CERTIFICATE POLICY & CERTIFICATE PRACTICE STATEMENT

DOCUMENT CODE   ICERT-INDI-MOWS
VERSION   3.9
DATE   22/05/2025

tinexta
infocert

CONTENTS

tinexta
infocert

tinexta
infocert

1 INTRODUCTION

1.1 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 (hereinafter briefly referred to as "CA") 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 is the Certificate Practice Statement of the Trust Service Provider InfoCert (hereinafter also simply "InfoCert"), which, among its trust services, also provides authentication services for websites. This CPS 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 2.1.4 of 1 March 2025 referred to hereafter as "Baseline Requirements"[BR] and Guidelines for Extended Validation Certificates 2.0.1 of 6 May 2024 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").

tinexta
infocert

1.2 Document name and Identification

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**. For version and release level information, please see the cover page and the par. 9.12.2

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 domain and organization validation controlling the domain for non-browser SSL application (A2A) **Also available for PSD2 with 1-year validity**	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 certificates requiring this policy)
Qualified Certificate (QWAC) for domain and organization validation controlling the domain for non-browser SSL applications (A2A) **Also available for PSD2 and OpenBanking services with 2-year validity**	1.3.76.36.1.1.45.5 Compliant with ETSI QNCP-w-gen policy — 0.4.0.194112.1.6 ***Also compliant with ETSI policy 0.4.0.194112.1.6 and ETSI policy 0.4.0.19495.3.1***

Table 1– OID

Qualified OV Certificate (QWAC) for domain and organization validation (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 certificates requiring this policy) For PSD2, also compliant with ETSI QCP-w-psd2 policy — 0.4.0.19495.3.1 **As of 20/05/2021, certificates under policy 1.3.76.36.1.1.45.2 are no longer issued**
Qualified Certificate (QWAC) EV for domain and legal entity validation (Extended Validation)	1.3.76.36.1.1.45.3 Compliant with ETSI QEVCP-w policies — 0.4.0.194112.1.4 CAbForum 2.23.140.1.1 **(Policy not used)**
OV certificate for validation of the domain and the organization that controls the domain (Organization Validation)	1.3.76.36.1.1.19.2 Compliant with ETSI OVCP policies — 0.4.0.2042.1.7 CAbForum 2.23.140.1.2.2 **As of 01/04/2021, certificates under policy 1.3.76.36.1.1.19.2 are no longer issued**
OV certificate for organization validation (Organization Validation)	1.3.76.36.1.1.19.5 compliant with ETSI OVCP policy 0.4.0.2042.1.7

**tinexta
infocert**

	CAB Forum 2.23.140.1.2.2
	As of 01/12/2023, certificates with policy 1.3.76.36.1.1.19.5 are no longer issued.

Table 2– OID

1.3 PKI PARTICIPANTS

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 managed and coordinated by Tinexta S.p.A.
Registered office	**Piazzale Flaminio 1/B, 00196 – Roma (RM)**
Operational offices	**Via Gian Domenico Romagnosi 4, 00196 - Roma (RM)**
	Via Fernanda Wittgens n. 2, 20123 Milano (MI)
	Piazza Luigi da Porto n. 3, 35131 Padova (PD)
Telephone number	**0683669635**
Legal Representative	**Danilo Cattaneo as Managing Director**
Tax Identification Number and Business Register Number	**07945211006**
REA Number	**RM – 1064345**
VAT Number	**07945211006**
Website	**https://www.infocert.it**

1.3.2 Registration authority (RA)

Registration Authorities or Local Registration Authorities (hereinafter briefly referred to as "RAs") 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, 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.

tinexta
infocert

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 National Competent Authority (hereinafter briefly referred to as "**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 (hereinafter briefly referred to as "**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.

1.3.7 National Competent Authority (NCA)

Under PSD2 [8], the national supervisory authority for financial intermediaries is the body responsible for authorizing PSPs in each Member State. When authorization is granted, the Competent National Authority (hereinafter also simply the "NCA") issues an authorization number and publishes this information in its public registers.

In other contexts, supervisory authorities for financial intermediaries in non-EU countries are also taken into consideration, and their public registers are consulted to verify PSP authorizations and authorization numbers.

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

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

tinexta
infocert

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:

Company name	**InfoCert – S.p.A**
	Head of Certification Services
	Piazza Luigi da Porto n. 3, 35131 Padova (PD)
Telephone number	**0683669635**
Digital signature Contact Center	**https://help.infocert.it/contatti/for more details**
Website	**https://www.firma.infocert.it, https://www.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 https://www.firma.infocert.it or https://www.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 Certificate Practice Statement has been approved by the Corporate Management following a review by the Head of Security and Policy, the Privacy Officer, the Head of Certification Services, the Head of Legal Department, the Head of Regulatory Affairs.

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

tinexta
infocert

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*
Audit Log (logbook)	The logbook is a collection of records made either automatically or manually, of the events foreseen under the Technical Regulations [5].
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])
Certificate Practice Statement (CPS)	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.
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 revocation or suspension	This is the operation with which the CA revoke or suspend the validity of the certificate before its natural expiry.
Certification key or root key	Pair of cryptographic keys used by the CA to sign the certificates and CRL
Conformity Assessment Body (CAB)	Body accredited under the eIDAS Regulation as competent to carry out the conformity assessment of the qualified trust service provider and of the qualified trust services it provides. It drafts the CAR.
Conformity Assessment Report (CAR)	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]).
Coordinated Universal Time	Time-scales with precision to the second as defined in ITU-R Recommendation TF.460-5.
CSR	A CSR (Certificate Signing Request) is a block of text used to request a Web authentication certificate. It contains the public key for which the certificate is to be issued, identifying information (such as a domain name), and proof of authenticity that includes integrity protection (for example, a digital signature).
Customer	An entity with which InfoCert has formalized a service supply contract in exchange for payment of a fee.
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])
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).
Electronic document	Any content stored in electronic format, in particular text or sound, visual or audio-visual recording (cf. eIDAS [1])
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])
Electronic identification means	A material and/or immaterial unit containing personal identification data, and which is used to access online services (see 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])

tinexta
infocert

Expiry	Definition
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])
Online Certificate Status Protocol (OCSP)	Protocol defined by IETF in RFC 6960. It enables applications to verify a certificate's validity in a faster and more accurate manner than CRL, which it shares data with.
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])
Private key	The asymmetric key pair element used by the Subject to place his digital signature on an electronic document (cf. CAD [2]).
Product	A hardware or software or their relevant parts, destined for use in providing the trust services (cfc. eIDAS [1])
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]).
Public official	Person who, as part of its role, is qualified under the law of reference to swear to the identity of natural persons
Qualified electronic time stamp	A temporary electronic validation that meets the requirements laid down in article 42 of the eIDAS Regulation (cf. eIDAS [1])
Qualified trust service	A trust service that meets the relevant requirements established in the Regulation (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])
Qualified web site authentication certificate (QWAC)	An authentication certificate of the web site that is issued by a qualified trust service provider and complies with the requirements found in annex IV (cf. eIDAS [1])
Relying Party	A natural or legal person who relies on an electronic identification or on a trust service (cf. eIDAS [1])
Signatory	A natural person who creates an electronic signature (cf. eIDAS [1])
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])
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])
Validation	The process for checking and confirming the validity of a signature (cf. eIDAS [1])
Validation data	Data used to validate an electronic signature (cf. 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])
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.

Table 2 – Definitions

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

tinexta
infocert

Acronym	Meaning
CAB	Conformity Assessment Body
CABForum	Certification Authority Browser Forum
CAR	Conformity Assessment Report
CC	Common Criteria
CIE	Electronic Identity Card
CRL	Certificate Revocation List
CSR	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

tinexta
infocert

1.6.3 References

Reference	Meaning
[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.
[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.
[ETSI401]	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI403]	ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
[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

Table 4 – References

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

CRLs and the CP/CPS are published and available 24 (twenty-four) hours a day, 7 (seven) days per week.

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

Revocation and suspension lists are published in the certificate public registry, accessible via the LDAP protocol or via HTTP protocol as indicated in the "CRL Distribution Points" of the certificate. Lists can be accessed through the software provided by the CA and/or through compliant products available on the market that can interpret LDAP and/or HTTP protocols.

The CA may provide additional access options to consult the list of published certificates and their validity.

2.3 Time or frequency of publication

2.3.1 Publication frequency of the Document

Frequency of publication of the Certificate Practice Statement, available as set out in section 2.2.1, varies to reflect any changes that have occurred. For major changes, the CA must undergo an audit by an accredited CAB, submit the certification report (CAR—Conformity Assessment Report) and the Certificate Practice Statement to the Supervisory Authority (AgID) and wait for a publication permission to be granted.

2.3.2 Publication frequency of the revocation and suspension lists

The CRLs are published every 24 (twenty-four) hours, as set out in section 2.2.3.

2.4 Access controls on repositories

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 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.

3.1.2 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.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation

3.1.4 Rules for Interpreting Various Name Forms

InfoCert complies with the X500 standard

3.1.5 Uniqueness of Names

The domain name can be found in the website's 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 that is present in the SubjectAlternativeName extension.

3.1.6 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.

The CA can Identify the Subscriber with any legal mean for that purpose.

The CA performs checks on the use of trademarks, and may refuse to issue or may request the revocation of a certificate 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.

tinexta
infocert

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 to ensure compliance with the CABForum Baseline Requirements for Publicly-Trusted TLS Server Certificates and the CABForum Guidelines for Extended Validation Certificates.

The domain names included in a website authentication certificate are verified in accordance with § 3.2.4 of the Baseline Requirements.

If the Distinguished Name subject of a certificate of web sites 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/topics/registers-business-insolvency-land/business-registers-search-company-eu_en?clang=en.

- 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 ICERT-INDI-MO for issuing certificates with a qualified signature to a natural and/or legal person.

tinexta
infocert

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.

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',

tinexta
infocert

'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

No Stipulation.

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 https://www.firma.infocert.it or https://www.infocert.it or by drawing up a trade agreement with the CA.

The systems hosting 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 these authorised purposes.

4.1.2 Enrollment Process and Responsibilities

The registration process includes the request by the Subscriber (the request form is available on the CA website https://www.firma.infocert.it or on the InfoCert website https://www.infocert.it), 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 who submits the qualified certificate on behalf of the legal person itself;
- 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 certificate qualified, 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;

- digitally sign the registration and certification request with a qualified signature, 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.

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 archives managed by ICANN.

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):

tinexta
infocert

- ▪ the DNS name of the site (sites) to be certified (in DNSName in the SubjectAlternativeName extension);

- ▪ the company name of the organization/body that owns the web site(s) to be certified must be included (in the Organization 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).

- ▪ the name of the province or region of the registered office of the organization/body that owns the website(s) to be certified (in the StateOrProvince field of the subject DN, Rome or Lazio).

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 at least 2048 and the modulus size in bits must be divisible by 8.

Regarding the ECDSA keys for which certification is requested

- • the key must represent a valid point on the NIST P-256, NIST P-384, or NIST P-521 elliptic curves
- • the use of other algorithms or key length is not permitted.

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.

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 used 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

tinexta
infocert

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.

Effective from 8 September 2017, InfoCert also performs the following check: during the initial validation process, it verifies the DNS for the existence of a CAA record for each dNSName in the subjectAltName (website authentication certificates). If no CAA record exists, InfoCert can proceed with certificate issuance. If a CAA record with the tag "issue" or "issuewild" exists, it must be set to "infocert.it" for InfoCert to proceed with certificate issuance. If a CAA record exists that does not list "infocert.it" as an authorized CA, InfoCert cannot proceed with certificate issuance and will ask the Subscriber to create a CAA record with the tag "issue" or "issuewild" set to "infocert.it".

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 or 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. The generation is carried out through procedures that require the simultaneous involvement of two trusted individuals.

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

No Stipulation

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 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.

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

tinexta
infocert

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 Certificate Modification

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 (twenty-four) hours from the receipt and authentication of the request are:

- the organization requests in writing that the CA revoke the certificate;

tinexta
infocert

- 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:
    o the key's secrecy has been breached;
    o 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 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:

- A 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,

tinexta
infocert

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 (twenty-four) hours, 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 to 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 revocation request is processed, and the new certificate status is published, within 24 (twenty-four) hours from the receipt and authentication of the request, except in cases where there are doubts about the authenticity of the request itself. In these cases, the CA reserves the right to carry out further checks, for example, to ascertain the identity of the applicant.

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 (twenty-four) hours. In the event that the need to revoke the certificate is verified, the CA, in agreement with the applicant and the entities involved, proceeds with the revocation of the certificate within 24(twenty-four) hours.

tinexta
infocert

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 generated and published every hour (ordinary issuance) and remains valid for 24 (twenty-four) 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 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 the CRL Distribution Points extension.

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

In addition to publishing the CRL in the LDAP and http, InfoCert also provides an OCSP service for checking the status of the certificate. The service URL is indicated in the certificate in the OCSP field of the Authority Information Access extension. The service is available 24 hours a day, 7 days a week.

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 by the CA for which the OCSP responder is authoritative.

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:

tinexta
infocert

- 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 in real-time, while the CRL information is updated hourly.

4.10.2 Service availability

The OCSP service and CRLs are available 24 (twenty-four) hours a day, 7 (seven) days per week. The answer in both cases is provided within 10 (ten) 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.

tinexta
infocert

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 Security 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 Milan 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.

tinexta
infocert

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 cloud infrastructure provided by third-party service providers, respectively, in the Frankfurt, Ireland and Milan European regions.

The suppliers employed by Infocert have compliance certifications in accordance with the ISO/IEC 27001:2013 e ISO/IEC 9001:2015 standards.

InfoCert has been ISO/IEC 27001:2005 certified since March 2011 for EA:33-35 activities. In March 2015, the company was certified according to the new version of the ISO/IEC 27001:2013 standard and has recently obtained ISO/IEC 27001:2022 certification.

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 is certified at the level of Rating 3 according to ANSI TIA 942.

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).

tinexta
infocert

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. The company adopts internal procedures for the secure deletion of data from enterprise-class storage devices through the use of suppliers who guarantee its deletion. Its waste management cycle is compliant with current national regulations and uses exclusively suppliers authorized for the transport and destination of the same.

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.

In the Disaster Recovery site, the onsite backup is locally stored and a backup copy is stored on third party off-site locations.

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 Number of people required to carry out the activities

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles that require separation of duties

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

tinexta
infocert

assigned.

In particular, the 'Validation Specialist' that manages the vetting phase is trained on PKI, identification and validation procedure, threats, ETSI and 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 Corporate 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 with the employee staff.

5.3.5 Job rotation frequency and sequence

On-site working or agile working (smart working) hours are distributed over an 8:00 a.m. to 7:00 p.m. time slot from Monday to Friday.

Supervision of the production environment at night and on public holidays is ensured by means of an on-call rotation plan drawn up by the head of the organisational unit at least 10 (ten) days in advance every month. Depending on the need, interventions may be carried out remotely (remote intervention) or require access to the premises.

Provided that the necessary technical and professional requirements are met, the Company ensures that as many workers as possible are on call, giving priority to employees who request it.

5.3.6 Sanctions for unauthorised actions

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

5.3.7 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

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 (twenty-three) 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

tinexta
infocert

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 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 27001. 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 27001, also highlighting the AgID and CAB.

Description of the procedure

- a security incident is open
- escalation and comunication to the stakeholder
- 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

tinexta
infocert

in extremely difficult or disastrous situations.

5.8 CA or RA Termination

If the certification activity being terminated, InfoCert will communicate its intention to the Supervisory Body (AgID) at least 3 (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.

More details are available in the document TSP Termination Plan of the Certification Time Validation and Qualified electronic signature validation Services available from the Certification Authority.

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;

tinexta
infocert

- 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 TO 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

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

6.1.3 Public key delivery 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 Public key delivery to relying parties

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 Trust-service Status List (TSL) published on the AgID website.

6.1.5 Key algorithm and key size

The certification asymmetric key pair is generated within the cryptographic hardware devices mentioned above.

The CA root keys that sign the issuing of new certificates can be:

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

The Subject keys may be

- asymmetric RSA keys with a length of not less than 2048 bits;
- EC asymmetric keys on one of the NIST P-256, NIST P-384, or NIST P-521 elliptic curves. The use of other algorithms or key length is not permitted.

6.1.6 Public key generation and quality checks

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

**tinexta
infocert**

6.1.7 Key usage purposes

6.1.7.1 Use of the CA key

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

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

6.1.7.2 Use of the Holder's key

Holder's key usage purposes are determined by the KeyUsage extension, as defined in the X509 standard. The certificates described in this operational manual are only allowed to be used for website authentication

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Cryptographic modules used by InfoCert for certification keys (CA) and OCSP responder are validated FIPS 140 Level 3 and/or Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 in Europe.

6.2.2 CA private key multi-person control

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

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

6.2.5 CA private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation

6.2.7 Private key transfer into or from a cryptographic module

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

6.2.8 Method of activating private key

The certification private key is activated by the CA software in dual control, that is, two people with specific roles and in the presence of the service manager.

The Subject or Subscriber on behalf 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 Method of deactivating private key

No Stipulation

6.2.10   Method of destroying CA private key

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

6.2.11   Cryptographic Module Rating

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 and key pair validity periods

A certificate validity period shall be determined based on:

- 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.

tinexta
infocert

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 (twelve) months.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

InfoCert gives strategic importance to secure handling of information and recognizes the need to continuously develop, maintain, monitor and improve its information security management system (SGSI) in accordance with ISO/IEC 27001 for EA:33-35 activities. InfoCert has been ISO/IEC 27001:2005 certified since March 2011 for EA:33-35 activities. In March 2015, the company was certified according to the new version of the ISO/IEC 27001:2013 standard and has recently obtained ISO/IEC 27001:2022 certification.

SGSI procedures and checks include:

- 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 Timestamping

InfoCert provides a qualified time stamping trust service. For the time stamp service, please refer the Certificate Practice Statement named ICERT-INDI-TSA available on the InfoCert website.

All InfoCert systems 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.

tinexta
infocert

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 Signature algorithm OID

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

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

7.1.4 Name forms

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

7.1.4.1 Issuer Information

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

7.1.4.2 EndUser information

See §3.2.2 e § 3.2.3.

7.1.4.3 SAN Extention

See §7.1.2.5

7.1.4.4 Subject DistinguishedName

See §7.1.2.5

7.1.4.5 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.

tinexta
infocert

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 as trusted service provider or qualified trust service provider under the eIDAS Regulation, the procedure provided for in Article 21 of the said Regulation must be carried out.

InfoCert has submitted to AgID a request for recognition as "qualified trust service provider" enclosing a Conformity Assessment Report (CAR) issued by a conformity assessment body (CAB) authorized by ACCREDIA.**Frequency or circumstances of assessment**

The conformity assessment report is issued every year. In this period one or more other audit session are performed.

8.2 Identity/qualifications of assessor

The control is carried out by:

Company name	**CSQA Certificazioni S.r.l.**
	Via S. Gaetano n. 74, 36016 Thiene (VI)
Telephone number	**+39 0445 313011**
Business Register Number	**Tax Identification Number 02603680246**
	Business Register no. 02603680246
	REA no. 258305
VAT Code	**02603680246**
Website	**https://www. csqa.it**

8.3 CAB's relationship to InfoCert

The service is provided by InfoCert as a qualified trust service provider within the meaning of Regulation (EU) No. 910/2014 of 23/07/2014, on the basis of a conformity assessment carried

tinexta
infocert

out by the Conformity Assessment Body CSQA Certificazioni S.r.l. pursuant to the above Regulation and to the ETSI EN 319 401 standard, and according to the eIDAS assessment scheme defined by ACCREDIA in accordance with the ETSI EN 319_403 and UNI CEI EN ISO/IEC 17065:2012 standards.

8.4 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 COMMUNICATION OF VERIFICATION RESULTS

The audit report produced by the CAB is sent to the the Italian supervisory body (AgID

The conformity assessment is shared with the service responsible and it is published no later than 3 (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 QWAC 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

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

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or suspension status information access fees

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

9.1.4 Fees for other services

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 Customers and apply specific fees.

9.1.5 Refund policy

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

9.2 Financial Responsibility

9.2.1 Insurance coverage

The InfoCert TSP has taken out an appropriate insurance policy covering operational risks and damages caused to third parties, as required by AgID Determination No. 185/2017. The policy provides for the following maximum coverage limits:

• EUR 3,000,000 per claim;
• EUR 6,000,000 per 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

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

9.4.1 Privacy plan

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

9.4.2 Information treated as private

Data 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 Controller of the processing of personal data

Company name	**InfoCert S.p.A**
Registered office	**Piazzale Flaminio 1/B, 00196 – Rome (RM)**
	00147 Roma

tinexta
infocert

Email	**richieste.privacy@legalmail.it**

9.4.5 Notice and consent to use private information

InfoCert's privacy notice is available on the website www.infocert.it at the following link: https://www.infocert.it/informative-privacy.

InfoCert will process the data in the manner and form required by law [4]. The processing will be based on an appropriate legal basis as described in the privacy notice.

In cases where identification requires the processing of biometric data, InfoCert will request consent before providing the service.

If the processing is carried out by another legal entity on behalf of InfoCert, the privacy notice will be made available by that third party, which will also collect consent where necessary.

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

No stipulation.

9.5 Intellectual Property Rights

The copyright in this document belongs to InfoCert. 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

InfoCert 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.

InfoCert 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

InfoCert 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, InfoCert 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, InfoCert 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 solely 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.

9.9.1 IndeMniTIES BY SUBSCRIBERS

No Stipulation

9.9.2 IndeMniTIES BY USERS

No Stipulation

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until otherwise communicated by InfoCert on its website.

9.10.2   Termination

The Contract will automatically terminate with a simultaneous interruption of the Service and revocation of the issued certificate in cases of non-compliance with the clauses indicated in the service supply contract. 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.

The effects produced by the Contract shall remain unaffected until its termination .

The Subscriber acknowledges that in the event of termination the Contract, for any reason whatsoever, it will no longer be possible to use the Service.

9.10.3   Effect of termination

Termination involves the immediate revocation of the certificate.

9.11 Individual notices and communications with participants

See section 1.5.2.

9.12 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.

9.12.1   Amendment history

Information	Description
Version/issue n°:	**3.9**
Date:	**22/05/2025**
Description:	Update of the InfoCert logo and Rome offices 1.1 Clarifications and correction of BR date and version § 1.2 Indicated policy not in use 1.3.76.36.1.1.45.3; indicated the new policy 1.3.76.36.1.1.45.5 to be used for QWAC PSD2 certificates with a two-year validity; correction of typos in policy 1.3.76.36.1.1.45.4; creation of Table 2 –

tinexta
infocert

Information	Description
	object identifier for policies not in use
	§ 1.3.7 Clarification regarding the verification of non-EU PSP authorizations through consultation of national supervisory authorities' registers
	§ 1.6.1 Removal of Public Key and Private Key definitions; correction of CSR definition
	§ 1.6.2 Correction of CSR acronym
	§ 5.1.1 Change of Disaster Recovery site, addition of new Cloud Region, removal of Figure 1
	§ 1.5.2 Update of InfoCert phone contact
	§ 2.3.1 Reference to the cited paragraph
	§ 3.1.5 Clarifications
	§ 3.1.6 Clarifications
	§ 3.2.2 Clarifications
	§ 3.2.5.2 Update
	§ 4.2 Clarifications and additions
	§ 4.2.1 Update
	§ 4.3 Clarifications
	§ 4.5.1 Update
	§ 4.9.2 Clarifications
	§ 4.9.3 Clarifications
	§ 4.9.4 Clarifications
	§ 4.9.7 Clarifications
	§ 4.9.9 Additions
	§ 4.9.10 Additions
	§ 4.9.12 Reference to the cited paragraph
	§ 4.10.2 Update
	Clarifications Appendix B
	Update of extensions in Table 20
	Addition of Table 26
	Update of reference to eIDAS Regulation
	Update of ISO 9001 and 27001 versions
	§§ 4.9.1.1, 4.9.5 Clarifications
	General review of document styles and formats
	§ 6.6 Clarifications on ISO/IEC 27001 certification
	§ 9.10.1 Termination update
	§ 9.4.5 Clarifications on Privacy Notice and consent to personal data processing
Reasons:	

Table 5 – Version 3.9

Information	Description
Version/issue n°:	**3.8**
Date:	**15/05/2024**
Description:	§ 1.1: Updated CabForum BR versions and EV guidelines
	§ 1.5.2: Deleted fax from contacts and contact update
	§§ 1.5.3, 9.12.1: Update of company business unit names
	§§ 1.6.1 e 1.6.2: Added "Customer", updated definitions and acronyms
	§§ 2.2.3, 2.3.1, 2.3.2: Clarifications on the publication address
	§§ 1.2, 1.4.1, 2.1, 3.2.2, 3.2.5.1, 4.1, 4.2, 4.3, 4.6.1, 5.2.2, 5.3.3, 5.7.3, 6.1.1.3, 6.1.2, 6.1.7, 8.6, 8.7, Annex A: Update following the termination of the InfoCert Organization Validation 2019 CA 3 and Infocert Organization Validation CA 3 subCAs
	§ 4.2: Clarifications about keys
	§ 4.9.5: Clarifications on revocation
	§ 4.10.1: Clarifications on OCSP
	§ 5.1.1: Review of description
	§ 5.1.3: Updated certification of the website

tinexta
infocert

Information	Description
	§ 5.1.7 and 5.1.8: Review of description § 5.3.5: alignment with ICERT-INDI-MO §§ 6.1.5, Annex A: Review e Update following new root EC § 6.1.7 and subsections: Clarifications about admitted KeyUsage § 6.2.1: Review of description § 6.6: Review of description § 8.3: Review of description § 9.4: Clarifications § 9.4.4: Update § 9.10.2: Review of description § 9.14: Review of description General revision with spelling and grammatical corrections, reformulations and clarifications
Reasons:	Update CabForum BR versions and EV guidelines General review Terminazione subCA InfoCert Organization Validation 2019 CA 3 e Infocert Organization Validation CA 3 Termination of the InfoCert Organization Validation 2019 CA 3 and Infocert Organization Validation CA 3 subCAs New CA root EC

Table 6 - Version 3.8

Information	Description
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

Table 7 – Version 3.7

Information	Description
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

Table 8 – Version 3.6

tinexta
infocert

Information	Description
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

Table 9 – Version 3.5

Information	Description
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

Table 10 – Version 3.4

Information	Description
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

Table 11 – Version 3.3

Information	Description
Version/issue n°:	**3.2**
Date:	**11/02/2020**
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

tinexta
infocert

Information	Description
	§ 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

Table 12 – Version 3.2

tinexta
infocert

Information	Description
Version/issue n°:	**3.1**
Date:	**27/11/2019**
Description:	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

Table 13 – Version 3.1

Information	Description
Version/issue n°:	**3.0**
Date:	**30/11/2018**
Description:	§ 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 Annual review Issuing of PSD2 compliant certificates Review of checks Modification of the company name TecnoInvestimenti o
Reasons:	Annual review Issuing of PSD2 compliant certificates Review of checks Modification of the company name TecnoInvestimenti

Table 14 – Version 3.0

Information	Description
Version/issue n°:	**2.1**
Date:	**20/06/2018**
Description:	§ 1.5.1 Contact update § 9.2.1 Insurance coverage § 9.9 Indemnities
Reasons:	Change in Call Center number Change in insurance ceilings

Table 15 – Version 2.1

Information	Description
Version/issue n°:	**2.0**
Date:	**06/12/2017**
Description:	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

Table 16 – Version 2.0

tinexta
infocert

Information	Description
Version/issue n°:	**1.1**
Date:	**08/02/2017**
Description:	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

Table 17 – Version 1.1

Information	Description
Version/issue n°:	**1.0**
Date:	**12/12/2016**
Description:	Definizioni: aggiornate alcune definizioni Introduzione: migliorata la descrizione del servizio OID per certificato non qualificato 1.3.76.36.1.1.19.2 § 4.2.1 Aggiunti dettagli sulla CSR § 4.2.4 Rivisti gli SLA Correzione forma e ortografia
Reasons:	New issuing of the document

Table 18 – Version 1.0

9.12.2 Revision procedures

The revision procedures in the Document are similar to the editing procedures. Revisions are approved by the Corporate Management and made jointly with: the Head of the Certification Services, the Head of Security and Policy, the Privacy Officer, the Head of Legal Department and the Head of Regulatory Affairs.

9.12.3 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.

9.12.4 Circumstances under which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Procedures

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

9.14 Competent Court

For a detailed description of Competent court, please refer to the contracts governing the service.

9.15 Governing Law

The law governing this Document is Italian law.

The following is a complete list of the main applicable laws for reference:

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended by Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024 (referred to as eIDAS).

[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

---

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

tinexta
infocert

ICERT-INDI-MOWS   Version **3.9** — **22/05/2025**

9.17 Other Provisions

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

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%)

Table 19 – Service provision times

pag. 64 di 72

InfoCert S.p.A. — All rights reserved

tinexta
infocert

ANNEX A: CA ROOT CERTIFICATES AND SUBCA HIERARCHY

InfoCert Root CA 3

http://cert.infocert.it/ca3/root/CA.crt

serial number: 7c35de37e34e4917f4a8d9f7c92bcaa4f9ee6afa

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: c35de37e34e4917f4a8d9f7c92bcaa4f9ee6afa

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) - withdrawn from the Trusted List

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

Certificate serial number: 44841e74619f52cb

http://cert.infocert.it/ca3/ovcf/CA.crt

serial number: 0249528bfbff7ddf

key identifier: 5f0ebbb9cf47920c26345605bfdc9d9e18bdc925

authority key identifier: 5b1bee037ba2dbe746c0c254aba150295ff156d7

InfoCert 2019 CA3 OV CamerFirma trusted - withdrawn from the Trusted List

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

Certificate serial number: 00c9cdd3e9d57d23ce

http://cert.infocert.it/ca3/ovcf2019/CA.crt

Serial number: 31b31444fdd6c2a78f0a9c

Key identifier: 8832bf09fb4239f472432068b8cfac8a92785d0c

Authority Key identifier: 5b1bee037ba2dbe746c0c254aba150295ff156d7

InfoCert Root EC CA 4

http://crl.ca4.infocert.it/rootec/CA.crt

Serial number: 364faea3e21e1495ad98a04d37561032d684f8aa

Key identifier: 6392601da952918722b916d50074776710367f55

InfoCert Organization Validation EC CA 4

http://crl.ca4.infocert.it/ovcaec/CA.crt

Issued by:

- CN: InfoCert Root EC CA 4
- OU: WSA Trust Service Provider.
- O: InfoCert S.p.A.
- C:IT

Certificate serial number: 364faea3e21e1495ad98a04d37561032d684f8aa

Serial number: 7caf82976bfb9b07c991bea9044d9ee60d19dbb8

Key identifier: 32c8242d82c162ebab0830424c120c2206b71941

authority key identifier: 6392601da952918722b916d50074776710367f55

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
- 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 TS 119 495

tinexta infocert

- **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. The following two values are allowed:"
  - o id-kp-serverAuth
  - o 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)
  - o 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:

  o **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).

  o **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

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

  o **QcType** (0.4.0.1862.1.6): it contains id-etsi-qct-web

SIGNATURE: § 7.1.3

QCStatement Extensions for QWAC PSD2

Estensione	Valore
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) 0 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	Unspecified PSP_AS PSP_PI PSP_AI PSP_IC
NCAName	*UTF8String (SIZE (1..256)) being the plain text name in English of the NCA*
NCAId	*UTF8String (SIZE (1..256))* • *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).*

Table 20 – Estensioni QCStatement per QWAC PSD2

tinexta
infocert

Format of CRL and OCSP

Extension	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCert
thisUpdate	Data in formato UTC
nextUpdate	Data della prossima CRL in formato UTC
Revoked Certificates List	Lista dei certificati revocati, con numero di serie e data di revoca/sospensione
Issuer's Signature	Firma della CA

Table 21 – Format of CRL and OCSP

Values and extensions for CRLs e OCSPs

CRLs have the following extensions:

Extension	Valore
Authority Key Identifier	Il valore dell'impronta 160-bit SHA-1 di issuerPublicKey
CRL number	Il numero univoco della CRL assegnato dalla CA
ExpiredCertsOnCRL	La data in formato GeneralizedTime dalla quale i certificati scaduti sono tenuti in CRL.
Issuing Distribution Point	Identifica il punto di distribuzione delle CRL e lo scopo: indica se la CRL è generata solo per certificati di CA, o certificati end-entity
Invalidity Date	Data in formato UTC che indica la data da cui si ritiene che il certificate sia invalido

Table 22 - Values and extensions for CRLs e OCSPs

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 del DN dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente.
Serial Number	Numero di serie del certificato

Table 23 – OCSP request

The OCSP response contains the following fields:

Field	Value
Response Status	Stato della rispsosta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificato firmatario della risposta OCSP.
Produced at	Data in formato GeneralizedTime di quando è stata generate la risposta OCSP
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 del distinguishName dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente
Serial Number	Numero di serie del certificato
thisUpdate	Data di verifica dello stato del certificato in formato GeneralizedTime
nextUpdate	Data in cui lo stato del certificato potrebbe essere aggiornato

Field	Value
Issuer Signature Algorithm	In base alla chiave del certificato di OCSP Responder, scelto tra sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)] ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)] ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)] ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

Table 24 – OCSP response

OCSP Extensions

The OCSP request can contain the following extensions:

Field	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.

Table 25 – OCSP Extensions

The OCSP request can contain the following extensions:

Campo	Valore
nonce	See Tab. 25
OCSP Archive Cutoff Extension	If a responder chooses to retain revocation information beyond a certificate's expiration this date represents the date from which revocation information beyond certificates expiration are retained.

Tabella 26 – Estensioni risposta OCSP