InfoCert Certification Body:
Authentication Certificates – Policy and Practice Statement
Document code: ICERT-INDI-MOCA

This page has been left
blank intentionally

Contents

1. Introduction to the ‘ ’ document

1.1 Changes introduced compared with the previous version of the ‘ ’

Version/Release No.:	1.5	**Version/Release date:**	18/07/23
Description of changes:	New InfoCert logo		
Reasons:	Rebranding		

Version/Release No.:	1.4	**Release Date:**	23/09/21
Description of changes:	Contact details and company information		
Reasons:			

Version No.:	1.3	**Version/Release date:**	15/02/16
Description of changes:	Addresses, telephone numbers and other company details		
Reasons:			

Version No.:	1.2	**Version/Release date:**	20/06/11
Description of changes:	Addresses and company details		
Reasons:			

Version No.:	1.1	**Version/Release Date:**	15 October 2007
Description of changes:	Operational address and call centre number		
Reasons:			

Version No.:	1.0	**Version/Release date:**	05/07/2007
Description of changes:	none		
Reasons:	First issue		

1.2 Purpose and scope of this document

This document sets out the rules governing the issuance and use of **Authentication Certificates** signed by the InfoCert Certification Authority and describes the operational procedures adopted by the Certification Authority itself for digital certification services.
The guidelines in this document apply to activities relating to InfoCert in its capacity as a Certification Authority, to Registration Offices, to those responsible for carrying out

the identification/registration of Subjects and/or to issue secure signature devices to them, for the Subjects themselves, and for Users.

The following documents were consulted in the preparation of this document:

- **InfoCert** Certification Authority – Subscription Certificates – Policy and Practice Statement
- **IETF** RFC 2527 (1999): "Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework".

1.3 Regulatory and technical l references

Regulatory references

[1] Legislative Decree No. 82 of 7 March 2005 (*Official Gazette* No. 112 of 16 May 2005) – Digital Administration Code (hereinafter referred to as CAD)

[2] Legislative Decree No. 159 of 4 April 2006 (Official Gazette No. 99 of 29 April 2006) – Supplementary and corrective provisions to Legislative Decree No. 82 of 7 March 2005, containing the Digital Administration Code.

[3] Presidential Decree No. 445 of 28 December 2000 (Official Gazette No. 42 of 20 February 2001) and its amendments pursuant to Presidential Decree No. 137/2003 (hereinafter referred to as the TU)

[4] CNIPA Resolution No. 4/2005 of 17 February 2005 (Official Gazette No. 51 of 3 March 2005) – Rules for the recognition and verification of electronic documents

[5] Legislative Decree No. 196 of 30 June 2003 (Official Gazette No. 174 of 29 July 2003)

[6] Decree of the President of the Council of Ministers of 30 March 2009 (Official Gazette No. 129 of 6 June 2009). Hereinafter referred to as **DPCM**

Technical references

[7] ETSI TS 102 042 *"Policy requirements for certification authorities issuing public key* certificates" – April 2002

[8] RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

[9] RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

[10] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[11] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

[12] InfoCert Certification Authority – Subscription Certificates, Policy and Practice Statement, ICERT-INDI-MO

1.4 Definitions

1.5 Definitions

The definitions used in the drafting of this document are listed below. For terms defined by the TU, the CAD and the Prime Ministerial Decree of 30 March 2009, please refer to the definitions set out therein. Where

appropriate, the corresponding English term – generally used in publications, standards and technical documents – is indicated in square brackets.

Certification Agreements *[Cross-certification]*
Cross-certification takes place between Certification Authorities belonging to different domains. In this process, the Certification Authorities certify one another. A necessary condition for cross-certification to take place is that they accept and share equivalent rules in the policy and practice statement.

Voluntary Accreditation
Recognition that the certifying body, upon request, meets the requirements of the highest level in terms of quality and security.

Self-certification:
This is a declaration, addressed to the Certification Authority, made personally by the individual who will be the subject of the digital certificate, by signing to confirm the existence of certain circumstances, facts and qualities, in accordance with Article 46 of Presidential Decree 445/00, and by assuming the responsibilities laid down by law.

***Time-stamping* authority**
This is the software/hardware system, managed by the Certification Authority, which provides the time-stamping service.

Certificate, Digital Certificate, X.509 Certificate *[Digital Certificate]*
A set of information designed to establish with certainty 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.

Qualified Certificate – see CAD

***Certification Authority* – see CAD Accredited**

Certification Authority – see CAD Qualified

Certification Authority – see CAD

Private Key and Public Key – see CAD

Emergency code
A pre-generated code issued by the Registration Authority to the subject for the purpose of authenticating a request to suspend a certificate.

Data for creating a signature – see CAD Data

for verifying a signature – see CAD

Secure signature creation device – see CAD
The secure signature device used by the subject consists of a plastic medium (usually a plastic card the size of a credit card) containing a microprocessor that meets the security requirements laid down by law. It is also known **as a microprocessor card** or **smart card**.

Digital Evidence
A sequence of binary symbols (bits) that can be the subject of a computerised procedure.

Electronic signature – see CAD

Qualified electronic signature – see CAD

***Digital signature* – see CAD Audit log**

The audit log consists of all records, whether made automatically or manually, of the events specified in the Technical Rules.

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 public register**.

***Time Stamp Token* – see DPCM policy and practice**

statement – see Article 38 of the DPCM

The policy and practice statement sets out the procedures that the Certification Authority applies in the performance of

service. In drafting the Manual, the guidelines set out by CNIPA and those found in international literature were followed

Public official

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

RAO – 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

The Certificate Register is an archive containing all valid certificates issued by the Certification Authority.

Public Register *[Directory]*

The Public Register is a repository containing:

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

Technical Rules

Technical rules for the creation, transmission, storage, duplication, reproduction and validation – including temporal validation – of electronic documents (DECREE OF THE PRESIDENT OF THE COUNCIL OF MINISTERS 13 January 2004).

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 person who requests the Certification Authority to issue digital certificates. If different from the subject, the subscriber's identity is entered in the 'Organisation' field of the X.509 certificate.

Role

The term 'Role' generically refers to the professional title and/or qualification held by the Subject, or any power to represent natural persons or private or public-law bodies, or membership of such bodies, as well as the exercise of public functions.

Coordinated Universal Time *[Coordinated Universal Time]*

A time scale accurate to the second, as defined in ITU-R Recommendation TF.460-5

Third Party – see CAD

The natural or legal person who, where applicable, gives their consent to the inclusion in the signature certificate of a Role of the Subject, or who authorises or requests the inclusion in the certificate of the name of the Organisation to which the Subject is affiliated

***Subject* – see CAD**

The natural person identified in the certificate as the holder of the private key corresponding to the public key contained in the certificate itself; the subject is attributed the digital signature generated using the private key of the key pair.

Registration Authorities *[Registration Authority]*

An entity appointed by the Certification Authority to carry out the activities necessary for the latter to issue the digital certificate and to deliver the secure signing device.

User *[Relying Party]*

A party that receives a digital certificate and relies on that certificate or on the digital signature based on that certificate.

1.6 Acronyms and abbreviations

ACBI – Association for Interbank Corporate Banking

CNIPA – National Centre for Information Technology in Public Administration

CAD – Digital Administration Code

This refers to Legislative Decree No. 82/2005 and subsequent amendments, *the 'Digital Administration Code*'.

CRL – Certificate Revocation List

DN – Distinguished Name

Identifier of the subject of a public key certificate; this code is unique amongst subjects who have a certificate issued by the Certification Authority.

DPCM – Decree of the President of the Council of Ministers

This refers to the Prime Minister's Decree of 13 January 2004.

DTS – Digital Time Stamping

A system for time-stamping certificates and documents.

ETSI – European Telecommunications Standards

Institute HSM – Hardware Security Module

It is a secure device for creating digital signatures, with functionality similar to that of smart cards, but with superior memory capacity and performance.

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 Subject Identifier

This is a code associated with the subject that uniquely identifies them with the Certification Authority; the subject has a different code for each certificate they hold.

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

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 a secure signing device, used by the subject to access the device's functions.

PUK
A personalised code for each smartcard, used by the subject to reactivate their device after it has been locked due to an incorrect PIN entry.

RRC
Acronym for Revocation Request Code, the name previously assigned to the emergency code and still occasionally used.

TSA – Time Stamping Authority
The certification authority registered with the CNIPA that certifies the keys of the systems (see TSU) which sign the time stamps (Time Stamp Tokens).

TST – Time-Stamp Token
A term used in international literature to refer to a time stamp.

TSU – Time Stamp Unit
The trusted component whose keys, certified by the TSA, sign the time stamps.

TU – Consolidated Act
This refers to Presidential Decree No. 445/2000 and its subsequent amendments, *'Consolidated Act of , legislative and regulatory provisions concerning administrative documentation*'.

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, by means of this key, the possession of the corresponding private key, thereby identifying the subject of that 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, Authentication Certificates issued by the InfoCert Certification Authority are issued at the subject's direct request, following the subject's physical identification, and are issued on a secure signing device (smart card).

This document sets out the rules governing the issue and use of Authentication Certificates (hereinafter also referred to more briefly **as 'Certificates'**) signed by the InfoCert Certification Authority, and describes the operational procedures adopted by the latter for digital certification services.

Authentication Certificates are issued and managed by the InfoCert Certification Authority in accordance with the procedures set out in this policy and practice statement, which are similar to those already defined for Signing Certificates (see the relevant policy and practice statement, ICERT-INDI-MO): Authentication Certificates must be used within the S/MIME and SSL protocols, with tools such as web browsers and email clients, to verify advanced electronic signatures created using a secure device. They may also, if required, be used for user authentication when accessing domains managed by Microsoft servers (SmartLogon).

By publishing this policy and practice statement and including references to this document in the Certificates, the Certification Authority enables Subscribers and Users to assess the characteristics and reliability of the certification service.

2.1 ’s document identification

This document is entitled **“Authentication Certificates – Policy and Practice** Statement” and is identified by the document code: **ICERT-INDI-MOCA**.

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

The object identifier (OID) of this document, referenced in the certificates, is as follows: 1.3.76.36.1.1.3 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-authentication-certificates	1.3.76.36.1.1.3

This document is available in electronic format on the Certification Authority’s website at http://www.firma.infocert.it/doc/manuali.htm.

2.2 Actors and Application Domains

2.2.1 Certification Authority

InfoCert is the **Certification Authority** that issues, publishes in the register and revokes **Authentication Certificates**, operating in accordance with the provisions set out in this policy and practice statement.
The full details of the organisation acting as the Certification Authority are as follows:

Table 2

Company Name	**InfoCert - Public Limited Company Company subject to the management and coordination of Tinexta S.p.A.**
Registered office	Piazza Sallustio 9, 00187 Rome
Operational headquarters	Via Marco e Marcelliano 45, 00147 Rome
Telephone number	06836691
Company Registration Number	**Tax Code 07945211006**
VAT number	**07945211006**

Website	http://www.firma.infocert.it/

2.2.2 Registration Offices

The Certifying Body makes use of Registration Offices throughout the country, which, including through their authorised representatives, carry out the following activities as an interface between the Certifying Body itself and the subscriber:

- Identification and registration of the subscriber;
- validation of the certificate application;
- distribution and initialisation of the secure signature device (smart card);
- initiation of the certification procedure for the Subscriber's/Subject's public key;
- providing support to the Subject and the Certification Authority in the renewal, revocation and suspension of certificates.

Registration Offices are authorised by the Certification Authority following appropriate training of the staff employed, who will be able to carry out identification procedures, and where necessary registration, even at the subscriber's premises.
The Certification Authority verifies that the procedures used by the Registration Office comply with the provisions of this manual.

2.2.3 Certificate Register

The lists of revoked and suspended certificates are published in a **public register** which also contains the certificates of subjects who have expressly requested this.
The certificate register, which contains **all** certificates issued by the Certification Authority, is **not** public.
The Certification Authority uses reliable systems to manage the **public register** and the **certificate register** in such a way as to ensure that only authorised persons may make entries and amendments, that the authenticity of the information is verifiable, that certificates are accessible for public consultation only in cases permitted by the subject, and that the operator is able to detect any event that compromises security requirements.
The address and methods of accessing the register are described in § 6.3.3.

2.2.4 Scope of Application

The scope of use of the Authentication Certificate comprises email products and web browsers, as well as specific applications issued or approved by the Certification Authority.

With email products, using the **S/MIME** standard, the Authentication Certificate can be used to verify the identity of a message's sender as well as to guarantee the confidentiality and integrity of its content.
With web browsers, via the **SSL** standard, it is possible to verify the identity of a party holding the Authentication Certificate who connects to a domain that is itself certified.
More generally, a user, by using their private key – for which an 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). In Microsoft network domains, it is possible to use strong authentication functions based on smart cards (smart logon). For this purpose, in addition to the subject's basic identification details, the certificate may contain control information specific to the Microsoft environment that is necessary to enable these services.

For a User 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 Subject's certificate be used to send them an encrypted message (to ensure the confidentiality of the 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.

Where certification agreements are in place, the Certification Authority recognises the validity of the rules of the other Certification Authority with which it has entered into the agreement, and vice versa. The certificate issued for the other Certification Authority will be used solely to verify that Certification Authority's signature on the certificates it issues.

2.3 Contact details for end users and communications

InfoCert is responsible for defining, publishing and updating this document. Questions, comments and requests for clarification regarding this policy and practice statement 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 3 35131 Padua

Telephone: +39 06836691
Fax: +39 0623328861
Digital Signature Call Centre: see the link https://help.infocert.it/contatti/

Website:
http://www.firma.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. 's 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;
2. that it does not act as a custodian of private keys relating to the corresponding 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 policy and practice statement;
5. the thorough protection of its own 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 described in this policy and practice statement;
7. the adaptation of its data security system to the minimum security measures for the processing of personal data.

3.1.2 Obligations of the Registration Authority

The Registration Office is required to ensure:

1. verification of the Subscriber's identity and the registration 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 requests for revocation or suspension 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 described in this policy and practice statement;
6. ensuring that its data security system complies with the minimum security measures for the processing of personal data.

The Registration Office shall deal directly with the Subscriber, the Certificate Holder, and is required to inform them of the provisions contained in this policy and practice statement.

3.1.3 Obligations of Subjects

The subject is required to:

1. ensure that the information provided to the Certification Authority for the certificate application is accurate, complete and up to date;
2. protect and store 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 functions of the secure signing device in a secure location separate from where the device itself is kept;
4. protect and store the unlock code (PUK) used to reactivate the secure signature device 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 secure signature device;
6. use the secure signature device personally and not transfer it or allow third parties to use it;
7. use the keys and the certificate solely in the manner set out in this policy and practice statement;
8. submit to the Certification Authority, without delay, a request for the revocation or suspension of certificates should any of the circumstances set out in this policy and practice statement (§ 6.4) arise;
9. 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, the limitations of liability and the limits of indemnity of the Certification Authority, as set out in this 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 register (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 policy and practice statement, or by their failure to take the appropriate measures of special diligence required of users of certification services to prevent harm 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 caused by 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 and practice statement is available:

- in electronic format on the Certifier's website (see § 2.1)
- in paper format, available both from the Certifying Body and at the Registration Offices.

3.3.2 Publication of certificates

Certificates issued are not usually published.
Users wishing to make their certificate public may submit a request by sending the relevant form (available on the website www.firma.infocert.it), digitally signed with the key corresponding to the certificate for which publication is requested. The form must be sent by email torichiesta.pubblicazione@cert.legalmail.it , following the procedure described on the website.

3.3.3 Publication of revocation and suspension lists

Revocation and suspension lists are published in the public certificate registry, which can be accessed via the LDAP or HTTP protocols at the address specified in the 'CRL Distribution Points' attribute of the certificate.
Access may be gained via software provided by the Certification Authority and/or features available in commercially available products that support the LDAP and/or HTTP protocols. The Certification Authority may make other methods available, in addition to the one indicated, for consulting the list of published certificates and their validity.

3.4 's personal data protection

Information relating to the subject that comes into the Certifying 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. public key, certificate, dates of revocation and suspension of the certificate).
In particular, personal data is processed by the Certification Authority in accordance with Legislative Decree No. 196 of 30 June 2003 and European Regulation 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, which has been fully binding since 25 May 2018.

3.5 Fees

3.5.1 Issue and renewal of the certificate

Fees apply for the issue and renewal of the Certificate of Authentication. These fees are based on the volume of data processed and are subject to market trends.

The fees are available on the websites https://www.firma.infocert.it/ and http://ecommerce.infocert.it or from the Registration Offices.

The cost of the secure signature device (which may already be available to the Subject for the Subscription Certificate) and the smart card reader are not included in these fees.

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 public register** (published certificates and the list of revoked or suspended certificates) is free of charge.

4. and Operational Manual

4.1 n and update procedures

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 changes 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 and practice statement will be promptly communicated to the Registration Offices.

4.2 Rules for publication and notification

The Policy and Practice Statement is published:

- in electronic format on the Certifier's website at http://www.firma.infocert.it/doc/manuali.htm
- in paper format, it may be requested from the Registration Offices or from the contact point for end users (see §. 2.3).

4.3 e Manager responsible for approval

This policy and practice statement is reviewed by the Head of Security and Policy, the Data Protection Officer, the Head of the Certification Service, the Legal Department and the Consultancy Division, and approved by company management.

5. Identification and Authentication

This chapter describes the procedures used for:

- identifying the subscriber at the time of applying for the issue of an Authentication certificate;
- authenticating the Subject in the event of the renewal, revocation or suspension of Authentication certificates.

5.1 Identification for the purposes of initial issue

The Certification Authority verifies the subscriber's identity with certainty before proceeding to issue the requested Authentication certificate.

The identification procedure requires the subscriber to be personally recognised by one of the entities referred to in § 5.1.1, which will verify their identity by checking a valid identity card or an equivalent document (see Article 35(2) of the Consolidated Act).

5.1.1 Entities authorised to carry out identification

The subscriber's identity may be verified by one of the following parties:

1. The Certifying Authority, including through its authorised representatives;
2. The Registration Office, including through its authorised representatives;
3. A public official.

5.1.2 Identification procedures

Identification is carried out by one of the parties listed in § 5.1.1, and the subscriber's physical presence is required.

The person carrying out the identification verifies the subscriber's identity by checking one of the following valid and unexpired documents, in accordance with Article 35 of Presidential Decree No. 445 of 28 December 2000:

- Identity card
- Passport
- Driving licence
- Boating licence
- Pension book
- Certificate of competence to operate heating systems
- Firearms licence

Other forms of identification may be accepted in addition to those listed, provided they bear a photograph and a stamp and have been issued by a government authority.

Upon identification, the subscriber is provided with an emergency code, which serves as the means of authentication within the secure communication system between the Certifying Authority and the subject.

Identification by public officials may also be carried out in accordance with the regulations governing their activities, including the provisions of Decree-Law No. 143 of 3 May 1991, as subsequently amended and supplemented.

5.1.2.1 Application for the issue of a certificate

The main steps the Subscriber must follow to obtain an Authentication certificate are:

a) to read this policy and practice statement and any further information documents;
b) follow the identification procedures adopted by the Certifying Authority as described in the following paragraphs;
c) provide all the information necessary for identification, accompanied, where required, by appropriate supporting documentation;
d) sign the registration application, thereby accepting the contractual terms and conditions governing the provision of the service.

5.1.2.2 Information to be provided by the subscriber

The registration application contains the information that must appear on the certificate and that which enables the relationship between the Certification Authority and the Subscriber/Subject to be managed effectively. The application form must be signed by the Subscriber/Subject.

The following information is mandatory:

- Surname and First Name
- Date and place of birth
- Tax reference number
- Residential address
- Details of the identification document presented, such as type, number, issuing authority and date of issue
- The Subject's personal email address.

5.2 Authentication for key renewal and certificate

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

NOTE

The dates indicated in the above 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 renew the certificate, prior to its expiry, by sending the Certifying Authority a renewal request authenticated with an advanced electronic signature: this signature is generated using the private key of the key pair to be renewed.

5.3 Authentication for requests for revocation or suspension

The certificate may be revoked or suspended:

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

The Certification Authority verifies the origin of the request for revocation or suspension.

5.3.1 Revocation or Suspension at the request of the Subject

The Certification Authority, including via the Registration Office, verifies the identity of the subscriber requesting revocation or suspension and ascertains the reasons for the request.

If the request is made by telephone or via the internet, in the case of suspension only, the subject authenticates themselves by providing the emergency code, which was supplied with the certificate they intend to revoke.
If the request is made at the Registration Office, the subject is authenticated using the procedures laid down for identification.

6. Operational Procedures

This chapter describes the procedures required to carry out the issuance, revocation, suspension and renewal of an Authentication Certificate.

6.1 Initial registration

In order to issue the certificate, a registration procedure must be carried out following identification, during which the subjects' details are stored in the Certification Authority's records.
Initial registration is carried out at the Certification Authority or at a Registration Office.

Once the initial registration phase is complete, there are two different methods for issuing digital certificates and delivering the secure signature device.

The first method (hereinafter referred to **as Case A**) allows the Certificate Holder/Subscriber to complete the certification process by taking possession of the smart card and the authentication certificate immediately after registration: in this case, the RAO will initiate the process of generating the key pair and, once the necessary checks have been carried out, issue the certificate in the presence of the Subscriber/Certificate Holder.

The second method (hereinafter referred to as **Case B**) involves separating the identification phase, carried out in the presence of the subscriber (the subject of the certificate), from the registration and issuance phase, which is subsequently carried out by the RAOs.
In both cases, the smart card is personalised by the Certification Authority using the PIN provided to the subscriber at the time of identification.
In **Case B,** the personalised smart card is handed over to the subscriber (now the subject) at a later stage.

The operational procedures for initial registration, the issue of the certificate and the delivery of the smart card, in cases where identification is carried out by a Public Official – even if carried out abroad – are described separately in Appendix A of this policy and practice statement.

6.2 Issue of the ‘ ’ certificate

6.2.1 Case A: Keys generated in the presence of the subscriber

This procedure requires the subscriber/subject, in possession of the microprocessor card, to be present at a Registration Office or at the Certification Authority.

1. The RAO, whilst verifying the Applicant’s identity, registers the Subject and initiates the certificate issuance procedure.
1. The automated procedure unlocks the secure signature device using the default PIN, enabling the generation of the encryption key pair. Should the secure signature device have a PIN different from the default one, the procedure requires the subject to enter the PIN.
2. The RAO, using their own device, signs the request for certification of the subscriber’s public key and sends it to the Certification Authority.
3. Once the certification process has been completed, including the necessary checks, the automated procedure personalises the secure signature device by entering the PIN previously provided to the subscriber during the identification phase

6.2.2 Case B: Keys generated by the Certification Authority

This procedure is carried out by RAOs, either at the Certification Authority’s premises or at the Registration Offices.

1. The RAO selects the registration details of a subscriber/subject and initiates the certificate request procedure.
2. The automated procedure unlocks the secure signature device using the default PIN, enabling the generation of the cryptographic key pair.
3. The RAO, using their own device, signs the certification request for the public key corresponding to the cryptographic key pair generated within the smartcard and sends it to the Certification Authority.
4. Once the certification process has been completed, including the necessary checks, the automated procedure personalises the secure signature device by entering the PIN previously provided to the subscriber during the identification phase.

The confidentiality of the personal PIN during the smart card (secure signing device) personalisation stages is guaranteed by appropriate encryption systems. This PIN, which is generated randomly, is stored securely within the Certification Authority’s systems and is communicated via secure procedures (automated procedures involving sealing in a sealed envelope) to the subject alone. The smart card, personalised in this way with the generated key pair, is protected by this personal PIN.

6.2.3 Key generation and protection of private keys

The signature key pair is generated by the subject using the functions offered by the microprocessor card (the secure signature device or smart card).
The subject’s private key is generated and stored in a secure area of the microprocessor card which prevents its export. Furthermore, should the security measures be breached, the device’s operating system renders the card unreadable, thereby protecting the data it contains. The asymmetric encryption algorithm used is RSA and the key length is 1024 bits.
To use the private key stored on the smart card, the holder must authenticate themselves correctly by entering their secret PIN.

6.3 Issuing the ‘ ’ certificate

The certificate is issued automatically by the Certification Authority’s procedures in accordance with the following steps:

1) the validity of the certificate request is verified by checking that:
- The Subscriber/Subject has been correctly registered and all the information necessary for the issue of the certificate has been provided;
- The subscriber/subject has been assigned a unique identification code amongst the Certification Authority’s users (IUT);
- the public key to be certified is a valid key of the required length;
- the request is genuine and the subject possesses the corresponding private key;
- the key pair functions correctly

2) the validity of the signature of the authorised person who validated the request is checked
3) the certificate is generated and published in the certificate register;
4) the certificate is stored within the subject’s secure signing device;
5) there are two scenarios:
   - (*Case A*): the subject is already in possession of the secure signature device, so the previous step concludes the procedure for issuing the authentication certificate.
   - (*Case B*): the secure signature device, initialised and protected by a PIN, is handed over to the subject in person by an official from the Registration Office.

6.3.1 Format and content of the certificate

The certificate is generated using the information provided by the subscriber during the identification process and set out in the application form signed by the subscriber.
The format of the certificates complies with the X.509 V.3 standard.

6.3.2 Validity of the certificate

The certificate is valid for up to three years from the date of issue or until the date of publication of its revocation or suspension, if these have taken place earlier.

6.3.3 Publication of the certificate

Upon successful completion of the certification procedure, the certificate will be entered into the reference register of certificates and will not be made public. Any subject wishing to make their certificate public may request this via the procedure described in §3.3.2.

6.3.4 Use of the Certificate

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

6.4 Revocation and suspension of a certified

The revocation or suspension of a certificate invalidates it and renders any use of the corresponding private key made after the time of revocation or suspension **invalid**.
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 registry.
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 Reasons for revoking a certificate

The Certification Authority may revoke a certificate on its own initiative 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;
- the relationship between the Subject and the Certification Authority is terminated;
- a substantial breach of this policy and practice statement is identified.

The Subject is entitled to request the revocation of a certificate for any reason deemed valid by and at any time.

6.4.2 Procedure for requesting revocation

The revocation request is made in different ways depending on the subscriber. The following cases apply:

Revocation at the initiative of the Subject

The subject may request revocation:

1. by telephoning the Certification Authority's Call Centre
2. via the Registration Office with which they are registered.

To make the request, the subject must provide their identification details, the unique identifier assigned to them (IUT), the reason for revocation, and the emergency code. If it is not possible to identify the subject with certainty, the Certificate may be suspended pending the correct identification of the subscriber (for example, by means of a written request for revocation). In the case of a revocation request made via the Call Centre, the subject must send the signed revocation request by certified email (PEC) or fax, accompanied by a photocopy, also signed, of a valid identity document.

Revocation on the Certifier's initiative

The Certification Authority initiates a revocation request as follows:

1. the Certification Authority notifies 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 Reasons for Suspending a Certificate

The Certification Authority suspends the certificate on its own initiative or at the subject's request.

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 or the Certification Authority has 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 request for suspension is made by the parties and in accordance with the procedures set out for requests for revocation, **specifying,** in this case, **the duration of the suspension period.**

The suspension procedure can also be initiated online via the Certification Authority's website.

Upon expiry of this period, the suspension will be followed either by a permanent revocation or by the reinstatement of the certificate's validity.

6.4.5 Reinstatement of a suspended certificate

Upon expiry of the requested suspension period, the certificate's validity is restored by removing the certificate from the Certificate Revocation and Suspension List (CRL).

6.4.6 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 registry.
The CRL is published on a scheduled basis every day.
Users are responsible for obtaining and consulting the CRL. The CRL is always issued in its entirety.
The Certification 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 relevant extension, the date and time of the revocation or suspension request.
The CRL format complies with the X.509 V3 standard.

6.4.7 Timing

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

6.5 Renewal of the ' ' Certificate

The certificate is valid for three years from the date of issue.
The renewal procedure requires the generation of a new key pair: the request for a new certificate must be initiated before the current certificate expires.
The new key pair is generated within the microprocessor card; the issue and publication of the certificate follow the procedure described for new applications.

The procedures for renewing the certificate are set out by the Certification Authority on its website (http://www.firma.infocert.it).

7. Management and operation of the CA

7.1 's security management

The Certification Authority has implemented a security system for the information system relating to 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 -operation 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.

The system is configured to undertake, depending on changes in the system's status, actions of the following types:

- logging of events;
- event recognition;
- troubleshooting;
- notifying operators.

7.2.1 Safety and quality checks

The Certification Body's operational and security procedures are subject to periodic checks relating both to internal compliance inspections against the operational procedures set out in the ISO 9001 standard and 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 security- s that have occurred also constitute a valid security measure.

7.3 nd 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 the cryptographic systems containing the certification keys.

7.4 Archived data

The following data is stored and maintained in the archives managed by the Certification Authority:

- registration data for 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.

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.

7.4.1 Data backup procedures

Data relating to networked systems is backed up daily via an automated archiving system.
Periodically, a copy of the media containing the backup data is stored in a security cabinet, to which access is restricted to duly authorised personnel only. A copy of these

Backup media are also transported to a secure location outside the Certification Body's premises, so that they remain available even in the event of a disaster.

To ensure that the entire system can be restored following any failures, backups are made of all other data and programmes necessary for the provision of the service. The methods and retention periods for these backups are the same as those for the data backup procedures.

7.5 's Certification Authority keys

Certification keys are generated on-board dedicated cryptographic hardware with security features compliant with ITSEC E3 accreditation. The certification key used to si[illegible] is a 4096-bit RSA key or, as part of a phase-out process, a 2048-bit RSA

Author unknown
23 September 2021 16:52:00

CA3 is set to 4096. CA2 is set to 2048. Shall we leave both as they are?

7.6 nd Quality Management System

All the Certifying Authority's operational processes described in this policy and practice statement, as well as all other activities carried out by the Certifying Authority, comply with the ISO 9001 standard. The Certification Body holds ISO 9001 certification for its quality management system.

7.7 Service Availability

The service is available at the following times:

Service	Time
Access to the public register of certificates (1) (includes certificates and CRLs)	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: 09:00–18:00; Sat: 09:00–12:00 (excluding public holidays)

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

8. Appendix A: Operating procedures in the event of identification by a public official

8.1 A.1: Operating procedures in the event of identification by public officials in Italy

At present, the procedure for issuing a certificate in the event of identification by public officials in Italy has not yet been established.

8.2 A.2: Operating procedures in the event of identification by public officials abroad

At present, the procedure for issuing the certificate in the event of identification by public officials abroad has not yet been established.