Website authentication certification service Certificate Policy - Certificate Practice Statement

DOCUMENT CODE	ICERT-INDI-MOWS
VERSION	3.7
DATE (dd/mm/yyyy)	18/04/2023

INFOCERT
TINEXTA GROUP

CONTENTS

1 INTRODUCTION

1.1 GENERAL OVERVIEW

A certificate links the public key to a set of information that identifies the person or the device/system that holds the corresponding private key: this natural or legal person and/or device/system is the **Subject** of the certificate. The certificate is used by other users to obtain the public key, distributed with the certificate, and to verify the certified electronic signature placed on a document or a challenge. The certificate guarantees the correspondence between the public key and the Subject. The level of reliability of this association is given by various factors: the modality with which the Certification Authority issued the certificate, the safety measures adopted, the obligations taken on by the Subject to protect its own private key and the guarantees offered.

This document contains the Cp and CPS, of **InfoCert Trust Service Provider** which, as part of its trust services, also offers web site and Client application certification services. This document contains the policies and practices followed by InfoCert in the control process of the requests, identification of applicants and the issue of certificates, safety measures adopted, obligations, guarantees and responsibilities, and in general, everything that makes a web site and Client application qualified certificate reliable, in compliance with the current regulations governing trust services and the requirements defined in the CAB Forum Guidelines documents (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 2.0.0 of 11 April 2023 referred to hereafter as “Baseline Requirements”[BR] and Guidelines for Extended Validation Certificates 1.8.0 of 30 November 2022 referred to hereafter as “EV Guidelines” [EVG]).

In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

By publishing this document and inserting the reference to this document in the certificates, users are given a chance to assess the characteristics and reliability of the certification service and subsequently the connection between the key and the Subject.

The content of this document is based on current regulations on the date of issue and acknowledges the recommendations of the document “Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” © Internet Society 2003.

This document also contains 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 [9], supplementing the Directive (EU) 2015/2366 (PSD2) [8], in accordance with the requirements defined by the ETSI TS 119 495 standard (referenced below as "PSD2 Certificates").

1.2 DOCUMENT NAME AND ID

This document is known as “InfoCert Trust Service Provider - Website and Client authentication service – CP/CPS” and is characteried by the document ID: **ICERT-INDI-MOWS**. The version and issuing level can be identified in the footnotes on each page.

Object Identifiers (OID) are associated with the document, described below, that are referred to in

the Certificate Policy extension of the certificates, depending on how they are going to be used. The *Object identifier* (OID) identifying InfoCert is 1.3.76.36.
The meaning of the OIDs is the following:

Extentions	Value
Qualified certificate (QWAC) for the validation of the domain and organization controlling the domain for non-browser SSL application (A2A) Also available for PSD2	1.3.76.36.1.1.45.4 compliant with the following policies: ETSI QEVCP-w 0.4.0.194112.1.4 CAbForum 2.23.140.1.2.2 (oid present in the certificates that require this policy) If PSD2, also compliant with ETSI policy QCP-w-psd2 0.4.0.19495.3.1
OV qualified certificate (QWAC) for the validation of the domain and organisation controlling the domain (Organization Validation) Also available for PSD2	1.3.76.36.1.1.45.2 compliant with the following policies: ETSI QEVCP-w 0.4.0.194112.1.4 CabForum 2.23.140.1.2.2 (oid present in the certificates that require this policy) If PSD2, also compliant with ETSI policy QCP-w-psd2 0.4.0.19495.3.1 ***From 20/05/2021 certificates are no longer issued with policy 1.3.76.36.1.1.45.2***
EV qualified certificate (QWAC) for the validation of the domain and organisation that controls the domain extended mode (Extended Validation)	1.3.76.36.1.1.45.3 compliant with the following policies: ETSI QEVCP-w **0.4.0.194112.1.4** CabForum 2.23.140.1.1 policies
OV certificate for the validation of the domain and organisation that controls the domain (Organization Validation)	1.3.76.36.1.1.19.2 compliant with the following policies: ETSI OVCP 0.4.0.2042.1.7 CabForum 2.23.140.1.2.2 policies **From 01/04/2021 certificates are no longer issued with policy 1.3.76.36.1.1.19.2**
OV certificate for the validation of organization (Organization Validation)	1.3.76.36.1.1.19.5 compliant with the following policies: ETSI OVCP 0.4.0.2042.1.7 CabForum 2.23.140.1.2.2

1.3 PARTICIPANTS AND RESPONSIBILITIES

1.3.1 CERTIFICATION AUTHORITY

The Certification Authority is the trusted third party that issues digital qualified certificates, signing them with its own private key, known as the CA key.
InfoCert is the Certification Authority (CA) that issues and revokes the digital qualified certificates,

operating in compliance with CAB Forum requirements, with the technical rules coming from the Supervisory Body and in line with what is established by the eIDAS Regulation[1].

The complete data of CA organization are as follows:

Company name	InfoCert – Società per Azioni Company under the management and coordination of Tinexta S.p.A.
Registered office	Piazza Sallustio no.9, 00187, Rome (ROME)
Operational headquarters	Via Marco e Marcelliano no.45, 00147, Rome (ROME)
Legal representative	Danilo Cattaneo As Managing Director
Registered with the Register of Companies under no.	Tax Code 07945211006
VAT number	07945211006
Web site	https://www.infocert.it

1.3.2 REGISTRATION AUTHORITY (RA)

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:

- the identification of the Applicant (Subscriber),
- the registration of the Subject's data
- sending the Subject's data to the CA systems,
- collecting certificate requests
- providing support to Subscriber and to the CA at any stages of generation, revocation or suspension of the certificates.

Basically, the Registration Authority is responsible for all the interface activities between the Certification Authority or the Subscriber, depending on the agreements reached. The representative mandate known as the "RAO Agreement", regulates the type of activities entrusted to the RA by the CA and the operating procedures for carrying them out.

The CA can delegate most of the activities to a Registration Authority, except for the validation of the domain and the certification of the public key that must be performed by the CA (with the methods provided).

The RAs are activated by the CA following suitable staff training (Validation Specialist); the CA checks the compliance of the procedures used as set out in this Document.

1.3.3 SUBSCRIBER

This is the natural or legal person, also known as Applicant, who requests the CA to issue digital certificates for a Subject, possibly covering costs and assuming the right to suspend or revoke the certificates themselves.

When looking in detail, the following cases can be identified:

- It can be the natural person who holds the power to request a certificate for the Subject (system);
- It can be the legal person who requests a certificate for the Subject (system).

1.3.4 SUBJECT

It is the system or WEB Site for which the Subscriber requests the certificate. In case of client authentication is the natural person owner of the certificate.

1.3.5 USER

It is a system or a person that verifies the Subject's digital certificate, and which relies (relying party in CabForum documents) on the validity of the certificate itself (and/or on the digital signature if present) to assess the correctness and validity of the certified device or certificate, within the contexts in which it is used.

1.3.6 AUTHORITY

1.3.6.1 AGENZIA PER L'ITALIA DIGITALE - AGID

The Agenzia per l'Italia Digitale (**AgID**), is the national supervisory body governing the trust services, in accordance with article 17 of the eIDAS Regulation. In this role, the AgID watches over qualified trust service providers established in Italy to ensure the compliance with the requirements set out in the Regulation.

1.3.6.2 CONFORMITY ASSESSMENT BODY

The conformity assessment body (**CAB)**, is an accredited body in accordance with eIDAS Regulation, capable of carrying out the conformity assessment of the qualified trust service provider and of the qualified trust services provided by it in line with the applicable regulations and standards.

1.3.6.3 NATIONAL COMPETENT AUTHORITY (NCA)

According to PSD2 [8], 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 [8], 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 APPROPRIATE CERTIFICATE USES

Primary use of those certificates is to enable efficient and safe electronic communication, trusted by a CA.
The certificates issued by the InfoCert CA, in accordance with this document, are Qualified Certificates in compliance with the article 45 of eIDAS Regulation “Requirements for qualified certificates for website authentication” or NOT qualified certificates for website and Client authentication in accordance with EIDAS Regulation.

1.4.2 PROHIBITED CERTIFICATE USES

Use of a certificate out of the limits and specific contexts found in this Document and contracts, and in any case, in violation of the limits of use (*key usage*, *extended key usage, user notice*) indicated in the certificate, is forbidden.
Any illegal use is forbidden.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

InfoCert is responsible for drawing up and publishing as well as updating this document.

1.5.2 CONTACTS

Questions, complaints, observations and requests for clarification regarding this Document must be sent to the address and person given below:

InfoCert S.p.A.
Head of the Digital Certification Service
Piazza Luigi da Porto no.3
35131 Padova
Telephone: +39 06 836691
Fax: +39 06 23328861
Digital Signature Call Center: see the link https://help.infocert.it/contatti/
Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

The Subject or Subscriber can request a copy of the documentation regarding him by filling out and sending the form found on the website www.firma.infocert.it and following the procedure shown there. The documentation will be sent in electronic format to the e-mail address indicated in the form.

Revocation requests and reports of suspected private key compromise, misuse of the certificate or other types of fraud or any other matter related to certificates should be sent to the following email addresses

psd2.certificates@infocert.it
certificates.webserver@infocert.it

or, if applicable, communicated by opening a ticket on the appropriate platform.
Revocation requests and reports of suspected private key compromise must follow the procedures described respectively in paragraphs 4.9.3 and 4.9.12.

1.5.3 PERSONS RESPONSIBLE FOR APPROVING THE CPS

This document is checked by the Security and Policies manager, by the Privacy manager, by the CA manager, the Legal Department and the Consultancy Area and is approved by company management.

1.5.4 CPS APPROVAL PROCEDURES

The editing and approval of the document follows the procedures established by InfoCert Quality Management System ISO 9001:2008.
With a frequency not exceeding one year, the trust service provider shall check whether this Document complies with its own certification service issuing process.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

The definitions used when drawing up this document are listed below. For the terms defined by the eIDAS Regulation [1] and by the CAD [2] please refer to the definitions established in them. Where appropriate, the corresponding English term generally used in standards and technical documents is given in square brackets.

EXPIRY	**DEFINITION**
CAB – Conformity Assessment Body	A body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides. It draws up the CAR.
CAR – Conformity Assessment Report	Report with which the conformity assessing body confirms that the qualified trust services provider and the trust services themselves comply with the requirements set out in the Regulation (cf. eIDAS [1]).
authentication	An electronic process allowing to confirm the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form (see eIDAS [1])
web site authentication certificate	A certificate to authenticate a website and link the site to the natural or legal person to whom the certificate is issued (cf. eIDAS [1])
qualified web site authentication	An authentication certificate of the web site that is issued by

certificate (QWAC)	a qualified trust service provider and complies with the requirements found in annex IV (cf. eIDAS [1])
certification key or root key	Pair of cryptographic keys used by the CA to sign the certificates and CRL
private key	The asymmetric key pair element used by the Subject to place his digital signature on an electronic document (cf. CAD [2]).
public key	The asymmetric key pair element intended to be made public. It is used to verify the digital signature applied to the electronic document by the Subject (cf. CAD [2]).
validation	The process for checking and confirming the validity of a signature (cf. eIDAS [1])
CSR	A CSR (Certificate Signing Request) is a coded file that contain the WEB Authentication certificate request. This file contains all the information that the Certification Authorities (CA) use to create the certificate.
validation data	Data used to validate an electronic signature (cf. eIDAS [1])
personal identification data	A collection of data which allows to establish the identity of a natural or legal person, or of a natural person who represents a legal person (cf. eIDAS [1])
data for the creation of an electronic signature	The unique data used by the signatory to create an electronic signature (cf. eIDAS [1])
device for creating an electronic signature	A configured software or hardware used to create an electronic signature (cf. eIDAS [1])
electronic document	Any content stored in electronic format, in particular text or sound, visual or audio-visual recording (cf. eIDAS [1])
electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (cf. eIDAS [1])
Signatory	A natural person who creates an electronic signature (cf. eIDAS [1])
Audit Log (logbook)	The logbook is a collection of records made either automatically or manually, of the events foreseen under the Technical Regulations [5].
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 (cf. 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])
On-line 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.
party relying on the certification	A natural or legal person who relies on an electronic identification or on a trust service (cf. eIDAS [1])
trust service provider	A natural or legal person who provides one or more trust services, either as a qualified or unqualified trust service provider (cf. eIDAS [1])
qualified trust service provider	A trust service provider who provides one or more qualified trust services and to whom the supervisory body grants the title of qualified trust service provider (cf. eIDAS [1])
Product	A hardware or software or their relevant parts, destined for use in providing the trust services (cfc. eIDAS [1])
public official	Person who, as part of its role, is qualified under the law of reference to swear to the identity of natural persons
Directory	The Directory is an archive storing: all the certificates issued by the CA for which the Subscriber requested their publication the list of revoked and suspended certificates (CRL).
revocation or suspension of a certificate:	This is the operation with which the CA revoke or suspend the validity of the certificate before its natural expiry.
trust service	An electronic service normally provided for remuneration and consisting in the following elements: creation, verification and validation of electronic signatures, electronic seals or electronic time stamp, electronic registered delivery services and certificates relating to those services; or creation, verification and validation of authentication certificates of the web site; or the preservation of electronic signatures, seals or certificates related to those services (cf. eIDAS [1])
qualified trust service	A trust service that meets the relevant requirements

	established in the Regulation (cf. eIDAS [1])
Coordinated Universal Time:	Time-scales with precision to the second as defined in ITU-R Recommendation TF.460-5.
electronic time stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time (cf. eIDAS [1])
qualified electronic time stamp	A temporary electronic validation that meets the requirements laid down in article 42 of the eIDAS Regulation (cf. eIDAS [1])
webCam	Small sized video camera, used for transmitting images in streaming via internet and for taking photos. Connected to a PC or integrated into a mobile device, it is used for video chat or video conferences.

1.6.2 ACRONYMS AND ABBREVIATIONS:

ACRONYM	MEANING
AgID	Agenzia per l'Italia Digitale: Supervisory Authority for Trust Service Providers
CA	Certification Authority
CAA	Certification Authority Authentication
CAB	Conformity Assessment Body
CABForum	Certification Authority Browser Forum
CAR	Conformity Assessment Report
CC	Common Criteria
CIE	Electronic Identity Card
CRL	Certificate Revocation List
CRS	Certificate Signing Request
DMZ	Demilitarised 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

EV	Certificate with extended organization validation
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name (è un nome di dominio non ambiguo che specifica la posizione assoluta di un nodo all'interno della gerarchia dell'albero DNS)
HSM	Hardware Secure Module: it is a safety device for the creation of the signature, with functionalities that are similar to smart cards, but with a larger memory and superior performance
http	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IR	Person responsible for Registration
ISO	International Organisation for Standardisation: founded in 1946, the ISO is an international organisation made up of national bodies for standardisation
ITU	International Telecommunication Union: founded in 1865, it is the international organisation that deals with defining telecommunication standards
IUT	Unequivocal Identification of the Owner: this is a code associated with the Subject that unequivocally identifies it to the CA; the Subject has different codes for each certificate in its possession;
LDAP	Lightweight Directory Access Protocol: protocol used to access the certificates register;
LoA	Level of Assurance
NCA	National Competent Authority
NTR Code	National Trade Register Code
OID	Object Identifier: consists of a sequence of numbers, registered in line with the procedure indicated in the ISO/IEC 6523 standard which identifies a certain object within a hierarchy;
OV	Organization validation. Type of WEB authentication certificate with verification of the organization in relation to the certified domain, or Client authentication with verification of the organization
PEC	Certified E-mail
PEM	Privacy Enhanced Mail format to store keys and certificates compliant with RFC 7468
PIN	Personal Identification Number: code associated with a safe

	signature device, used by the Subject to access the functions of the device itself
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure: group of resources, processes and technological means that allow trusted third parties to check and/or guarantee the identity of a subject, as well as associate a public key to a subject
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
RFC	Request for Comment: document that holds information or specifications regarding new research, innovations and methods in the IT world, requested to be assessed by the community by the writers.
RSA	It comes from the initials of the inventors of the algorithm: River, Shamir, Adleman
ISMS	Information security management systems
SPID	Digital Identity Public System
SSCD – QSSCD	Secure Signature Creation Device: device for the creation of an electronic signature Qualified Secure Signature Creation Device: qualified device for the creation of an electronic signature
TIN	Tax Identification Number
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X509	ITU-T Standard for the PKIs
X500	ITU-T Standard for LDAP services and directory

1.6.3 RIFERENCE

[BR]	CA/Browser Forum, “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”.
[EVG]	CA/Browser Forum, “Guidelines For The Issuance And Management Of Extended Validation Certificates”.
[RFC3647]	Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” © Internet Society 2003.

[RFC5280]	Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013
[RFC6962]	Request for Comments: 6962, Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013
[PSD2]	Art 34 Regolamento Delegato (UE) 2018/389 [9], di attuazione della Direttiva (UE) 2015/2366 (PSD2) in conformità con i requisiti definiti dallo standard ETSI TS 119 495
[ETSI411-1]	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. V1.2.2
[ETSI411-2]	ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. V2.2.2
[ETSI401]	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers V2.2.1
[ETSI403]	ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers V2.2.2
[UNICEI]	UNI CEI EN ISO/IEC 17065:2012
[GDPR]	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[DLGS196]	Decreto Legislativo 30 giugno 2003, n. 196
[X.509]	Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
[TP]	TSP Termination Plan available from the CA

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

CRLs and the CP/CPS are published and available 24/7. Above tests pages

InfoCert Organization Validation CA 3:
https://valid.ovcf.ca3.infocert.it
https://expired.ovcf.ca3.infocert.it
https://revoked.ovcf.ca3.infocert.it

InfoCert Organization Validation 2019 CA 3:
https://valid.ovcf2019.ca3.infocert.it
https://expired.ovcf2019.ca3.infocert.it
https://revoked.ovcf2019.ca3.infocert.it

2.2 PUBLICATION OF CERTIFICATE INFORMATION

2.2.1 PUBLICATION OF THE CP/CPS

This Document can be found in electronic format on the Certification Authority's website (cf. § 1.5.2).
This Document, root certificates and other information relating to the CA provided for by law are published in a list of certifiers (at the link https://eidas.agid.gov.it/TL/TSL-IT.xml) and on the Certification Authority's web site (cf. § 1.5.2).

2.2.2 PUBLICATION OF CERTIFICATES

No stipulation

2.2.3 PUBLICATION OF REVOCATION AND SUSPENSION LISTS

The revocation and suspension lists are published in the public register of certificates accessible via LDAP protocol at the address: ldap://ldap.infocert.it or via http protocol at the address http://crl.infocert.it. This access can be made by the software made available by the CA and/or the functions found in the available products on the market which interpret the LDAP and/or HTTP protocol.
The CA may make other methods available other than the one indicated to consult the list of certificates published and their validity.

2.3 TIME OR FREQUENCY OF PUBLICATION

2.3.1 PUBLICATION FREQUENCY OF THE DOCUMENT

This document is published if changes have occurred. If changes are important, the CA must undergo an audit by an accredited CAB, submit the certification report (*CAR – Conformity Assessment Report*) and the CP/CPS to the Supervisory Bodies (AgID) and wait for permission to publish.

2.3.2 PUBLICATION FREQUENCY OF THE REVOCATION AND SUSPENSION LISTS

The CRLs are published every 24 hours.

2.4 ACCESS CONTROLS ON REPOSITORIES

The information regarding CRLs and CP/CPS are publicly available; the CA did not place any restrictions on access on reading and implemented all counter-measures to prevent unauthorised changes/deletion.

3 IDENTIFICATION AND AUTHENTICATION

3.1.1 NAMING

3.1.2 TYPE OF NAMES

The certificate’s Subject is identified with Distinguished Name (DN) attribute that, therefore, must be present and complied with the X500 standard. Certificates are generated according with ETSI standards for issuing qualified certificates and CABForum guidelines.
SSL Wildcard certificate contains an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate. Before issuing, the CA checks if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (for example "* .com", "* .it”); if it is the case, the CA reject the request.

3.1.3 NEED FOR NAMES TO BE MEANINGFUL

The Subject Distinguished Name (SDN) certificate’s attribute unequivocally and clearly identifies the subject (organisation, device or other object) to whom the certificate is issued.

3.1.4 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

No stipulation

3.1.5 RULES FOR INTERPRETING VARIOUS NAME FORMS

InfoCert complies with the X500 standard

3.1.6 UNIQUENESS OF NAMES

The domain name can be found in the WEB site authentication certificate. This can be checked in the archives managed by ICANN (Internet Corporation for Assigned Names and Numbers).
InfoCert applies the uniqueness of each subject name by including the domain (s) in the SubjectAlternativeName extension of the certificate.
The commonName if present must contain a domain also contained within the SubjectAlternativeName.

3.1.7 RECOGNITION, AUTHENTICATION AND ROLE OF THE REGISTERED TRADEMARKS

When the Subscriber requests a certificate from the CA, he promises to operate in full respect of the national and international standards on intellectual property.
CA can Identify the Subscriber with any legal mean for that purpose.
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 Subscriber when he applies for a certificate to be issued.
The identification procedure involves the Subscriber being identified by the CA, even via the RA or its appointers, who shall check the identity via one of the methods defined in this Document.

InfoCert can, at its own discretion, refuse to process the request for a certificate.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

InfoCert establishes that the Subscriber possesses or controls the private key corresponding to the public key to be certified, by checking the signature of the certificate request via the private key corresponding to the public key to be certified.

In the case of Client authentication certificates, the private key can be generated by the CA itself.

3.2.2 AUTHENTICATION OF ORGANISATIONS IDENTITY

Bearing in mind the responsibility of the CA, the identity of the Subscriber is ascertained by the persons qualified to perform the identification task.
The CA maintains internal policies and procedures that are reviewed regularly in order to comply with the requirements of the Baseline Requirements and the Extended Validation Guidelines.
The names of the domains included in a web site OV qualified certificate shall be verified according to what is specified in § 3.2.2 of the Baseline Requirements.
If the Distinguished Name subject of a certificate of web sites or client authentication contains a name in the organisation attribute, the CA shall check the name of the organisation and its existence as specified in § 3.2.2.1 of the Baseline Requirements via the use of government or third party databases or via direct communication with the body that oversees the creation and recognition of a legal entity in the country where it has been established.
Specifically:

- for private Italian or foreign companies, verifications are based on the Company registration report extracted from the business registers where the legal entity is registered; access to business register data is through the service provided by Innolva for consulting the Business Register via the link: https://areainterna.assicom.com/area_interna/ or through the portal https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do.
- for Italian public administrations, verifications take place through the IPA portal https://indicepa.gov.it/ipa-portale/.

3.2.2.1 SUBSCRIBER IDENTIFICATION

The Subscriber's identification shall be ascertained by the persons qualified to perform recognition in the same ways described in the INFOCERT-INDI-MO for issuing certificates with a qualified signature to a natural and/or legal person.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

No stipulation

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

No stipulation

3.2.5 VALIDATION OF AUTHORITY

Based on the information provided by the Subscriber, InfoCert shall proceed with the necessary checks on the data communicated: they must be consistent with each other and, in the case of WEB site authentication certificates, with what has been published in the public registers that record the

Internet domain property (for Italy www.nic.it).
For Public Administrations, reference should be made to national indexes (for Italy www.indicepa.gov.it).
In the case of PSD2 certificates, InfoCert verifies the specific attributes provided by the Requesting Party (authorization number, name and state of the NCA, role of the PSP) using the authentic information made available by EBA within its central registry or, where appropriate, 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.
Furthermore, the content of the CSR (certificate signing request) shall be checked as it must also contain information consistent with what was indicated in the request form (§ 4.2.1).
Any irregularity will make it impossible to issue the certificate. InfoCert reserves the right to ask for additional documentation if it were to become necessary to confirm the authenticity of the requests received.

3.2.5.1 AUTHENTICATION OF FQDNS

Once the information has been certified and approved, InfoCert shall perform the **Domain Control Validation**, that is, it runs a check to ensure that the Subscriber actually has the effective availability of the site that is going to be certified.

DEFINITION	**MEANING**
OV Certificate	InfoCert shall check the right of the Subscriber to use each domain of which it requests the certification by one or more of the following means provided by [BR]: **[BR] section "3.2.2.4.7 DNS Change"** By confirming the presence of a request token in a DNS TXT record on an Authorization Domain Name. **[BR] section "3.2.2.4.4 Constructed Email to Domain Contact"** By sending a random value to an email address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name and receiving a confirming response utilizing the Random Value. **[BR] section "3.2.2.4.18 Agreed-Upon Change to Website v2"** By confirming the presence of a Request Token within a file under the "/.well-known/pki-validation" directory on an Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. InfoCert shall carry out the same aforementioned checks and the controls provided for the authentication of a legal person (please refer to the InfoCert Document ICERT-INDI-MO for qualified certificates).
EV or QWAC	InfoCert shall check the right of the Subscriber to use each domain of which it

Certificate	requests the certification by one or more of the following means: **[BR] section "3.2.2.4.7 DNS Change"** By confirming the presence of a request token in a DNS TXT record on an Authorization Domain Name. **[BR] section "3.2.2.4.4 Constructed Email to Domain Contact"** By sending a random value to an email address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name and receiving a confirming response utilizing the Random Value. **[BR] section "3.2.2.4.18 Agreed-Upon Change to Website v2"** By confirming the presence of a Request Token within a file under the "/.well-known/pki-validation" directory on an Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port. InfoCert shall carry out the same aforementioned checks and the controls provided for the authentication of a legal person (please refer to the InfoCert Document ICERT-INDI-MO for qualified certificates).

Effective from 01/10/2021, the validation of the domain remains valid for 398 days, so that for other requests relating to the same domain the validation operations will not be repeated until the expiration of this period.

3.2.5.2 AUTHENTICATION FOR AN IP ADDRESS

The use of private or internal domain names or reserved private IP addresses is not allowed in any case.

3.2.6 CRITERIA FOR INTEROPERATION

No stipulation

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

InfoCert does not provide for re-key request but only for new issues (see chapter 3 procedure). One month prior to the certificate expiring, it will send the Subscriber a note informing them of the imminent expiration date.

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

No stipulation

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

No stipulation

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The revocation request shall be signed by the subscriber. For details see § 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT FOR A CERTIFICATE APPLICATION

The certificate can be requested by a natural person who represents the legal person by directly contacting the CA following the procedures found on the site www.firma.infocert.it or by drawing up a trade agreement with the CA.

The systems hosting the client or the web sites for which certification is requested need to be located in protected sites in order to prevent any compromising, loss, identification, change or unauthorised use of the server's private key.

Furthermore, these systems need to provide adequate logical security guarantees, that is

- be managed according to documented procedures;
- be protected by firewalls;
- be suitably configured;
- be provided with a control system that limits access to the server itself exclusively to authorised users for authorised purposes.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

The registration process includes the request by the Subscriber (the request form is available in InfoCert website), the request for certification of the public key corresponding to the private key that in the case of Client authentication can be generated by the CA and signing of the contracts, not necessarily in this order.
In the process, the different figures involved have different roles and run parallel with the successful outcome of the issuing:

- The Subscriber is responsible for providing correct, true information on its identity, carefully reading the material made available by the CA and following the instructions of the CA in submitting the request for the certificate; these responsibilities shall be undertaken by the legal representative or person with appropriate power of attorney;
- The Certification Authority is ultimately responsible for identifying the Subscriber and ensuring the success of the registration process of the certificate.

4.2 CERTIFICATE APPLICATION PROCESSING

In order to obtain a web site authentication or client certificate that is either qualified or not, the Subscriber must:

- read this document, the contractual documents and any further informative documentation;
- follow the identification procedures adopted by the CA as described in section 3;
- supply all the information needed for the identification, complete, where necessary, with suitable documentation;
- sign the registration and certification application accepting the contractual conditions that govern the service being provided, on the analogical or electronic forms made available by the CA.

The Subscriber, identified as the legal representative or natural person with power of attorney, **is obliged to provide the following information:**

- name and surname of the Subscriber;
- tax code or similar identification code of the Subscriber (TIN) for foreign citizen
- details of the Subscriber's ID document, type, number, issuing body and its issuing date;
- e-mail for sending communications from the CA to the Subscriber;
- name of the legal person (organisation) holding control of the web sites mentioned in the certification request;
- VAT number or Company Registration number for Italian organisations, VAT code or NTR (national trade register) for foreign organisations.

In the case of PSD2 certificates, the subject (PSP), identified in the legal representative or natural person with 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 the payment service provider (PSP) and has issued the authorization number.

In case of WEB site authentication certificates, the Subscriber must also provide the form that can be found at www.infocertssl.it, filled in and digitally signed.
The Subscriber must provide the CSR (certificate signing request) in PKCS#10 format with PEM (Privacy-Enhanced Mail) codification, digitally signed. In case the CSR can't be sign by the subscriber, InfoCert verified the origin and integrity with different equivalent method.
The name of the domain (or domains) for which the certification is requested, must be precisely indicated in the form and in the CSR; if they are domains of a level beyond the second one, it will be sufficient to check for the presence of the main domain in the aforementioned archives.
The CSR is generated by the Subscriber once the asymmetric key pair has been created; this file, as

well as the information indicated below, will contain the signature of the web site generated with the private key corresponding to the public key to be certified, in order to provide proof of possession of the private key itself.

At the very least, the following information shall be included in the CSR file in the specific fields provided by the PKCS#10 standard (indicated below in brackets):

- the DNS name of the site (sites) to be certified (in DNSName in the SubjectAlternativeName extension);
- the company name of the organisation/body that owns the web site(s) to be certified must be included (in the Organisation field of the subject DN);
- The country code of the organisation/body that owns the web site(s) to be certified (in the Country field of the subject DN, e.g. Italy = IT);

The following information can be included in the CSR file in the specific fields foreseen by the PKCS#10 standard (indicated below in brackets):

- the DNS name of the web site (of one of the sites) to be certified (in the Common Name field of the subject DN).

In order to provide adequate security guarantees, the length of the public key generated according to the RSA algorithm and for which the certification is requested (and the corresponding private key) must be no less than 2048 bits.
The public key certificate can be issue for any kind of Web server found on the market, using the cryptographic algorithms permitted in the SSL protocol, and supported by most of the Web browsers.

In case of Client authentication certificates, the Subscriber must also provide the form that can be found at www.firma.infocert.it/documentazione/, filled in and digitally signed. For multiple requests, the Subscriber can provide in addition an Excel sheet, also digitally signed.
The Subscriber can provide the CSR (certificate signing request) in PKCS#10 format with PEM (Privacy-Enhanced Mail) codification, digitally signed.
The name of the domain (or domains) for which the certification is requested, must be precisely indicated in the form and in the CSR.
The CSR is generated by the Subscriber or by the CA. In case of creation by the Subscriber, once the asymmetric key pair has been created, this file, as well as the information indicated below, will contain the signature of the Client generated with the private key corresponding to the public key to be certified, in order to provide proof of possession of the private key itself.

At the very least, the following information shall be included in the CSR file in the specific fields provided by the PKCS#10 standard (indicated below in brackets):

- the company name of the organisation/body that owns the client to be certified must be included (in the Organisation field of the subject DN);
- the country code of the organisation/body that owns the client to be certified (in the Country field of the subject DN, e.g. Italy = IT);
- the location of the organization/body that owns the client to be certified (in the locality field

of the subject DN, e.g. Italy = IT);

- the name organization/body that owns the client to be certified (in the Common Name field of the subject DN).

In order to provide adequate security guarantees, the length of the public key generated according to the RSA algorithm and for which the certification is requested (and the corresponding private key) must be no less than 2048 bits.

The CA shall not accept any responsibility for failure to comply with the safety conditions given above.

The information provided is stored in the CA archives (registration stage) and will be the elements for generating the certificate.

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

During the initial registration and collection stage of the request for registration and certification, the CA or the RA shall identify each Subscriber and carefully check the information provided according to the methods specified in this document.

With the exception of the domain validation, the CA may delegate the performance of all, or any part, of the RA function to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements. The domain validation must be performed by two different people in trusted role (Validation Specialist).

Effective as of 8 September 2017, as part of the issuance process, the CA checks the DNS for a CAA record for each dNSName in the subjectAltName (WEB site authentication certificates). The value of the CAA record with tag "issue" or "issuewild" must be "infocert.it". If it exists and doesn’t contain “infocert.it” as authorised CA, InfoCert will stop the process and ask the Subscriber whether to proceed despite that record.

InfoCert also checks the certificate against an internal database of previously revoked certificates and rejected certificate requests to identify suspicious certificate requests.

4.2.2 APPROVAL OR REJECTION OF THE APPLICATION FOR A CERTIFICATE

After the initial registration, the CA or the RA can refuse to complete the issuing process of a certificate if there is incomplete or lack of information, negative or incomplete assessment of coherence and consistency of the information provided, of anti-fraud checks, doubts surrounding the Subscriber's identity or Subject’s data, etc. The CA is not obliged to provide an explanation why they declined a certificate request.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time that lapses from when the application is made up to the moment the certificate is generated depends on the kind of request method chosen by the Subscriber and any need to collect further information. No more than 15 days shall elapse from when the CA has correctly identified the Subscriber and the legal person that he represents, and has correctly authenticated the certification application, to when the certificate is generated.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

InfoCert generates the certificate in a protected environment as described in chapter five. In the case of EV or qualified OV certificates, the generation is done using procedures that provide for the simultaneous intervention of two trusted people (dual control).

4.3.2 NOTIFICATION TO THE SUBSCRIBERS THAT THE CERTIFICATE HAS BEEN GENERATED

Once generated, the certificate is sent to the Subscriber in the agreed mode.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONCLUDING ACTIONS FOR ACCEPTANCE OF THE CERTIFICATE

The Subscriber is the only person in charge of installing the certificate on its own software.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CERTIFICATION AUTHORITY

No stipulation

4.4.3 NOTIFICATION TO OTHER SUBJECTS

In conformity to RFC 6962, web authentication pre-certificates are submitted to two different Certificate Transparency (CT) logs for one-year certificates.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

The Subscriber needs to protect the private key from unauthorised access or fraudulent usage.
The Subscriber must guarantee the protection of secrecy and storage of the emergency code needed to suspend the certificate, it must use the certificate exclusively for the methods provided in that Document and under current national and international laws.
The Subscriber must not use private keys for which the certificate has been revoked or suspended or make use of a certificate generated by a CA that has been revoked.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

End user must know where the certificate is used as shown in this Document and in the certificate itself. End user must check the validity of the certificate prior to using the public key contained in it and that the certificate has not been expired or revoked, by checking the relative lists in the certificates register or relative validation service.

4.6 CERTIFICATE RENEWAL

Renewal of the certificate means the issue of a new certificate to the Applicant without changing the public key or any other information on the certificate. InfoCert does not provide this feature.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

InfoCert does not provide for certificate renewal but for new issue only. The expiry notice is not sent in case of Client authentication certificates.

4.7 CERTIFICATE RE-KEY

It consists of creating a new certificate with a new public key and serial number while maintaining the same Subject information.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

It is essential to generate new keys if one wishes to request the re-issuing of the certificate. The new certificate will have the same subject DN data while it could have different values of validity periods, key identifiers, CRL and OCSP distribution points and be signed by a different CA key.

4.7.2 REQUEST FOR CERTIFICATE RE-ISSUING

The request for re-issuing the certificate is validated by the CA in line with the specifications given in § 3.2.5 and § 4.1.

4.7.3 PROCESSING CERTIFICATE RE-ISSUING REQUESTS

Processing complies with what is set out in para. 4.2.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See 4.3.2.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

See 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

No stipulation.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See 4.4.3.

4.8 CHANGE TO THE CERTIFICATE

No stipulation.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The revocation of a certificate removes its validity prior to the established expiry date. Revoked or suspended certificates are inserted in a revocation and suspension list (CRL) signed by the CA who issued them, published in the register of certificates on an established periodic basis. The CA can

impose an unscheduled issuing of the CRL under particular circumstances.
Verification can also be done through the OCSP online service.
The suspension takes away the validity of the certificate for a temporary period. For certificates issued according to this CPS, suspension is not envisaged.

4.9.1 CIRCUMSTANCES FOR REVOCATION

4.9.1.1 CIRCOSTANZE PER LA REVOCA DEL CERTIFICATO DEL RICHEDENTE

The conditions for which the request for revocation must be made within 24 hours are:

- the organization requests in writing that the CA revoke the certificate;
- the organization notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- the private key has been compromised, that is, one of the following cases has arisen:
    - the key's secrecy has been breached;
    - vent has occurred that has compromised the level of the key's reliability;
- the CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (eg when the owner of the domain and / or the network has not renewed the registration, following a provision of judicial authority, etc.);

The conditions for which the request for revocation must be made within five days are:

- the Subject can no longer use the key in its possession (breakage of the device where it is stored);
- a change of the Subject’s data found in the certificate is recorded, to the point that said data is no longer correct and/or true (eg the company has closed);
- the relationship between the Subject and the CA comes to an end, that is, between the Subscriber and CA;
- significant failure to comply with this Document is verified;
- the CA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- the certificate contains wrong data;
- the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted;
- the CA obtains evidence that the Certificate was misused;
- it turns out that a wildcard certificate is used to authenticate a subordinate FQDN in a fraudulent manner;
- incorrect certificate profile, due to a CA error (eg incorrect values in extensions);
- the certificate is not CABForm compliant;

- provision of judicial authority.

4.9.1.2 CIRCOSTANZE PER LA REVOCA DEL CERTIFICATO DELLA CA SUBORDINATA

No Stipulation

4.9.2 WHO CAN REQUEST REVOCATION

Revocation can be requested by:

- The legal representative (Applicant) of the organization that owns the domain (in case of WEB site authentication certificates) or a natural person with a power of attorney, at any time and whatever reason.
- Other third parties involved (Es: Relying Parties Application Software Suppliers) can inform the CA of serious or important facts that required a revocation. Furthermore, anyone can report to the CA facts or circumstances that may, depending on the case, cause the CA to consider the necessity of revoking the certificate.
- In the case of a PSD2 certificate, the NCAs that issued the authorization number to the payment service provider (PSP) in the certificate.
- Judicial authority.

The certificate can be compulsorily revoked by the CA with a notice of 24 hours or 5 days, based on the cases identified by the requirements of the CabForum [BR] and [EVG].

4.9.3 PROCEDURES FOR REVOCATION REQUEST

The Subscriber can request the certificate revocation by filling out the specific form made available on the CA site www.firma.infocert.it and at the RAs, providing the reasons for the request, by attaching the relative documentation, if available, and specifying the data of the Subject of the certificate communicated to the CA when the certificate was issued. The request must be made in writing, digitally signed and sent to e-mail addresses or by opening a ticket as described in paragraph 1.5.2.

The CA shall verify the authenticity of the request and proceed with revoking the certificate.

In the case of a PSD2 certificate and that the request has come from NCA, the CA will investigate the reason for this request.

Additional methods for requesting a revocation by the Applicant can be specified in agreements stipulated with the CA.

Should the need arise, the CA has the right to revoke the certificate communicating this to the Subscriber and providing the reason for the revocation as well as the date and effective time.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The grace period for the revocation request is the time that can elapse between the identification of an event for which it is necessary to request the revocation of the certificate, and the moment when the revocation request is sent to the CA. If the private key corresponding with the certificate is lost or compromised, the Subscriber must request the revocation of the certificate as soon as possible.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The request is processed within 24 hours in the most serious cases or 5 days in other cases. If the request is properly authenticated, it is processed immediately.

The request for revocation that comes from Third Parties involved that informs the CA of reasonable and important causes for the revocation of the certificate, is taken care of by providing a preliminary report to the applicant for the certificate and to the subjects involved in the request within 24 hours. In the event that the need to revoke the certificate is verified, the CA in agreement with the applicant and the entities involved decides the date on which the certificate will be revoked. In any case, the revocation date must not exceed the terms described above. The date must be agreed taking into account some aspects such as the impacts of the revocation, the type of problem detected, the number of certificates involved, the origin of the request (eg judicial authority) and the current legislation.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Prior to relying on information found in the certificate, the user must confirm the validity of the certificate as provided for by the IETF PKIX standards, including checking the validity, the concatenation of the issuer-subject names, the policy and key usage limits, the revocation status via CRL or OCSP service for each certificate in the chain.

4.9.7 CRL ISSUANCE FREQUENCY

The revoked or suspended certificates are inserted in a revocation and suspension list (CRL) signed by the CA and published in the Public Register. The CRL is published every hour (ordinary issuing) and remains valid for 24 hours. Under circumstances, the CA may impose an unscheduled issuance of the CRL (immediate extraordinary issue), for example in the case where the revocation or suspension of a certificate occurs if there is a suspicion that the private key’s secrecy has been compromised (immediate revocation or suspension). The CRL is always issued in its entirety. When the CRL is published, it is certified by using the date provided by the Time Stamping Authority InfoCert system as time reference and a recording is made in the logBook to certify for the publication in question. Each element in the CRL list contains the date and time of revocation or suspension in the specific extension. The CA can publish separately other CRLs, subsets of the general CRL, to reduce the network load. The acquisition and consulting of the CRL shall be done by the users. The CRL to be consulted for the specific certificate is indicated in the certificate itself in compliance with current regulation.

4.9.8 MAXIMUM LATENCY PERIOD OF THE CRLS

The CRL is published few minutes after his generation and no more than one hour.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

As well as the publication of the CRL in the LDAP registers and http, InfoCert also makes available an OCSP service for checking the status of the certificate. The service’s URL is shown into the certificate. The service is available 24/7.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The CA supports the GET method for requests as described in RFC 6960. In accordance with CabForum, OCSP responders do not respond with the 'good' status for certificates that have not been issued.

4.9.11 OTHER FORMS OF REVOCATION PUBLISHING AVAILABLE

No stipulation

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

To report the compromise of a key, users can contact InfoCert as indicated in paragraph 1.5.2.

The methods for demonstrating key compromise are:

- sending a CSR which must be signed with the compromised private key and which must contain the value communicated by InfoCert in the CN;
- the response to a challenge provided by InfoCert which must be signed with the compromised private key.

Detailed operating instructions will be communicated by InfoCert.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

No stipulation.

4.9.14 WHO CAN REQUEST SUSPENSION

No stipulation

4.9.15 PROCEDURES FOR SUSPENSION REQUEST

No stipulation

4.9.16 LIMITS ON SUSPENSION PERIOD

No stipulation

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

Information on the status of the certificates is available via CRL and the OCSP service. The serial number on the revoked certificate remains in CRL even after the certificate's validity has expired and at least until the CA certificate expires.
The information provided by the OCSP service is updated within 5 minutes, while the CRL information is updated hourly.

4.10.2 SERVICE AVAILABILITY

The OCSP service and CRLs are available 24/7. The answer in both cases is provided within 3 seconds from receiving the corresponding request.

4.10.3 OPTIONAL FEATURES

No stipulation

4.11 END OF SUBSCRIPTION

The relationship of the Subject and/or Subscriber with the Certification Authority ends when the certificate expires or is revoked, with the exception of specific cases defined at contractual level.

4.12 KEY ESCROW AND RECOVERY

No stipulation

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

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

- a physical level aimed at ensuring the security of environments where CA 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.

InfoCert Security policies are reviewed no less than yearly; they are also updated against any significant changes. Each revision is tracked in the document even when no changes had to be made.

5.1 PHYSICAL CONTROLS

The measures implemented 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 and;
- Magnetic media storage sites

5.1.1 SITE LOCATION AND CONSTRUCTION

The InfoCert primary delivery site is located at the company's headquarters 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 40 Gbit/s MPLS 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 business continuity services with RTO/RPO values close to zero, some components of the CA services related to the publication of CRLs and OCSP are hosted on the AWS cloud, respectively, in the Europe Frankfurt Region and the Europe Ireland Region.

AWS has compliance certifications under ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 standards.

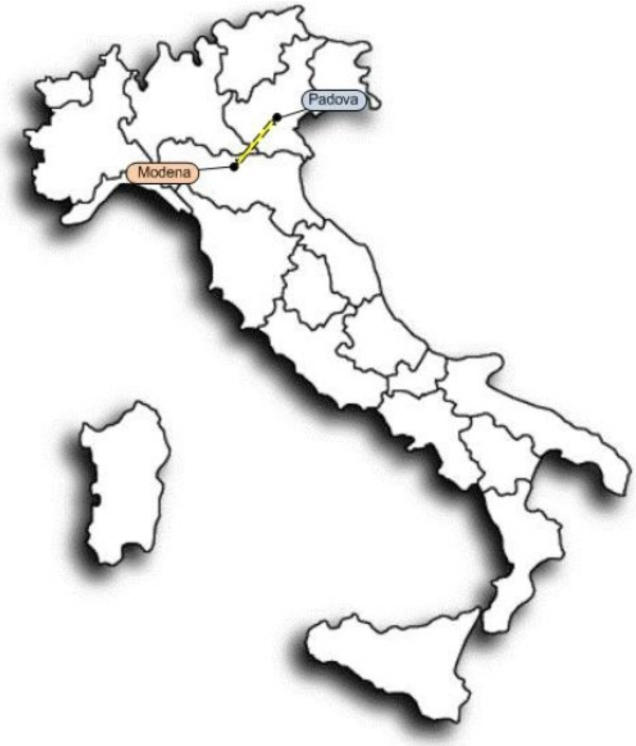

FIGURE 1 - INFOCERT DATA CENTRE LOCATION AND DISASTER RECOVERY SITE

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

The delivery site in Padua, while not being certified, has the characteristics of a 3 tier Data Centre.
The technical rooms are fitted with an electric power supply system designed to prevent breakdowns and, above all, disservices. The system's power supply includes the most modern technology with a view to increasing reliability and ensuring redundancy for essential functionalities.
The power supply infrastructure includes:

- UPSs, fitted with AC accumulators;
- AC voltage available (220-380V AC);
- redundant power supply cabinets with protected lines and with a size suitable for the agreed absorption;
- emergency generator service;
- automatic commutation system and synchronisation between generators, network and batteries (STS).

Each technological cabinet installed into the Data Centre uses two electrical lines that guarantee

the HA in the event that one of the two available lines gets interrupted.
The technological cabinet is monitored remotely; continuous controls are carried out on the status of the electric lines (on/off) and the electrical power absorbed (each line should not exceed 50% of the load).
The technical area is normally maintained between 20°C and 27°C with a relative humidity level of between 30% and 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 served by emergency generators in the event of a power cut. Cabinet refrigerating capacity is guaranteed with a maximum foreseen load of 10kW and a maximum of 15kW on two cabinets side by side.

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 rooms 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 eco-friendly ARGON IG-01 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 MEDIA STORAGE

With regard to the storage platform, the current solution uses NetApp systems (FAS 8060) for the NAS part. For the SAN part was implemented an infrastructure based on EMC2 technology (including VNX 7600, VNX 5200 and XtremIO) which is managed through the VPLEX storage virtualisation layer. This infrastructure is managed through ViPR.

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 BACK-UP

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

The key roles are covered by figures with the necessary experience, professionalism and technical and legal skills, that are continually checked on an annual basis.
The list of names and the organisation chart of the figures in key roles was deposited at the AgID with the first credit and is constantly kept up to date in order to follow the natural evolution of the company organisation.

5.2.2 NUMERO DI PERSONE RICHIESTE PER LO SVOLGIMENTO DELLE ATTIVITÀ

Keys management takes place in a access restricted area and involves two trusted people ('dual control'). For certificate vetting of OV, EV e QWAC at least two people ('Validation Specialist')are involved.

5.2.3 IDENTIFICAZIONE E AUTENTICAZIONE PER CIASCUN RUOLO

Truested people involved must authenticate to the system with his own personal role assigned.

5.2.4 RUOLI CHE RICHIEDONO LA SEPARAZIONE DEI COMPITI

Different people cover different trusted roles.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Once the yearly Human Resources plan has been drawn up, the Head of the Function/Organisational Structure identifies the specifications and resource skills to be inserted (*job profile*). Following this, and in conjunction with the selection manager, the research and selection process begins.

5.3.2 BACKGROUND CHECK PROCEDURES

The candidates identified participate in the selection process facing an initial cognitive-motivational interview with the head of HR and a second technical interview with the head of the Function/Organisational Structure, aimed at checking the skills declared by the candidate. Further verification tools are exercises and tests.

5.3.3 TRAINING REQUIREMENTS

As a guarantee that no single individual can singularly compromise or alter the global security of the system or do anything unauthorised, the operating management of the system will be assigned to different people, with separate, clearly defined roles. The member of staff assigned to the programming and providing of the certification service is selected based on his experience in programming, creating and managing IT services as well as of his reliability and reserved nature. Training is periodically arranged to develop familiarity with the assigned roles. Prior to placing a member of staff on operational duty, training is given with a view to providing every kind of skill (technical, organisational and procedural) required to carry out the tasks assigned.
In particular, the ' Validation Specialist' that manages the vetting phase is trained on PKI,

identification and validation procedure, threats, CabForum requirements ([BR] e [EVGL]). Documentation of this training is provided upon request.

5.3.4 RETRAINING FREQUENCY

At the start of each year, an analysis of training needs is carried out, preparatory to defining the training to be given throughout the year. The analysis is structured as follows:

- Meeting with Management to collect the data relating to the training requirements needed to satisfy company aims;
- Interview with Heads to gather data on training requirements specific to their own areas;
- Return of the collected data to Company Management for closure and approval of the Training Plan.

Within the month of February, the Training Plan as defined is shared and made public.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation

5.3.6 SANCTIONS FOR UNAUTHORISED ACTIONS

Please refer to the “Metalworkers and private industry plant installation National Collective Bargaining Agreement” (“CCNL Metalmeccanici e installazione impianti industria privata”) for the procedures on imposing sanctions.

5.3.7 CONTROLS ON NON-EMPLOYEE STAFF

Non-employees who participate in the issue of certificates are subject to the same functional and safety conditions as employees who work in the same positions.

5.3.8 DOCUMENTATION TO BE SUPPLIED BY PERSONNEL

When being hired, the employee must provide a valid copy of an identification document, as well as a copy of a valid health card and a passport type photo for his/her badge to access the areas. He/she will subsequently have to fill out and sign the authorisation to process personal data and the commitment to not disseminate confidential news and/or documents. Lastly, he/she must review InfoCert’s Code of Ethics and Netiquette policy.

For each role, the necessary documentation or details are provided to perform the tasks: in particular this CPS, the Baseline Requirements, the EV Guidelines, the Network Security Requirements of the CabForum.

5.4 AUDIT LOGGING PROCEDURES: LOGBOOK MANAGMENT

Events linked to the management of the CA and life of the certificate are collected in the logBook as provided by the Guidelines and technical rules [5].

5.4.1 TYPES OF EVENTS RECORDED

Security events are recorded as well as starting up and turning off, system crashes and hardware breakages, firewall activities and routers and attempts to access the PKI systems.

All the data and documents used at the identification and acceptance of the Subscriber’s request stage, are kept: a copy of the identity card, contract and Chamber of Commerce company

registration etc.
Events linked to the registration and life cycle of the certificates are recorded: the certificate requests, the certificate's registrations and its generation, distribution and any revocation/suspension.
Each event is saved with system date and time of the event.

5.4.2 FREQUENCY OF PROCESSING LOGBOOK

The processing and grouping of data as well as back-up are completed at least monthly on the InfoCert electronic documents preservation services that are compliant with the applicable legislation on the long-term preservation of electronic documents.

5.4.3 RETENTION PERIOD LOGBOOK IS KEPT FOR

The logBook is kept for at least 20 years by the CA and is made available upon request to Auditors.
Logs related to the life cycle of the certificate shall be preserved for at least 20 years after the expiration of the certificate, up to a maximum of 23 years from the date of issuance.

5.4.4 RETENTION PERIOD FOR LOGBOOK

The protection of the logBook is guaranteed by the InfoCert electronic documents long-term Preservation Services.

5.4.5 BACK-UP PROCEDURES FOR THE LOGBOOK

The compliant long-term Preservation Services for electronic documents carries out a back-up procedure policy, as set out in the safety manual of the above-mentioned services.

5.4.6 LOGBOOK COLLECTION

The collection of event logs is done via automatic ad hoc procedures; back-up occurs in the manner provided for by the InfoCert compliant long-term Preservation Services and described in the safety manual of the above-mentioned system.

5.4.7 NOTIFICATION IN THE EVENT OF VULNERABILITY IDENTIFICATION

No stipulation.

5.4.8 VULNERABILITY ASSESSMENTS

InfoCert periodically carries out vulnerability assessments on the System and anti-penetration tests. Based on the results, it sets in motion all the countermeasures to ensure applications are safe.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF ARCHIVED RECORDS

The records relating to the most important events of a Certification Authority are drawn up and archived.

5.5.2 RETENTION PERIOD

Records are preserved for 20 years by the Certification Authority in InfoCert long-term

Preservation Services of electronic documents.

5.5.3 PROTECTING THE RECORDS

Protection is guaranteed by the compliant InfoCert documents long-term Preservation Services.

5.5.4 ARCHIVE BACKUP PROCEDURES

The compliant long-term Preservation Services for InfoCert electronic documents implement a back-up policy and procedure, as set out in the safety manual of the above-mentioned system.

5.5.5 REQUIREMENTS FOR THE TIMESTAMP AND RECORDS

No stipulation

5.5.6 ARCHIVES BACK-UP SYSTEM

The collection of records is done via automatic ad hoc procedures and back-up occurs in the manner provided for by the compliant InfoCert long-term Preservation Services and described in the safety manual of the above-mentioned system.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY THE INFORMATION ARCHIVED

The data are all stored on the compliant InfoCert long-term Preservation Services of electronic documents, which provide for timely checks on system status and data integrity.
The exhibition of data is carried out as established by the law.

5.6 KEY CHANGEOVER

The CA periodically replaces the certification private key used for signing the certificates, in order to allow the Subject to be able to use the certificate in his possession up until it is renewed. Each replacement will lead to a change in this manual and communication to the Supervisory bodies (AgID).

5.7 CA PRIVATE KEY COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

The CA has described the procedures for managing incidents under the SGSI certificate ISO 27000. Any incident, as soon as it is reported, is subject to strict analysis and identification of corrective countermeasures and is recorded by the service manager. The report is digitally signed and sent to the compliant InfoCert long-term Preservation Services; a copy is also sent to AgID, together with the declaration of actions to be taken aimed at eliminating the causes that may have given rise to the accident, if under the control of InfoCert.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the event of breakdown of the HSM signature safety device containing the certification keys, the spare copy of the certification key is used, suitably stored and kept, and there is no need to revoke the corresponding CA certificate.
The software and data are subject to regular backups as provided by internal procedures.

5.7.3 PROCEDURES IN THE CASE OF THE CA PRIVATE KEY BEING COMPROMISED

The compromise of the certification key is considered a particularly serious event as it would invalidate the certificates signed and issued using that key. Particular focus is, therefore, placed on protecting the certification key and all the system's development and maintenance activities that can have an impact on it.
InfoCert described the procedure to be followed in the event of the key becoming compromised, under the SGSI certificate ISO 27000, also highlighting the AgID and CAB.
Description of the procedure

- a security incident is open
- escalation and comunication to the stakeholder
- notification to CamerFirma (root della subCA InfoCert)
- the service is close
- the private key is deleted from HSM
- notification to AGID (Supervisory Body) to update the EUTSL (EU Trusted list)
- notification to the CAB
- notification to customer

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

InfoCert has adopted the necessary procedures for ensuring the continuity of the service even in extremely difficult or disastrous situations.

5.8 CA TERMINATION

If the certification activity being terminated, InfoCert will communicate its intention to the Supervisory Body (AgID) at least three months in advance, indicating, if necessary, the replacement certifier and the certificate register and relevant documents holder. Equally in advance, InfoCert shall inform all those holding certificates issued by their own CA, of the activities termination. In the communication, if there is no replacement certifier indicated, it will clearly be specified that all certificates that have not yet expired at the moment of termination of the CA’s activities, are revoked.
It is possible to ask InfoCert for more details.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 KEY PAIR GENERATION FOR CA

In order to provide its service, the Certification Authority needs to generate a certification 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 following 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.

6.1.1.2 KEY GENERATION FOR RA

No Stipulation

6.1.1.3 KEY GENERATION FOR SUSBSCRIBER

All the request not in line with the prevision in § 6.1.5 e § 6.1.6 will be refused.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

For Client authentication certificates only, InfoCert supplies to the subscriber the key pair and the whole certification chain, through Password protected PKCS # 12.

The CA will revoke all the certificates corresponding to the private key, if it is communicated to an unauthorized Applicant.

6.1.3 HANDING OVER OF THE PUBLIC KEY TO THE CA

Subscribers generate Key Pairs and submit the Public Key to CA in a CSR as part of the certificate request process. The request is signed.

6.1.4 CA PUBLIC KEY DELIVERY TO USERS

The CA public key is kept in the CA certificate. The CA certificate is made available to users in such a way as to make it impossible for it to be replaced. The certificate is made public through the inclusion in the lists of trusted Root CAs managed by the main manufacturers of operating systems and browsers and through the Trust-service Status List (TSL) published on the Agid website.

6.1.5 ALGORITHM AND LENGTH OF THE KEYS

The pair of certification asymmetrical keys is generated inside a cryptographic hardware device mentioned above. The RSA asymmetrical algorithm with keys of a length no less than 4096 bits is used.

The Subject keys can 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 QUALITY CHECKING AND PUBLIC KEY GENERATION

The CA confirms that public keys meet the requirements of §6.1.6 of the [BR].

6.1.7 KEY USAGE PURPOSES

The purpose for using the private key is determined by the KeyUsage extension as defined in the X509 standard. The only use permitted for the certificates described in this Document is the authentication of web sites.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CONTROLS AND STANDARDS OF THE CRYPTOGRAPHIC MODULE

The cryptographic modules used by InfoCert for the certification keys (CA) and for the OCSP responder are validated FIPS 140 Level 3 and/or 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.

6.2.2 MULTI-USER CONTROL OF THE CA PRIVATE KEY

Access to the devices containing the certification keys only takes place with two people authenticated at the same time.

6.2.3 CA PRIVATE KEY ESCROW

No stipulation.

6.2.4 CA private key backup

The backup of the keys is contained in a safe which can only be accessed by the member of staff who has no access to the HSM devices. Any reinstating, therefore, requires the presence of both the member of staff who has access to the devices and the member of staff who has access to the safe.

6.2.5 CA PRIVATE KEY ARCHIVAL

No stipulation.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

No stipulation

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The certification key is generated and backed-up in a protected area of the cryptographic device that inhibits its exportation. Furthermore, the device's operating system, in the event of its protection being forced, blocks the device or makes it illegible.

6.2.8 PRIVATE KEY ACTIVATION METHOD

The certification private key is activated by the CA software in dual control, that is, two people with specific roles and in the presence of the service manager.
The Subject or Applicant legal representative of the legal person is in charge of protecting its own private key with a safe password to prevent unauthorised use. In order to activate the private key, the Subject must authenticate itself.

6.2.9 PRIVATE KEY DEACTIVATION METHOD

n/a

6.2.10 METHOD FOR DESTROYING THE CA PRIVATE KEY

The InfoCert member of staff entrusted with this role deals with the destruction of the private key when the certificate has expired or been revoked, according to the safety procedures provided for by the safety policies and device manufacturer’s guidelines.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See § 6.2.1

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

See § 5.5

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The period of validity of the certificate is determined on the basis of:

- the state of technology;
- the state of art of the cryptographic knowledge;
- the planned use for the certificate itself.

The certificate’s validity interval is expressed inside.
Starting from 01/09/2020 the certificates conforming to CAbForum requirements are valid for no more than one year. PSD2 QWAC certificates issued to a natural or legal person are valid for no more than two years.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data are generated in accordance with the HSM manufacturers' specifications and according to the safety practices adopted by the certifier.

6.4.2 ACTIVATION DATA PROTECTION

The protection of certificate activation data is borne by the Applicants. For the CA keys, see §.6.1.1

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No Stipulation

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The operating system of computers used in certification activities for generating keys, for generating certificates and for managing the certificates register, are secured (via hardening procedures), that is, they are configured in order to minimise the impact of any vulnerability by eliminating all the functions that are of no use for the operation and management of the CA.
Access to the system by the Administrators, appointed for the purpose in compliance with current legislation, is done via an on-demand root application that allows for the use of privileges of the root user only subject to individual authentication. Accesses are tracked, logged and stored for 12 months.

6.5.2 COMPUTER SECURITY RATING

No stipulation.

6.6 CONTROL SYSTEM OPERATION

InfoCert attributes strategic important to the safe processing of the information and recognises the need to constantly expand, maintain, control and improve an Information Safety Management System (SGSI) in compliance with ISO/IEC 27001 standard.
InfoCert has been certified ISO/IEC 27001:2005 since March 2011 for the EA:33-35 activities. In March 2015 it was certified for the new version of the ISO/IEC 27001:2013 standard.
Procedures and controls are provided in SGSI for:

- Asset Management;
- Access Control;
- Physical and Environmental security;

- Operation Activities security;
- Communications security;
- Acquisition, Development and Maintenance of the Systems;
- Incident Management;
- Operational Continuity.

All the procedures are approved by the relative heads and shared internally in the InfoCert document management system.

6.7 NETWORK SECURITY CONTROLS

InfoCert created a safety infrastructure of the network for the certification service, based on the use of firewall mechanisms and SSL protocol in order to create a safe channel between the Registration Offices and the certification system, as well as between this and the administrators/operators.
InfoCert's systems and networks are linked to the Internet in a controlled manner by a firewall system that allows for the connection to be split into safety areas that are progressively greater: Internet network, DMZ (Demilitarised Zone) or Perimeter networks and Internal Networks. All the traffic that flows between the various areas is subject to acceptance by the firewall, based on a set of established rules. The rules defined on the firewalls are designed on the basis of “default deny” principles (what is not expressly permitted is forbidden by default, that is, the rules will only permit what is strictly necessary for the correct functioning of the application) and “defence in depth” (further levels of defence are organised, firstly at network level, via successive firewall barriers, and lastly the hardening at system level).

6.8 TIME-STAMPING

InfoCert provides a service of qualified time stamping (see CPS named ICER-IND-TSA, published in InfoCert website)
All InfoCert system are syncronized with the same time sources of the time stamping service.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The information indicated in the certification request appears in the certificate. The certificate format produced complies with eiDAS Regulation; this way full readability and verifiability is guaranteed in the context of the European standards and certifiers.
InfoCert uses the ITU X.509 version 3 standard for the entire PKI structure.
The root certificate and subCAs paths are in the Appendix.

7.1.1 VERSION NUMBER

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

7.1.2 CERTIFICATE EXTENSIONS

Qualified certificates are characterised by the extension found in the qcStatement clause 3.2.6 of IETF RFC 3739. Their use is regulated by the ETSI 319 412-5 standard.
See the Appendix B for the extensions.

7.1.2.1 ROOT CA CERTIFICATE

See Annex A

7.1.2.2 SUBCA ROOT CERTIFICATES

See Annex A

7.1.2.3 END USER CERTIFICATES

See §7.1.2.5

7.1.2.4 ALL CERTIFICATES

Other extension can be used in conformance to §7.1.2.5

7.1.2.5 RFC 5280 COMPLIANCE

The certificate is compliant to RFC 5280 and CabForum guidelines [BR] e [EVG]

7.1.3 SIGNING ALGORITHM OBJECT IDENTIFIERS

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 contains an unequivocal serial number inside the CA that issued it.

ISSUER INFORMATION

The issuer DistinguishName is the DistinguishName of the CA that issue the certificate.

ENDUSER INFORMATION

See §3.2.2 e § 3.2.3.

7.1.4.1 SAN EXTENTION

See §7.1.2.5

7.1.4.2 SUBJECT DISTINGUISHEDNAME

See §7.1.2.5

ROOT CA AND SUBCA CERTIFICATE INFORMATION.

See Apendix A

7.1.5 NAME CONSTRAINTS

See section 3.1.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

See section 1.2.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

See section 7.1.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.2 CRL PROFILE

To form the lists of revoked CRLs, InfoCert uses the RFC5280 profile "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)" and adds to the basic format, extensions as defined by RFC 5280: "Authority Key Identifier", "CRL Number "," Issuing Distribution Point "and" expiredCertsOnCRL ".

7.2.1 VERSION NUMBER

All the certificates issued by InfoCert are X.509 version 2.

7.2.2 CRL EXTENSIONS

For the CRL extensions, see Annex B.

7.3 OCSP PROFILE

To be able to establish the certificate revocation status without making a request to the CRL, InfoCert makes OCSP services available that comply with the RFC6960 profile “X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol – OCSP”. This protocol specifies the data that needs to be exchanged by an application that wishes to check the certificate status and OCSP service.

7.3.1 VERSION NUMBER

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

7.3.2 OCSP EXTENSIONS

For the OCSP extensions, see Annex B.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In order to obtain the qualification of qualified and unqualified trust service provider, in compliance with the EIDAS Regulation, it is essential to complete the process provided for under article 21 of the above mentioned Regulation.
InfoCert presented the specific request to AgID to obtain recognition as “qualified trust service provider” attaching a conformity assessment report to the Regulation (Conformity Assessment Report - CAR) issued by an assessment body authorised by the national appointed body (CAB), which in Italy is ACCREDIA.
InfoCert offers the Service as qualified trust service provider under EU Regulations 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., in compliance with the Regulations mentioned above and the ETSI EN 319 401 Standard, according to the eIDAS assessment layout drawn up by ACCREDIA based on the ETSI EN 319_403 and UNI CEI EN ISO/IEC 17065:2012 standards.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The conformity assessment report is issued every year. In this period one or more other audit session are performed.
InfoCert will publish in his website the conformity assessment report in three months after it has been released.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The control is carried out by:

Company name	CSQA Certification S.r.l.
Registered office	Via S. Gaetano no. 74, 36016 Thiene (Vicenza)
Telephone no.	+39 0445 313011
Registered with the Register of Companies under no.	Tax Code 02603680246 Vicenza Company Register no. 02603680246 / REA no. 258305
VAT number	02603680246
Web site	http://www.csqa.it

8.3 RELATIONS BETWEEN INFOCERT AND CAB

InfoCert and CSQA have no financial interests nor business relations.
There are no trade or partnership relations that could create bias in favour of, or against InfoCert in CSQA's objective assessment.

8.4 TOPICS COVERED BY ASSESSMENT

The CAB is called upon to assess conformity compared to the Document, the Regulation and applicable rules of the procedures adopted, CA organisation, role organisation, staff training and contractual documents.

8.5 ACTIONS TAKEN AS A RESULT OF NON-COMPLIANCE

In the event of non-compliance, the CAB will decide whether to send a report to the AgID anyway or reserve the right to carry out another audit after the non-compliance has been rectified.
InfoCert aims to deal with all non-compliance aspects as quickly as possible, setting in motion all the actions required for improvement and adaptation.

8.6 COMUNICAZIONE DEI RISULTATI DELLE VERIFICHE

The audit report produced by the CAB is sent to the the Italian supervisory body (AgID), and to "AC Camerfirma SA" which, being the CA Root that certifies the InfoCert subCA and maintains relations with Mozilla and communicates the results of the audit.
The conformity assessment is shared with the service responsible and it is published no later than three months from the date of the audit.
Internal audits are carried out in compliance with an annual audit program and concern specific aspects of the service, as well as broader aspects relating to the certification authority. The results of these audits are communicated to the service manager and to all the people directly involved.

8.7 SELF AUDITS

During the period in which the CA issues certificates, the internal auditor deals with periodic or aperiodic audits. The internal auditor checks the quality of the service by coordinating or performing periodic audits on a quarterly basis, on the issuance of SSL certificates: sample verification of the certificates issued (3%), their life cycle and existing evidence relating to the controls carried out for the purpose of issuing the certificates themselves. The internal auditor also has the task of verifying that the certificate issuance service complies with what is described in the CP / CPS, in the ETSI standards and in the CABForum guidelines.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 FEES FOR ISSUING AND RENEWING CERTIFICATES

The fees are available from these sites https://www.firma.infocert.it/ and https://ecommerce.infocert.it, or from the Registration Authority. The CA creates trade agreements with the RAs, and/or the Applicants applying specific rates.

9.1.2 FEES FOR ACCESSING CERTIFICATES

No stipulation.

9.1.3 FEES FOR ACCESSING REVOCATION OR SUSPENSION STATUS INFORMATION

Access to the list of revoked or suspended certificates is free.

9.1.4 FEES FOR OTHER SERVICES

The fees are available from these sites https://www.firma.infocert.it/ and https://ecommerce.infocert.it, or by the Registration Authorities.
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 can exercise the right to withdraw from contract within 14 days from the date of its conclusion and to obtain refund of the paid price. Instructions for exercising the right to withdrawal and refund request are available at https://help.infocert.it/ or at RA offices.

9.2 FINANCIAL RESPONSIBILITIES

9.2.1 INSURANCE COVERAGE

TSP InfoCert has stipulated an insurance contract covering risks during work and damage caused to third parties, whose text was negotiated and accepted by AgID; insurance coverage limits are:

- 10,000,000 Euro for a single accident
- 10,000,000 Euro for the second year.

9.2.2 OTHER ASSETS

No stipulation

9.2.3 WARRANTY AND INSURANCE COVERAGE FOR END-ENTITIES

See section 9.2.1.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Handling confidential information is not part of the activities mentioned in this document.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

No stipulation

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

No stipulation

9.4 PRIVACY OF PERSONAL INFORMATION

Save as expressly permitted, any Subject's/Subscriber's information acquired by the CA while performing its routine activities shall be considered as confidential and non-publishable, except for those specifically intended for public use [e.g. public key, certificate (if requested by the Subject), certificate revocation and suspension dates]. Particularly, personal data are processed by the Certification Authority in accordance with Legislative Decree No. 196 of 30 June 2003 and Regulation (EU) 2016/679 of the Parliament [DLGS196] and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which will be fully binding as from 25 May 2018 [GDPR]. .

9.4.1 PRIVACY PLAN

InfoCert adopts a set of policies via which it implements and integrates the protection of personal data within its Information Security Management System certificate ISO 27001, sharing with this latter system the process for continuous improvement.

9.4.2 INFORMATION TREATED AS PRIVATE

Data that falls under the corresponding definition found in the current law is handled as personal [4]; personal data refers to any information regarding the physical person, identified or identifiable, even indirectly, via 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 revocation and suspension dates – is not considered personal data.

9.4.4 PERSONAL DATA PROTECTION RESPONSIBILITY

InfoCert S.p.A.
Operating Headquarters
Via Marco e Marcelliano, 45
00147 Rome
richieste.privacy@legalmail.it

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

The privacy report can be found on the website www.infocert.it.
Prior to carrying out any personal data processing, InfoCert shall proceed with obtaining authorisation to the processing in compliance with the law [4].

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

The disclosure of data on request from the Authorities is mandatory and is done following the instructions established step by step by the Authorities themselves.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Not applicable.

9.5 INTELLECTUAL PROPERTY RIGHTS

The copyright in this document belongs to InfoCert SpA. Rights are partially reserved.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA 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. Annex to the Commission Implementing Regulation 2015/1502.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

In the latter case, representation is carried out by a mandate given by InfoCert to the Registration Office 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 Statement, 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.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

The Subscriber is responsible for the truthfulness of the data communicated in the Registration and Certification Request. If at the time of the identification the Subscriber has concealed his or her real identity or falsely declared to be another person or declared false information about legal 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 document (revocation and suspension of the certificate).

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

See §4.5.2

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No Stipulation

9.7 DISCLAIMERS OF WARRANTIES

The Certification Authority does not provide any warranties on (i) the proper operativity and safety of hardware and software used by the Subscriber; (ii) the use of a 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 certificate - or of any message, deed or document associated with it or created by means of the keys to which the certificate is referred; (v) the secrecy and/or integrity of any message, deed or document associated with the certificate or created by means of the keys to which the certificate is referred to.

The Certification Authority guarantees only the functioning of the Service, according to the levels speficied in paragraph 9.17 of this Certificate Practice Statement.

9.8 LIMITATIONS OF LIABILITY

The Certification Authority does not assume any obligation on monitoring the content, type, or electronic format of documents and/or, eventually, of hashes transmitted by the IT procedure specified by the Subscriber or the Subject, and does not assume any responsibility.

Except in case of wilful misconduct or 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 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 third parties unauthorized by InfoCert tampering or interfering with the service or equipment.

9.9 INDEMNITIES

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

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 to the Certificate, as indicated in the “Validity” section of the Certificate.

9.10.2 TERMINATION

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 (Payment), 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, about the resolution of disputes relating to online contracts and services offered online, there is the possibility of resorting to the Online Dispute Resolution (ODR) procedure, 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 Subscriber breaces 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 Subcriber 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 Subscriber 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 TERMINATION EFFECTS

Termination involves the immediate revocation of the certificate.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

See section 1.5.2.

9.12 DOCUMENT AMENDMENTS

The CA reserves the right to make changes to this document for technical purposes as well as changes to procedures intervening both as a result of laws or regulations and to maximise the work cycle. Each new version of the Document cancels and replaces the previous versions that remain, however, applicable to certificates issued during their validity and up until their first expiry date. In any case, an annual review is scheduled.
Variations that do not have a significant impact on users lead to the increase in the number of documents released, while variations with a significant impact on users (such as, for example, changes regarding operative procedures) lead to an increase in the number of versions of the document. In any case, the manual will rapidly be published and made available following the methods provided.
If the changes are relevant, the CA must undergo an audit by an accredited CAB, present the certification report (*CAR – Conformity Assessment Report*) and the Document to the Supervisory Bodies (AgID) and wait for permission to publish.

Version/issue n°:	3.7
Date	18/04/2023
Description	InfoCert logo update § 1.1 updating CabForum BR versions and EV guidelines § 1.2 QEVCP-w policy name update §§ 5.1.1, 5.1.3, 5.1.5 Review of facility aspects § 5.4.2 Revision of the description § 5.8 Modification of notice periods in case of termination §§ 6.1.5, 7.1.3 Algorithms and keys review § Annex B CRL and OCSP format update

Reasons	Update CabForum BR and EV version guidelines Periodic review Rebranding

Version/issue n°:	3.6
Date	06/05/2022
Description	§ 1.1 updating CabForum BR versions and EV guidelines § 1.6.3 deletion of versions § 3.2.2 disclosure of verification sources § 5 Periodicity of review of security policies. §§ 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.5.2, 5.5.3, 5.5.4, 5.5.6, 5.5.7, 5.7.1 clarifications regarding regulatory long-term preservation § 6.3.2 description update § Appendix B Description of certificate extensions Formatting for document accessibility
Reasons	Update CabForum BR and EV version guidelines Periodic review

Version/issue n°:	3.5
Date	10/09/2021
Description	§ 1.1 update of CabForum BR and EV guidelines versions § 1.5.2 change of contact information § 3.2.5.1 modification of the reuse period for domain validation
Reasons	Contact information and CabForum BR and EV guidelines update

Version/issue n°:	3.4
Date	14/06/2021
Description	§ 1.1 update of CabForum BR and EV guidelines versions § 1.2 policy disposal § 1.5.2 adding contacts for revocation requests and other communications on suspected key compromise or fraud § 3.2.5 improved description of validation methods with reference to

	[BR] § 4.2.1 clarification on the CAA record § 4.9.12 procedure description in case of key compromise § 5.1.1 technology upgrade Spelling and form corrections
Reasons	Periodic review

Version/issue n°:	3.3
Date	29/10/2020
Description	§ 1.1 and § 1.6.3 update of CabForum BR and EV guidelines versions § 1.2: clarification on use of CabForum policy 2.23.140.1.2.2 § 1.2 removal of obsolete sentence § 1.3.5: description improvement § 3.1.1 description improvement § 3.1.6 modified paragraph title § 3.2.2 description improvement § 3.3.0 and § 4.6.1: adjustment to a new procedure § 4.4.3 and § 6.3.2 adjustment for up to one-year duration of certificates compliant with CabForum regulations. § 4.9.1.1: added circumstance of revocation § 5.1.1: technology update § 5.3.8: added reference to CabForum Network Security Requirements § 1.1 update of CabForum BR and EV guidelines versions § 1.5.2 contacts update § 3.2.5.1 modification of the reuse period for domain validation
Reasons	Contacts update Update of CabForum BR and EV guidelines

Version/issue n°:	3.2
Date	11/02/20202
Description	New SubCa § 1.1 New version BR ed EV guidelines CabForum § 1.3.4 Owner § 1.3.5 Relying Party § 1.5.1 new paragraph § 1.6.3 new paragraph § 2.1 New test URL for subCa § 3.2.6 new paragraph § 3.3 new paragraph 3.3.1 e 3.3.2. § 3.4 new paragraph § 4.4.3 CT Log mngt

	§ 4.6 better description § 4.7 new paragraph 4.7.4, 4.7.5, 4.7.6, 4.7.7 § 4.9 new paragraph 4.9.1.2 § 4.9.8 better description § 5.2.2 new paragraph § 5.2.3 new paragraph § 5.2.4 new paragraph § 5.3.3 better description § 5.3.5 No Stipulation § 5.3.7 new condition § 5.3.8 better description § 5.3.8 better description § 5.5.2 better description § 5.5.3 better description § 5.7.3 better description § 5.8 Better description § 6.1.1.1 modified title § 6.1.1.2 new paragraph § 6.1.1.3 new paragraph § 6.1.2 better description § 6.1.4 better description § 6.1.6 better description § 6.3.2 certificate validity Client e Server § 6.4.1 new paragraph § 6.4.2 new paragraph § 6.4.3 new paragraph § 6.5.2 new paragraph § 7.1.2 new paragraph 7.1.2.1, 7.1.2.2, 7.1.2.3, 7.1.2.4, 7.1.2.5 § 7.1.4 new paragraph 7.1.4.1, 7.1.4.2, 7.1.4.2.1, 7.1.4.2.1, 7.1.4.2.2, 7.1.4.3, 7.1.4.3.1 § 7.1.7 new paragraph § 7.1.8 new paragraph § 7.1.9 new paragraph § 6.8 new paragraph § 8.6 new paragraph § 8.7 new paragraph§ 9.6.2 new paragraph § 9.6.3 new paragraph § 9.6.4 new paragraph § 9.6.5 new paragraph § 9.9.1 new paragraph § 9.9.2 new paragraph § 9.9.3 new paragraph § 9.12.2 better description § 9.12.3 better description § 9.16.4 new paragraph § 9.16.5 new paragraph

Reasons	New root SubCa Summary RFC3647 Substitute n/a with No Stipulation New BR and EV guidelines CabForum

Version/issue n°:	**3.1**
Version/issue date:	27/11/2019
Description of changes:	Description of client authentication certificates added. § 1.1 BR and EV CabForum guidelines updated § 1.2 OID updated § 3.2.5 phone call as an additional method of domain validation added
Reasons:	Annual revision Issuing client certification certificate BR and EV CabForum guidelines updating

Version/Issue no.:	**3.0**
Version/Issue Date:	30/11/2018
Description of changes:	§ 1.1 Upgrade of CABForum documents version, PSD2 description, CABForum policy error correction § 1.2 OID and description updated § 3.1.5 CommonName deprecated § 3.2.5 CA preliminary investigation for PSD2 certificates § 3.2.5 Domain validation mode updated § 4.2 PSD2 request processing § 4.9 Revocation, paragraph revision
Reasons:	Annual review Issuing of PSD2 compliant certificates Review of checks Modification of the company name TecnoInvestimenti

Version/Issue no.:	**2.1**
Version/Issue Date:	20/06/2018
Description of changes:	§ 1.5.1 Contact update § 9.2.1 Insurance coverage § 9.9 Indemnities
Reasons:	Change in Call Center number Change in insurance ceilings

Version/Issue no.:	**2.0**
Version/Issue Date:	06/12/2017
Description of changes:	Some definition updated Ortography correction Dropped all about l Domain Validation Best described RA rola Added other revocation motivation Added link to CA e subCA Corrected seciton numeration of chapter 4
Reasons:	Aligning the manual to the most recent CAB Forum requirements of 7 January 2017

Version/Issue no.:	**1.1**
Version/Issue Date:	08/02/2017
Description of changes:	Definitions: updates of some definitions Introduction: the description of the service has improved OID for unqualified 1.3.76.36.1.1.19.2 certificate § 4.2.1 Details added on the CSR § 4.2.4 SLA's reviewed Form and spelling correction
Reasons:	Aligning the manual to the most recent CAB Forum requirements of 7 January 2017

Version/Issue no.:	1.0
Version/Issue Date:	12/12/2016
Description of changes:	
Reasons:	new issuing of the document

9.12.1 REVISION PROCEDURES

The revision procedures in the Document are similar to the editing procedures. Revisions are made jointly with the Head of the Certification Service, Head of Security, Head of Privacy, the Legal Office and the Consulting Area, and approved by management.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This document is reviewed and updated at least once every year. Even if no changes are made to the document, the version number is increased, a log entry is added and the review date is updated.
The Document is published:

- in electronic format on the InfoCert website

(address: http://www.firma.infocert.it/doc/manuali.htm)

- paper format can be requested from the Registration Authority or from the contact person for end users.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

Please consult the contract governing the service for details of dispute resolution methods.

9.14 GOVERNING LAW

For consumers, jurisdiction shall be in the city where the consumer resides. For those other than consumers, jurisdiction shall be in Rome. In the agreements between CA and RA, between CA and the Applicant or between CA and the Subject, a different jurisdiction can be established.

9.15 COMPLIANCE WITH APPLICABLE LAW

The law governing this Document is Italian law.
The following is a complete list of the main applicable laws for reference:

[1] EU Regulation no. 910/2014 of the European Parliament and Council dated 23 July 2014 governing electronic identification and trust service for electronic transactions in the entire market and that repeals Directive 1999/93/EC (also referred to as *eIDAS Regulation*).

[2] Italian Legislative Decree no. 82 dated 7 March 2005, (OJ no. 112 of 16 May 2005) – Digital administration Code (also referred to as *CAD*) as amended.

[3] not used

[4] Italian Legislative Decree no. 196 of 30 June 2003, (OJ no. 174 of 29 July 2003) – Privacy Policy as amended and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as on the free movement of such data (in force since 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 related national transposing legislation.

[8] 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;

[9] 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.

Furthermore, all the circular letters and deliberations from the Supervisory Authorities[1], as well as the implementation acts provided for under the eIDAS Regulation [1].

9.16 MISCELLANEOUS PROVISIONS

Please consult the contract governing the service for any other regulation not found in this Document.

9.16.1 ENTIRE AGREEMENT

The entire agreement is publicly available in InfoCert Website.

9.16.2 ASSIGNMENT

The assignment of validation to an RA is accompanied by a special agreement between InfoCert and the organization acting as Registration Authority for InfoCert.

9.16.3 SEVERABILITY

If a national court declares a provision of this document to be invalid, the other provisions remain valid. The CA will modify its procedures the minimum to remain as close as possible to the guidelines.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

See terms and conditions

9.16.5 FORCE MAJEURE

See terms and conditions

9.17 OTHER PROVISIONS

The service provision times are (with the exception of different contractual agreements):

SERVICE	TIMES
Access to the public certificates archive (includes the certificates and CRLs).	From 0:00 to 24:00 24/7 (99% minimum monthly availability)
Revocation and suspension of certificates.	From 0:00 to 24:00 24/7
Other activities: registration, generation.	From 9:00 to 17:00 from Monday to Friday excluding holidays
Request and/or timestamp checking.	24/7 (minimum availability 99%)

[1] Available on the website http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

ANNEX A: CA ROOT CERTIFICATES AND SUBCA HIERARCHY

InfoCert Root CA 3
http://cert.infocert.it/ca3/root/CA.crt
serial number: c35de37e34e4917f4a8d9f7c92bcaa4f9ee6afa
key identifier: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert Organization Validation SHA256 - CA 3
Issued by:

- CN: InfoCert Root CA 3
- OU: WSA Trust Service Provider.
- O: InfoCert S.p.A..
- C:IT
- Certificate serial number: 44841e74619f52cb

http://cert.infocert.it/ca3/ovca/CA.crt
serial number: 7d04f008647c18b07ee55a1f5a45874c7b45855b
key identifier: 070bf5de8672fc47ade69234e42f8ae6a1a7b95a
authority key identifier: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert Extended Validation SHA256 - CA 3
Issued by:

- CN: InfoCert Root CA 3
- OU: WSA Trust Service Provider.
- O: InfoCert S.p.A..
- C:IT

http://cert.infocert.it/ca3/evca/CA.crt
serial number: 6b445ba522e87824cff71ce8444f9bb887f5e4b1
key identifier: 2495f85228f235c5b1856b458850c84719b3ef81
authority key identifier: d6dfbc3fe137e715f774ce1bd62605e57846691d

InfoCert CA3 OV (CamerFirma trusted)
http://cert.infocert.it/ca3/ovcf/CA.crt
Issued by:

- CN:Global Chambersign Root – 2008
- O:AC Camerfirma S.A.
- SN:A82743287
- L:Madrid (see current address at www.camerfirma.com/address)
- C:EU
- Numero di serie certificato: 44841e74619f52cb

serial number: 0249528bfbff7ddf

key identifier: 5f0ebbb9cf47920c26345605bfdc9d9e18bdc925
authority key identifier: 5b1bee037ba2dbe746c0c254aba150295ff156d7

InfoCert 2019 CA3 OV CamerFirma trusted
http://cert.infocert.it/ca3/ovcf2019/CA.crt
Issued by:

- CN:Global Chambersign Root – 2008
- O:AC Camerfirma S.A.
- SN:A82743287
- L:Madrid (see current address at www.camerfirma.com/address)
- C:EU
- Numero di serie certificato: 00c9cdd3e9d57d23ce

Serial number: 31b31444fdd6c2a78f0a9c
Key identifier: 8832bf09fb4239f472432068b8cfac8a92785d0c
Authority Key identifier: 5b1bee037ba2dbe746c0c254aba150295ff156d7

ANNEX B: CRL AND OCSP FORMAT

CERTIFICATE EXTENSIONS

The extensions contained in the issued certificates and their valorization are shown in the list below, and valorization is done in accordance with the ETSI standards for issuing qualified certificates and according to CABForum guidelines.

VERSION: it contains the value 3 as described in§ 7.1.1
SERIALNUMBER: automatically assigned by the issuing CA
INNER SIGNATURE: § 7.1.3

ISSUER: it contains the following fields valorized with the DN of one of the issuing CAs as shown in § Annex A:

- CountryName
- OrganizationName
- OrganizationalUnitName
- OrganizationIdentifier
- CommonName

VALIDITY: § 6.3.2, it contains the following fields:

- NotBefore
- NotAfter

SUBJECT: it contains information about the subject that identifies the organization; it may contain the following fields that are subject to variations in relation to the certificate, further details are specified at the § 3.1:

- **CountryName:** Country code according to ISO 3166, which identifies the country where the Organization holding the certificate is headquartered
- **OrganizationName**: Registered name of the Organization (legal person) holding the certificate and verified in the manner described in§ 3.2
- **OrganizationalUnitName**: (deprecated from 01/09/2022)
- **OrganizationIdentifier:** identifier of the Organization holding the certificate; if for PSD2 it is valued as defined in § 5.2.1 ETSI EN 119 495
- **CommonName:** it contains a Fully Qualified Domain Name (FQDN) among those present in the SAN extension
- **StateOrProvinceName:** it contains the name of the province or region where the

Organization is headquartered

- **LocalityName:** it contains the name of the city where the Organization is is headquartered
- **StreetAddress:** [EVG] § 9.2.6
- **PostalCode**: [EVG] § 9.2.6
- **SerialNumber**: [EVG] § 9.2.5
- **BusinessCategory**: it contains the type of activity carried out by the Organization in accordance with [EVG] § 9.2.3
- **JurisdictionLocalityName**: [EVG] § 9.2.4
- **JurisdictionStateOrProvinceName**: [EVG] § 9.2.4
- **JurisdictionCountryName**: [EVG] § 9.2.4

PUBLIC KEY: § 6.1.5

EXTENSIONS:

- **AuthorityKeyIdentifier**: it identifies the public key corresponding to the private key used to sign the certificate
- **KeyUsage**: it contains the purpose of the key contained in the certificate and follows the guidelines of CABForum [BR] § 7.1
- **ExtKeyUsage**: it contains one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes contained in the KeyUsage extension
  - id-kp-serverAuth
  - id-kp-clientAuth
- **CRLDistributionPoints**: it contains the publication URLs of the CRLs, see § 2.2.3
- **AuthorityInformationAccess**: it contains information for accessing the issuing CA's services, such as the URL of the online validation service - OCSP (see § 7.3) and the publication URL of the CA certificate.
- **SubjectKeyIdentifier**: it contains the public key identifier of the certificate
- **SubjectAlternativeName**: it contains the authenticated FQDNs (see § 3.2.5)
  - dnsName
- **CertificatePolicies**: it contains one or more criteria consisting of an OID and optional qualifiers indicating the policies under which the certificate was issued and the purposes for which it can be used, see § 1.2; it also contains the publication address of this Certificate Practice Statement (CPS).
- **qcStatements**: (*Qualified Certificate Statements*) extension present only in the case of qualified certificates (QWAC); it contains an extension for the inclusion of declarations that identify specific properties of the certificate:
  - **QcCompliance** (0.4.0.1862.1.1): it contains the declaration of compliance with eIDAS

Regulation (EU) No. 910/2014 and is present in every qualified certificate issued in accordance with this Certificate Practice Statement (CSP).

- **QcEURetentionPeriod** (0.4.0.1862.1.3): it contains the value 20, meaning the number of years of evidence preservation as described in the § 3.1.3, 4.9, 5.4.3, 5.5.1
- **QcEuPDS** (0.4.0.1862.1.5): it contains the publication URL of the PKI Disclosure Statements (PDS)
- **QcType** (0.4.0.1862.1.6): it contains id-etsi-qct-web

SIGNATURE: § 7.1.3

QCSTATEMENT EXTENSIONS FOR QWAC 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).

FORMAT OF CRL AND OCSP

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

VALUES AND EXTENSIONS FOR CRLS E OCSPS

CRLs have the following extensions:

Extension	Value
Authority Key Identifier	The value of the issuerPublicKey 160-bit SHA-1 imprint value
CRL number	The unequivocal number of the CRL assigned by the CA
ExpiredCertsOnCRL	The GeneralizedTime format date from which the expired certificates are kept in CRL.
Issuing Distribution Point	Identifies the distribution point of the CRLs and the aim: indicates if the CRL is generated only for CA certificates or end-entity certificates
Invalidity Date	Date in UTC format that indicates the date from which the certificate is regarded as invalid

The OCSP request contains the following fields:

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

The OCSP response contains the following fields:

Field	Value
Response Status	OCSP response status
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN of the certificate signatory of the OCSP response
Produced at	Date in GeneralizedTime format that indicates when the OCSP 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 issuer's DN
Issuer Key Hash	Issuer's public key hash.
Serial Number	Certificate serial number
This Update	Certificate status verification date in GeneralizedTime format
Next Update	Date when the certificate status could be updated
Issuer Signature Algorithm	Based on the OCSP Responder certificate key, chosen among 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)]s
Issuer’s Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

OCSP EXTENSIONS

The OCSP request can contain the following extensions:

Extension	Value
nonce	An arbitrary number that can be used only once. Cryptographically it links a request to its response to prevent replica attacks. It is contained in a requestExtensions in the case of a request, while in the case of a response it can be contained in a responseExtension.