of legal persons or membership in such legal persons;
- Exercise of public duties, representation powers of organisations and public law bodies or membership in such organisations/bodies.

Certificates showing the Role information shall comply with the recommendations of AgID determination no.147/2019 [13].
The Subject shall produce an appropriate statement (including a self-certification) to

demonstrate that the Role specified in the certificate exists[9]. Except in cases of wilful misconduct or gross negligence, the CA assumes no responsibility regarding any self-certified information included by the Subject in the certificate.
However, where the Organisation has authorised issuance of a certificate to the Subject, its company/corporate name and corporate ID shall be included in the certificate even if the latter contains no Role information. In this case, the CA shall check Subject-submitted documentation for formal validity. Requests for certificates containing Role and/or Organisation information may only be submitted by organisations with a defined legal form.

3.2.5 Validation of authority

The CA or the RA check the required identification information, as defined in paragraphs 3.2.2, 3.2.3 and 3.2.4, and validate the request.
The CA or RA, where provided for or necessary, may use public databases to validate the information provided by the applicant.

In case of QSealC PSD2 request, the CA or RA verifies the specific attributes provided by the Applicant (authorization number, name and state of the NCA, role of the PSP) using the authentic information made available by EBA in its central registry or possibly in the registers made available by the NCAs of each member state.
If the national NCA has provided rules for the validation of these attributes, the TSP applies the rules indicated.

3.3 Identification and authentication for renewal or re-issue with new keys

This section describes the procedures used to authenticate and identify the Subject when they request a renewal of their certificate or a re-issue of the same with new and different encryption keys.

3.3.1 Identification and authentication of a Subject for re-issue with new keys

The re-issuing of a certificate with new keys can be carried out before the certificate expires, i.e. when "not after" is subsequent to the date of the request; using the tools provided by the CA, the Subject may make the request, signed with the private key corresponding to the public key contained in the certificate already in their possession. In this case we can also call it **renewal with re-certification of new keys**.

The Subject may request a re-issue of the certificate even after the expiry of the previous certificate, i.e. when “not after" is prior to the date of the request. The certifier can use the recognition of the

[9] If the request to include the Role into the certificate has been made through the sole Subject’s self-certification, the certificate cannot show information regarding the organization to which the Role is connected.

Subject and the secure link established previously between the Subject's credentials and their recognition. This link is ensured by the double authentication factor that was associated to the subject itself during recognition.

The recognition is kept valid for a maximum of four years but only if the applicant's identity documents or further attributes linked to Subject's identity have not expired in the meantime.

The certifier may decide for information security or fraud issues, to invalidate the recognition even before the 4 years have elapsed.

3.3.2 Identification and authentication of a Subject for re-issue with new keys after revocation

N/A

3.3.3 Identification and Authentication of a Subject for renewal of certificates

This paragraph describes Subject authentication and identification procedures used to process qualified signature certificate renewal requests, keeping the same encryption keys.
The certificate validity period is indicated in the "Validity" field of each certificate by the "Not Before" and "Not After" attributes. Outside this date range (including hours, minutes and seconds) a certificate shall be considered invalid.
A Subject may however renew his certificate before it expires by using the tools provided by the CA. The renewal request is signed with the private key whose corresponding public key is contained in the certificate to be renewed. A certificate may not be renewed after its revocation or expiry and a new certificate needs to be issued instead.

3.4 Identification and authentication for revocation or suspension requests

Certificate revocation or suspension may take place by authenticated request of the Subject or the Subscriber (or the Concerned Third Party, where the latter has agreed to inclusion of Role information in the certificate), or on the initiative of the CA.

3.4.1 Request by the Subject

The Subject may request revocation or suspension by completing and signing, even digitally, the form available on the CA website (see § 4.9).
If the revocation request is made through an Internet form, the Subject authenticates himself with the emergency code received upon certificate issuance or through any other authentication method described in the contract received upon registration.
The subject in possession of a remote signature can also request revocation using his private area which he/she can access through a two-factors authentication system (§ 4.2.2)
If the request is made at a Registration Authority office, the Subject's authentication is performed through the identification method.

If the Subject is a legal person, the request for revocation or suspension must be made by a legal representative or a person having a suitable power of attorney.

3.4.2 Request by the Subscriber

A Subscriber or a Concerned Third Party requesting revocation or suspension of a certificate held by a Subject shall authenticate himself by signing the Request for Revocation or Suspension Form provided by the CA. The request shall be forwarded as specified in paragraph § 4.9.3 or 4.9.15.2. The Certification Authority reserves the right to set out additional methods for submission of revocation/suspension requests by the Subscriber, that need to be agreed with the Subscriber itself.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Applications for qualified certificates for natural persons may be submitted by:

- The Subject,
  - either directly to the CA on www.firma.infocert.it; or
  - through a Registration Authority.
- The Subscriber on behalf of the Subject,
  - either directly to the CA on www.firma.infocert.it or by entering into a commercial agreement with the CA; or
  - through a Registration Authority; or
  - signing the mandate with representation with the CA and becoming Registration Authority within an IT domain.

Applications for qualified certificates for legal persons may be submitted by:

- The Subscriber who represents the legal person,
  - either directly to the CA on www.firma.infocert.it or by entering into a commercial agreement with the CA;
  - Through special Registration Authorities specifically instructed to issue such certificates.

4.1.2 Registration process and responsibility

The registration process includes: Subject application, generation of key pair, public key certification request, and signature of the contract (not necessarily in that order).

Each party involved in the process has specific responsibilities and jointly contributes to successful certificate issuance:

- The Subject is responsible for providing correct and truthful information on his identity, reading carefully the material made available by the CA – including through the RA – and following CA and/or RA instructions while submitting a qualified certificate application. If the Subject is a legal person, those responsibilities fall on the legal representative or the attorney who submits the qualified certificate application;
- The Subscriber, if present, is responsible for informing the Subject on whose behalf he is requesting a certificate about the obligations arising from the certificate, as well as for providing correct and truthful information about the identity of the Subject and for following processes and indications given by the CA and/or RA;

- The Registration Authority, if present, is responsible for – including through the Registration Appointee – the Subject/Subscriber identification, informing the subjects about the obligations arising from the certificate and following in detail the processes defined by the CA;
- The Certification Authority is ultimately responsible for Subject identification and successful registration of the qualified certificate.

If the Subject is a legal person, when the keys are generated in a Subject's device, the Subscriber must also send the request in PKCS#10 format signed by the Subscriber itself.

4.2 Certificate application processing

To obtain a signature certificate, the Subject and/or Subscriber must:

- Read carefully this Certificate Practice Statement, the contract documents and any additional information folders;
- Comply with the identification procedures adopted by the Certification Authority as described in paragraph 3.2.3;
- Provide all information required for identification together with any appropriate documentation (when required);
- Sign the registration and certification request and accept the contractual terms governing service provision, using the relevant analogical or electronic forms prepared by the CA.

4.2.1 Performance of identification and authentication functions

4.2.1.1 Natural person

In case of a certificate requested for a natural person the following information must be provided by the Subject and/or Subscriber:

- Surname and Name
- Date and Place of Birth;
- Tax Code or similar identification code (TIN), or, in its absence, a similar identification code such as the number of the identity document; in cases where the country's privacy legislation does not allow public use of this information, InfoCert will not include it in the certificate.
- Residence address;
- References of the ID proof used for identification (e.g. document type, number);
- An e-mail address for submission of communications from the CA to the Subject;
- A mobile phone number, for emergency contacts and for transmission of the

OTP, where this OTP technology is used.

The e-mail address and mobile phone number provided to the RA, shall be valid and shall uniquely identify the Subject. The e-mail address shall be used for any communications from the RA and for sending emergency codes (ERCs) and expiry notices. This specification is not applicable in the case of LongTerm and OneShot certificates.

Optionally, the Subject (or Subscriber) may provide an alternate name by which he is commonly known, to be entered in a special field of the certificate SubjectDN called commonName. If no alternate name is provided by the Subject and/or by the Subscriber, the commonName field will be filled in with the Subject's name and surname.

4.2.1.2 Legal person

In case of a certificate requested for a legal person the following information must be provided by the Subscriber that acts as legal representative or attorney of the legal person:

- Surname and Name of the Subscriber;
- Tax Code or similar identification code (TIN) held by the Subscriber;
- References of the document ID used for Subscriber identification (e.g. document type, number, issuer and date of issue);
- An e-mail address for transmission of communications from the CA to the Subscriber;
- Name of the Subject (legal person);
- VAT Number or Company Registration Number for Italian Subjects, VAT Code or NTR for foreign Subjects.

In case of a legal person wishing to certify its key pair, the Subscriber shall also send the application in PKCS#10 format signed by the Subscriber itself.
The information provided is stored in the CA archives (registration phase) and serves as a basis for generating the qualified certificate.

In case of a QSealC PSD2 request, the subject (PSP), identified as the legal representative or a natural person with a power of attorney, must provide the following additional information:

- authorization number that uniquely identifies the payment service provider (PSP);
- role(s) of the payment service provider (PSP);
- the name and state of the competent national authority (NCA) that has authorized payment service provider (PSP) and has issued the number of authorizations.

4.2.1.3 Registration

During the initial registration phase and collection of the registration and certification request, the Subject or Subscriber (legal representative of the legal entity) is provided with the security codes required to activate the signature device or the signature procedure, if remote, and to request suspension of the certificate (ERC code or similar code, if provided for in the contract). Said security codes are delivered electronically and transmitted in encrypted files.

The issue of security codes delivered in sealed envelopes is being discontinued. It may only be used in rare cases where the electronic mode cannot be used.

The CA may provide that the signature PIN is chosen autonomously by the Subject or by the Subscriber legal entity's legal representative; In such cases, the Subject or the Subscriber shall remember the PIN.

The CA may also provide that the signature certificate for remote procedure can be used by means of an authentication system provided by the RA, having a security level that is at least substantial or high upon analysis of the features of the system itself, within the certification perimeter of the secure signature device. In the aforementioned cases the authentication system can also be used for a possible certificate suspension and revocation request.

4.2.2 Approval or rejection of certificate applications

Following initial registration, the CA or RA may refuse to complete the issuance of a signature certificate due to lack of or incomplete information, consistency and anti-fraud checks, where the identity of the Subject/Subscriber is unclear etc.

4.2.3 Maximum time for processing certificate application

The time lag between registration application and certificate issuance depends on the application method chosen by the Subject (or by the Subscriber) and on whether any additional information needs to be collected or the device is to be physically delivered.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Certificates issued on a signature device (smartcard or token)

The RA generates the cryptographic key pair directly on a secure signature device using the applications supplied to it by the CA after secure authentication.
The RA sends the Certification Authority a public key certification request in PKCS#10 format. The request is digitally signed with a specially authorised, qualified signature

certificate. After confirming that the signature on the PKCS#10 is authentic and that the subject is entitled to submit the request, the Certification Authority generates a qualified certificate that is sent through a secure channel located inside the device.

4.3.1.2 Certificates issued on a remote signature device (HSM)

The Subject or the Subscriber log on to the RA services or applications.
The RA generates the cryptographic key pair directly on the HSM located at the QTSP premises. Then the RA sends to the Certification Authority a public key certification request through a secure channel.
After confirming that the subject is entitled to submit the request, the Certification Authority generates a qualified certificate that is stored in the HSM.

4.3.1.3 Certificates issued through a Card Management System

The RA generates the cryptographic key pair directly on the device by means of an authenticated Card Management System. The system, which manages the complete lifecycle of the cryptographic device, sends the digitally signed public key certification request to the Certification Authority in PKCS#10 format. The request is sent through a secure and authenticated channel.
After confirming that the signature on the PKCS#10 is authentic and that the subject is entitled to submit the request, the Certification Authority generates a qualified certificate that is sent through a secure channel located inside the device.

4.3.1.4 Certificates issued to legal persons

The RA generates the cryptographic key pair directly on the HSM. Then the RA sends the Certification Authority a public key certification request in PKCS#10 format. The request is digitally signed with a specially authorized, qualified certificate used for automatic signature.
After confirming that the signature on the PKCS#10 is authentic and that the subject is entitled to forward the request, the Certification Authority generates the qualified certificate, which is then stored in the HSM.
If the key pair is generated inside the HSM device of the Subject, the PKCS#10 is signed and sent by the Subject itself. The Certification Authority, after confirming that the signature on the PKCS#10 is authentic and that the subject is entitled to forward the request, generates the qualified certificate, which is stored in the HSM.

4.3.1.5 Issue of certificates for testing purposes

Sometimes it is necessary to use certificates to perform some tests in a production environment.
In these cases, before issuing the certificate it is necessary to proceed with the registration of the data. This registration must be approved by the Head of the CA.
In the foreseen cases, the Registration Office must be the Office used by InfoCert for internal issues, or the Office used by the Customer's procedure subject to a test session.

The data used for registration must clearly indicate in the Subject that it is a test certificate and not an actual certificate.
This procedure cannot be used for load tests or cyclic tests on registrations and emissions. When the specific test session is no longer needed, the certificate must be revoked ex officio.

4.3.2 Notification of certificate issuance to Subscribers

If the certificate is issued on a cryptographic device, the Subject (or the Subscriber) does not need to be notified of the certificate issuance as the certificate is stored in the device delivered to him.

In the case of LongTerm and OneShot certificates, the CA notifies the Subscriber with an automated procedure that the Subject's certificate has been issued. The Subscriber shall inform the Subject according to the forms and methods provided for in the contract.
In other cases, the Subject will receive the notification via the email address indicated at the time of registration. This information can also be shared with the Subscriber.

4.3.3 Activation

4.3.3.1 Activation of the signature device (smartcard o token)

After receiving the device, the Subject, using the activation codes confidentially given to him and the special software provided by the CA, proceeds to activate the device choosing at the same time a signature PIN, a confidential security parameter whose secrecy and protection are placed exclusively on the Subject itself.

4.3.3.2 Activation of remote signature device (HSM)

After logging on to the CA website using the activation codes confidentially given to him, the Subject – or, in case of a legal person, the Subscriber – selects a signature PIN, a confidential security parameter whose secrecy and protection are placed exclusively on the Subject itself. To confirm the PIN, the Subject/Subscriber enters the One Time Password received via SMS, generated via token or the token-app associated with the certificate.
In some cases, the certificate can be issued already active and usable.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

N/A

4.4.2 Publication of the certificate by the CA

Following successful completion of the certification procedure, the certificate will be entered in the relevant Certificate Registry and will not be made public. A Subject wishing to publish his certificate may request to do so following the procedure described in §2.2.2. The request will be processed within three business days.
This possibility is not provided for LongTerm and OneShot certificates.

4.4.3 Notification of certificate issuance to other entities

N/A

4.5 Key pair and certificate usage

4.5.1 Private key and certificate usage by Subject

Any signature device or remote signature authentication tool must be kept by the Subject in a secure manner. The Subject must keep private key usage validation information separately from the device, if present, or from the tools or authentication codes. He must further ensure the protection of privacy and the preservation of the emergency code required for certificate suspension, while using his certificate solely in the manner prescribed by this Certificate Practice Statement and by applicable national and international laws.

The Subscriber must not place any electronic signatures using private keys for which the relevant certificate has been revoked or suspended and must refrain from using signature certificates issued by revoked CAs.
In the case of closed IT domains, the LongTerm and OneShot certificate shall only be used to sign documents that refer to the specific relation between Subscriber and Subject.

4.5.2 Public key and certificate usage by Relying Party

Relying Parties must be familiar with the certificate's scope of use as indicated in the Certificate
Practice statement and in the certificate itself. They must also confirm a certificate's validity before using the public key contained in it, ensure that the certificate has not been suspended or revoked by checking the relevant lists in the Certificates Registry and confirm the existence and content of any key pair use restrictions, as well as of any representation powers and professional qualifications.

4.5.3 Use restrictions and value limits

The RA may be requested, by submitting adequate supporting documentation, to include in the qualified certificate the following usage limits set by AgID:

- The certificate holder must use the certificate only for the purposes for which it

is issued.

- The certificate may be used only for relations with the [the subject with which the certificate can be used].

Qualified certificates used for automatic signature contain use restrictions prescribed by AgID:

- The certificate may be used only for automatic procedure signature purposes.

Certificates issued on the basis of the AutID method 4 via the eIDAS node or on the basis of the eDocID method 6, have the OID 1.3.76.16.5 and the following usage limit:

- Certificate not usable to request SPID digital identity.

The certificates issued on the basis of identification method 4-AutID, using SPID digital identities, have OID 1.3.76.16.5 and the following use restriction:

- "Certificate issued through the Sistema Pubblico di identita Digitale (SPID), digital identity, not usable to require other SPID digital identity".

Legal entity certificates with LEI codes issued for PoC (Proof of Concepts) contain the following use limitation:

- The use of the certificate is limited to the sealing of documents used in the Proof of Concepts on the embedding of LEI codes in electronic seal certificates.

The Subject or the Subscriber may further request to the Certification Authority the inclusion in the certificate of personalized use restrictions (max 200 characters). Requests for inclusion of additional special use restrictions will be reviewed by the CA for compliance with legal, technical and interoperability requirements.

With regard to the limits of use foreseen for the Spanish Public Administrations, the considerations provided in Annex C and the legislative references [17], [18], [19] apply.

Usage limits for LongTerm and OneShot certificates

LongTerm certificates can be limited only to the use in the domain specified by the contract, for the subscription of digital documents made available to the Subject by the CA or the Subscriber. In this case, the digital documents may be related to relationships between the Subscriber and the Subject.

The LongTerm certificate then shows one of the following usage limits:

- The certificate can be used only in the relationships between the holder and the Subscriber (max 200 characters).
- Certificate for subscribing to products and services made available by

[Subject Name] (max 200 characters).

The **OneShot certificate** has the following usage limit:

- The use of the certificate is technically limited to the signature of the underlying documents.

Without prejudice to the responsibility of the CA referred to in CAD (art.30), it is the Relaying Party's (the person who receives the signed document) responsibility to verify compliance with the limits of use and value included in the certificate. The CA is therefore not liable for damages resulting from the use of a qualified certificate that exceeds the limits set by the same or deriving from exceeding the limit value.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Renewal allows the Subject to obtain a new certificate from a certificate already in their possession that is about to expire. Renewal means that the new certificate will contain the same Subject identification data, the same public key and a new expiry date. For LongTerm and OneShot certificates and for the those issued to a legal person, the renewal is not foreseen but a new recognition and a new issue are made.

4.6.2 Who can request certificate renewal

The Subject may request renewal of a certificate prior to its expiration only if the certificate has not been revoked and if all the information provided upon previous issuance is still applicable. A certificate may not be renewed after its expiration date, and a new certificate should be requested instead. The renewal procedure exclusively applies to certificates issued by InfoCert.

4.6.3 Processing certificate renewal requests

Certificate renewal is performed through a specific service provided by the CA as part of its business and contractual relations with the Subject and with the RA (where present).

4.7 Re-issue with new keys

4.7.1 Reasons for re-issuing with new keys

Re-issuing the certificate with a new key (re-key) allows a Subject already identified and in possession of a certificate to certify a different key pair, while keeping the same identification data. The expiry date of the new certificate is defined contractually.

By way of non-limiting example, the reason could be the re-certification of a new key pair on a remote device, close to the expiry of the certificate or the disposal of the device, or alternatively, the replacement of weak encryption keys with strong encryption keys generated with stronger algorithms.

The procedure applies exclusively to certificates issued by InfoCert.

4.7.2 Who can request a re-issue with new keys?

The request may be made by the Subject or Applicant before the certificate expires or afterwards, as long as all the information supplied at the time of the previous issue and the evidence gathered during the recognition phase are still valid. If the identity document is no longer valid, the certificate cannot be reissued.

4.7.3 Processing the re-issue request with new keys

The re-issue with new keys is carried out through a service provided by the CA within the framework of the commercial and contractual relations established with the Subject and the RA, if applicable.

4.8 Certificate modification

N/A

4.9 Certificate Revocation and Suspension

If a certificate is revoked or suspended, it is invalidated before its expiration date. Any signatures placed after the revocation is published become invalid. Revoked or suspended certificates are included in a revocation and suspension list (the "CRL") signed by the CA. This list is issued and published in the Certificate Registry at set intervals. Under special circumstances, the CA may force issuance of an unplanned CRL. Revocation and suspension become effective as of the time of issuance of the list, which is certified by the date of event registration entered in the Certification Authority's Audit Log.
The revocation status information is kept available at the Certification Authority for 20 years after the expiry of the CA root certificate by issuing and storing the last CRL by means of InfoCert's digital preservation services.

4.9.1 Circumstances for revocation

A revocation request must be submitted in the following circumstances:

1. The private key is compromised or one of the following scenarios applies:
    - the secure signature device containing the key has been lost;
    - the secrecy of the key or of its activation code (PIN) has been broken or, in the case of remote signature certificates, the OTP device has been compromised or lost;

- an incident has occurred which has compromised key reliability;

2. The Subject is no longer able to use the secure signature device in his possession, for example due to a failure;
3. A change occurs in the Subject's personal data – including Role information – contained in the certificate which makes such data no longer true and/or accurate;
4. The contractual relationship between the Subject/Subscriber and the CA is terminated;
5. A condition of non-compliance with this Certificate Practice Statement is determined.

4.9.2 Who can request revocation

The revocation of the certificate may be requested:

- by the Subject holding the certificate;
- by the Subscriber, or Concerned Third Party;
- ex officio by the CA;
- by the NCA, in case of revocation of QSealC PSD2.

4.9.3 Procedure for revocation request

A revocation can be requested by entitled subjects using the following procedures.

4.9.3.1 Revocation request by the Subject

The revocation request is submitted by the Subject using the forms available on the CA website. The request must be signed by the Subject and delivered to the RA or, alternatively, sent to the CA by letter, fax or certified e-mail accompanied by a copy of a valid ID document. Furthermore, the CA or RA can make available additional methods for submitting the request for revocation, as long as those methods provide for a correct identification of the Subject. The CA or RA shall give appropriate notice to the Subject.

Upon confirmation of the authenticity of the request, the CA revokes the certificate and promptly notifies the Subject of the revocation.
If information on the Role of the Subject is included in the certificate referred to in the revocation request, the revocation will be notified by the CA to any Concerned Third Parties with whom the CA has entered into special agreements. If the name of the Organisation is included in the certificate referred to in the revocation request, the CA shall notify such organisation.
Additional methods for requesting revocation by the Subject may be specified in any agreements between the Subject and the CA.

In case of revocation request of LongTerm and OneShot certificates (except for short-term ones), the Subject may request certificate revocation authenticating himself through the systems provided by RA and/or CA through application services, following the formalities described in the contractual documentation. By definition of the short-term certificate itself, no request for revocation by the Subject is foreseen.

4.9.3.2 Revocation request by the Subscriber or the concerned third party

The same methods applicable for Subject's revocation request apply for the revocation request of the Subject's certificate submitted by the Subscriber or the Concerned Third Party. The Subscriber shall specify the Subject details as provided to the CA at the time of certificate issuance.

Upon confirmation of the authenticity of the request, the CA notifies the Subject by the communication means established upon certificate request and revokes the certificate. Additional methods for revocation requests may be specified in any agreement between the subject and the CA or RA.

In the event of a revocation request for LongTerm and OneShot certificates(except for short-term ones), the Subscriber may request the revocation of the Certificate of the Subject by authenticating himself through the systems made available by the CA, as well as through application services, operating in the manner described in the contractual documentation. By definition of the short-term certificate itself, no request for revocation by the Subscriber is foreseen.

4.9.3.3 Revocation by the CA/Ra ex officio

Where necessary, the CA/RA may revoke a certificate by giving prior notice to the Subject and specifying the circumstances for revocation as well as the date and time of effect.
If information on the Role of the Subject is included in the certificate to be revoked, the revocation will be notified by the CA/RA to any Third Parties Concerned with whom the CA has entered into special agreements. If the name of the Organisation is included in the certificate referred to in the revocation request, the CA shall notify the revocation to such organisation. The CA / RA will communicate the revocation also to the Subscriber.

In exceptional cases, the CA may also revoke short-term certificates, upon prior notice to the Subject and the Subscriber, providing the reason for revocation and the starting date and time.

4.9.3.4 Request of the NCA

In the event of a request for revocation of QSealC PSD2, the revocation may be requested by the NCA which issued the authorization number to the payment service provider (PSP), shown in the certificate.

4.9.4 Revocation request grace period

The CRL grace period is the time period between the time of publication by the CA of the next CRL and the time of expiration of the current CRL. To avoid inconveniences to any involved party, this period is longer than the time needed by the CA to generate and publish a new CRL. In this way the current CRL remains valid at least until it is replaced by the new CRL.

4.9.5 Time within which the CA must process the revocation request

Request is processed within 24 (twenty-four) hours, unless additional authenticity checks are required. If correctly authenticated, the request will be processed immediately, otherwise the certificate will be suspended while waiting for further authenticity checks.

4.9.6 Requirements for verifying the revocation

N/A

4.9.7 CRL issuance frequency

Revoked or suspended certificates are included in a revocation and suspension list (the "CRL") signed by the CA and published in the Public Registry. The CRL is issued on a scheduled basis every hour (ordinary issuance). Under special circumstances, the CA may force issuance of an unscheduled CRL (immediate extraordinary issuance), e.g. when the revocation or suspension of a certificate is based on suspicious private key secrecy impairment (immediate revocation or suspension). The CRL is always fully issued. The time of CRL issuance is determined using the date given as a time reference by the InfoCert time stamping authority system and the registration is recorded in the Audit Log. Each item of the CRL list contains the date and time of revocation or suspension in its extension. The CA reserves the right to publish separate CRLs as generic CRL subsets in order to ease network load. It is the responsibility of Relying Parties to obtain and consult the CRL. The CRL to be consulted for a specific certificate is indicated in the certificate itself in compliance with applicable regulations.

4.9.8 Maximum latency for CRLs

Once verified the authenticity of the request, the maximum latency between the submission of the request for revocation or suspension and its implementation through CRL issuance is 1 hour.

4.9.9 On-line revocation/status checking availability

In addition to publishing the CRL in LDAP e HTTP registers, the Certification Authority provides an OCSP certificate status checking service. The relevant URL is shown in the certificate. The service is available 24 X 7.
Consistency between the OCSP service and the CRL is guaranteed within a maximum of one hour. Consistency of the OCSP service and the update of information issued by the service in relation to updates of the CRL, is bound by the time required to update the CRL itself as defined in the previous paragraph.
Certificate status information will be made available until the root CA certificate expires.

4.9.10 Requirements for online verification services

See Annex B

4.9.11 Other forms of revocation

N/A

4.9.12 Specific requirements in case of compromise

N/A

4.9.13 Circumstances for suspension

Suspension must take place if the following conditions arise:

1. A revocation request has been filled, but its authenticity cannot be determined in due time;
2. The Subject, the Subscriber, the Concerned Third Party, the RA or the CA have acquired evidence of doubts about the certificate's validity;
3. Doubts about the security of the signature or OTP device (if present) have arisen;
4. Temporary termination of certificate validity is required.

In the above cases, a request for certificate suspension is requested, possibly specifying its duration. On expiry of the suspension period, or at the request of reactivation of the certificate, its validity may be either revoked completely or re-established.
In the event of suspected identity theft, the CA may carry out a precautionary suspension without prior notice.

4.9.14 Who can request suspension

Suspension can be requested by the Subject at any time and for any reason. In addition, certificate suspension may be requested by the Subscriber or by the Concerned Third Party for the reasons and ways established by this document CPS. Eventually, a certificate may be suspended ex officio by the CA.

4.9.15 Procedure for suspension request

The easiest way to request suspension of the certificate is by means of the website in the dedicated section. The duration of the suspension is determined by the subject submitting the request; if not specified, the certificate remains suspended until the certificate expires and is then revoked. Suspensions end at 24:00:00 of the last day of the requested suspension period.
For some customers, a reactivation function is made available on the basis of specific agreements; in this case, the certificate can only be reactivated if still valid.

4.9.15.1 Suspension request by the Subject

A Subject may request certificate suspension by one of the following methods:

1. Through the Suspension feature available on the CA website or, in case of remote signature certificates, through the MySign portal (a tool provided by InfoCert for the remote signature certificate management). To submit a request, the Subject must provide the required data and use the emergency code received upon certificate issuance;
2. Where applicable, through the Suspension by OTP feature available on the website specified in the contractual documents received upon registration;
3. By calling the CA call centre and providing the required information. If no emergency code is available and only as long as the suspension request is based on a key compromise incident, the call center shall, after verifying the phone number from which the call originates, activate immediate certificate suspension for a period of 10 (ten) calendar days, while waiting for a written request signed by the Subject. If such request is not received by the CA within the above deadline, the certificate will be reactivated;
4. Through the Registration Authority, which requests the necessary data and performs all the necessary checks on Subject's identity before sending a certificate suspension request to the CA;
5. By using the suspension function available on the WEB site of the RA that interfaces to the CMS services.

If Role information on the role of the Subject is included in the certificate referred to in the suspension request, the suspension will be notified by the CA to any Concerned Third Parties with whom the CA has entered into special agreements. If the name of the Organisation is included in the certificate referred to in the suspension request, the CA shall notify the suspension to such organisation.
The CA will communicate the suspension to the Subscriber as well, if foreseen by the contract related to the suspended certificate.
By definition of the short-term certificate itself, no request for revocation by the Subject is foreseen.

4.9.15.2 Suspension request by the Subscriber or concerned third party

To request suspension of the Subject's certificate, the Subscriber or Concerned Third Party shall complete the dedicated form available on the CA website or at RA offices and specify the circumstance for the request, as well as include any relevant documentation and the Subject details as provided to the CA at the time of certificate issuance.
Upon confirmation of the authenticity of the request, the CA notifies the Subject by the communication means established at the time of certificate request and suspends the certificate. Additional methods for suspension requests submitted by the Subscriber or by the Third Party Concerned may be specified in any agreements entered with the CA.

In the event of a suspension request for LongTerm and OneShot certificates (except for short-term certificates), the Subscriber may request the suspension of the subject's certificate by authenticating itself to the systems made available by the CA, also through application services, in the ways described in the contractual documentation.
By definition of the short-term certificate itself, no request for revocation by the Subject is foreseen.

4.9.15.3 Suspension on the Initiative of the CA

Except for urgent cases, the CA gives notice to the Subject in advance about intention to suspend the certificate, providing the reason for the suspension and the suspension start and end date. This information will in any case be provided to the Subject at the earliest convenience.
If information on the Role of the Subject is included in the certificate to be suspended, the revocation will be notified by the CA to any Third Parties Concerned with whom the CA has entered into special agreements. If the name of the Organisation is included in the certificate to be suspended, the CA shall notify the suspension to such Organisation.

If the contract related to the certificate to be suspended foresees it, the CA will also communicate the suspension to the Subscriber.

4.9.16 Limits on suspension period

The duration of the suspension period is determined by the person submitting specific request and may not exceed the period of validity of the certificate. On expiry of the requested suspension period, certificate validity is re-established by removing the certificate from the revocation and suspension list (CRL). Reactivation is effective within 24 hours from the suspension end date. If the suspension end date coincides with the certificate expiration date, suspension will be turned into revocation, with effect from the beginning of the suspension.
If stated by the contract, Certificate reactivation may be requested before the suspension end date.

In cases where the certificate has been suspended through a CMS, it is possible to use the reactivation function available on the WEB site interfacing with the CMS services.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status information is available through CRL and OCSP responder. A revoked certificate serial number is retained in the CRL even after the validity of the certificate has expired and at least until the CA certificate expiration. Certificate information from the OCSP is updated in real time.

4.10.2 Service availability

The OCSP service and the CRL are available 24 hours a day, 7 days a week.

4.10.3 Optional features

N/A

4.11 End of Subscription

The relationship between the Subject and/or Subscriber with the Certification Authority is terminated when the certificate expires or is revoked, except in special cases defined by contract.

4.12 Key escrow and recovery

N/A

5 SECURITY MEASURES AND OPERATIONAL CONTROLS

InfoCert as a TSP has implemented an information security system for its digital certification service. The security system is divided into three levels:

- A physical level aimed at ensuring the security of environments where TSP manages the service;
- A procedural level of strictly organisational nature;
- A logical level involving provision of hardware and software technology to address the problems and risks associated with the type of service and the infrastructure used.

This security system is designed to avoid the risks arising from the malfunction of systems, networks and applications, as well as unauthorised interception or data modification.
An excerpt of the InfoCert security policy can be requested by email to infocert@legalmail.it.
Security policies at InfoCert are reviewed no less than on a yearly basis, and are updated for any relevant changes. Each review is tracked within the document itself even when no changes have been necessary.

5.1. Physical Controls

The implemented measures provide adequate security on:

- Site and construction features;
- Active and passive anti-intrusion systems;
- Physical access control;
- Power supply and air conditioning;
- Fire protection;
- Flood protection;
- Magnetic media storage modes;
- Magnetic media storage sites.

5.1.1. Site location and construction

InfoCert's primary service provision site is located in Padua. The Disaster Recovery site is in Modena and is connected to the above Data Center by a dedicated redundant connection on two separate MPLS 40 Gbit/s each circuits upgradable to 100 Gbit/s.
Within both sites, rooms protected with several physical and logical security systems have been created. Each room hosts the computer equipment that is at the core of the digital certification, time stamping and remote/automatic signature services.
For services that need business continuity with RTO / RPO values close to zero, some components of the CA services relating to publication of the CRLs and the OCSP are hosted on AWS cloud, respectively, in Frankfurt Europe Region and in Ireland Europe Region. Furthermore, in order to guarantee the business continuity for the CA "InfoCert

Qualified Electronic Signature CA 4", an encrypted copy of the data is carried out on the AWS cloud in Milan, Europe.

AWS has certifications of conformity in accordance with the ISO/IEC 27001: 2013, 27017: 2015, 27018: 2019 and ISO/IEC 9001: 2015 standards.

Figure 1 - location of InfoCert's primary service provision site and of the Disaster Recovery

5.1.2. Physical access

Access to the Data Center is governed by the InfoCert security procedures. A bunker area located inside the Data Center hosts the CA systems, which require an additional security factor.

5.1.3. Power supply and air conditioning

While not certified as such, the primary service provision site in Padua meets the requirements of a Tier 3 Data Center.
The technical rooms are equipped with an electric power supply system designed to prevent failures, especially malfunctions. Power systems feature state-of-the-art technology to increase reliability and ensure redundancy of the more critical features required by the delivered services.
The power supply infrastructure includes:

- Uninterruptible power supply units, with accumulators and based on alternating current (UPS);

- Alternating Voltage availability (220-380V AC);
- Cabinets powered by redundancy with protected lines sized for the agreed absorption;
- Emergency generator service;
- Automatic switching and synchronisation between generators, network and batteries (STS).

Each technology cabinet installed at the Data Center is powered by two power lines that assure the HA in case of outage of one of the two available lines.

The technology cabinet is monitored remotely, with constant power line status (on/off) and power consumption checks (each line must not exceed 50% of the load).
Temperature inside the technical area is normally kept between 20° and 27°, with relative humidity level of 30% to 60%. Systems are equipped with condensing batteries with a sealed collection and drainage system of the condensate controlled by anti-flooding probes. The entire conditioning system is dedicated to emergency generators in case of power failure. Cooling capacity for each cabinet is ensured with a maximum expected load of 10KW and a maximum of 15KW on two flanked cabinets.

5.1.4. Flood prevention and protection

The location of the site does not pose risks to the environment resulting from proximity to "dangerous" installations. During building design, appropriate arrangements have been made to isolate potentially hazardous premises, such as those containing the generator set and the thermal plant. Equipment room is on the ground floor above street level.

5.1.5. Fire prevention and protection

The Data Center hosts a smoke detection system operated by a NOTIFIER-addressable analogue station with optical sensors positioned in the environment and in the false ceiling and air sampling sensors installed underfloor and in air ducts.
The automatic fire detection system is connected to ARGON IG-01eco-friendly gas suppression systems.
In the event of simultaneous activation of two detectors in the same area, the gas is discharged into the area concerned.
Each fire compartment has a dedicated fire extinguishing system.
In addition, portable extinguishing media compliant with applicable laws and regulations are present.

5.1.6. Storage media

With regard to the storage platform, the current solution uses NetApp systems (FAS 8060) for the NAS part. For the SAN part an infrastructure for the call center based on Infinidat technology was implemented, including no. 2 enclosure InfiniBox of

generation F4000 and F6000; for the CA part, 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 differentiated waste collection and sustainable waste disposal. Regarding the information content of electronic waste, all media are cleansed of data prior to disposal according to applicable procedures or through certified sanitation companies.

5.1.8. Off-site backup

Off-site backup takes place at the Disaster Recovery site through an EMC Data Domain 4200 device, on which the primary Data Domain of the Padova site replicates backup data.

5.2. Procedural controls

5.2.1. Key roles

Key roles are covered by personnel having the necessary experience, professionalism and technical/legal expertise, which are constantly verified through annual assessments.
The list of names and organizational charts of key figures has been deposited in AgID when the first accreditation occurred and is constantly updated to reflect the natural evolution of the Company's organization.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Following the annual Human Resource planning, the Function/Organizational Structure Manager identifies the characteristics and skills of the resource to be inserted (job profile). Subsequently, in conjunction with the Staff Selection Manager, the search and selection process are triggered.

5.3.2. Background check procedures

Selected candidates participate in the selection process by taking part in an initial cognitive-motivational interview with the Staff Selection Manager and in a subsequent technical interview with the Function/Organizational Structure Manager, in order to check the skills declared by the candidate. Additional verification tools include exercises and tests.

5.3.3. Training requirements

To prevent any person from individually affecting or altering overall system security or performing unauthorized activities, the operational management of the system is entrusted to different resources, each with separate and well-defined tasks. The personnel in charge of certification service design and provision is an InfoCert employee who was selected for his background in the design, implementation and management of IT services and for his characteristics of reliability and confidentiality. Training sessions are planned periodically to raise awareness on assigned tasks. In particular, prior to the inclusion of staff in operating activities, training courses are carried out to provide all the necessary (technical, organizational and procedural) skills to carry out assigned tasks.

5.3.4. Retraining frequency

At the beginning of each year, training requirements are analyzed in order to define the training courses to be held during the year. The analysis is based on following steps:

- Meeting with management to collect data on the training requirements needed to achieve business objectives;
- Feedback from the area managers in order to identify the specific training needs from each area;
- Forwarding of collected data to Corporate Management for Training Plan closing and approval.

Once defined, the Training Plan is shared and made public by February.

5.3.5. Job rotation frequency

On-site working or agile working (smart working) hours are distributed over an 8:00 a.m. to 7:00 p.m. time slot from Monday to Friday.
Supervision of the production environment at night and on public holidays is ensured by means of an on-call rotation plan drawn up by the head of the organisational unit at least 10 days in advance every month. Depending on the need, interventions may be carried out remotely (remote intervention) or require access to the premises.
Provided that the necessary technical and professional requirements are met, the Company ensures that as many workers as possible are on call, giving priority to employees who request it.

5.3.6. Sanctions for unauthorized actions

Sanctions are imposed in accordance with the National Employment Contract for Metalworkers and Installation of Private Industrial Plants ("CCNL Metalmeccanici e installazione impianti industria privata").

5.3.7. Checks on non-employee staff

Access to non-employee personnel is governed by a specific corporate policy.

5.3.8. Documentation to be supplied by personnel

Upon recruitment, employees must provide a copy of a valid identity document, as well as a copy of a valid health card and a passport type photo for their access badge. Subsequently, they will be required to complete and sign a written consent to the processing of personal data and a confidentiality agreement, and to review InfoCert's Code of Ethics and Netiquette policy.

5.4. Audit Log management

CA management and certificate life-cycle records are collected in the Audit Log as required by the Regulation and by the Technical Requirements [5].

5.4.1. Types of records archived

Archived records include security events, startup and shutdown events, system crashes and hardware failures, firewall and router activity, and PKI system access attempts.
All the data and documents used during identification and acceptance of the Subscriber requests are retained, including copies of ID documents, contracts, business registration excerpts etc.
Certificate registration and life-cycle events are also recorded. These include certificate issuance and renewal requests, certificate registration, generation, distribution and (possibly) revocation/suspension.
All events concerning the personalization of the signature device are recorded.
All physical accesses to high security premises where the CA machines reside are recorded.
All logical accesses to the CA applications are recorded.
All signature device customization events are also archived. Each event is saved with its system date and time.

5.4.2. Frequency of Audit Log processing and archiving

Data collection, clustering and archiving on InfoCert preservation services is carried out on a monthly basis.

5.4.3. Retention period for Audit Log

The Audit Log is retained by the CA for almost 20 years. Logs related to certificate's lifecycle are preserved for at least 20 years after the expiry of the certificate, up to a maximum of 23 years from the date of issue.

5.4.4. Protection of Audit Log

Audit Log protection is ensured by the InfoCert electronic document preservation services.

5.4.5. Audit Log backup procedures

Electronic document preservation services implement backup policies and procedures that are compliant with the requirements of its security manual.

5.4.6. Audit Log collection system

Event logs are collected through ad hoc automatic procedures and archived in the InfoCert preservation services according to the methods described in the preservation system security manual.

5.4.7. Notification of vulnerability

N/A

5.4.8. Vulnerability assessments

InfoCert performs periodic System vulnerability assessments and penetration tests. Based on the results, all the necessary countermeasures are implemented to secure applications.

5.5. Records archival

5.5.1. Types of records archived

Records for each major Certification Authority event are drawn up and archived. Such records are stored for a 20 years period by the Certification Authority in the InfoCert preservation system.

5.5.2. Protection of archives

Protection is ensured by InfoCert's preservation services.

5.5.3. Archive backup procedures

Document preservation services implement backup policies and procedures that are compliant with the requirements of its security manual.

5.5.4. Requirements for time-stamping of records

N/A

5.5.5. Archive collection system

Records are collected through specific automatic procedures and archived in the

InfoCert-compliant document preservation system according to the methods described in its security manual.

5.5.6. Procedures to obtain and verify the information archived

Data are all stored by means of the preservation services on which regular accurate checks on the status of the system and the integrity of the data are carried out. Data are displayed in accordance with the relevant standards.

5.6. CA key changeover

The CA periodically replaces the private certification key used for signing signature certificates in order to enable the Subject to use his certificate until its expiry date. Each key changeover results in an amendment of this Certificate Practice Statement and is notified to AgID.

5.7. CA private key compromise and disaster recovery

5.7.1. Incident handling procedures

The CA has described its incident handling procedures in its ISO 27000-certified information security management system (SGSI). Any incident detection is immediately followed by incident analysis, detection of corrective countermeasures and drawing up of a report by the service manager. The report is digitally signed. In accordance with Article 19 of the eIDAS Regulation, a copy is also sent to AgID, along with a statement of measures aimed at removing the potential causes of the incident, if under the control of InfoCert.

5.7.2. Computing resources, software and/or data are corrupted

In the event of a failure of the HSM secure signature device containing the certification keys, an appropriately saved and stored certification backup key is used instead, and there is no need to revoke the corresponding CA certificate.
Software and data are subject to regular backups as provided by internal procedures.

5.7.3. CA private key compromise procedures

Certification key compromise is regarded as a particularly critical event as it invalidates issued certificates and the revocation status information signed with that key. Therefore, special focus is given to protection of the certification key and to all system development and maintenance activities that may have an impact on it.
Although it is a rare event, InfoCert has set up a detailed procedure to be followed within the ISO 27000 certified ISMS, reporting it to the CAB.
Once the compromise of the CA private key has been ascertained, InfoCert will promptly proceed:
- to inform the Italian Supervisory Body AgID and the CAB for the removal of the key

from the TSL,
- to notify RAs and customers, whether Subjects or Subscribers, through direct communication, where possible, and through communication on the InfoCert website,
- to revoke the affected certificates, to proceed, if necessary, with the issuance and accreditation of a new CA root, and to reliably provide information on the certificates revocation status.

5.7.4. CA continuity capabilities after a disaster

InfoCert has adopted the procedures required to ensure continuity of its service even in highly critical or disaster situations.

5.8. CA or RA Service termination

The CA shall communicate its intention to terminate certification activities to the Supervisory Authority (AgID) and to the Conformity Assessment Body (CAB) with a notice of at least 3 months, and, where applicable, shall indicate a replacement Certification Authority in charge of keeping the Certificates Registry and related documentation. The same notice period must also be given by InfoCert to all holders of certificates issued by it to notify them of the termination of its activities. If the notification contains no indication of a replacement Certification Authority, it shall clearly specify that all certificates that are not expired at the time of termination of certification activities will be revoked.
In case of termination of the CA, revocation status information will be provided through the issue of a last CRL compliant with the ETSI 319 411-1 standard.
More details are available in the document TSP Termination Plan of the Certification and Time Validation Services available from the Certification Authority.

6 TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

In order to provide its service, the Certification Authority needs to generate a key pair used to sign the Subject certificates.
Such keys are generated solely by staff specifically in charge of this function. Key and signature generation takes place within dedicated and certified cryptographic modules, as required by current legislation.
Protection of the CA private key is ensured by the key generation and usage cryptographic module. The private key can only be generated if two key generation employees are simultaneously present. Key generation takes place in the presence of the service manager.
CA private keys are duplicated for the sole purpose of being recovered after secure signature device breakdown. Duplication takes place through a controlled procedure by which the key and its context are duplicated on multiple devices as required by HSM device safety criteria.
The cryptographic module used for key generation and signature complies with requirements that ensure:

- Compliance of the pair with minimum requirements imposed by the generation and verification algorithms used;
- A fair probability of generation of possible pairs;
- Identification of the Subject activating the generation procedure;
- That signature generation takes place inside the device so that the value of the private key being used cannot be intercepted.

6.1.1 Subject key pair generation

Asymmetric keys are generated within a secure signature creation device (SSCD or QSCD, HSM type) using native features provided by the devices themselves. In the event that the device is not provided by the CA, the Subscriber must ensure that it complies with applicable laws by providing appropriate documentation and subjecting it to periodic audits. In the case of HSM InfoCert reserves the right to chair the Key Ceremony.

6.1.2 Private key delivery to Subscriber

Private keys are contained in the cryptographic device, which can be either an SSCD or a QSCD.

For remote and automatic remote certificates the cryptographic device is always an HSM. By delivering the cryptographic device to the Subject, the latter comes into full possession of the private key, which he can only use by entering a PIN that is known exclusively to him.

Where the registration procedure is performed in the presence of the Subject, the device is delivered as soon as the keys are generated.

If the registration process is not performed in the presence of the Subject, the device is delivered according to the methods provided by the contract, paying attention that the device and its instructions for use travels on different channels or are delivered to the Subject at two different moments in time. In some cases, the Subject may already have the devices available, as they have been delivered in advance according to safe procedures and against identification of the Subject.

6.1.3 Public key delivery to the CA

N/A

6.1.4 Public key delivery to relying parties

If the Subscriber requires it, the certificate is published in the public registry where it can be retrieved by the Relying Party. LongTerm and OneShot certificates are excluded.

6.1.5 Key algorithm and key size

The certification asymmetric key pair is generated within the cryptographic hardware devices mentioned above.
The CA root keys that sign the issuing of new certificates can be:

- RSA asymmetric keys with a length of not less than 4096 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI document TS 119 312 - Cryptographic Suites with a length of not less than 256 bits.

The Subject keys may be

- asymmetric RSA keys with a length of not less than 2048 bits;
- EC asymmetric keys on one of the elliptic curves provided by ETSI TS 119 312 - Cryptographic Suites document with length not less than 256 bits.

6.1.6 Public key generation and quality checks

Devices are certified according to high security standards (see § 6.2.1) and ensure that the public key is correct and random. Prior to issuing a certificate, the CA verifies that the public key has not been used before.

6.1.7 Key usage purposes

6.1.7.1 Use of the CA key

The CA key is only used for signing Holder's certificates, Revocation Lists and OCSP certificates. The KeyUsage extension of the CA certificate contains certificate signature(keyCertSign) and CRL signing (cRLSign).

OCSP responses are signed by means of special certificates with extKeyUsage enhanced with ocspSigning.

6.1.7.2 Use of the Holder's key

Key usage purposes are determined by the KeyUsage extension, as defined in the X509 standard. Most of the certificates described in this Operating Manual contain "non-repudiation" KeyUsage only. Exceptions identified with specific OIDs are admissible so as to allow the "non-repudiation" and "digital signature" pair and the "non-repudiation", "digital signature" and "key encryption" triplet too. The latter triplet is used, for example, in the context of Spanish public administrations in accordance with regulatory references [17], [18], [19].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Cryptographic modules used by InfoCert for certification keys (CA) and OCSP responder are validated 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) in Europe.
Smart cards 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.
Cryptographic modules used by InfoCert for remote and automatic signature are validated FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL4.

6.2.2 CA private key multi-person control

Access to devices containing the certification keys can only occur when two users are simultaneously authenticated.

6.2.3 CA private key escrow

N/A

6.2.4 CA private key backup

Key backup is contained in a safe whose access code is solely given to personnel who do not have access to HSM devices. Key restoration therefore requires that both personnel in charge of the device and employees who have access to the safe are present at the same time.

6.2.5 CA private key archival

N/A

6.2.6 Private key transfer into or from a cryptographic module

N/A

6.2.7 Private key storage on cryptographic module

The certification private key is generated and stored in a secure area of the cryptographic device, managed by the certifier, which prevents its export. In addition, if an attempt at forcing the protection occurs, the operating system of the device blocks the device or makes itself unreadable.

6.2.8 Method of activating private key

The certification private key is activated by the CA software in dual control, that is by two employees with specific roles and in the presence of the service manager.
The Subject or Subscriber acting as legal representative of a legal person is responsible for protecting his private key with a strong password to prevent unauthorized use. To activate the private key, the Subject must authenticate himself.

6.2.9 Method of deactivating private key

N/A

6.2.10 Method of destroying CA private key

InfoCert staff in charge of this role deals with the destruction of the private key when the certificate expires or is revoked, according to security procedures provided by security policies and device manufacturer specifications.

6.2.11 Cryptographic module rating

N/A

6.3 Other aspects of key pair management

N/A

6.3.1 Public key archival

N/A

6.3.2 Certificate and key pair validity periods

A certificate validity period shall be determined based on:

- The state of technology;

- The state of the art for cryptographic technologies;
- The intended use of the certificate.

Validity periods are stated on each certificate as set out in Section § 3.3.1.
Currently, the CA certificate has a duration of 16 years. Certificates issued to natural or legal persons are valid for not more than 39 months.

6.4 Private key activation data

Please refer to sections 4.3.3. and 6.3.

6.5 Computer security controls

6.5.1 Specific computer security requirements

The operating system of computers used in certification activities involved in key generation, certificate generation and certificate registry management are hardened, i.e. they are configured to minimize the impact of any vulnerabilities by eliminating features that are not required for CA operation and management.
System administrators appointed for this purpose in accordance with applicable regulations shall access the system by means of a root on demand application, that enables root user privileges to be used only after individual authentication. Each access is traced, logged and stored for 12 months.

6.6 Control system operation

InfoCert gives strategic importance to secure handling of information and recognizes the need to continuously develop, maintain, monitor and improve its information security management system (SGSI) in accordance with ISO/IEC 27001. InfoCert has been ISO/IEC 27001:2005 certified since March 2011 for EA:33-35 activities. In March 2015, the company was certified according to the new version of the ISO/IEC 27001:2013 standard.
SGSI procedures and checks include:

- Asset management;
- Accesses control;
- Physical and environmental security;
- Security of operating activities;
- Communications security;
- System acquisition, development and maintenance;
- Incident management;
- Business continuity.

All procedures are approved by their supervisors and shared internally over the

InfoCert document management system.

6.7 Network security controls

For its certification service, InfoCert has designed a network security infrastructure based on firewalling mechanisms and on the SSL protocol to provide a secure channel between the Registration Authorities and the certification system, and between the certification system and administrators/operators.
InfoCert systems and networks are connected to the Internet in a controlled way by means of firewall systems that allow splitting up the connection into progressively more secure areas: Internet networks, DMZ (Demilitarized Zone) or Perimeter Networks, and Internal networks. All traffic flowing between areas is subject to acceptance by the firewall, based on a set of established rules. Firewall rules are designed based on "default deny" (what is not expressly permitted is forbidden by default, or the rules will only allow what is strictly necessary for the application to properly work) and "defense in depth" (increasing layers of defense are arranged, first at the network level, through successive firewall barriers, and finally at system level through hardening) principles.

6.8 Time stamping trust service

InfoCert provides a qualified time stamping trust service. For the time stamp service, please refer to the network security controls included in document named ICERT-INDI-TSA available at the InfoCert's website.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1. Certificate profile

The certificate shows the information given in the certification request.
The generated certificate profile complies with the requirements of eIDAS Regulation [1] and determination no. 147/2019 [13]. This guarantees full certificate readability and verifiability in relation to the regulatory framework and European certification authorities.
InfoCert uses the ITU X.509, version 3 standard for its entire PKI structure.
Annex A specifies the path of root certificates and Subjects, be they natural or legal persons.

7.1.1. Version number

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

7.1.2. Certificate extensions

Qualified certificates are marked by the extensions specified in qcStatement clause 3.2.6 of IETF RFC 3739. Their use is governed by ETSI 319 412-5. For extensions, please see Annex A.

7.1.3. Signature algorithm OID

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

- sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]
- ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]
- ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]
- ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

.

7.1.4. Name forms

Each certificate is given a unique serial number within the issuing CA.

7.1.5. Name constraints

Please refer to paragraph 3.1.

7.1.6. Certificate OID

Please refer to paragraph 1.2.

7.2. CRL profile

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

7.2.1. Version number

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

7.2.2. CRL extensions

For CRL extensions, please see Annex A.

7.3. OCSP profile

To determine a certificate's revocation status without querying the CRL, InfoCert uses the OCSP service compliant with the protocol RFC6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”. This protocol specifies the data to be exchanged between an application wishing to verify the status of the certificate and the OCSP service.

7.3.1. Version number

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

7.3.2. OCSP extensions

For OCSP extensions, please see Annex A.

8 COMPLIANCE AUDITS AND ASSESSMENTS

In order to obtain the qualification as trusted service provider or qualified trust service provider under the eIDAS Regulation, the procedure provided for in Article 21 of the said Regulation must be carried out.
InfoCert has submitted to AgID a request for recognition as "qualified trust service provider" enclosing a Conformity Assessment Report (CAR) issued by a conformity assessment body (CAB) authorized by ACCREDIA.
The service is provided by InfoCert as a qualified trust service provider within the meaning of Regulation (EU) No. 910/2014 of 23/07/2014, on the basis of a conformity assessment carried out by the conformity assessment body CSQA Certificazioni S.r.l. pursuant to the above Regulation and to the ETSI EN 319 401 standard, and according to the eIDAS assessment scheme defined by ACCREDIA in accordance with the ETSI EN 319_403 and UNI CEI EN ISO/IEC 17065:2012 standards.

8.1. Frequency and circumstances of conformity assessment

Conformity assessments are repeated every two years. Each year the CAB performs a surveillance audit.

8.2. Identity/qualifications of assessor

Assessments are performed by:

Company Name	CSQA Certificazioni S.r.l.
Registered office	Via S. Gaetano n. 74, 36016 Thiene (VI)
Telephone number	+39 0445 313011
Companies' Register Registration No.	Codice Fiscale 02603680246 Registro Imprese VI n. 02603680246 / REA n. 258305
VAT No.	02603680246
Website	http://www.csqa.it

8.3. CAB's relationship to InfoCert

InfoCert and CSQA are not linked by financial interests or business relationships.
There are no ongoing commercial or partnership relationships that may create a bias for or against InfoCert in CSQA's objective assessments.

8.4. Topics covered by assessment

The CAB is asked to assess the compliance of adopted procedures, CA organization, organization of roles, personnel training and contractual documentation with the

Certificate Practice Statement, the Regulation and any applicable legislation.

8.5. Actions taken as a result of non-conformity

In the event of non-conformity, the CAB shall decide whether to send a report to AgID or whether to repeat the audit after the non-conformity has been remedied.
InfoCert commits to resolve all non-conformities in a timely manner by implementing all necessary improvement and adjustment actions.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1 Fees for issuing, renewing and re-issuing certificates with new keys

In the case of LongTerm or OneShot certificates, as a rule, the costs for issuing the certificate are payed by the Subscriber and not by the Subject, based on rates defined by the service contract between the Subscriber and InfoCert.
Furthermore, fees can be consulted at https://www.firma.infocert.it/ and http://ecommerce.infocert.it, or at Registration Authority offices. The CA may enter into commercial agreements with RAs and/or Subscribers and apply specific fees.

9.1.2 Certificate access fees

Access to the public registry of issued certificates is free of charge.

9.1.3 Revocation or suspension status information access fees

The list of revoked or suspended certificates can be accessed free of charge.

9.1.4 Fees for other services

These fees can be consulted at https://www.firma.infocert.it/ and http://ecommerce.infocert.it, or at Registration Authority offices.
The CA may enter into commercial agreements with RAs and/or Subscribers and apply specific fees.

9.1.5 Refund policy

If the service is purchased by a consumer, the Subject has the right to terminate the agreement within 14 days from the date of its conclusion and to obtain refund of the paid price. Instructions for exercising the right of withdrawal and claim reimbursement are available at https://help.infocert.it/ or at RA offices.

9.2 Financial responsibility

9.2.1 Insurance coverage

The TSP InfoCert has entered into an insurance contract to cover operational risks and damage to third parties, the text of which has been processed and accepted by AgID. The following ceilings apply:

- EUR 10,000,000 per individual claim;
- EUR 10,000,000 per annuity.

9.2.2 Other assets

N/A

9.2.3 Insurance or warranty coverage for end-entities

Please refer to paragraph 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No confidential information is managed as part of the activities covered by this Certificate Practice Statement.

9.3.2 Information not within the scope of confidential information

N/A

9.3.3 Responsibility to protect confidential information

N/A

9.4 Privacy

Unless expressly permitted, any Subject's/Subscriber's information acquired by the CA while performing its routine activities shall be regarded as confidential and non-disclosable, except for information specifically intended for public use [e.g. public key, certificates (if requested by the Subject), certificate revocation and suspension dates]. In particular, personal data shall be processed by the Certification Authority in accordance with Legislative Decree No. 196 of 30 June 2003 and with European Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection of natural persons with regard to the processing of personal data and on the free movement of such data, fully binding from 25 May 2018 [4].

9.4.1 Privacy plan

InfoCert adopts a set of policies through which it implements and integrates personal data protection within its ISO 27001 certified information security management system, with which it shares a continuous improvement process.

9.4.2 Information treated as private

Data defined as "personal data" in the applicable legislation [4] is treated as personal data. Personal data therefore stands for any information about a natural person that is identified or may be identified, even indirectly, by means of reference to any other information, including a personal identification number.

9.4.3 Information not deemed private

Information that is to be disclosed by the CA technical management – i.e. public key, certificate (if requested by the Subject), and certificate revocation and suspension dates – is not deemed private.

9.4.4 Controller of the processing of personal data

InfoCert S.p.A.
Operational seat:
Via Marco e Marcelliano 45
00147 Roma
richieste.privacy@legalmail.it

9.4.5 Privacy disclosure and consent to use private information

The privacy disclosure is available at www.infocert.it**.** Specific information may be present on the Subscriber's website, which collects the processing consent on behalf of InfoCert. Before processing personal data, InfoCert collects the consent to use such data in the manners and form prescribed by law [4].

9.4.6 Disclosure pursuant to judicial or administrative requests

Disclosure of information requested by an Authority is mandatory and is carried out in the manner established from time to time by the Authority concerned.

9.4.7 Other information disclosure circumstances

N/A

9.5 Intellectual property rights

The copyright in this document is owned by InfoCert S.p.A. All rights reserved.

9.6 Representations and warranties

InfoCert retains responsibility for complying with the procedures prescribed in its information security policy, including when certain functions are delegated to a third party, according to art. 2.4.1. of the Annex to the Commission Implementing EU Regulation 2015/1502.
In the latter case, representation is carried out by a mandate given by InfoCert to the Registration Office (RA) in which the liability regime and the obligations of the parties are defined. In particular, the Registration Office is committed to carry out the registration activities in compliance with the current legislation and the procedures set out in the Practice Statements, with particular reference to the personal identification of those who sign the request for digital certification, and the transmission of the results of these activities to InfoCert.

The Subject is responsible for the truthfulness of the data communicated in the Registration and Certification Request. If at the time of the identification the Subject has concealed his or her real identity or falsely declared to be another person by using techniques including, but not limited to, forgery or alteration of identification documents, or acted in such a way as to compromise the identification process and the related results indicated in the certificate, he or she shall be held responsible for all damages that the Certification Authority and/or third parties could receive from the inaccuracy of the information contained in the certificate, with the obligation to guarantee and indemnify the Certification Authority against any claims for compensation.
The Subject and Subscriber are also liable for damages to the Certification Authority and/or third parties in case of delay in the activation of the procedures provided for in point 4.9 of this Statement (revocation and suspension of the certificate).

9.7 Limitation of warranty

The Certification Authority does not provide any warranties on (i) the proper operativity and safety of hardware and software used by the Subject; (ii) the use of private keys, secure signature devices – where present – and/or certificates of signature different from those provided by current regulations and this Practice Statement; (iii) the continuity of national and/or international electricity and telephone lines; (iv) the validity and relevance, including probatory, of the subscription certificate - or of any message, deed or document associated with it or created by means of the keys to which the certificate is referred, without prejudice to the effectiveness of the handwritten signature recognized to the qualified electronic signature, in accordance with the art. 25 of Regulation EU n. 910/2014; (v) the secrecy and/or integrity of any message, deed or document associated with the subscription certificate or created by means of the keys to which the certificate is referred to (any violation of the latter, usually, are detectable by the owner or by the receipient through the appropriate verification procedure).
The Certification Authority guarantees the functioning of the Service only, according to the levels speficied in paragraph 9.17 of the Certificate Practice Statement.

9.8 Limitation of liability

The Certification Authority does not assume any obligation on monitoring the content, type, or electronic format of documents and/or, eventually, *hashes* transmitted by the IT procedure specified by the Subscriber or the Subject, and does not assume any responsibility for the validity and traceability of the procedure to the actual will of the Subject.
Except in case of wilful misconduct or gross negligence, the Certification Authority shall not be liable for any direct or indirect damage suffered by the Subjects and/or third parties as a result of the use or non-use of the subscription certificates issued in accordance with the provisions of this Statement and the General Conditions of

Certification Services.
InfoCert is not responsible for any direct and/or indirect damage also deriving from: (i) loss, (ii) improper storage, (iii) improper use of identification and authentication tools and/or (iv) failure of the Subject in complying with the recommendations mentioned above.
Moreover, the Certification Authority is not liable for any damages and/or delays due to malfunctioning or arrest of the computer system and internet network, since the phase of formation of the Contract for the Certification Services (hereinafter also referred to as "Contract"), and also during its execution.
Except in the case of wilful misconduct or gross negligence, InfoCert shall not be burdened with charges or liability for direct or indirect damages of any nature or importance that may occur to the Subject, Subscriber and/or third parties caused by tampering or interfering with the service or equipment and carried out by third parties not authorized by InfoCert.

9.9 Indemnities

InfoCert is responsible for any directly determined damage, intentionally or by negligence, to any natural or legal person, as a result of failure to comply with the obligations set out in Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 and InfoCert's failure to use all the appropriate measures to avoid the damage.

The Subcriber or the Subject will have the right to obtain, as compensation for the damages directly suffered as a result of the behavior referred to in the previous paragraph, an amount that can not in any case exceed the maximum values foreseen by art. 3, c. 7 of the Regulation attached to the Determination 185/2017 of the Italian Digital Agency (AgID), for each claim and per year.

The refund may not be requested if the lack of access is attributable to the improper use of the certification service or to the telecommunication network operator or due to incidental events, force majeure or causes not attributable to InfoCert such as strikes, revolts, earthquakes, acts of terrorism, popular riots, organised sabotage, chemical and/or bacteriological events, war, floods, measures put in place by competent authorities about inadequacy of structures, hardware and/or software used by the Applicant.

9.10 Term and termination

9.10.1 Term

At the end of the relationship between the CA and the Subject, between the CA and the RA, between the CA and the Subscriber, the certificate is revoked. The Certification Agreement between the Certification Authority and the Subject shall have a duration

equal to that of the Subscription Certificate, as indicated in the "Validity" section of the Certificate.
In accordance with the procedure indicated in this Certificate Practice Statement, the Subject may request renewal of the certificate before it expires, either keeping the same keys or re-certifying new keys. The renewal shall entail the extension of the certification contract until the expiration or revocation of the renewed certificate, and the payment of the fees defined for that service. An expired or revoked certificate may not be renewed.

9.10.2 Termination

The effectiveness of the Contract is suspensively conditioned by the positive outcome of the identification of the Owner. In the event of a negative outcome of the identification, therefore, the digital certificate will not be issued by the Certifier or, if issued, will be considered ineffective from the moment of its issue and the Contract will be considered terminated by law.
The Contract will automatically terminate with a simultaneous interruption of the Service and revocation of the issued certificate, in the event that the Subject and/or Subscriber is in breach of the provisions contained in the clauses of the Contract referred to the art. 3 (Responsibility of the Subject and Subscriber); art. 4.6 (Intellectual Property), art. 8 (Obligations of the Subject); art. 11 (Payments), art. 12.3 (on the obligation to notify cases and reasons for suspension and revocation of the certificate); if applicable, art. 45 (Other Obligations of the Subject and Subscriber); if applicable, Art. 47 (Other Obligations of the Subject and Subscriber), as well as the provisions of this Certificate Practice Statement. The resolution will occur by right when the interested party declares the other party by PEC or registered letter a.r., that it intends to make use of this clause.

If the Subject is a consumer, civil disputes relating to the contract concluded by the consumer are assigned to the mandatory territorial jurisdiction of the court of the consumer's place of residence or domicile.
The consumer can voluntarily avail the out-of-court dispute resolution methods provided by the italian Consumer Code and other applicable laws.
It should also be noted that, pursuant to the purposes of EU Regulation no. 524/2013, there is the possibility of resorting to the Online Dispute Resolution (ODR) procedure for disputes relating to online contracts and services offered online. The procedure is provided by the European Commission and available at the following link: https://webgate.ec.europa.eu/odr/.
The Certification Authority has the right to withdraw at any time from the Certification Services Agreement with 30 days notice and, consequently, to revoke the certificate.
In all cases where the Subject or Subscriber breach their obligations, the Certification Authority may suspend the provision of the Service, including the suspension of the Certificate. In particular, in the event of missing payment of the Service fee, InfoCert shall be entitled to terminate the Contract with the Subscriber and the Subject at any

time and in any case without prior notice and obligation, consequently revoking any issued certificate.
In case of withdrawal of the Subject or revocation of the certificate the payment is due, and if already done InfoCert retains it also as a withdrawal fee.
The effects produced by the Contract shall remain unaffected until its termination.
The Subject acknowledges that in the event of termination of the Contract, for any reason whatsoever, it will no longer be possible to use the Service.

9.10.3 Effect of termination

Termination results in immediate revocation of the certificate.

9.11 Official communication channels

Please see contact channels in paragraph 1.5.1.

9.12 Amendments to Certificate Practice Statement

The CA reserves the right to amend this document for technical reasons or to reflect any changes to the procedures that have occurred because of legal or regulatory requirements or as a result of work cycle optimisation. Each new version of this Certificate Practice Statement supersedes all previous versions, which remain, however, applicable to certificates issued during the validity of those versions and until the first date of expiration of those certificates.
Increasing document release numbers indicate amendments that do not have a significant impact on relying parties, whereas increasing document version numbers indicate amendments that significantly impact relying parties (such as significant changes affecting operating procedures). In any event, the Certificate Practice Statement will be promptly published and made available in the prescribed ways. Every technical or procedural amendment to this Certificate Practice Statement will be promptly notified to RAs.

For major changes, the CA must undergo an audit by an accredited CAB, submit the certification report (CAR – Conformity Assessment Report) and the Certificate Practice Statement to AgID and wait for a publication permission to be granted.

9.12.1 Amendment history

Version/Release n°:	4.10
Version/Release date:	20/09/2023
Description of changes:	Clarifications on SelfQ and Re-key
Reasons:	Request from AgID

Version/Release n°:	4.9
Version/Release date:	29/05/2023
Description of changes:	§§ 3.2.3, 3.2.3.5 New identification method
Reasons:	Added new identification method

Version/Release n°:	4.8
Version/Release date:	18/04/2023
Description of changes:	Changing of InfoCert logo and formatting § 1.2 Adding of new OIDs §§ 1.2, 3.1.1, 3.1.5, 3.2.4, 7.1, 9.15 Adding of reference to AgID determination no. 147/2019 §§ 3.3, 4.6, 4.7, 9.1, 9.10 Clarifications on key renewal and re-certification § 3.2.3.1, 3.2.3.5 Clarifications added §§ 5.1.1, 5.1.3, 5.1.5 Review of facility aspects § 5.4.2 Review of description § 5.6 Correction of description § 5.8 Change of notice periods in the event of termination § 6.1.5 Clarification added § 6.1.7.2 Changing of Admitted KeyUsage

	§ Appendix A Update of CRL and OCSP format
Reasons:	General review Rebranding

Version/Release n°:	**4.7**
Version/Release date:	17/03/2022
Descrizione modifiche:	§ 1.2 Updated descriptions on OID chart § 1.6.1 Updated "LongTerm" and "OneShot" definitions and short-term certificates introduction § 3.1.1 Derogation to RFC 5280 for the length of some subjectDN fields § 3.1.5 Added LEI codes in certificates for legal person § 3.2.5 Corrections to paragraph references § 3.2.3 Added "Recognition through method 7 – ContoID" § 4.5.1 Updated description § 4.5.3 Updated description and added usage limit for legal person certificates with LEI code for PoC § 4.9.3 Clarifications for short-term certificates § 4.9.5 Updated revocation processin time § 4.9.9 Clarification on the consistency of OCSP and CRL § 4.9.15 Clarifications on short-term certificates § 5 Periodicity of Security Policy Reviews § 5.4.3 Clarification on retention period §§ 5.4.4. 5.5 Updated description § 6.1.2 Updated description § 6.4 Correction to paragraph references § Annex A Simplified description of certificate extensions Formatting for document accessibility purposes

Motivation:	General review Formatting update

Version/Release n°:	4.6
Version/Release date:	10/09/2021
Description of changes:	§ 1.5.1 Contacts update
Motivation:	Contacts change

Version/Release No.	4.5
Version/Release date	18/05/2021
Description of changes	§ 3.1.1 Added detail of application of the Agid resolution accordingly to the context $ 3.1.6 Clarification on the use of trademarks § 3.2.3, 3.2.4, 3.2.5 Revised paragraph organisation § 3.2.3 Added reference to "CPS Addendum - Acceptable identity documents" § 3.2.3.3 Clarification on the use of the SignID mode § 4.2.1, 4.2.2, 4.2.3 Revised paragraph organisation § 4.3.1 Description update § 4.5.3 Added reference to use limits for Spanish certificates § 4.9, 5.8 Clarification on revocation status information § 4.9.15.1 Description update § 5.1.1 Technology update § 5.3.5 Description update § 5.3.7 Description update § 5.8 Revised description § 5.5.6 Revised description § 6.1.5 e 7.1.3 Algorithms and key length update § 6.1.7 Description update § 6.1.7.2 Added exception on the purpose of using the private key § 9.15 Added reference laws in the Spanish context and "CPS Addendum - Acceptable identity documents"

	§ Annex A New CA root added § Annex B Update commercial name verification sw § Annex C Insertion of Spanish Citizen's Qualified Certificate Formal corrections, updated definitions, acronyms, references
Motivation	New CA Roots

Version/Release No.	4.4
Version/Release date	10/02/2021
Description of changes	§ 4.2.1 Update on the mandatory and univocal e-mail address and mobile phone number $ 4.2.2 Electronic delivery mode of the security envelope, by default § 4.9.13 Added the opportunity of a precautionary suspension subject to the CA's discretion
Motivation	Request from AgID

Version/Release No.	4.3
Version/Release date	15/06/2020
Description of changes	§ 3.2.3 Update of the list of recognition methods § 3.2.3.4 Identity recognition by eIDAS node interoperability framework § 3.2.3.5 Distinction between attended VideoID and unattended VideoID with supportive bank transfer § 3.2.3.6 eDocID - Recognition with electronic identity documents § 4.5.3 Amendment to the paragraph with introduction of usage limits for autID and eDocID recognitions § 4.9.15 and § 4.9.16 clarification relating to duration of the suspension period
Motivation	Broader recognition methods Clarifications and typos

Version/Release No.	4.2
Version/Release date	24/03/2020
Description of changes	§ 5.1.1 Technological update and new reference to AWS cloud § 5.1.6 Technological update of the storage media § Annex A – addition of the new CA Electronic Signature Qualified Root "InfoCert Qualified Electronic Signature CA 4"
Motivation	New CA root

Version/release No.	4.1
Version/release date	10.10.2019
Description of changes	§ 3.1.5 Added the possibility of using as a unique identifier the provisions of the eIDAS eID Profile document of eIDAS cooperation network
Motivation	-

Version/release No.	4.0 (never published version, updates reported to 4.1)
Version/release date	14.06.2019
Description of changes	Formal corrections, updating definitions, acronyms, references § 1.2 Update document version, description OID agIDcert § 1.3.5 Update for underage § 1.6.1 Introduction of OneShot Certificates, LongTerm Certificates, and Computer Domain § 2.2.3 Update CRL distribution points § 3.1.1 Update for AgID determination 121/2019 § 3.1.5 Update for AgID determination 121/2019 § 3.2.6 Clearer description § 4.3.1.5 Description of certificates issued for testing purposes § 4.5.3 Added use limit for emission with SPID and updated value limit description § 4.9.2 Clearer description

	§ 5.1.1 Clarification on the location of the Data Center § 5.3.7 Filled physical access description § 5.4.1 Added log description physical and logical accesses Incorporation of the following paragraphs of the two manuals: • § 2.2.2 Certificate Publication • § 3.1.3 Anonymity and pseudonymity of Subscribers • § 3.2.3.4 Recognition through Method 4 – AUTID • § 4.1.1 Who can submit a certificate application • § 4.3.2 Notification of certificate issuance to Subscribers • § 4.4.2 Publication of the certificate by the CA • § 4.5.1 Private key and certificate usage by Subject • § 4.6.1 Circumstance for certificate renewal • § 4.9.3 Procedure for revocation request • § 4.9.15 Procedure for suspension request • § 6.1.1 Subject key pair generation • § 6.1.2 Private key delivery to Subscriber • § 6.1.4 Public key delivery to relying parties • § 6.2.7 Private key storage on cryptographic module • § 9.1.1 Certificate issuance or renewal fees • § 9.4.5 Privacy disclosure and consent to use private information § 9.10.2 Termination
Motivation	Merger of ICERT-INDI-MO, version 3.5 of 11/30/2018 and ICERT-INDI-ENT, version 3.5 of 11/30/2018. Update to the Agid determination 121/2019. Clarifications.

Version/release No.	3.5
Version/release date	30.11.2018
Description modification	§ 1.2 Update OID and description § 1.3 Updated corporate name/ID of the group § 3.2.6 Identification of PSP legal entity in PSD2 § 4.2.1.2 Legal person information within PSD2 § 4.9 Request for revocation by the NCA for PSD2 Typos corrections and references

Motivation	QSealC Seal Certificate issuing in accordance with PSD2 directive Change Corporate Name/ID TecnoInvestimenti

Version/Release No.	3.4
Data Version/Release	20.06.2018
Description modification	§ 1.5.1 Modified call center number § 9.2.1 Updated insurance coverage caps
Motivation:	-

Version/Release No	3.3
Data Version/Release	04.09.2018
Change Description:	Chapter 1 Correction of "digital signature" in "qualified electronic signature". Some terminology corrections for better understanding, adding some definitions of terms used in the document § 3.1.5 Partial paragraph rewrite for better comprehensibility § 3.2.3 Rewriting table and subparagraphs for better clarity of content and contextualisation on European markets. Extension mode 4 AutID to electronic identification means of Member States. Defining a specific document with accepted document types and electronic identification means § 4.2 Partial paragraph rewriting for better comprehension and contextualisation on European markets § 4.2.2 Additional authentication systems § 4.3.3.2 Certificate Issuance Option Already Active § 4.5.3 Inserting an additional usage limit § 4.9.15 and 4.9.16 Suspension and reactivation via CMS

	§ 9.4 Added GDPR References § 9.6, 9.7, 9.8, 9.9, 9.10 paragraph rewriting for better contextualization User Certificates: Added Legal Entity Certificates on QSCD, fixed some errors
Motivations:	-

Version/release No.	3.2
Version/release date	02.05.2017
Description of changes	• Added information about the "InfoCert Qualified Electronic Signature CA 2" • Added some OID about the "InfoCert Qualified Electronic Signature CA 2" • Orthographic corrections
Motivation	-

Version/release No.	3.1
Version/release date	27.01.2017
Description of changes	• §3.2.3 removed all references to SPID as an authentication tool for identification • §3.2.3.1 added details on recognition by the employer • § 4.8.12 added suspension reactivation method
Motivation	-

Version/release No.	3.0
Version/release date	12.12.2016
Description of changes	N/A
Motivation	New document release

9.12.2 Procedure for amendment

Procedures for amending the Certificate Practice Statement are similar to those used for editing it. Amendments are made in consultation with the Head of Certification Service, the Head of Security, the Privacy Manager, the Legal Office and the Consultancy Department and are approved by corporate management.

9.12.3 Notification mechanism and period

This Certificate Practice Statement is published:

- in electronic format on the TSP website (address: http://www.firma.infocert.it/doc/manuali.htm);
- in electronic format in the public list of accredited certification authorities held by AgID;
- in hard copy, either from the Registration Authorities or through the end-user contact details.

9.12.4 Circumstances under which OID must be changed

N/A

9.13 Dispute resolution provisions

For a detailed description of dispute resolution provisions, please refer to the contracts governing the service.

9.14 Competent court

For consumers, the competent court shall be the court of the city where the consumer is domiciled. For persons other than consumers, the competent court shall be the court of Rome. A different jurisdiction may be provided for in agreements between the CA and RA, between the CA and the Subscriber or between the CA and the Subject.

9.15 Governing law

The governing law of this Certificate Practice Statement shall be the Italian law.
Below is a non-exhaustive list of the main applicable regulatory standards:

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 referenced as eIDAS Regulation);

2. Legislative Decree No. 82 of 7 March 2005 (Official Gazette No 112 of 16 May 2005), entitled "Codice dell'amministrazione digitale" (also referred to as CAD), as amended;

3. Not used
4. Legislative decree No 196 of 30 June 2003 (Official Gazette No 174 of 29 July 2003), entitled "Codice Privacy" and subsequent amendments and European Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection of natural persons with regard to the processing of personal data and on the free movement of such data, fully binding starting form 25 May 2018;
5. Not used
6. Not used
7. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and pertaining implementation regulation;
8. Preliminary verification - 24 September 2015 [4367555] Processing of personal data as part of the "Issuing process with webcam recognition" for electronic qualified or digital signature;
9. CNIPA Resolution no. 45 of 21 May 2009, as amended by subsequent resolutions (substituted [13] from July 5, 2019);
10. AgID Resolution no. 189/2017;
11. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, known as Payment Services Directive – PSD2;
12. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
13. AgID determination no. 121/2019 ver 1.1 (replacing CNIPA resolution 45/2009) and subsequent correction by determination no. 147/2019.
14. CPS Addendum - Acceptable identity documents.
15. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
16. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
17. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
18. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
19. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

All circulars and resolutions issued by the Supervisory Authority[10], as well as any implementation acts provided for in the eIDAS Regulation [1] also apply.

9.16 Miscellaneous provisions

Please refer to the relevant service agreements for any other provision not included in this Certificate Practice Statement.

9.17 Other provisions

Service provision times are as follows (unless otherwise agreed):

Service	Time
Access to public certificate registry (includes certificates CRLs and OCSP).	From 0:00 to 24:00 7 days a week (maximum availability 99%)
Request Certificate revocation and suspension.	From 0:00 to 24:00 7 days a week (maximum availability 99%)
Other activities: registration, generation, issuance, renewal[11].	From 9 a.m. to 5 p.m. From Monday to Friday excluding holidays From 9 a.m. to 1 p.m. on Saturdays
Time stamp request and/or verification.	24/7 (minimum availability: 99%)

[10] Available at https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata

[11] Registration activities are carried out at Registration offices, whose office hours may vary. InfoCert shall in any event guarantee delivery of its service at the times indicated above.

ANNEX A

9.18 Electronic Signature Qualified Root "InfoCert Firma Qualificata 2"

```
0 1318: SEQUENCE {
  4    1038:   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    133:     SEQUENCE {
  34     11:       SET {
  36      9:         SEQUENCE {
  38      3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  43      2:           PrintableString 'IT'
            :          }
            :        }
  47     21:       SET {
  49     19:         SEQUENCE {
  51      3:                 OBJECT IDENTIFIER organizationName (2 5 4 10)
  56     12:           UTF8String 'INFOCERT SPA'
            :          }
            :        }
  70     34:       SET {
  72     32:         SEQUENCE {
  74      3:                         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
  79     25:           UTF8String 'Certificatore Accreditato'
            :          }
            :        }
  106    20:       SET {
  108    18:         SEQUENCE {
  110     3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
  115    11:           PrintableString '07945211006'
            :          }
            :        }
  128    37:       SET {
  130    35:         SEQUENCE {
  132     3:           OBJECT IDENTIFIER commonName (2 5 4 3)
  137    28:           UTF8String 'InfoCert Firma Qualificata 2'
            :          }
            :        }
            :      }
  167    30:     SEQUENCE {
  169    13:       UTCTime 19/04/2013 14:26:15 GMT
  184    13:       UTCTime 19/04/2029 15:26:15 GMT
            :      }
  199   133:     SEQUENCE {
  202    11:       SET {
  204     9:         SEQUENCE {
  206     3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  211     2:           PrintableString 'IT'
            :          }
            :        }
  215    21:       SET {
  217    19:         SEQUENCE {
  219     3:                 OBJECT IDENTIFIER organizationName (2 5 4 10)
  224    12:           UTF8String 'INFOCERT SPA'
            :          }
            :        }
  238    34:       SET {
  240    32:         SEQUENCE {
  242     3:                         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
  247    25:           UTF8String 'Certificatore Accreditato'
            :          }
            :        }
```

```
274    20:          SET {
276    18:            SEQUENCE {
278     3:              OBJECT IDENTIFIER serialNumber (2 5 4 5)
283    11:              PrintableString '07945211006'
         :              }
         :            }
296    37:          SET {
298    35:            SEQUENCE {
300     3:              OBJECT IDENTIFIER commonName (2 5 4 3)
305    28:              UTF8String 'InfoCert Firma Qualificata 2'
         :              }
         :            }
         :          }
335   290:        SEQUENCE {
339    13:          SEQUENCE {
341     9:            OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
352     0:            NULL
         :            }
354   271:          BIT STRING, encapsulates {
359   266:            SEQUENCE {
363   257:              INTEGER
         :                     00 C5 A1 6E 5E 03 49 37 01 C5 3E FE FD AE 29 C9
         :                     44 84 6A F1 5E 5A 8E 52 9B 40 40 92 D2 8F 2B 0F
         :                     EC 86 8A 2A D1 B1 21 E5 FC 1C D6 AF C5 16 83 90
         :                     B9 10 34 49 6A 97 EB 78 1A 02 0F C8 99 38 97 31
         :                     DB 1F BD 9C D4 BB 36 48 7D 3A 5F BB 82 A3 98 86
         :                     44 7D FE 15 4D 52 71 B7 2B CE F8 80 3C 1F B2 7A
         :                     A5 19 D5 C2 A4 1B 2C 86 43 5C 01 B2 8A F1 A5 11
         :                     14 79 A8 E4 5B 6C 2C 0E 26 3F 0D 8C 9E 4C 6D 48
         :                         [ Another 129 bytes skipped ]
624     3:              INTEGER 65537
         :              }
         :            }
         :          }
629   413:        [3] {
633   409:          SEQUENCE {
637    15:            SEQUENCE {
639     3:              OBJECT IDENTIFIER basicConstraints (2 5 29 19)
644     1:              BOOLEAN TRUE
647     5:              OCTET STRING, encapsulates {
649     3:                SEQUENCE {
651     1:                  BOOLEAN TRUE
         :                  }
         :                }
         :              }
654    88:            SEQUENCE {
656     3:                OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
661    81:              OCTET STRING, encapsulates {
663    79:                SEQUENCE {
665    77:                  SEQUENCE {
667     4:                    OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
673    69:                    SEQUENCE {
675    67:                      SEQUENCE {
677     8:                        OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
687    55:                        IA5String
         :                      'http://www.firma.infocert.it/documentazione/manu'
         :                      'ali.php'
         :                        }
         :                      }
         :                    }
         :                  }
         :                }
         :              }
744    37:            SEQUENCE {
746     3:              OBJECT IDENTIFIER issuerAltName (2 5 29 18)
751    30:              OCTET STRING, encapsulates {
753    28:                SEQUENCE {
755    26:                  [1] 'firma.digitale@infocert.it'
         :                  }
         :                }
         :              }
783   213:            SEQUENCE {
786     3:                OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
791   205:              OCTET STRING, encapsulates {
794   202:                SEQUENCE {
797   199:                  SEQUENCE {
```

```
 800  196:                    [0] {
 803  193:                      [0] {
 806   42:                        [6]
    :                         'http://crl.infocert.it/crls/firma2/ARL.crl'
 850  146:                        [6]
    :                                  'ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20'
    :                                 'Qualificata%202,ou%3DCertificatore%20Accreditato'
    :                              ',o%3DINFOCERT%20SPA,c%3DIT?authorityRevocationLi'
    :                         'st'
    :                            }
    :                         }
    :                      }
    :                    }
    :                  }
    :                }
    :              }
  999   14:          SEQUENCE {
 1001    3:            OBJECT IDENTIFIER keyUsage (2 5 29 15)
 1006    1:            BOOLEAN TRUE
 1009    4:            OCTET STRING, encapsulates {
 1011    2:              BIT STRING 1 unused bit
    :                      '1100000'B
    :                    }
    :                  }
 1015   29:          SEQUENCE {
 1017    3:                  OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
 1022   22:            OCTET STRING, encapsulates {
 1024   20:              OCTET STRING
    :                      93 DD 21 FC 03 D0 15 0A 72 AD A3 CC D5 9A 09 9D
    :                      38 8B 9D E9
    :                    }
    :                  }
    :                }
    :              }
    :            }
 1046   13:    SEQUENCE {
 1048    9:                  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 1059    0:      NULL
    :            }
 1061  257:    BIT STRING
    :            96 1D 20 03 BC 24 21 EB F5 D4 D3 FE 4A 72 E4 06
    :            69 82 8F 17 A0 84 16 FE AF 6D 35 03 F0 66 47 5D
    :            FD B0 1F 80 B8 9B A2 5B DB 93 B6 53 B2 25 65 56
    :            FD F9 05 BF 6B 84 CE 7C 48 A3 F5 5D AF 5C DB A0
    :            9F F3 2E 33 86 8A 65 55 B8 5F 29 11 95 08 B8 F5
    :            BB 51 17 74 F8 42 51 06 FC 59 67 0C D0 0C 8B 39
    :            78 F7 AA 16 CC 87 BE D4 2F 42 BD 79 A4 6B C1 30
    :            04 35 B9 78 DC 9C BA E4 73 C7 B9 B3 67 93 D5 3D
    :                  [ Another 128 bytes skipped ]
:}
```

9.19 Electronic Signature Qualified Root “InfoCert Qualified Electronic Signature CA 3”

```
 0 1881: SEQUENCE {
 4 1345:   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  165:     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 41:      SET {
 75 39:       SEQUENCE {
 77  3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82 32:         UTF8String 'Qualified Trust Service Provider'
     :        }
     :       }
116 26:      SET {
118 24:       SEQUENCE {
120  3:         OBJECT IDENTIFIER '2 5 4 97'
125 17:         UTF8String 'VATIT-07945211006'
     :        }
     :       }
144 53:      SET {
146 51:       SEQUENCE {
148  3:         OBJECT IDENTIFIER commonName (2 5 4 3)
153 44:         UTF8String
     :          'InfoCert Qualified Electronic Signature CA 3'
     :        }
     :       }
     :     }
199 30:    SEQUENCE {
201 13:      UTCTime 12/12/2016 16:34:43 GMT
216 13:      UTCTime 12/12/2032 17:34:43 GMT
     :     }
231 165:   SEQUENCE {
234 11:      SET {
236  9:       SEQUENCE {
238  3:         OBJECT IDENTIFIER countryName (2 5 4 6)
243  2:         PrintableString 'IT'
     :        }
     :       }
247 24:      SET {
249 22:       SEQUENCE {
251  3:         OBJECT IDENTIFIER organizationName (2 5 4 10)
256 15:         UTF8String 'InfoCert S.p.A.'
     :        }
     :       }
273 41:      SET {
275 39:       SEQUENCE {
277  3:         OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282 32:         UTF8String 'Qualified Trust Service Provider'
```

```
    :         }
    :       }
316  26:      SET {
318  24:        SEQUENCE {
320   3:         OBJECT IDENTIFIER '2 5 4 97'
325  17:         UTF8String 'VATIT-07945211006'
    :         }
    :       }
344  53:      SET {
346  51:        SEQUENCE {
348   3:         OBJECT IDENTIFIER commonName (2 5 4 3)
353  44:         UTF8String
    :          'InfoCert Qualified Electronic Signature CA 3'
    :         }
    :       }
    :     }
399 546:    SEQUENCE {
403  13:      SEQUENCE {
405   9:        OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416   0:        NULL
    :       }
418 527:      BIT STRING, encapsulates {
423 522:        SEQUENCE {
427 513:          INTEGER
    :          00 B7 C1 D3 BF 11 CB A8 28 B6 91 DD E1 11 85 9F
    :          9D 9A 51 25 B3 B2 BC B2 AE AD DF 3E 5D 9F 5A A0
    :          F9 E4 64 C8 34 40 DA AB 7A EC 98 62 05 38 EC 91
    :          EA 84 F9 07 E6 58 DE 58 34 A0 EB 0D 11 19 50 BA
    :          E9 C0 13 C7 60 08 DB E5 AE 00 50 E9 7C 10 16 09
    :          9E 4D F4 EC 7B 14 99 6F D0 A4 67 68 CD 7D 88 1E
    :          D1 3E DA 25 BC 3C 66 61 8D B6 5D D6 F8 CF BA 7A
    :          55 96 86 62 CC 3F 9D D1 B0 2B 58 03 A7 21 49 BC
    :                [ Another 385 bytes skipped ]
944   3:         INTEGER 65537
    :         }
    :       }
    :     }
949 400:    [3] {
953 396:      SEQUENCE {
957  15:        SEQUENCE {
959   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
964   1:         BOOLEAN TRUE
967   5:         OCTET STRING, encapsulates {
969   3:           SEQUENCE {
971   1:             BOOLEAN TRUE
    :           }
    :         }
    :         }
974  88:        SEQUENCE {
976   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
981  81:         OCTET STRING, encapsulates {
```

```
983  79:          SEQUENCE {
985  77:            SEQUENCE {
987   4:              OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
993  69:              SEQUENCE {
995  67:                SEQUENCE {
997   8:                  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1007  55:                    IA5String
     :                'http://www.firma.infocert.it/documentazione/manu'
     :                'ali.php'
     :                }
     :              }
     :            }
     :          }
     :        }
     :      }
1064 239:       SEQUENCE {
1067   3:       OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1072 231:        OCTET STRING, encapsulates {
1075 228:          SEQUENCE {
1078 225:            SEQUENCE {
1081 222:              [0] {
1084 219:                [0] {
1087  37:                  [6] 'http://crl.infocert.it/ca3/qc/ARL.crl'
1126 177:                  [6]
     :                'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
     :                'd%20Electronic%20Signature%20CA%203,ou%3DQualifi'
     :                'ed%20Trust%20Service%20Provider,o%3DINFOCERT%20S'
     :                'PA,c%3DIT?authorityRevocationList'
     :                }
     :              }
     :            }
     :          }
     :        }
     :      }
1306  14:       SEQUENCE {
1308   3:       OBJECT IDENTIFIER keyUsage (2 5 29 15)
1313   1:       BOOLEAN TRUE
1316   4:       OCTET STRING, encapsulates {
1318   2:         BIT STRING 1 unused bit
     :            '1100000'B
     :          }
     :        }
1322  29:       SEQUENCE {
1324   3:       OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1329  22:        OCTET STRING, encapsulates {
1331  20:          OCTET STRING
     :            9B 3B 1B 18 6A 3E A2 04 03 F4 D7 99 10 CF 97 11
     :            4C F1 AA DE
     :          }
     :        }
     :      }
```

```
    :     }
    :   }
1353  13:   SEQUENCE {
1355   9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1366   0:     NULL
    :   }
1368 513:   BIT STRING
    :   54 49 DC F3 76 1F BF 5D 33 B7 78 3A 26 72 4B 2B
    :   50 79 22 70 4A 7E DA EB 8F 26 3C 7F 8D CB 08 8E
    :   96 A6 EB 00 93 5D 82 1D 48 C8 E0 FF C6 1D 69 32
    :   3F E8 F3 FC 7A C7 9C 33 4B 19 FA 13 37 01 7F 54
    :   12 49 A3 51 19 6C 3B 0C 50 F1 D2 97 83 7B CF 4F
    :   58 F4 82 27 98 FB C7 11 97 B8 D7 FC 73 F2 96 41
    :   D1 13 25 07 5A 77 B1 E4 BE 6C 0E BD FA D8 CA 58
    :   5B DC 4B 08 4F EC CC 9F CD E9 E8 9E 7D 43 27 4D
    :         [ Another 384 bytes skipped ]
    :  }
```

Electronic Signature Qualified Root "Infocert Qualified Electronic Signature CA 4"

```
  0 1693: SEQUENCE {
  4 1157:   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  165:     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   41:       SET {
 75   39:         SEQUENCE {
 77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   32:           UTF8String 'Qualified Trust Service Provider'
       :          }
       :        }
116   26:       SET {
118   24:         SEQUENCE {
120    3:           OBJECT IDENTIFIER '2 5 4 97'
125   17:           UTF8String 'VATIT-07945211006'
       :          }
       :        }
```

```
144  53:    SET {
146  51:      SEQUENCE {
148   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
153  44:        UTF8String
     :          'InfoCert Qualified Electronic Signature CA 4'
     :        }
     :      }
     :    }
199  30:   SEQUENCE {
201  13:     UTCTime 23/03/2020 09:21:16 GMT
216  13:     UTCTime 23/03/2036 10:21:16 GMT
     :    }
231 165:   SEQUENCE {
234  11:     SET {
236   9:      SEQUENCE {
238   3:        OBJECT IDENTIFIER countryName (2 5 4 6)
243   2:        PrintableString 'IT'
     :        }
     :      }
247  24:     SET {
249  22:      SEQUENCE {
251   3:        OBJECT IDENTIFIER organizationName (2 5 4 10)
256  15:        UTF8String 'InfoCert S.p.A.'
     :        }
     :      }
273  41:     SET {
275  39:      SEQUENCE {
277   3:        OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282  32:        UTF8String 'Qualified Trust Service Provider'
     :        }
     :      }
316  26:     SET {
318  24:      SEQUENCE {
320   3:        OBJECT IDENTIFIER '2 5 4 97'
325  17:        UTF8String 'VATIT-07945211006'
     :        }
     :      }
344  53:     SET {
346  51:      SEQUENCE {
348   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
```

```
353   44:         UTF8String
      :           'InfoCert Qualified Electronic Signature CA 4'
      :         }
      :       }
      :     }
399  546:    SEQUENCE {
403   13:      SEQUENCE {
405    9:        OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416    0:        NULL
      :       }
418  527:      BIT STRING, encapsulates {
423  522:        SEQUENCE {
427  513:          INTEGER
      :           00 B3 F6 00 3B 90 01 2E AC 2A 26 9E CB 03 0C 02
      :           E3 8A C3 14 FE F6 22 6B 6B B5 31 8E 44 8B 01 C2
      :           80 46 B8 E9 3B A6 84 84 4A AB 45 D4 60 D5 67 AF
      :           9D 57 BA DC EC AE AE AF 4F DD 71 4C 63 9E E2 81
      :           AF 71 16 A6 D2 4A C7 EE 7B EB 2B A4 18 14 6E 35
      :           C8 33 C6 BF AD 43 F9 10 90 97 73 A0 5C 87 B0 19
      :           5E 1E 87 E7 45 70 BE 68 19 EB 53 34 56 15 A5 D4
      :           84 57 6A AA 69 25 F0 48 1C 3A 59 B6 2B EF D9 68
      :           E3 CA 7D E6 39 30 BC BE 38 55 6A 08 D9 F7 B5 37
      :           8A ED B6 15 25 D3 E8 95 B3 3B 3F 7D B4 4F C0 EB
      :           D5 44 D4 A0 7E 93 4A 37 84 8D 2D 3B A2 77 44 48
      :           BC 29 F0 AE 98 85 0A 04 BE DD 3E 4A 73 BA 09 9A
      :           F9 9C DE B8 29 0D A2 E9 70 01 68 37 CB 53 36 80
      :           7B 04 C3 71 64 FE 20 91 B2 37 A1 B5 C7 B9 15 68
      :           C8 22 C5 C2 D8 DC 5D 7C F6 92 E7 D6 12 4B AA C6
      :           61 A9 C8 F3 FE E6 6C 89 8E A5 28 8A 20 7D D1 1F
      :           A8 D4 34 A2 C0 24 E5 07 BB E3 1F AF 07 5C 46 AB
      :           1C 05 52 92 7B FE C4 C4 BD 87 66 FE 2F 4D F3 D9
      :           20 08 45 81 6E A0 03 A3 6E F7 38 DB A0 76 DD 8C
      :           D1 1F 0A E8 6E DB 6F 55 F0 EE 19 6D E7 AA 63 5C
      :           32 03 43 D1 F5 6C 08 16 93 DC 2D 00 B7 38 30 2F
      :           92 56 02 69 BA 0C 9E E2 B9 31 29 DB 2D 29 27 BF
      :           B1 94 9D 36 EE 2E 6F 2D E6 E8 43 17 93 E1 79 EB
      :           76 03 EB 30 7D 39 01 B0 6E 92 51 8D 1B 75 A3 7C
      :           E6 07 F2 24 96 DA 91 A6 5A AC 14 14 2D 8C 79 9C
      :           F4 CD 5A 78 A6 6A B2 7A 6D 2D 5C 78 91 D6 F6 D1
      :           0D 6E 24 4B A6 81 35 4C 58 E8 CA 21 B5 FA 7F 6C
```

```
    :          9A 03 45 51 DA F8 C8 17 2E 6B 95 3D F3 29 C7 DF
    :          80 AC 6D 59 B8 B9 6C 85 9F 9E EC CC 54 76 B4 94
    :          0A 0C 12 93 19 14 B2 E3 87 1D 9C 25 78 4C 9E 75
    :          70 B0 37 5F A9 EF EC 86 FD F8 5A 9B 5F A7 E6 85
    :          9E 5E DD 4A 98 58 86 8C 61 73 1D FF F0 C2 36 98
    :          99
944   3:         INTEGER 65537
    :        }
    :      }
    :    }
949 213:    [3] {
952 210:      SEQUENCE {
955  15:       SEQUENCE {
957   3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
962   1:         BOOLEAN TRUE
965   5:         OCTET STRING, encapsulates {
967   3:           SEQUENCE {
969   1:             BOOLEAN TRUE
    :            }
    :          }
    :        }
972  88:       SEQUENCE {
974   3:         OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
979  81:         OCTET STRING, encapsulates {
981  79:           SEQUENCE {
983  77:             SEQUENCE {
985   4:               OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
991  69:               SEQUENCE {
993  67:                 SEQUENCE {
995   8:                   OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1005  55:                     IA5String
    :                 'http://www.firma.infocert.it/documentazione/manu'
    :                 'ali.php'
    :                 }
    :                }
    :              }
    :            }
    :          }
    :        }
1062  54:       SEQUENCE {
```

```
1064   3:         OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1069  47:         OCTET STRING, encapsulates {
1071  45:           SEQUENCE {
1073  43:             SEQUENCE {
1075  41:               [0] {
1077  39:                 [0] {
1079  37:                   [6] 'http://crl.ca4.infocert.it/qc/ARL.crl'
      :                 }
      :               }
      :             }
      :           }
      :         }
      :       }
1118  14:       SEQUENCE {
1120   3:         OBJECT IDENTIFIER keyUsage (2 5 29 15)
1125   1:         BOOLEAN TRUE
1128   4:         OCTET STRING, encapsulates {
1130   2:           BIT STRING 1 unused bit
      :            '1100000'B
      :         }
      :       }
1134  29:       SEQUENCE {
1136   3:         OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1141  22:         OCTET STRING, encapsulates {
1143  20:           OCTET STRING
      :            5D 7C 6B 61 E8 AC 90 EB 5E C9 D7 BE B4 E3 34 2E
      :            5C 2B 1C DF
      :         }
      :       }
      :     }
      :   }
      : }
1165  13:  SEQUENCE {
1167   9:    OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1178   0:    NULL
      :  }
1180 513:  BIT STRING
      :    80 F2 2D 1C 50 0B 6C 38 DE 22 99 D7 69 5B 92 95
      :    99 AE FD FD 7A 3A 4D 06 D0 01 E3 CE 56 DC AF 5B
      :    A6 23 EB CD 35 DB 11 C0 72 27 79 E6 7B 91 E6 4F
```

```
:    D5 77 D6 68 E3 D2 48 B3 E9 49 D6 5B D4 57 3F E0
:    9E 46 E4 0E F4 CF 66 E6 28 6A 91 F1 BE 3F 42 44
:    0E 75 EB A8 1A D4 24 2C 65 36 9B D5 1E 82 2B 45
:    29 18 3A CC 91 51 66 69 7D FE 6E E2 63 94 DA E1
:    E9 82 AE 9B CE 5E B9 7B 7C E3 08 97 94 DB 57 C9
:    EC D1 9A 71 2B DE 25 2B 85 77 2B 7F 99 97 16 4D
:    7B 84 A9 DF DA 75 C6 62 8B 3B 65 B3 C3 D7 5C 42
:    BA AB FB CE 2D 6B AA B6 EB 6E AD EA 84 52 F1 0F
:    C8 E0 64 9C A1 07 94 9E CF E0 22 E2 D1 3D 71 DD
:    B5 90 6B D5 69 5E 86 7A BF 4D 6C 50 B5 EC CF 8F
:    E4 15 DE 37 C8 5F CE 7A 8A 3E 52 C1 DE AB CF 08
:    1B E9 8D 1D A0 14 8C A7 67 C0 77 3F A4 55 1C F3
:    7A E9 CE 7D C1 99 BE D0 32 37 81 F9 39 95 AF 46
:    EE B8 B3 22 16 9C AA 1D A2 EA F2 B1 67 93 3B 4B
:    2F 71 80 91 5B CE 7F 0D EF F2 BD 31 73 C2 2A 8F
:    E3 F1 B3 99 F0 97 10 4F DE 15 C9 B5 89 ED A7 14
:    0B 57 96 70 AF 76 D2 F0 F9 5E 35 19 5E 4D 67 7F
:    1E 23 D3 FA F6 6E CA DF B1 60 DE 35 38 81 08 21
:    FF 7E 4E 06 3C 8E 75 55 78 AC 55 F0 73 40 84 D2
:    76 97 FE 1E FE 42 E7 9D F3 69 5B BD 45 09 89 AF
:    C9 11 A6 12 E0 E6 BB 34 87 51 21 78 38 FA 4B DA
:    B9 57 6C 3A 85 65 01 DB 7D 27 64 89 C3 83 DD 44
:    0B BF 91 46 EC 94 88 0A DB 7D 4F BD 79 5D 5E 2C
:    07 D0 5D E0 87 6B 3E 68 4F 79 CA DF 1F 15 89 60
:    C2 09 B9 4A 5F D6 D3 38 B0 F8 9A 4F 26 A4 34 D6
:    62 9E 2A 7C 50 BF 43 7E AE F0 5C 31 F2 99 BE DD
:    6B 97 12 E6 42 94 45 44 19 C0 01 33 E4 C8 FA 0B
:    E2 BB D1 F2 A3 25 4A B8 58 12 C3 2A E9 BD 9C FF
:    8D 31 41 5C 8D DC 55 9B B3 DB 9A 64 A0 56 14 8A
:  }
```

9.20 Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature EC CA 4”

```
 0 872: SEQUENCE {
 4 751:   SEQUENCE {
 8   3:     [0] {
10   1:       INTEGER 2
     :     }
```

```
13  20:    INTEGER 0D 32 E7 F4 61 63 3C 34 DE 12 56 26 8E 51 91 97 08 F2 91 EF
35  10:    SEQUENCE {
37   8:     OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
     :    }
47 168:    SEQUENCE {
50  11:     SET {
52   9:      SEQUENCE {
54   3:       OBJECT IDENTIFIER countryName (2 5 4 6)
59   2:       PrintableString 'IT'
     :       }
     :      }
63  24:     SET {
65  22:      SEQUENCE {
67   3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
72  15:        UTF8String 'InfoCert S.p.A.'
     :       }
     :      }
89  41:     SET {
91  39:      SEQUENCE {
93   3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
98  32:        UTF8String 'Qualified Trust Service Provider'
     :       }
     :      }
132  26:    SET {
134  24:     SEQUENCE {
136   3:      OBJECT IDENTIFIER '2 5 4 97'
141  17:       UTF8String 'VATIT-07945211006'
     :       }
     :      }
160  56:    SET {
162  54:     SEQUENCE {
164   3:      OBJECT IDENTIFIER commonName (2 5 4 3)
169  47:       UTF8String
     :         'InfoCert Qualified Electronic Signature EC CA 4'
     :       }
     :      }
     :    }
218  30:    SEQUENCE {
220  13:     UTCTime 07/06/2021 08:43:18 GMT
235  13:     UTCTime 07/06/2036 09:43:18 GMT
```

```
    :     }
250 168:    SEQUENCE {
253  11:     SET {
255   9:      SEQUENCE {
257   3:        OBJECT IDENTIFIER countryName (2 5 4 6)
262   2:        PrintableString 'IT'
    :        }
    :       }
266  24:     SET {
268  22:      SEQUENCE {
270   3:        OBJECT IDENTIFIER organizationName (2 5 4 10)
275  15:         UTF8String 'InfoCert S.p.A.'
    :        }
    :       }
292  41:     SET {
294  39:      SEQUENCE {
296   3:        OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
301  32:         UTF8String 'Qualified Trust Service Provider'
    :        }
    :       }
335  26:     SET {
337  24:      SEQUENCE {
339   3:        OBJECT IDENTIFIER '2 5 4 97'
344  17:         UTF8String 'VATIT-07945211006'
    :        }
    :       }
363  56:     SET {
365  54:      SEQUENCE {
367   3:        OBJECT IDENTIFIER commonName (2 5 4 3)
372  47:         UTF8String
    :          'InfoCert Qualified Electronic Signature EC CA 4'
    :        }
    :       }
    :     }
421 118:    SEQUENCE {
423  16:     SEQUENCE {
425   7:      OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
434   5:      OBJECT IDENTIFIER secp384r1 (1 3 132 0 34)
    :       }
441  98:     BIT STRING
```

```
    :       04 5A 3E C7 0A 5F EB BB 35 7B 85 FF B8 3C AD 7C
    :       D6 06 9B D0 A1 F9 6A E5 7F 95 9B D3 BE 74 E8 64
    :       D0 01 7F F2 B9 ED FF 8B 0C 97 66 6C 28 AC 26 20
    :       B1 28 96 F7 11 12 15 05 B9 94 75 FB CA 95 19 D0
    :       45 57 CD 7B 0E 7E DB A2 89 25 F1 F8 5A 4F 0B 59
    :       CF 9A 8C 68 9E C8 2E 69 56 94 5E 90 83 6F 9D 64
    :       FD
    :     }
541 215:    [3] {
544 212:      SEQUENCE {
547  15:       SEQUENCE {
549   3:        OBJECT IDENTIFIER basicConstraints (2 5 29 19)
554   1:        BOOLEAN TRUE
557   5:        OCTET STRING, encapsulates {
559   3:          SEQUENCE {
561   1:            BOOLEAN TRUE
    :           }
    :         }
    :       }
564  88:       SEQUENCE {
566   3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
571  81:        OCTET STRING, encapsulates {
573  79:          SEQUENCE {
575  77:            SEQUENCE {
577   4:              OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
583  69:              SEQUENCE {
585  67:                SEQUENCE {
587   8:                  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
597  55:                  IA5String
    :                'http://www.firma.infocert.it/documentazione/manu'
    :                'ali.php'
    :                }
    :              }
    :            }
    :          }
    :        }
    :      }
654  56:       SEQUENCE {
656   3:        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
661  49:        OCTET STRING, encapsulates {
```

```
663  47:          SEQUENCE {
665  45:            SEQUENCE {
667  43:              [0] {
669  41:                [0] {
671  39:                  [6] 'http://crl.ca4.infocert.it/qcec/ARL.crl'
     :                }
     :              }
     :            }
     :          }
     :        }
     :      }
712  14:      SEQUENCE {
714   3:        OBJECT IDENTIFIER keyUsage (2 5 29 15)
719   1:        BOOLEAN TRUE
722   4:        OCTET STRING, encapsulates {
724   2:          BIT STRING 1 unused bit
     :           '1100000'B
     :        }
     :      }
728  29:      SEQUENCE {
730   3:        OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
735  22:        OCTET STRING, encapsulates {
737  20:          OCTET STRING
     :           8C DF 7C B8 F0 94 15 36 0B 7F DF 81 71 F5 DB 41
     :           5D 3B FD FC
     :        }
     :      }
     :    }
     :  }
     : }
759  10:  SEQUENCE {
761   8:    OBJECT IDENTIFIER ecdsaWithSHA384 (1 2 840 10045 4 3 3)
     : }
771 103:  BIT STRING, encapsulates {
774 100:    SEQUENCE {
776  48:      INTEGER
     :       7C AF 22 1A 96 90 7C 55 72 88 49 DC B4 03 B6 7B
     :       E4 5F B2 2A CB 78 33 CC D6 EC 38 10 86 F4 21 41
     :       39 7B 78 EA 3D 59 10 BA BA 8C 30 E5 D6 09 2D FC
826  48:      INTEGER
```

```
:      23 5D F8 C0 B2 26 9C D8 0D DA 64 EB 88 50 AB F2
:      44 8F 85 BE 9A 59 7A C1 35 7A 66 4D 54 96 B1 60
:      14 9A 2A C5 8D 63 93 A7 7B 14 78 8E AF 53 03 E3
:    }
:   }
: }
```

9.21 Certificate extensions

The extensions included in the certificates issued and their values are listed below:

VERSION: contains the value 3 as described in § 7.1.1

SERIALNUMBER: automatically assigned by the issuing CA

INNER SIGNATURE: § 7.1.3

ISSUER: contains the following fields valued with the DN of one of the issuing CAs as shown in § Appendix A:

- CountryName
- OrganisationName
- OrganisationUnitName
- OrganisationIdentifier
- CommonName

VALIDITY: maximum 39 (thirty-nine) months, contains the following fields:

- NotBefore
- NotAfter

SUBJECT: contains information relating to the requesting natural person or legal entity. It may contain the following fields, which are subject to variations depending on the type of certificate, further details are specified in § 3.1.

In the case of a certificate issued to a natural person:

- **CountryName**: country code according to ISO 3166.

- **OrganizationName**: when a natural person is associated with an Organisation, the certificate subject field may identify this Organisation using the OrganizationName and OrganizationIdentifier attributes

- **OrganizationalUnitName**: when the attributes related to the Organisation are present, this value contains additional information about the Organisation itself and may appear no more than 4 (four) times

- **OrganizationIdentifier**: see definition of OrganizationName, identifier of the Organisation to which the entity belongs, may be set to the value defined in § 5.1.4 of ETSI EN 319 412-1 (e.g. "VATIT-TaxIdentificationNumber", "NTRIT-IdentifierNationalTradeRegister)

- **GivenName**: Subject's first name

- **Surname**: Surname of the Subject

- **SerialNumber**: identifier of the entity; may be set as defined in § 5.1.3 ETSI EN 319 412-1 and § 3.1.5 of this CPS

- **Title**: particular qualification or role of the Subject, see § 3.2.4. of this CPS

- **LocalityName**

- **DNQualifier**: unique identifier within the CA assigned to the Subject

- **Pseudonym**: valued with the Subject's pseudonym, if GivenName and Surname are present this value cannot be present

- **CommonName**: name of the requesting natural person

In the case of a certificate issued to a legal person:

- **CountryName**: country code according to ISO 3166.
- **OrganisationName**: Registered name of the legal entity
- **OrganizationIdentifier**: identifier of the organisation of the legal entity, may be set as defined in § 5.1.4 ETSI EN 319 412-1 and § 3.1.5 of this CPS
- **CommonName**: name of the legal entity
- **StateOrProvinceName**
- **LocalityName**

PUBLIC KEY: § 6.1.5

EXTENSIONS:

- **AuthorityKeyIdentifier**: identifies the public key which corresponds to the private key used to sign the certificate
- **KeyUsage**: critical marked extension that defines the purpose of the key contained in the certificate and complies with the recommendations ETSI EN 319 412-2 and ETSI EN 319 412-3
- **CRLDistributionPoints**: contains the CRL publication URLs, see § 2.2.3
- **AuthorityInformationAccess**: contains the information to access the services

of the issuing CA, such as the URL of the online validation OCSP service (see § 7.3) and the publication URL of the CA certificate.

- **SubjectKeyIdentifier**: contains the public key identifier of the certificate

- **SubjectDirectoryAttributes**: may be present and contain additional attributes associated with the subject:

- **DateOfBirth**

- **SubjectAlternativeName**: contains e-mail addresses, DNS names, IP addresses and URIs associated with the certificate subject
    - **RFC822Name**: e-mail address of the Subject

- **CertificatePolicies**: contains one or more policies consisting of an OID and optional qualifiers indicating the policies according to which the certificate was issued and the purposes for which it may be used, see § 1.2, 4.5.3, it also contains the publication address of this CPS

- **qcStatements**: (Qualified Certificate Statements) contain an extension for the inclusion of statements identifying specific certificate features:

- **QcCompliance** (0.4.0.1862.1.1): contains the declaration of compliance with European regulation § 9.15 and is present in all certificates issued in accordance with this Operating Manual.

- **QcEuLimitValue** (0.4.0.1862.1.2): if applicable, contains the amount and currency as defined in § 4.5.3

- **QcEURetentionPeriod** (0.4.0.1862.1.3): contains the value 20, intended as the number of years of evidence retention as described in § 3.1.3, 4.9, 5.4.3, 5.5.1

- **QcSSCD** (0.4.0.1862.1.4): if present, states that the private key relative to the

public key contained in the certificate resides in a Qualified Signature/Seal Creation Device (QSCD) see § 1.2

- **QcEuPDS** (0.4.0.1862.1.5): contains the publication URL of the PKI Disclosure Statements (PDS)

- **QcType** (0.4.0.1862.1.6): contains one of the following values according to the purpose for which the certificate is issued
  - id-etsi-qct-esign
  - id-etsi-qct-eseal

- **pkixQCSyntax-v2** (1.3.6.1.5.7.0.18.11.2): if present, contains the semantics for attributes and names contained in certificate fields and extensions as defined by RFC3739:
  - id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1)
  - id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)

SIGNATURE: § 7.1.3

9.22 QCStatement extensions for QSealC PSD2

ETSI extensions: etsi-psd2-qcStatement (QcType)::= 0.4.0.19495.2	*SEQUENCE{* *rolesOfPSP RolesOfPSP,* *nCAName NCAName,* *nCAId NCAId }*
RolesOfPSP	*SEQUENCE{* *roleOfPspOid RoleOfPspOid,* *roleOfPspName RoleOfPspName }*
RoleOfPspOid	itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2

	itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
RoleOfPspName	PSP_AS PSP_PI PSP_AI PSP_IC
NCAName	*plain text name in English of the NCA*
NCAId	• *2 character ISO 3166 country code representing the NCA country;* • *hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and* • *2-8 character NCA identifier without country code (A-Z uppercase only, no separator).*

9.23 CRL and OCSP format

Extension	**Value**
Issuer Signature Algorithm	Based on the CA root certificate key, chosen from sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer Distinguished Name	InfoCert
thisUpdate	Date in UTC format

nextUpdate	Date of next CRL in UTC format
Revoked Certificates List	List of revoked certificates, with serial number and revocation/suspension dates
Issuer's Signature	Signature of the CA

9.24CRL and OCSP values and extension

CRLs have the following extensions

Extension	**Value**
Authority Key Identifier	The value of issuerPublicKey's 160-bit SHA-1 hash
CRL number	Unique CRL number assigned by the CA
ExpiredCertsOnCRL	Date in GeneralizedTime format from which expired certificates are held in the CRL. The value is set to the date of Issuance
Issuing Distribution Point	Identifies the distribution point and purpose of CRLs: it indicates whether a CRL is generated for CA certificates-only, or subject certificates-only (end-entity)
Invalidity Date	Date in UTC format indicating the date from which it is believed that the certificate is invalid

OCSP requests contain 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] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Issuer DN hash
Issuer Key Hash	Issuer public key hash
Serial Number	Certificate serial number

OCSP responses contain the following fields:

Field	Value
Response Status	Status of the OCSP response
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN of the signer certificate of the OCSP response
Produced at	Date in GeneralizedTime format indicating when 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] OR sha-384 [2 16 840 1 101 3 4 2 2] OR sha-512 [2 16 840 1 101 3 4 2 3]
Issuer Name Hash	Hash of the DistinguishName of the issuer
Issuer Key Hash	Hash of the Public key of the issuer
Serial Number	Certificate's serial number
thisUpdate	The verification date in GeneralizedTime format of the certificate status
nextUpdate	The date in which the certificate status may be updated
Issuer Signature Algorithm	Based on the OCSP Responder certificate key, chosen from sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-

	with-SHA512(4)]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

OCSP requests may contain the following extensions:

Extension	**Value**
Nonce	An arbitrary number that can only be used once. It cryptographically binds a request to its response to prevent replay attacks. It is contained in a request Extensions in the case of a request and may be contained in a response Extensions in the case of a response.

ANNEX B

9.25 Tools and methods for digital signature placing and verification

InfoCert provides a special product called "GoSign" available free of charge at www.firma.infocert.it. Dike allows:

- The placing of a digital signature on documents by Subjects who hold a certificate issued by InfoCert;
- Verification of signatures placed on digitally signed documents based on the format set out in the Regulation's implementation acts

GoSign operational environments, hardware and software prerequisites and all information required for product installation can be found on the website shown above. User instructions are included in the product and can be accessed through the Help function. GoSign can sign any type of file. The ability to view a file depends on the availability on the user's workstation of a suitable display software.
For a fee and in accordance with any trade agreements established from time to time with RAs, Subscribers, Subjects or Relying Parties, InfoCert may provide additional signature and/or signature verification products or services.
Electronic documents signed with certificates issued by InfoCert can also be verified through other tools capable of interpreting the signature formats provided. These tools are outside the InfoCert liability.

For example, electronic documents signed with certificates issued by InfoCert in PAdES (PDF Advanced Electronic Signatures) compliant format, can also be verified using the Adobe Reader software.

ANNEX C

This annex provides the list and features of qualified certificates for Spain.
At the moment, the only certificate considered is the Spanish Citizen's Qualified Certificate, which determines the identity of the signatory natural person acting on his/her own behalf.
In general, Spanish public administrations require certificates to be issued for the following uses:
- Authentication based on X.509v3 certificates;
- Electronic signature, advanced or qualified, based on X.509v3 certificates;
- Asymmetric or mixed encryption based on X.509v3 certificates.

The applicable Spanish regulatory references are those between [15] and [19].

The policy for the Spanish citizen's qualified certificate on a qualified device is as follows:

Certificate policy statement of the "Spanish Citizen" issued to natural persons and qualified device-based keys (QSCD)	**1.3.76.36.1.1.10.16.1.1.1** **Compliant with policy QCP-n-qscd 0.4.0.194112.1.2**

9.26 Qualified Certificate of the Spanish Citizen natural person on QSCD issued by the CA root "InfoCert Qualified Electronic Signature CA 4".

Field	**Value**
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 4
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*)***

GivenName:	*Name (mandatory)*
Surname:	*Surname**s** (mandatory)*
SerialNumber:	*as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINES**-NIF or NIE", "**PASES-**PassportNumber", "**IDCES-**DNI or TIE CardNumber") (mandatory)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Common Name	*<DNI or NIE of the subject> + "" + <Name of the subject> <First Surname of the subject> (mandatory)*
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Directory Name	*(mandatory)*
	*Certificate holder **name** (mandatory) (OID 1.3.6.1.4.1.17326.30.7)*
	*Certificate holder **First Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.8)*
	*Certificate holder **Second Surname** (mandatory) (OID 1.3.6.1.4.1.17326.30.9)*
	*Certificate **Description** (mandatory) (OID 1.3.6.1.4.1.17326.30.10) ("CERTIFICADO ELECTRONICO CUALIFICADO DE CIUDADANO")*
User Notice	*Certificado cualificado de Ciudadano. Consulte las condiciones de uso en http://www.firma.infocert.it/documentazione/manuali.php (mandatory)*

(*): it contains the country consistent with the legal Jurisidction under which the certificate is issued

NOTICE

For some formats, executable codes (such as macros or commands) can be entered in the document which do not affect its binary structure but do enable functions which may alter acts, facts or data included in the document. Digitally signed files containing such codes do not count towards Article 25 (2) of the Regulation [1] and cannot be deemed equivalent to a handwritten signature. It is the responsibility of the Subject to use dedicated product features to ensure that no such executable codes are contained in the document.