INFOCERT CERTIFICATION BODY
AUTHENTICATION CERTIFICATES FOR THE NATIONAL SERVICES CARD – CERTIFICATE POLICY

Document code: ICERT-INDI-CPCA-CNS
Version: 8
Date: 26/07/2024

Contents

1. Introduction to the document 2
1.1 Changes introduced since the previous edition 2
1.2 Purpose and scope of the document 4
1.4 Definitions 4
1.5 Acronyms and abbreviations 6
2. General information 7
2.1 Document identification 7
2.2 Actors and Application Domains 8
2.3 Contact details for end users and communications 9
3. General Rules 9
3.1 Obligations and Responsibilities 10
3.2 Liability 11
3.3 Publication 11
3.5 Rates 12
4. Certificate Policy Administration 12
4.1 Updating Procedures 12
4.2 Rules for publication and notification 12
5. Identification and Authentication 12
5.1 Authentication for key and certificate renewal 13
5.2 Authentication for revocation or suspension requests 13
6. Operational procedures 13
6.1 Format and content of the certificate 13
6.2 Validity of the certificate 13
6.3 Use of the certificate 14
6.4 Revocation and suspension of a certificate 14
6.5 Renewal of the Certificate 15
7. Management and operation of the CA 15
7.1 Security management 16
7.2 Operations management 17
7.3 Disaster Management Procedures 17
7.4 Archived data 17
7.5 Certification Authority Keys 17
7.6 Quality system 18
7.7 Service Availability 18

1. Introduction to this document

1.1 Changes introduced since the previous issue

Version/Release No.:	8
Version/Release date:	26 July 2024
Description of changes:	Company addresses and contact details, correction of typographical errors, clarifications regarding certificate status verification services, revision of information on the certification authority's algorithms and keys.
Reasons:	Periodic review of the document

Version/Release No.:	7
Version/Release date:	18 July 2023
Description of changes:	New InfoCert logo
Reasons:	Rebranding

Version/Release No.:	6
Release Date:	28/09/2021
Description of changes:	Company references
Reasons:	Review and amendment of company references

Version/Release No.:	5
Version/Release date:	07/11/2018
Description of changes:	Company addresses and contact details; insurance section removed; publication of certificates removed (3.3.2 and 6.3); updates to regulatory references regarding the Data Protection Commissioner and the GDPR; and updates to the relevant paragraphs (7.4 and 7.4.1)
Reasons:	Revision and amendment of company addresses and contact details

Version/Release No.:	4
Version/Release date:	27/01/2014
Description of changes:	Company addresses and contact details, insurance policies, quality and safety certifications
Reasons:	

Version No.:	1.3
Version/Release date:	20 June 2011
Description of changes:	Company addresses and contact details
Reasons:	

Version No.:	1.2
Version/Release date:	03/07/2009
Description of changes:	Removal of the requirement for subjects not to hold an electronic identity card
Reasons:	Regulatory changes

Version/Release No.:	1.1
Version/Release date:	15/10/07
Description of changes:	Address of the operational headquarters
Reasons:	

Version No.:	1.0
Version/Release date:	01/08/2007
Description of changes:	None
Reasons:	First issue

1.2 Purpose and scope of the document

This document contains the general rules (policy) governing the issuance and use of **Authentication Certificates for the National Services Card (CNS)** signed by the InfoCert Certification Authority. Hereinafter, for brevity, this is referred to as the 'Certificate Policy'. The operational procedures adopted by the Issuing Authority and by the Certification Authority itself for the provision of digital certification services are set out in the CNS policy and practice statement drawn up and made available by the Issuing Authority itself.

The guidelines in this document apply to activities relating to InfoCert in its capacity as a Certification Authority.

1.3 Regulatory References

[1] Legislative Decree No. 82 of 7 March 2005 (Official Gazette No. 112 of 16 May 2005) – Code of Digital Administration and subsequent amendments (hereinafter 'CAD')

[2] Decree of the President of the Council of Ministers of 22 February 2013 (Official Gazette of 21 May 2013) (DPCM 22 February 2013)

[3] Legislative Decree No. 196 of 30 June 2003 (Official Gazette No. 174 of 29 July 2003) – the Privacy Code, as amended, and 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 (in force since 25 May 2018).

[4] Decree of the President of the Republic No. 117 of 2 March 2004 (Official Gazette No. 105 of 6 May 2004) and subsequent amendments

[5] Technical and safety regulations relating to the technologies and materials used in the production of the National Services Card (Official Gazette No. 296 of 18 December 2004)

[6] Guidelines for the issuance and use of the National Services Card, Version 3.0, dated 15 May 2006, issued by the National Centre for Information Technology in Public Administration

[7] AgID Decision – Update to the document "National Services Card (CNS) – File System" v. 11

1.4 Definitions

The definitions used in the drafting of this document are listed below. For terms defined in [1], [2] and [4], please refer to the definitions set out in the decrees themselves. Where appropriate, the corresponding English term – generally used in publications, standards and technical documents – is indicated in square brackets.

Optional accreditation
The recognition, by the certifying body that requests it, that it meets the requirements of the highest level in terms of quality and security.

National Service Charter
The document issued in electronic form to enable online access to services provided by public administrations.

Electronic Certificate, Digital Certificate, X.509 Certificate *[Digital Certificate]*

A set of information designed to definitively establish the correspondence between the name of the certified party and their public key.

The certificate contains other information, including:

- the Certification Authority that issued it;
- the period during which the certificate may be used;
- other fields (extensions) that specify additional characteristics of the certificate.

***Certification Authority [CA]* – see CAD [1]**

Accredited Certification Authority – see CAD [1]

Qualified Certification Authority – see CAD [1] Private Key and Public Key – see CAD [1] Data for creating a signature – see CAD [1]

Data for verifying a signature – see CAD [1]

Secure signing device

The secure signing device used by the subject consists of a plastic card the the size of a credit card or a USB token containing a microprocessor. It is also known **as a microprocessor card**, **a smart card** or **a token.** It complies with the security requirements set out in current legislation.

Issuing Authority

The body responsible for creating and issuing the CNS.

It is the Public Administration that issues the CNS and is responsible for the security of the issuance process and the issuing of the card, ensuring the proper management of the CNS's lifecycle.

Digital Record

A sequence of binary symbols (bits) that may be the subject of an IT procedure.

Electronic signature – see CAD [1]

Qualified electronic signature – see CAD [1]

Digital signature – see CAD [1]

Certificate Revocation List *(CRL)*

This is a list of certificates that have been rendered 'invalid' before their natural expiry date.

The process is termed 'revocation' if permanent, and 'suspension' if temporary.

When a certificate is revoked or suspended, its serial number is added to the CRL, which is then published in the certificate registry.

Digital time stamping

The result of the IT procedure by which a date and time, enforceable against third parties, are assigned to one or more electronic documents.

Policy and Practice Statement

The policy and practice statement sets out the procedures that the Certification Authority and the Issuing Authority follow when providing the service of issuing and managing the CNS and the associated certificate.

Public Official

A person who, within the scope of their duties, is authorised under the relevant legislation to verify the identity of natural persons.

Registration Authority Officer

A person responsible for verifying the identity and, where applicable, any specific attributes of a Subject, as well as for initiating the certification procedure on behalf of the Certification Authority.

Certificate Register *[Directory]*

The Certificate Directory is a public archive containing:

- valid certificates issued by the Certification Authority for which Subjects have requested publication;
- the list of revoked and suspended certificates (CRL).

Revocation or suspension of a certificate
This is the process by which the Certification Authority cancels the validity of a certificate before its natural expiry date. See List of Revoked or Suspended Certificates – CRL.

Applicant *[Subscriber]*
This is the individual who applies to the Issuing Authority for the issue of the CNS.

Holder *[Subject]*
This is the individual in whose name the CNS is issued and who is identified in the digital certificate as the legitimate holder of the private key corresponding to the public key contained in the certificate itself: the Subject is assigned the advanced electronic signature generated using the private key of the key pair.

***Registration Authorities [RA]*/Local Registration Centre [CDRL]** The Issuing Authority or another body delegated by the Issuing Authority, subject to the conclusion of service agreements with the Certification Authority, carries out the activities necessary for the latter to issue the digital certificate and to deliver the CNS.

User *[Relying Party]*
A party that receives a digital certificate and relies on that certificate or on the advanced electronic signature based on that certificate.

1.5 Acronyms and abbreviations

CNS – National Services Card CRL

– Certificate Revocation List

List of revoked or suspended certificates.

DN – Distinguished Name
Identifier of the subject of a public key certificate; this code is unique amongst the Certificate Authority's users.

ETSI – European Telecommunications Standards Institute IETF – Internet Engineering Task Force
The IETF is an open, international community of network designers, operators, vendors and researchers involved in the evolution of Internet architecture and standard Internet operations.

ISO – International Organisation for Standardisation
Founded in 1946, ISO is an international organisation comprising national standardisation bodies.

ITU – International Telecommunication Union
An intergovernmental body through which public and private organisations develop telecommunications. The ITU was founded in 1865 and became the regulatory body for telecommunications standards.

IUT – Unique Identifier of the Subject
This is a code associated with the subject that uniquely identifies them to the Certification Authority; the subject has different codes for each role for which they are authorised to sign.

LDAP – Lightweight Directory Access Protocol
A protocol used to access the certificate repository.

OID – Object Identifier
It consists of a sequence of numbers, registered in accordance with the procedure set out in the ISO/IEC 6523 standard, which identifies a specific object within a hierarchy.

PIN – Personal Identification Number

A code associated with the CNS, used by the user to access its functions. Other functions installed on the CNS require function-specific PINs.

PUK

A personalised code for each CNS, used by the subject to reactivate their signature device following its lockout due to an incorrect PIN entry. Other functions installed on the CNS require function-specific PUKs.

RAO – Registration Authority Officer (OdR)

2. General Information

A digital certificate is the association between a public encryption key and a set of information identifying the subject who holds the corresponding private key, also known as the subject of the asymmetric key pair (public and private). The certificate is used by other parties (the Users) to derive the public key, which is contained within and distributed with the certificate, and to verify, through this, the possession of the corresponding private key, thereby identifying the subject of the key.

The certificate guarantees the correspondence between the public key and the subject. The degree of reliability of this association depends on various factors, such as, for example, the manner in which the Certification Authority issued the certificate, the security measures adopted and the guarantees offered by the Certification Authority, and the obligations undertaken by the subject to protect their private key.
In this regard, CNS Authentication Certificates issued by the InfoCert Certification Authority are issued at the subject's direct request, following the subject's physical identification by the Issuing Authority or another party delegated by it, and are issued on a secure signing device (smart card or token).

This document contains the general rules governing the issue and use of Authentication Certificates for the National Services Card (CNS) (hereinafter also referred to more briefly **as 'Certificates'**) signed by the InfoCert Certification Authority.

CNS Authentication Certificates are issued and managed by each Issuing Authority in accordance with the procedures set out in the CNS policy and practice statement (hereinafter also referred to more briefly as **the policy and practice statement**), which is drawn up and made publicly available by the Issuing Authority itself. CNS Authentication Certificates are generally used within the SSL/TLS protocol with tools such as web browsers.

The InfoCert Certification Authority publishes this Certificate Policy and includes a reference to this document in the certificate. The Issuing Authority publishes the policy and practice statement. Together, these documents enable Subscribers and Users to assess the characteristics and reliability of the certification service.

2.1 Document identification

This document is entitled **"Authentication Certificates for the National Services Card – Certificate** Policy" and is identified by the document code: **ICERT-INDI-CPCA-CNS**.

The version and date of issue are shown at the bottom of each page.

The object identifier (OID) of this document is as follows: `1.3.76.36.1.1.4`
This OID identifies:

InfoCert	1.3.76.36
Certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Cp-CNS-authentication-certificates	1.3.76.36.1.1.4

This document is available in electronic format on the Certification Authority's website at https://www.firma.infocert.it/documentazione/

2.2 Actors and Application Domains

2.2.1 Certification Authority

InfoCert is the **Accredited Certification Authority** that issues, publishes (if required) in the register and revokes **CNS Authentication Certificates**, operating in accordance with the provisions set out in this Certificate Policy.
The certificate of the InfoCert Certification Authority issuing CNS certificates, which is required to verify the signature affixed to the CNS certificates themselves, is included in a digitally signed list on the AgID website. This list contains all self-signed certificates of the Italian Certification Authorities that issue CNS certificates.
The full details of the organisation acting as the Certification Authority are as follows:

Company name: InfoCert – Società per azioni – A company subject to the management and coordination of Tinexta S.p.A.
Registered office: Piazza Sallustio 9, 00187, Rome (RM)
Operational offices:

- 45 Via Marco e Marcelliano, 00147, Rome (RM)
- 2 Via Fernanda Wittgens, 20123 Milan (MI)
- Piazza Luigi da Porto 3, 35131 Padua (PD)

Legal representative: Danilo Cattaneo, in his capacity as Chief Executive Officer
Telephone number: 06 836691
Tax code and Company Register number: 07945211006
REA number: RM - 1064345
VAT number: 07945211006
Website: https://www.infocert.it

2.2.2 Issuing Authority

The Issuing Authority is the public administration body that issues the CNS and is responsible for the security of the issuance process and the issuing of the card, ensuring the proper management of the CNS's lifecycle.
The registration of data relating to subscribers for the CNS certificate is carried out, either directly or through delegated bodies, by the Issuing Authority, which acts as the Registration Authority.
The Registration Authorities, possibly through their authorised representatives, act, amongst other things, as an interface between the Certification Authority itself and the subscriber. Set out below is a list of activities carried out at the Registration Authority:

- Identification and registration of the subscriber;
- validation of the certificate application;

- distribution and initialisation of the CNS;
- initiation of the certification procedure for the Subscriber's/Subject's public key;
- support for the Subject and the Certification Authority in the renewal, revocation and suspension of certificates.

The operational procedures are set out in detail in the CNS policy and practice statement published by the Issuing Authority.

2.2.3 Certificate Register

The certificate revocation and suspension lists are published by the Certification Authority.

2.2.4 Applicability

The CNS is a network authentication tool. Consequently, the primary scope of use for the CNS Authentication Certificate is web browsers; it may also be used by email clients, as well as specific applications issued or approved by the Certification Authority.

With web browsers, using the **SSL/TLS** standard, it is possible to verify the identity of a party holding a CNS Authentication Certificate who connects to a domain that is itself certified.

More generally, a user, by using their private key – for which a CNS Authentication Certificate exists for the corresponding public key – generates an advanced electronic signature that guarantees the origin of the information they transmit over the network and its integrity (i.e. that it has not been altered by third parties).

For a user to be able to rely on the use of a private key, the corresponding certificate must be valid, i.e. it must not have expired, been suspended or revoked.

Should a certificate belonging to a subject be used to send an encrypted message to that same subject (confidentiality of content), the loss of the private key by the subject will make it impossible to decrypt the message: the Certification Authority **does not, under any circumstances, back up the subject's private key**.

2.3 Contact details for end users and communications

InfoCert is responsible for drawing up, publishing and updating this document. Questions, comments and requests for clarification regarding this Certificate Policy should be addressed to the address and contact person indicated below:

InfoCert S.p.A.
Head of the Digital Certification Service Piazza Luigi da Porto No. 3 35131 Padua Telephone: 06 836691
Call Centre: see the link https://help.infocert.it/contatti/ for further details Web: https://www.firma.infocert.it, https://www.infocert.it
Email: firma.digitale@legalmail.it

Communications from the Certification Authority to the Subscriber will be sent by email to the address provided by the Subscriber at the time of identification.

3. General Rules

This chapter sets out the general terms and conditions under which the Certification Authority provides the certification service described in this manual.

3.1 Obligations and Responsibilities

3.1.1 Obligations of the Certification Authority

The Certification Authority is required to ensure:

1. the association between the subject and the certified public key, as communicated to it by the Issuing Authority;
2. that it does not act as a custodian of private keys relating to the corresponding CNS Authentication Certificates;
3. the issue and renewal of a certificate requested in accordance with these procedures and its availability electronically;
4. the revocation or suspension of the certificate, giving prompt notice thereof in accordance with the provisions of this Certificate Policy;
5. the thorough protection of its private keys using hardware and software capable of ensuring the necessary security criteria;
6. the management of operations and infrastructure relating to the digital certification service in accordance with the rules and procedures laid down for the Certifying Authority by the Technical Rules [5] and described in this Policy;
7. the alignment of its data security system with the minimum security measures for the processing of personal data, in accordance with the provisions of the Digital Administration Code, EU Regulation No 679/2016 and Legislative Decree of 30 June 2003,
   No. 196 and subsequent amendments and additions [3].

3.1.2 Obligations of the Issuing Body

The Issuing Authority is required to ensure:

1. the verification of the subscriber's identity and the recording of their details;
2. that the subscriber is expressly informed of the need to protect the confidentiality of the private key and of the storage and use of secure signature devices;
3. that all data and documents obtained during the identification process are communicated to the Certification Authority for the purpose of initiating the certificate issuance procedure;
4. the verification and forwarding to the Certification Authority of any revocation or suspension requests initiated by the subject at the Registration Office;
5. that operations relating to the digital certification service, entrusted to the Registration Office by the Certification Authority, are carried out in accordance with the rules and procedures set out in its policy and practice statement and in compliance with the rules laid down in this policy, in the specific manner detailed in the service agreements;
6. ensuring that its data security system complies with the minimum security measures for the processing of personal data, in accordance with the provisions of EU Regulation No 679/2016 and Legislative Decree No 196 of 30 June 2003, as amended and supplemented [3].

The Issuing Authority, using delegated bodies where necessary, shall deal directly with the Subscriber, the Subject, and is required to inform them of the provisions contained in this Certificate Policy.

3.1.3 Obligations of Subjects

The subject is required to:

1. ensure that the information provided to the Issuing Authority in support of the CNS application is accurate, complete and up to date;
2. protect and safeguard their private keys with the utmost care in order to ensure their integrity and confidentiality;
3. protect and store the activation code (PIN) used to enable the CNS's functions in a secure location separate from where the device itself is kept;

4. protect and store the unlock code (PUK) used to reactivate the CNS in a secure place separate from where the device itself is kept;
5. take any other measures necessary to prevent the loss, compromise or misuse of the private key and the CNS;
6. use the keys and the certificate solely in accordance with the procedures set out in this Certificate Policy;
7. submit to the Issuing Authority, without delay, a request for the revocation or suspension of certificates should any of the circumstances set out in the CNS policy and practice statement, made available by the Issuing Authority, arise;
8. take all appropriate organisational and technical measures to prevent harm to others.

3.1.4 Users' Obligations

A User who uses a certificate of which they are not the subject has the following obligations:

1. to be aware of the scope of use of the certificate and the limitations of liability of the Certification Authority and the Issuing Authority, as set out in this Certificate Policy and in the policy and practice statement;
2. to verify the validity of the certificate before using the public key contained therein. The validity of the certificate is ascertained by checking that it has not expired, been revoked or suspended;
3. to use the data contained in the certificate registry (e.g. revocation lists) solely for the purpose of verifying the certificate's validity;
4. take all appropriate organisational and technical measures to prevent harm to others.

The User is solely responsible for any use of the certificate that does not comply with the above.

3.2 Liability

3.2.1 Limitations of Liability

The Certification Authority shall under no circumstances be liable for events for which it is not responsible and, in particular, for any damage suffered by the Registration Authority, the Subject, the Subscriber, the Users or any third party caused directly or indirectly by their failure to comply with the rules set out in this Certificate Policy; or by their failure to take the appropriate measures of special diligence required of users of certification services to prevent damage to third parties; or by the commission of unlawful acts.
The Certification Authority shall not be liable for any breach of obligation or, in any event, for any harmful event resulting from unforeseeable circumstances or force majeure.

3.2.2 Express termination clause

The Certification Authority is entitled to terminate the contractual relationship, in accordance with Article 1456 of the Civil Code, as provided for in the contract entered into with the other party.

3.3 Publication

3.3.1 Publication of information relating to the Certifier

This Policy is available:

- in electronic format on the Certifier's website (see § 2.1) in paper
- format at the Certifier's premises.

3.3.2 Publication of revocation and suspension lists

Revocation and suspension lists are accessible via LDAP, HTTP and OCSP protocols. The addresses are published directly within the certificates issued, as required by the X.509 v3 standard. Access may be gained via software provided by the Certification Authority and/or features available in commercially available products that utilise the aforementioned protocols.

The Certification Authority may make other methods available, in addition to the one indicated, for verifying the validity of certificates.

3.4 Protection of personal data

Information relating to the subject of the certificate that comes into the Certificate Authority's possession in the course of its normal activities is to be regarded, unless express consent is given, as confidential and not to be published, with the exception of information explicitly intended for public use (e.g. dates of revocation and suspension of the certificate).
In particular, personal data is processed by the Certification Authority in accordance with Regulation No 679/2016 and Legislative Decree No 196 of 30 June 2003, as amended and supplemented [3].

3.5 Fees

3.5.1 Issue and renewal of the certificate

Fees apply for the issue and renewal of the CNS Authentication Certificate. These fees are available from the Issuing Authority or the bodies delegated by it (RA).

3.5.2 Revocation and suspension of the certificate

The revocation and suspension of the certificate are free of charge.

3.5.3 Access to the certificate and revocation lists

Access to the register of published certificates and to the list of revoked or suspended certificates is free of charge.

4. Administration of the Certificate Policy

4.1 Procedures for updating

The Certification Authority reserves the right to make changes to this document for technical reasons or due to changes in procedures resulting from legislation or regulations.

Errors, updates or suggestions for amendments may be reported to the user contact indicated in § 2.3.
Editorial and typographical corrections and other minor changes will result in an increment to the document's release number, whilst changes with a significant impact on users (such as major changes to operational procedures) will result in an increment to the document's version number. In all cases, the manual will be promptly published and made available in accordance with the established procedures.
Any technical or procedural changes to this policy will be promptly communicated to the Registration Offices.

4.2 Rules for publication and notification

This Policy is published in electronic format on the Certification Authority's website at https://www.firma.infocert.it/documentazione/.

5. Identification and Authentication

The Certification Authority shall establish an appropriate secure channel through which it receives the request for the CNS certificate from the Issuing Authority. The Certification Authority shall authenticate the Issuing Authority before proceeding to issue the requested CNS Authentication Certificate.
The identification of the CNS Certificate subscriber is carried out by the Issuing Authority.
The operational procedures required for the identification and authentication of the subscriber are set out in the policy and practice statement provided by the Issuing Authority.

5.1 Authentication for the renewal of keys and certificates

The certificate contains details of its validity period in *the 'validity'* field, with the attributes 'valid from' (*not before*) and 'valid *until' (not after).*

The dates specified in the aforementioned attributes are expressed in the format

```
year-month-day-hours-minutes-seconds-timezone
{YYYYMMDDHHMMSSZ}
```

in the UTCTime representation specified by the reference standard [7].

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

The subject may, however, renew it before it expires. Renewal requires the generation of a new key pair. The renewal procedures are set out in the Issuing Authority's policy and practice statement.

5.2 Authentication for Requests for Revocation or Suspension

The certificate may be revoked or suspended:

- at the subject's request
- on the initiative of the Issuing Authority
- on the initiative of the Certification Authority.

The procedures for submitting a request for revocation or suspension are set out in the policy and practice statement provided by the Issuing Authority.
The Certifier verifies the origin of the request for revocation or suspension.

6. Operations

This chapter describes the procedures required to carry out the issuance, revocation, suspension and renewal of a CNS Authentication Certificate from the perspective of the Certification Authority. The operational steps for registering the subject, generating keys and issuing the certificate are set out in the policy and practice statement provided by the Issuing Authority.

6.1 Certificate format and content

The profile of the generated certificate complies with that published on the AgID website http://www.agid.gov.it/.
Compliance with the Technical Rules for the issuance of a CNS is declared in the Certificate Policy extension (2.5.29.32) with OID 1.3.76.16.2.1.

6.2 Validity of the certificate

The certificate is valid for three years from the date of issue or until the date of publication of its revocation or suspension, if these occur before its expiry.

6.3 Use of the Certificate

The scope of use of the Authentication Certificate comprises web browsers as well as specific applications issued by the Certification Authority, as described in § 2.2.4.

6.4 Revocation and suspension of a certificate

The revocation or suspension of a certificate renders it invalid and **invalidates** any use of the corresponding private key made after the time of revocation or suspension. Revoked or suspended certificates are included in a Certificate Revocation List (CRL) signed by the Certification Authority and published at predetermined intervals in the certificate register.
The revocation and suspension of a certificate take effect from the time of publication of the list and render the certificate and any use of the corresponding private key made after that time invalid.

6.4.1 Grounds for revoking a certificate

The Certification Authority may revoke a certificate on its own initiative, on the initiative of the Issuing Authority or at the request of the subject.

It is mandatory to request revocation if any of the following conditions apply:

- the private key has been compromised, or one of the following circumstances applies:
  - the device containing the private signature key has been lost or stolen;
  - the confidentiality of the private key or the activation code required to access it has been compromised;
  - any event has occurred that has compromised the reliability of the private key;
- The subject is no longer able to use the secure signing device containing the private key in their possession (e.g. failure of the secure device);
- there is a change to the subject's details contained in the certificate;
- a substantial breach of this manual or the Issuing Authority's policy and practice statement is identified.

6.4.2 Procedure for requesting revocation

The procedures for requesting the revocation of the Certificate are set out in the Issuing Authority's policy and practice statement.

The Subject may also request the revocation of their certificate from the Certification Authority by following the procedures set out on its website www.firma.infocert.it.

Revocation on the Certifier's initiative
The Certification Authority shall notify the Subject in advance – except in cases of justified urgency – of its intention to revoke the certificate, stating the reason for revocation and the effective date; the certificate revocation procedure is then completed by adding the certificate to the Certificate Revocation List (CRL).

6.4.3 Grounds for the suspension of a certificate

The Certification Authority shall suspend the certificate on its own initiative, at the request of the Issuing Authority or at the request of the subject.

Suspension must be carried out if the following conditions arise:

1. a revocation request has been made without it being possible to verify the authenticity of the request in good time;

2. the Subject, the Issuing Authority or the Certification Authority have grounds for doubting the validity of the certificate;
3. it is necessary to suspend the validity of the certificate.

6.4.4 Procedure for requesting suspension

The procedures for requesting the suspension of the Certificate are set out in the Issuing Authority's policy and practice statement.

The Certificate Holder may also request the suspension of their certificate from the Certification Authority by following the procedures set out on its website www.firma.infocert.it.

Suspension initiated by the Certification Authority follows the same procedure as that for revocation.

6.4.5 Publication and frequency of CRL issuance

Revoked or suspended certificates are included in a Certificate Revocation and Suspension List (CRL), signed by the Certification Authority, entered and published in the certificate register.

The CRL is published on a scheduled basis every hour (routine issuance). The CA may, in exceptional circumstances, trigger an unscheduled issuance of the CRL (immediate extraordinary issuance). Users are responsible for obtaining and consulting the CRL. The CRL is always issued in its entirety. The Certificate Authority reserves the right to publish other CRLs separately, as subsets of the more general CRL, in order to reduce network load. The CRL to be consulted for a specific certificate is indicated in the certificate itself, together with information on the protocol to be used. Each entry in the CRL contains, in the appropriate extension, the date and time of the revocation or suspension request. The CRL format complies with the X.509 V3 standard.

6.4.6 Timing

The maximum time between a request for revocation or suspension and its implementation via the publication of the CRL is 24 hours.

6.4.7 Online services for checking certificate revocation status

In addition to publishing the CRL in LDAP and HTTP registries, InfoCert also provides an OCSP service for checking the certificate status. The service's URL is specified in the certificate. The service is available 24 hours a day, 7 days a week.

Consistency between the OCSP service and the CRL is guaranteed within a maximum of one hour. The consistency of the OCSP service and the updating of the information issued by the service itself in relation to CRL updates is subject to the waiting time required to update the CRL itself, as defined in the preceding paragraph.

Information on the certificate's status will be made available until the root CA certificate expires.

6.5 Certificate Renewal

The certificate is valid for a maximum of three years from the date of issue. The procedure for requesting a new certificate, which involves the generation of a new key pair, must be initiated by the subject before the certificate expires.

A Subject wishing to renew their digital certificate must request the issue of a new certificate before the expiry of the one in their possession.

Once the expiry date has passed, renewal will no longer be possible and a new registration will be required.

Private signature keys for which the corresponding public key certificate has expired may no longer be used.

The procedures for renewing the certificate are set out in the Issuing Authority's policy and practice statement.

7. Management and operation of the CA

7.1 Security Management

The Certification Authority has implemented an information security system for the digital certification service.
The security system implemented is structured across three levels:

- a physical level, which aims to ensure the security of the premises where the Certification Authority operates the service,
- a procedural level, covering purely organisational aspects,
- a logical level, through the implementation of hardware and software measures that address the issues and risks associated with the type of service and the infrastructure used.

This security system is designed to prevent risks arising from the malfunctioning of systems, the network and applications, as well as from the unauthorised interception or alteration of data.

7.2 Operations Management

Management procedures and automated systems are in place to monitor the status of the certification system and the Certifier's entire technical infrastructure.
Automatic monitoring tools are in place, enabling the Certification Authority to monitor the system by assessing the events and states in which the system finds itself.

7.2.1 Security and quality audits

The Certification Authority's operational and security procedures are subject to periodic checks relating to quality certification (ISO 9001), Service Management System certification (ISO 20000) and information security management certification (ISO 27001), as well as to internal audits. These checks aim to verify the correct application of the prescribed procedures and their effective functioning in relation to the set objectives.
In addition to process auditing activities, analyses and checks are scheduled to be carried out on the logs generated by applications and systems during normal operation. The purpose of this activity is to verify that all events that have occurred fall within the scope of normal operations and that no events compromising security have taken place. The logging and subsequent traceability of events that have occurred also constitute a valid security measure.

The website https://www.infocert.it contains references to the certifications obtained from the Certification Body.

7.3 Disaster Management Procedures

The Certification Authority has adopted the necessary procedures to ensure service continuity even in highly critical situations, using redundant components and backup systems.
In the event of a disaster, operations will be resumed using backup copies of the data and cryptographic systems containing the certification keys.

7.4 Archived Data

The Issuing Authority is the data controller for personal data. The Certification Authority processes the personal data in its possession for the provision of the service in accordance with current legislation [3], putting in place safeguards that meet at least the minimum requirements set out therein.
The following data is stored and maintained in the archives managed by the Certification Authority:

- registration details of key subjects;
- certificates issued, suspended and revoked;
- link between the subject's identification code and the signing device;
- session data relating to the system and services, and other data necessary to track operations relevant to security purposes.

Access to the data contained in the various archives is restricted to duly authorised personnel only, thereby ensuring the confidentiality and integrity of the data. The Certification Authority does not process sensitive data [3].

7.4.1 Data backup procedures

Software and data are subject to regular backups as required by internal procedures.

7.5 Certification Authority Keys

Certification keys are generated on dedicated cryptographic hardware with security features compliant with FIPS 140 Level 3 accreditation and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 in Europe. The root CA keys that sign the issuance of new certificates may be:

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

7.6 Quality System

All the Certification Authority's operational processes described in this policy and practice statement, as well as all other activities of the Certification Authority, comply with the ISO 9001 standard.

7.7 Service Availability

Unless otherwise agreed in a contract, the service is available at the following times:

Service	Time
Access to the public certificate repository (1) (includes certificates, CRLs and OCSPs)	From 00:00 to 24:00, 7 days a week
Certificate revocation and suspension (1)	From 00:00 to 24:00, 7 days a week
Other activities: registration, generation, publication, renewal (2)	Mon–Fri: from 09:00 to 17:00 Saturday: 09:00 to 13:00 (excluding public holidays)

(1) The service may not be available during the specified time slot due to maintenance work or force majeure.
(2) Registration is carried out at the Issuing Authority's Registration Offices, which may have different opening hours. In any case, the Certification Authority guarantees the provision of its service during the times stated above.