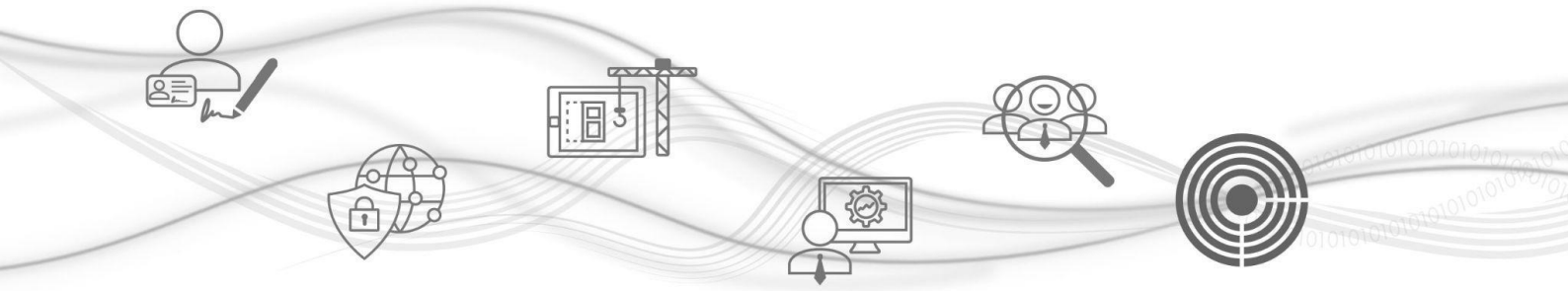
Operating Manual

Certificate Policy & Certificate Practice Statement for Certification and Time Stamping Services



Category	**Operating Manual**	Document Code	**NAM-MO-FDMT-**	**Namirial S.p.A.**
Prepared by	**Margherita Menghini**	Confidentiality note	**Public Document**	**The Legal Representative**
Verified by	**Franco Tafini**	Version	**3.1**	**Massimiliano Pellegrini**
Approved by	**Massimiliano Pellegrini**	Date of issue	**17/10/2022**	—

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 17-10-2022 08:37:24
IP address: 151.0.245.58

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italy | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | VAT No. IT02046570426
Trade and Companies Register of Ancona and Tax Code No. 02046570426 - Economic and Administrative Index (REA) No. AN157295
Recipient Code T04ZHR3 | Fully paid-up Share capital € 7,762,625.20

Table of contents

History of changes

VERSION	3.1
Date	17/10/2022
Reason	Update
Changes	Service Contacts and HelpDesk updated

VERSION	3
Date	19/05/2022
Reason	Update
Changes	All paragraphs revised, merged with Certification Practice Statement

VERSION	2.5
Date	24/04/2020
Reason	Update
Changes	Extension of the definition section; Updating of the certification section; Extension of LRA obligations; Extension of methods of identification;

VERSION	2.4
Date	14/06/2018
Reason	Revision
Changes	Document revised to comply with Regulation (EU) 679/2016 §6.1 DPO updated §6.2 Data subjects' rights updated

VERSION	2.3
Date	30/06/2017
Reason	Update
Changes	- Entry of new CA to issue Qualified Certificates for Electronic Signature and Electronic Seal

VERSION	2.2

Date	30/05/2017
Reason	Update
Changes	- Entry of issue of Qualified Certificates for Electronic Signature and Electronic Seal

VERSION	2.1
Date	23/05/2017
Reason	Update
Changes	- Entry of issue method of paper envelope with Active Certificates

VERSION	2.0
Date	12/12/2016
Reason	Update
Changes	Entry of self-enrol issue method with identification at IR and device provided by the Certification Authority

VERSION	1.9.1
Date	08/07/2016
Reason	Update
Changes	Updating of OID Timestamp Authority

VERSION	1.9
Date	15/06/2016
Reason	Update
Changes	Update following the implementation of the eIDAS regulation

VERSION	1.8
Date	08/10/2015
Reason	Update
Changes	Update on how to identify and register the user.

VERSION	1.7

Date	01/07/2014
Reason	Update
Changes	Update to Restrictions on Use and Certificate Policies. Addition of signature types. The procedure for renewing certificates has been changed. Correction of some typos within the document. The procedure for how personal signature devices and secret codes are handed over and how the digital blind envelope is displayed has been changed.

VERSION	1.6
Date	31/10/2013
Reason	Update
Changes	Replacement of article references of Italian Prime Ministerial Decree 30/03/2009 with Italian Prime Ministerial Decree 22/02/2013. Update to LRA obligations (§ 3.4). Updating of the Certificate Policy (§ 4.1). Update to the procedure for displaying the digital blind envelope (§ 5.4.7.1). Updating of the webcam identification procedure (§ 5.2.1).

VERSION	1.5
Date	01/10/2013
Reason	Update
Changes	General review of the document. Introduction of operating procedures for automatic/remote signature. Changing the renewal procedure. Introduction of webcam identification.

VERSION	1.4
Date	20/02/2013
Reason	Update
Changes	Chap. 1 Versions and References Chap. 2 Overview. Chap. 13 How the user is identified and registered.

	Chap. 17 How to deliver the blind envelope. Chap. 26 Macros and Controls.

VERSION	1.3
Date	07/03/2011
Reason	Update
Changes	Chap. 21 Operating procedures for using the signature verification software. Chap. 22 Operating procedures for generating digital signatures. Chap. 19 Certificate Directory

VERSION	1.2
Date	10/01/2011
Reason	Update
Changes	Chap. 21 Operating procedures for using the signature verification software.

VERSION	1.1
Date	08/10/2010
Reason	The maximum duration of the Qualified Certificate is specified.
Changes	Chapter 17.1 Renewing the Qualified Certificate

VERSION	1.0
Date	23/08/2010
Reason	First version
Changes	-

Technical and regulatory references

In providing its services, the Certification Authority complies with the European and national rules and regulations applicable at the time of issue. All applicable regulations and laws are set out in the following table and provided to the personnel of the Certification Authority.

NUM.	REGULATION	DESCRIPTION
[I]	Lgs. D. no. 159, 4/4/2006	Italian Legislative Decree no. 159 of 4 April 2006 Additional and corrective provisions to Italian Legislative Decree no. 82 of 7 March 2005 on the digital administration code.
[II]	Italian Prime Ministerial Decree 12/10/2007	Decree of the Prime Minister of 12 October 2007 Extension of the deadline authorising the self-declaration of compliance with the safety requirements set forth in Article 13, paragraph 4, of the Italian Prime Ministerial Decree", published in Official Gazette no. 13 of 30 October 2003
[III]	Lgs. D. 82/2005	Italian Legislative Decree no. 82 of 7 March 2005 Digital Administration Code (CAD), as amended and supplemented by Italian Legislative Decree no. 179 of 26 August 2016.
[IV]	CNIPA/CR/48	CNIPA Circular 6 September 2005 Procedures for submitting an application for registration on the public list of Certification Authorities set forth in Article 28, paragraph 1, of Presidential Decree no. 445 of 28 December 2000.
[V]	Italian Prime Ministerial Decree 22/02/2013	Decree of the Prime Minister 22 February 2013 Technical regulations on the generation, affixing and checking of advanced, qualified and digital electronic signatures.
[VI]	REGULATION (EU) 2016/679	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL of 27 April 2016 concerning the protection of natural persons with regard to the processing of personal data, as well as the free circulation of that data, and that repeals directive 95/46/EC (general regulation on data protection)
[VII]	PD 445/2000	Italian Presidential Decree no. 445 of 28 December 2000 Consolidation act of legislative and regulatory provisions on administrative documents
[VIII]	CNIPA 45/2009	CNIPA Resolution no. 45 of 21 May 2009 as amended. This resolution repealed: CNIPA Resolution no. 4 of 17 February 2005 CNIPA Resolution no. 34 of 18 May 2006 Rules for the identification and checking of electronic

NUM.	REGULATION	DESCRIPTION
		documents.
[IX]	CNIPA Restrictions on use in QCs	Restrictions on use guaranteed to users pursuant to Article 12, paragraph 6, letter c) of CNIPA Resolution no. 45 of 21 May 2009
[X]	Directive (EU) 2015/2366	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC
[XI]	RFC 3647	Certificate Policy and Certification Practices Framework
[XII]	RFC 5280	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[XIII]	ETSI TS 101 456	Policy requirements for Certification authorities issuing qualified certificates
[XIV]	ETSI TS 101 862	Qualified Certificate profile
[XV]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[XVI]	ITU-T X.509 ISO/IEC 9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[XVII]	DigitPA CD 69/2010	DigitPA - Commissioner's decision no. 69/2010 Amendment to Resolution no. 45 of 21 May 2009 of the National Centre for IT in Public Administration, on "Rules for the identification and checking of electronic documents", published on 3 December 2009 in the Official Gazette of the Italian Republic - general series - no. 282.
[XVIII]	CAD 30/12/2010 no. 235	Amendments and additions to Italian Legislative Decree no. 82 of 7 March 2005 on the Digital Administration Code, pursuant to Article 33 of Italian Law no. 69 of 18 June 2009.
[XIX]	Lgs. D. 231/2007	"Implementation of directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing as well as of directive 2006/70/EC laying down its implementing measures".
[XX]	Lgs. D. no. 83 of 22 June 2012	Urgent measures for infrastructure, construction and transport. Article 22 DigitPA and the Agency for the Dissemination of Innovation Technology are abolished. The two bodies merge into Agenzia per l'Italia Digitale (Agency for Digital Italy).
[XXI]	RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP.

NUM.	REGULATION	DESCRIPTION
[XXII]	RFC 3161	Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - August 2001.
[XXIII]	MD 9/12/2004	Decree of the Italian Ministry of the Interior, the Minister for Innovation and Technology and the Minister for the Economy and Finance of 9 December 2004, Technical and Security Rules concerning the technologies and materials used for the production of the National Service Card published in the Official Gazette no. 296, 18 December 2004.
[XXIV]	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[XXV]	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[XXVI]	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[XXVII]	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[XXVIII]	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[XXIX]	ETSI EN 319 411-3	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
[XXX]	ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[XXXI]	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[XXXII]	ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal entities
[XXXIII]	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

NUM.	REGULATION	DESCRIPTION
[XXXIV]	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[XXXV]	ETSI TS 119 495	Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking
[XXXVI]	eIDAS no. 910/2014	Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[XXXVII]	QSCD	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[XXXVIII]	TSL	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[XXXIX]	Electronic Signature Formats	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Table 1: Technical and regulatory references

Definitions and acronyms

The meanings of acronyms and specific terms are given here, except for those commonly used.

TERM OR ACRONYM	MEANING
AgID	Agenzia per Italia Digitale (Agency for Digital Italy).
Belonging to the Organisation	Employees and/or associates for whom the Organisation requires the issue of a Qualified Certificate (e.g. Companies, Entities, Trade associations, etc.).
Time-stamping authority	The software/hardware system - managed by the Certification Authority - that provides the time stamping service.
Digital Certificate, Qualified Certificate	An electronic document that certifies, with a digital signature, the association between a public key and the identity of a natural person.
Disposable certificate	Qualified Signature Certificate with short validity interval (e.g. 30 days) and 60-minute interval of use
Certification Authority	The public or private organisation authorised to issue digital Certificates by way of a certification procedure that complies with international standards and applicable Italian and European regulations.
Private key	The cryptographic key used in an asymmetric encryption system; each private key is associated with a public key and is only held by the Subject who uses it to digitally sign documents.
Public key	The cryptographic key used in an asymmetric encryption system; each public key is associated with a private key and is used to check the digital signature affixed to an electronic document by the Subject of the asymmetric key.
CIE	Carta d'Identità Elettronica (Electronic Identity Card): this is the identification document intended to replace the paper identity card on the Italian territory.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (National Centre for IT in Public Administration), the Control Body established by the Department for Innovation and Technology of the Prime Minister's Office.
CNS	Carta Nazionale dei Servizi (National Service Card)

TERM OR ACRONYM	MEANING
CRL – Certificate revocation and suspension list	A list of Certificates that have been rendered "invalid" by the Certification Authority before their natural expiry date. Revocation makes the Certificates "invalid" permanently. Suspension makes the Certificates "invalid" for a specified time.
CRS	Carta regionale dei servizi (Regional Service Card)
CUC	The Codice Univoco Certificato (Certificate Unique Code) indicated on the Request for Registration and inserted in the Certificate. It uniquely identifies the Certificate issued by the Certification Authority.
CUT	The Codice Univoco Titolare (Unique Subject Code) indicated on the Request for Registration
Relying party	The subject to whom the document and/or digitally signed electronic evidence is addressed.
Secure Device for Signature Creation	A device for creating an Electronic signature that meets the requirements of Annex II of eIDAS.
eIDAS	Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
Audit log	It consists of all the records, made automatically or manually, of the events envisaged by the Basic Technical Regulations.
IUT	Identificativo Univoco del Titolare (Unique Subject Identifier), different for each Certificate issued.
LDAP [Lightweight Directory Access Protocol]	A standard protocol for querying and changing directory services (follows the X.500 standards).
LRA [Local Registration Authority]	The natural person or legal entity appointed to carry out the operations involved in issuing the Certificates, according to the methods identified and described in this Manual. The entity must have entered into service agreements with the Certification Authority in advance. The LRA can use RAOs for identification, registration and issue.
Time Stamp	The time reference that enables time validation.
Operating Manual	The public document filed with AgID that defines the procedures applied by the Certification Authority in the carrying-out of its activities.
OID [Object Identifier]	A sequence of numbers recorded according to the ISO/IEC 6523 standard that identifies a particular object within a hierarchy.

TERM OR ACRONYM	MEANING
OCSP [Online Certificate Status Protocol]	A protocol that allows the validity of a Certificate to be checked in real time.
Organisation	An organised group of users (e.g. entities, companies, professional associations, Organisations, etc.) that have entered into agreements with the Certification Authority to issue digital signature Certificates to their employees and/or members.
OTP	One-Time Password. Number code generated by a physical device used to carry out a two-factor authentication.
PIN [Personal Identification Number]	Code associated with a secure signature device, used by the Subject to access the device's functions
PSD2	Payment Services Directive on payment services in the internal market
PUK	Personalised code used by the Subject to reactivate his/her device following its lock due to incorrect PIN entry.
RA	The Registration Authority identifies Qualified Certificate Subscribers by applying the procedures defined by the Certification Authority.
RAO	The Registration Authority Officer is expressly appointed by Namirial to identify and register on its behalf the operations of the Subject and issue the certificates. This person must belong to an LRA.
Contact Person	The natural person in charge of preparing each document required for the signature life cycle and who maintains contact with the Certification Authority.
Certificate Directory	The list of Certificates issued by the Certification Authority; the list includes revoked and suspended Certificates, which can be managed electronically.
Revocation of the Certificate	The operation whereby the Certification Authority cancels the validity of the Certificate before its natural expiry date from a given non-retroactive moment onwards.
Subscriber	The Subscriber requests the Certification Authority to issue Qualified Certificates. If the Subscriber is not the same person as the Subject of the Certificate, the identity of the Subscriber will be included in Organisation field of the X.509 certificate.
RSA	Asymmetric encryption algorithm based on public and private keys.

TERM OR ACRONYM	MEANING
Trust Service	An electronic service defined under the eIDAS Regulation that can be (a) creating, checking and validating electronic signatures, electronic seals, electronic time stamps, electronic certificate delivery services; Certificates related to these services; b) services for creating, checking and validating Web Site Authentication Certificates; c) signature preservation services; electronic seals or certificates relating to such services
Qualified trust service	A trust service that meets the requirements of the eIDAS Regulation and provides the relevant guarantees in terms of security and quality.
SHA-256 [Secure Hash Algorithm]	Encryption algorithm that generates a 256-bit fingerprint.
Seal	A set of electronic data attached, or connected by logical association, to other electronic data, in order to guarantee their origin and integrity.
Suspension of the Certificate	The operation whereby the Certification Authority suspends the validity of the Certificate before its natural expiry date for a defined non-retroactive period of time.
Interested Third Party	The natural person or legal entity consenting, in accordance with the regulations, to the issue of Qualified Certificates stating that he/she/it belongs to an Organisation or indicating any powers of representation or qualifications and positions held. He/she/it has the right/duty to request the revocation or suspension of the Certificate if the requirements on the basis of which it was issued change
Subject	The Signer, i.e. a natural person who creates an Electronic Signature
Token	The physical device (smart card or USB key) containing the private key of the Subject.
X.509	An ITU-T standard for public key infrastructures (PKI)

Table 2: Definitions and acronyms

Cross-reference table

The following table cross-references the topics envisaged by Art. 40, paragraph 3, of the Italian Prime Ministerial Decree of 22 February 2013 with the corresponding sections of this document.

Art. 40, paragraph 3, of Italian Prime Ministerial Decree, 22 February 2013	Operating Manual
▪ data identifying the Certification Authority	0
▪ data identifying the version of the operating manual	1.2
▪ person in charge of the operating manual	1.2
▪ definition of the obligations of the Certification Authority, the Subject and the Subscribers for information for checking signatures	1.4
▪ definition of responsibilities and possible restrictions on damage	9.4
▪ address of the Certification Authority's website where fees are published	1.3.1
▪ how the user is identified and registered	3
▪ key generation method for creating and checking the signature	4.6
▪ how the Certificates are issued	4.5
how to submit requests and how to manage the suspension and revocation of Certificates	4.13.3
how to replace keys	4.15
how to manage the Certificate directory	7.6
how to access the Certificate directory	7.5
how to affix and define the Time Reference	Appendix A
personal data protection methods	9.5.1
operating procedures for using the signature checking system set forth in Art. 14, paragraph 1	Appendix A
operating procedures for generating qualified electronic signatures and digital signatures	Appendix A

Summary description of Namirial S.p.A.

Namirial S.p.A. is an information technology and web engineering company that has found its own specific place within the Information Technology by orienting its software production towards the new and increasingly evident needs to adapt the Italian production system to the new highly competitive and globalised economic scenarios.
Within a national economic structure characterised for the most part by the activity of small and medium-sized companies, it was considered essential to develop software solutions and services that were also accessible on internet networks and capable of responding to emerging technological and innovative problems in a professional manner while maintaining high operating cost-effectiveness.
The company is headquartered in a modern structure of over two thousand square metres, where an Internet Data Centre is operational, equipped with all the security systems required for the inviolability of the structure and able to support users also with regard to any hosting, housing and server farm needs in general.

Namirial S.p.A. is:

AgID (former DigitPA)-accredited Qualified Certification Authority and is authorised to issue Qualified Certificates compliant with Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC European Directive 1999/93/EC, CNS Certificates and Time Stamps.

AgID (former DigitPA)-accredited Certified Email Address Provider since 26/02/2007, authorised to manage certified email inboxes and domains.

AgID (former DigitPA)-accredited SPID provider since 13/04/2017, and Certified (IT273825) pursuant to:

- ITALIAN PRIME MINISTERIAL DECREE 24/10/2014;
- Commission Implementing Regulation (EU) 2015/1502
- Regulation (EU) 910/2014 eIDAS, art. 24

for the provision of Digital Identification Trust Services.

Digital Curator, in compliance with:

- Technical Regulations pursuant to Art. 71 of the Digital Administration Code;
- Regulation (EU) 910/2014 eIDAS, art. 24;

for the provision of Standardised Preservation Trust Services.

ISO 9001 certified. Namirial holds Certificate No. 223776 issued by **Bureau Veritas Italia S.p.A.**

ISO/IEC 27001 certified. Namirial holds certificate no. IT280490 issued by **Bureau Veritas Italia S.p.A.**

Adobe certified. Since June 2013, Namirial has been a **member of the AATL** (Adobe Approved Trust List).

Namirial can also boast the strategic acquisitions of **Netheos**, a leading company in the French market specialising in digital identification and onboarding solutions, and **Evicertia**, a Spanish QTSP established in the Iberian Peninsula and Latin America.
Both acquisitions strengthen Namirial's portfolio as well as its presence in the international market, and also lead to an expansion and improvement of the company's skills.

Service Contacts and HelpDesk

To receive information on Namirial S.p.A.'s offer and certification services, the following contact details are available:

telephone: (+39) 071 63494
email: commercialeca@namirial.com
web: http://www.namirialtsp.com

The following contact details are available to receive technical information and support on the service:

email: supportoca@namirial.com
web: http://www.namirialtsp.com

The service operates on weekdays according to the following timetable:

from 9.00 am to 1.00 pm and from 3.00 pm to 7 pm

1. Introduction

1.1 Purpose and scope

This document represents the **Operating Manual** as well as the **Certificate Policy and Certification Practice Statement of the digital certification service provided by Namirial S.p.A.**, and its purpose is to describe the rules and operating procedures adopted by Namirial for all activities relating to the issue and management of Qualified Subscription Certificates and Time Stamps. The Manual also describes the procedures to guarantee an adequate level of security and reliability of Qualified Certificates in compliance with the regulations in force at the date of issue, as well as the policies and procedures relating to the Certification Authority's personnel appointed to intervene during the entire life cycle of the Certificates.
The structure and contents of this Operating Manual are based on the standard RFC 3647 framework.
With the entry into force of the eIDAS Regulation, it is no longer envisaged for Certification Authorities to have a set of documents fragmented into an Operating Manual, Certificate Policy and Certification Practice Statement: for this reason, the Certification Authority has drawn up a single document that serves the purposes of technical information, consultation and training that this Manual fulfils in accordance with the aforementioned Regulation.

The Certification Authority's documentation is organised according to the principles of the ETSI EN 319 400 series standard, specifically ETSI EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates" from ETSI and ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates" (available at http://www.etsi.org). Therefore, it is broken down as follows:

a) The **NAMIRIAL Trust Services Practice Statement** describes the general procedures adopted by the Certification Authority in the provision of qualified services;

b) specific parts relating to the certification service (e.g. Certificate policy, identification procedures, operating procedures of the specific service, etc.) are described in the Service **Operating Manual** (this document), in accordance with national standards;

c) specific parts relating to the Time Stamping service are described in this Manual.

The rules and indications contained in this document also apply to Qualified Digital Signature Certificates issued by Namirial to be installed on CNSs (National Service Card) at the request of the issuing Public Administrations (Issuing Bodies). For special cases or

subjects for which specific obligations/regulations and/or operating procedures are required, additional documents are issued as "addenda".

1.2 Document Name and Identifier

This document called "NAMIRIAL-FDMT-MO" is identified by its revision level and release date on all pages. The preamble of the document also contains a paragraph with the history of the changes made.
At least once a year, the Certification Authority carries out a compliance check of the certification service delivery process and, where necessary, updates this document also in view of the development of regulations and technological standards.
This document and any further documents issued for special subjects and cases, as an addendum to the Operating Manual, are published by the Certification Authority and AgID and can be consulted, electronically, at (pursuant to Art. 40 paragraph 2 of the Italian Prime Ministerial Decree of 22 February 2013)

http://support.namirial.com/it/
https://docs.namirialtsp.com/[1]

This URI is indicated in the *cSPuri* field of the "Certificate Policies" extension of Qualified Certificates, Time Stamping Servers and OCSPs.
The document is published in signed PDF format to ensure its origin and integrity.
The responsibility for this Operating Manual lies with the Certification Authority, in the person of the "Person in charge of the certification and time validation service" (Art. 40 paragraph 3 letter c) of the Italian Prime Ministerial Decree of 22 February 2013), who is in charge of drafting, publishing and updating it.
Communications concerning this document can be sent for the attention of the above-mentioned contact person at the following addresses:

Email: supportoca@namirial.com
Telephone: (+39) 071 63494
Fax: (+39) 071 60910

Namirial S.p.A. guarantees the compliance of its Certificates with the Root ASN.1 OID indicated below in the document.

The Object Identifier (OID) identifying Namirial S.p.A. is iso(1) identified-organisation(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

[1] The pointing of this address is http://support.namirial.com/it/.

This OID is included in the CertificatePolicy extension of the Certificates, in accordance with the policies described in paragraph 7 Policy, restrictions on use and management of Certificates.

1.3 PKI participants and responsibilities

The players mentioned in this document are:

a) the Certification Authority (**CA**)
b) the Registration Authority (**RA**)
c) the Local Registration Authority (**LRA**)
d) the Registration Authority Officer (**RAO**)
e) the **Subject** in whose name the Certificate is registered
f) the **Subscriber** (The person who submits the request for certification to the CA and carries out the identification and registration phases)
g) the **Relying party**
h) the Interested Third Party
i) the Registration Clerk (**IR**)

1.3.1 Certification Authority

Namirial S.p.A. is an **Accredited Certification Authority** (CA) that issues, publishes in the directory and revokes Qualified Subscription Certificates and CNSs, in compliance with the technical regulations in force.
The Certification Authority is a trusted third party that signs the Certificates issued by it with its own private key (CA key or root key) and manages the status of the Certificates.
The Certification Authority is identified as shown in the following table.

Company Name:	**Namirial S.p.A.**
Registered Office:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Place where the service is provided:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
VAT Reg. No:	IT02046570426
Register of Companies:	Ancona
REA:	02046570426

Share capital:	7,762,625.20€ fully paid up
Service website:	http://www.namirialtsp.com
URL of the User Portal:	https://portal.namiriatsp.com
Website of the Certification Authority:	http://www.namirial.com
Service email (Certified Email Address):	firmacerta@sicurezzapostale.it
Email of the Certification Authority:	supportoca@namirial.com

Table 3: Data identifying the Certification Authority

1.4 Organisation of personnel

The personnel in charge of providing and controlling the certification service are organised in compliance with Art. 38 of the Italian Prime Ministerial Decree of 22 February 2013. In particular, the following organisational figures are defined:

- Security manager
- Person in charge of the certification and time validation service
- Person in charge of the technical management of systems
- Person in charge of technical and logistical services
- Auditing manager
- Person in charge of the registration of Subjects (RA) and Help Desk;

The responsibilities described above also fall under the trusted roles envisaged by the ETSI EN 319-401 standard, as described in the dedicated section "Trusted Roles".
The figures listed above can make use of external employees and collaborators to carry out the activities for which they are responsible.
If necessary, registration officers can also operate at remote locations.
In order to expand working methods, registration functions can also be performed by third parties, with offices distributed throughout the territory, on the basis of special agreements signed with Namirial. In this case, these third parties ("Local Registration Authority", LRA) operate in accordance with what is described in this document and, for special subjects and/or cases, in the specific "addendum to the operating manual", if any.

The Certification Authority Namirial S.p.A:

- abides by current regulations concerning Digital Signatures as amended, and by the eIDAS no. 910/2014 regulation;
- arranges for the positive identification of the Subscriber and the Subject;

- verifies the authenticity of the certification request;
- specifies the powers of representation, or other qualifications associated with the professional activity or positions held, in the Qualified Certificate, with the consent of the interested third party, following verification of the documentation submitted by the Subscriber confirming that they hold such powers, qualifications and/or positions;
- requires, when envisaged and before issuing the Certificate, proof of possession of the private key and checks the correctness of the key pair;
- issues and manages the Qualified Certificate only in the circumstances permitted by the Subject of the Certificate according to the methods or in the circumstances set out in art. 32, paragraph 3, letter b) of Italian Legislative Decree 82/2005 (Digital Administration Code), in compliance with Regulation (EU) 206/679 (GDPR), as amended;
- supplies or indicates to the Subject the secure signature devices used in the process of issuing the Qualified Certificate for key generation, private key storage and signature operations, capable of protecting the data used to create the signature of the Subject using security measures in line with the regulations in force and with current scientific and technological knowledge;
- provides the Subject with comprehensive, clear information on the certification procedure and the technical eligibility criteria, as well as the characteristics and restrictions on using the signatures issued based on the certification service;
- does not act as a repository for the entirety of the data used to create the signature of the Subject;
- does not copy or duplicate the private signature keys of the party to whom the Certification Authority provides the certification service;
- promptly publishes the revocation and suspension of the Qualified Certificate, in the following circumstances:
    a) if requested by the Subject,
    b) if requested by the Interested Third Party from whom the latter derives its powers,
    c) in response to an order by the authorities,
    d) suspected misuse or falsification,

in accordance with the technical regulations set out in the Italian Prime Ministerial Decree of 22 February 2013 as amended;

- guarantees a secure and prompt Certificate revocation and suspension service, and guarantees the reliable, prompt and secure publication of lists of suspended and revoked signature Certificates, making sure that no more than 24 hours elapse from the revocation or suspension request to its publication;
- ensures precise determination of the data and time of issue, expiry, revocation and suspension of Qualified Certificates;
- records the issue of Qualified Certificates in the audit log, specifying the date and time they were generated; the moment of generation of the Certificate is confirmed using a time reference;
- keeps a record, including electronically, of all information relating to the Qualified Certificate from the time of its issue and for at least 20 (twenty) years, including for the purposes of providing proof of certification in the event of legal

proceedings;
- provides electronic access to a copy of the lists of certificates signed by AgID relating to the Certification Keys referred to in the Italian Prime Ministerial Decree of 22 February 2013
- uses reliable systems to manage the Certificate directory using measures to ensure that only authorised persons can input information and make changes, that the authenticity of the information can be verified, and that the Certificates are available to be consulted by the public only under the circumstances approved by the Subject;
- provides at least one system that enables the Subject to check the Qualified Signature;
- in the event of termination of the service, informs the Subjects, at least 60 (sixty) days in advance, that all certificates that have not expired at the time of termination will be revoked and, at the appropriate time, arranges for their revocation, or provides details of the substitute certification authority that will handle such certificates;
- adopts security measures for personal data processing, pursuant to Regulation (EU) 206/679 (GDPR).

1.4.1 Registration Authority

The Registration Authority (RA) is responsible for carrying out the following activities:

1) identifying the Subject or the Subscriber
2) accepting and validating the requests relating to the issue and management of Certificates
3) registering the Subjects and their organisation
4) authorising the CA to issue the requested Certificates
5) issuing the Certificate and, as a result, notifying the customer

The function of RA is carried out by Namirial employees authorised to operate by means of a mandate and after passing a specific training session.

1.4.2 Local Registration Authority

The Local Registration Authority (LRA) is the natural person or legal entity, authorised by the Certification Authority, responsible for activities relating to the issue of Certificates, in accordance with the procedures identified and described in this document, after signing a contractual mandate with the Certification Authority. The LRA may rely on its Registration Authority Officers (RAOs) for identification, registration and issue. The LRA carries out the same tasks as the RA, but by means of external parties distributed throughout the territory.
In addition to the RAOs, the LRA can appoint natural persons or legal entities to carry out exclusively the activity of registering Subjects (IR Registration Clerks).

The LRA, via the RAO, is required to:

- provide the Subject with comprehensive, clear information on the certification procedure and the technical eligibility criteria, as well as the characteristics and restrictions on using the signatures issued on the basis of the certification service;
- inform the Subject of the signing method and the type of Certificate attached to it and the proper custody of the signature credential;
- inform the Subject of his/her obligations with regard to storing the signature credential, with the utmost diligence, and separately from the signature device containing the private key in the case of a Certificate issued on a physical device;
- inform the Subject of his/her obligations with regard to storing any OTP device provided with the utmost care;
- request, when required and before issuing the Certificate, proof of possession of the private key and check the correctness of the key pair;
- inform the Subject of the adopted security measures for personal data processing, pursuant to Regulation (EU) 206/679 (GDPR);
- arrange for the positive identification of the person who applies for certification;
- verify the authenticity of the certification request;
- provide the Certification Authority with all data and documents obtained while identifying the Subject and envisaged by the Certification Authority's procedures, in order to ensure that the procedures involved in issuing the Certificate can begin promptly;
- verify and send the Certification Authority any revocation/suspension requests by the Subject to the LRA;
- scrupulously comply with the rules issued by the Certification Authority and set out in this document;
- ensure that the Subscriber and Subject have read the General Contract Conditions;
- deliver to the Subscriber and Subject a copy of the application documents for the issue of the Certificate signed by them.

In cases where the Local Registration Authority is established at one of the particular bodies of the PA, such as the Armed Forces and Police, at its express request, the activities and responsibilities for data collection and archiving may be managed directly by the LRA.

RAOs are authorised by the Certification Authority to perform their duties, following appropriate training of the personnel in charge. Without prejudice to the right to recourse, the Certification Authority is solely and exclusively responsible in relation to third parties for activities carried out by the LRA.

The Certification Authority periodically verifies that the procedures adopted by the LRA and its RAOs comply with the instructions provided in this document. In any case, at the simple request of the Certification Authority, the LRA must send it all documentation in

its possession in relation to each request to issue subscription Certificates from each Subject.

1.4.3 Subject

The Subject is the entity identified within the Certificate as the owner of the private key associated with the public key delivered within the Certificate.

The Subject can be:

- a natural person
- a natural person identified in association with a legal entity
- a legal entity (Organisation or a business unit or department identified in association with an Organisation)

The Subject of Qualified Certificates is required to:

- read this document before applying for the Qualified Certificate and comply with its requirements to the extent of its remit;
- provide all the information requested by the Certification Authority, taking personal responsibility for the reliability of that information;
- notify the Certification Authority of any changes to the information provided at the time of registering: personal details, residence, telephone numbers, email address, etc.;
- keep exclusive knowledge or availability of the signature creation data (PIN, PUK and/or OTP) and the emergency code, and store them diligently;
- keep separately from the device containing the private key, in order to guarantee its integrity and maximum confidentiality, in the case of a Certificate issued on a physical device;
- keep exclusive possession of any OTP device provided, and store it with the utmost care;
- not use the Qualified Signature for tasks and purposes other than those for which it was issued;
- put the measures specified in this Manual in place to avoid applying Qualified Signatures to documents containing macro instructions or executable codes that modify the acts or facts set out therein, thus rendering the signature void;
- submit suspension requests, according to the methods set out by the Certification Authority, specifying the reason and the period for which validity of the Certificate must be suspended;
- request the immediate revocation of Qualified Certificates relating to the keys contained on signature devices no longer in his/her possession, or that are defective;
- submit revocation requests, according to the methods set out by the Certification Authority, specifying the reason and effective date;
- report any loss or theft of the signature device to the competent authorities;
- visit the LRA or the Certification Authority, following a Certificate suspension request, to request, if necessary, its revocation using the dedicated form;

- use only signature devices indicated or provided by the Certification Authority in accordance with this manual;
- put suitable security measures in place (e.g. anti-virus/anti-malware) to prevent fraudulent use of the signature devices.

1.4.4 Subscriber

The Subscriber is a natural person or legal entity applying for a Certificate. This may coincide with the Subject, or act on behalf of one or more Subjects with whom the organisation is related (interested third party). For example, the Subscriber can be a company that applies for Certificates for its employees to do business on behalf of the organisation.
Depending on whether the Subject of the Certificate is a natural person rather than a legal entity, the relationship between Subscriber and Subject must fall within the following cases.

Natural person
In order to apply for a Certificate for a natural person, the Subscriber is:

- the natural person;
- a natural person appointed to represent the Subject; (NOTE: local law provisions can direct the transfer of responsibility to third parties). In this case, the Subscriber is referred to as the "Interested Third Party"; the Certificate includes the legal entity and/or role.
- any entity with which the natural person is associated (e.g. the organisation where the natural person is employed or a non-profit legal entity of which the natural person is a member).

Legal entity
In order to apply for a Certificate for a legal entity, the Subscriber is:

- Any entity legally recognised to represent the legal entity
- A legal representative or a legal entity with powers of signature at its subsidiaries, departments or business units.

The Subscriber is required:

- to collect, having received explicit consent from the Subjects, the data required for registration purposes in the form required by the Certification Authority;
- to request the revocation and suspension of the Certificates, according to the methods specified in this Document, whenever the conditions on the basis of which the Certificate was issued to the Subject are no longer met. (e.g., termination of the work activity, change of roles, suspension, etc.);
- to promptly notify the Certification Authority of any change in the circumstances specified at the time of issuing the Certificate, relevant to its use;
- to send revocation or suspension requests to the Certification Authority, signed and stating the reasons for it, by specifying the effective date (and duration, in

the event of suspension).

1.4.4.1 Interested Third Party

The Interested Third Party coincides with the company or organisation to which the Subject is related and which has made the request for the Certificate on its behalf.
In this case, the Subject is identified by the Interested Third Party's representative, who signed an agreement with the CA.

1.4.5 Relying party

The Relying party is a natural person or legal entity to whom the document is addressed, whose affixed Signature Certificate can be verified by reference to a public key inserted within the Certificate of the Subject. The Relying parties, in order to check the validity of a Certificate, must always refer to the Namirial CA's revocation information (CRL - Certificate Revocation List).
The Relying parties must comply with the obligations contained in this document.
Persons checking digital signatures generated using certificate keys are required to check:

- that the Certificate of the Subject has been issued by an accredited Certification Authority;
- the authenticity of the Certificate containing the public key of the signer of the document;
- that the Certificate is not included on the Certificate Revocation and Suspension List (CRL),
- the validity of the signature by means of an application or OCSP,
- the existence of and compliance with any restrictions on the use of the Certificate used by the Subject;
- the integrity of the document received, using verification software that complies with current regulations.

1.5 Using the Certificate

The Certificates issued by Namirial are valid for the purpose of applying digital signatures on electronic documents that can be used as evidence to third parties.
Any misuse of the Certificates issued by Namirial in accordance with the provisions contained in this document and within the PKI Disclosure Statement is not allowed.
Namirial reserves the right to immediately revoke any improperly used Certificate of which it becomes aware.
The appropriate competence and knowledge required for the correct use of the Certificate is assumed.

2. Managing the Operating Manual

This document is defined, published and updated by Namirial. Any amendment to this document is subject to an internal verification process, approved by senior management and notified to the Agenzia per l'Italia Digitale (AgID). Questions, comments or complaints regarding this Operating Manual should be sent by email to supportoca@namirial.com or by certified email to firmacerta@sicurezzapostale.it.
Namirial S.p.A. periodically updates its public documentation available on the organisation's website.

2.1 Publication and archiving

2.1.1 Archiving

The Namirial repository is available at

https://docs.namirialtsp.com/
http://support.namirial.com

The CA manages the repository independently and is directly responsible for it.

2.1.2 Publishing the Certificates

The CA publishes the following documents on its website:

- Trust Service Practice Statement (TSPS)
- Certification Practice Statement (CPS) and Certificate Policy (CP), integrated in this Operating Manual (MO)
- Root CA certificates

Namirial S.p.A. operates in accordance with the current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published therein: http://www.cabforum.org.
In case of any inconsistency between this document and the Requirements, the latter will prevail.

2.1.3 Frequency of publication

This document and its annexes are published on the CA website whenever they are updated. Each major change is subject to check by AgID.

2.1.4 Controlling access to public records

This document and its annexes are publicly available and accessible for reading only.

3. Identification and Authentication (I&A)

3.1 Naming

Namirial issues each Certificate in compliance with the following Standards:

- ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal entities
- ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

The Subscription Certificates show the "no repudiation" value for the key use extension. The "subject" field in the Certificate contains intelligible information that enables the identification of the owner of the Certificate (natural person or legal entity).
In case of Certificates in the name of natural persons, the "subject" field contains, at least:

- countryName;
- givenName and surname
- commonName

In the case of Certificates of legal entities, the "subject" field contains, at least:

- countryName;
- organization Name
- organizationIdentifier
- commonName

3.1.1 Meaning of names

The attribute of the Distinguished Name (DN) Certificate uniquely identifies the party to which the Certificate is issued.

3.1.2 Rules for interpreting name types

Namirial complies with the X500 standard.

3.1.3 Uniqueness of names

Natural person

Name, surname and an identification code are indicated on the Certificate to guarantee the uniqueness of the Subject. For Italian citizens, the subject's unique code is the tax code, while for foreign citizens, a unique code taken from the identity document presented during the identification phase can be defined.
Therefore, in the absence of a tax code or equivalent attribute, in the case of a Certificate whose Subscriber is foreign, the following may be indicated in the Certificate:

- an identification code taken from a valid identity document, used in the identification procedure
- a unique identifier determined by the CA and base 64 encoded

For Italian Subscribers, the tax code must be specified as it is used by public administrations to identify the citizen.

Legal entity

In case of a legal entity, the company name, tax code and VAT number are stated in the Certificate.
If the Subscriber is a public administration, i.e. an entity without a VAT number, the IPA code is indicated.

3.1.4 Pseudonymy of Subscribers

Namirial procedures include the possibility of including a pseudonym for the Subscriber, at the Subscriber's specific request.

3.1.5 Identification, authentication and role of registered trademarks

It is specified that within the Seal Certificate, in the commonName field the Subscriber is allowed to enter a free text if he/she wishes to specify a different nomenclature than the company name (e.g. trademark).
The Subscriber, when entering, assumes responsibility for populating this field in that the CA does not check the alternative entered.

3.2 Initial validation of identity

The identity validation process consists in Namirial checking the identity of the Subscriber and the identity of the Subject if the latter is different from the former (e.g. the Subject is acting on behalf of one or more separate Subjects to which it is related). Namirial will ask both parties to provide identity information and supporting documents to carry out the identification. The procedures for issuing a Qualified Certificate are:

- Registration

- Identification

The officers of the Registration Authority or of a delegated office carry out the registration and identification under the control and responsibility of Namirial.
The delegated process can be carried out by:

- Namirial operators
- The entity to which Namirial delegates its identification activities

The identification is based on locally valid documents, such as a valid identity document. Namirial keeps identification documents or certificates issued by an appropriate and authorised source, and retains this information for the period required by the regulations (20 years).

3.2.1 Accepted identity documents

The Subject or Subscriber can identify him/herself by means of a valid identity document or an equivalent identity document pursuant to Art. 35 of Italian Presidential Decree 445/2000. By way of example, the following is a list of documents that may be presented by Italian citizens, provided that they bear a photograph of the Subject, the wet signature of the Subject and stamp and are issued by a State Authority:

- Identity card,
- Passport,
- Driving licence,
- Boat licence,
- Pension book,
- Licence to operate thermal installations,
- Gun licence.

In case of Local Registration Authorities operating internationally or foreign citizens applying for a Certificate in Italy, the documents that can be submitted can be consulted in the PRADO database (https://www.consilium.europa.eu/prado/en/prado-start-page.html).
The person carrying out the identification has the right to exclude the admissibility of the document used by the Subject if it is deemed not to meet the stated requirements.
In order to ensure the protection and management of their personal data in full compliance with Regulation (EU) 2016/679 (GDPR), each Subscriber will be provided in advance with the privacy policy and, in case of identification by means of a video identification system, will be asked to consent to the registration and processing of their data by the Certification Authority's employees.

3.3 Authentication methods for Natural Persons

The identity of the Subject can be ascertained by the following methods and in accordance with Art. 24 of the eIDAS Regulation.

Method	Parties authorised to carry out identification	Technological conditions of authentication required for identification
In person	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Clerk (IR)	None
LiveID	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Clerk (IR)	None
FEQ	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Clerk (IR)	Qualified electronic signature issued by a QTSP
SPID/CIE	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Clerk (IR)	Using a pre-existing means of electronic identification (SPID digital identity or CIE)
National electronic identification	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA)	Use of a pre-existing national electronic identification means, notified by the Member State
AML processes	Subjects to whom obligations are addressed Anti-Money Laundering pursuant to the implementation regulations of Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of	AgID-authorised authentication process

	the financial system for the purpose of money laundering and terrorist financing, and subsequent implementing EU regulations as amended (PSD2 Regulation)	

3.3.1 In-person identification (*de visu*)

Identification by an RAO

In case of the issue of Qualified Certificates to natural persons, if the Subject is the same as the Subscriber, the latter can be identified "in person" (*de visu*). The *de visu* identification method requires the simultaneous physical presence of the Subject and the operator authorised to perform the identification, which can correspond to:

- personnel authorised by the Certification Authority or LRA registration offices via the RAOs;
- public official;
- registration clerk (IR).

If the Subject is not also the Subscriber, the process will involve the Interested Third Party, i.e. the company or organisation with which the Subject is associated, and that acts as Subscriber on his/her behalf.

Identification by a Public Official

If the Subscriber coincides with the Subject, he/she fills out the request for the issue of Certificates and the declaration in lieu of affidavit (downloading the form from the "*Documents*" section of the https://support.namirial.com/ website), goes to a Public Official and signs the request and the declaration by having his/her wet signature authenticated, pursuant to the regulations governing their activities and the provisions of Italian Decree Law no. 143 of 3 May 1991 as amended.

Identification by an RAO via IDCheck app

Also in this way, identification is carried out by an RAO who will use the Namirial IDCheck app, developed according to OWASP guidelines[2]. The application is only available after issuing a voucher and only to RAOs who have successfully completed the mandatory training course.

During this process, the RAO acquires the identity document and the tax code on the health card through the app, which reads the data contained therein using OCR

[2] The top 10 OWASP (Open Web Application Security Project) is a document of secure web development guidelines.

technology. The app also binds the Subscriber to be recognised after taking a photograph, which is taken by the RAO. The app then performs a face match between these captures and the photograph inside the identity document.
If the outcome of the identification is positive, the RAO can issue the Certificates. Otherwise, a new identification will have to be made.

Identification by the Registration Clerk

In this case, identification is performed by a person referred to as the Registration Clerk (Incaricato alla Registrazione - IR) who belongs to a third-party organisation and requires the Subscriber (who must also be the Subject of the Certificate) to present in person before the clerk. These parties (the IRs) can operate after the signing of a contract between the Certification Authority and the Third-Party Organisation. The latter indicates its operator who is identified with this role and who must act in accordance with the procedures established and contained in this Operating Manual with regard to the identification phases, registration of the Subscriber's data, verification of the correct filling in of the Registration and Certificate Request Form, affixing of the wet signature on the contract and, when required, delivery by hand of the device.
The Subscriber must present himself/herself to the IR by showing:

- the Registration and Certificate Request Form containing the Subscriber's personal data;
- the Identity Document complying with those envisaged by paragraph 3.2.1
- general contract conditions;
- privacy policy;

For identification purposes, the IR can check the identity of the Subscriber by matching it with a valid identity document, making sure that, in the case of pre-registration via the Web, the Document is the same as the one already uploaded in the procedure and must refrain from accepting any other form other than the one issued by the Certification Authority.
The Registration and Certificate Request Form is signed with a wet signature by the Subscriber in front of the IR.
If the digital blind envelope is used, after delivery of the device, the Certification Authority forwards the envelope to the email address provided by the Subject and signed at the time of delivery of the device in the presence of the IR.
It is hereby made known that the Subscriber, by signing the Certificate Registration and Application Form, assumes the obligations set forth in paragraph 9.8.3.
In any case, responsibility for registration, identification and validation lies with the Certification Authority.

Identification by a contact person of the Interested Third Party that signed an agreement

The Interested Third Party, in the person of the Contact Person, collects and forwards to the Certification Authority the following documents, duly signed:

- Certificate request form
- a copy of a valid identity document or equivalent identification document pursuant to art. 35 of Italian Presidential Decree 445/2000.

These documents may be signed by advanced electronic, qualified or wet signature.

3.3.2 Identification via LiveID+

Identification via LiveID+ is done by establishing a web-based contact with an authorised operator of the CA, identifiable as an RAO or an IR.
At the start of the session, each Subscriber will be informed that for security reasons the video call (video/voice) will be recorded and stored in accordance with the provisions of art. 32, paragraph 3, letter j) of the CAD and that in the event of false statements, forgery in the deeds, use or exhibition of false documents or documents containing data no longer compliant with the truth, will be subject to the penal sanctions envisaged by art. 76 of Italian Presidential Decree 445/2000.
Only after the Subscriber's consent may the video conference recording be started, which will begin with the repetition of the consent request procedure.
The specific electronic identification and registration procedures devised by the Certification Authority and implemented by its employees are not made public for security reasons.
In detail, recording data consisting of audio video files and structured metadata in electronic format are stored in a protected form for a period of twenty years with the Certification Authority. This procedure in use meets the requirements of art. 32, paragraph 3, letter a) of the CAD.

3.3.3 Identification via self procedure

Another way of video identification is through self identification. This process was checked and certified by a Conformity Assessment Body (CAB) accredited by the Italian accreditation body Accredia.
Compared to what has already been described in the previous paragraph, the user will be guided by the system to perform the following steps during a registered session after consent:

- Providing an identity document and a document containing a unique identifier (tax code on health card for Italian citizens or equivalent for citizens of foreign states);
- Filming one's own face;
- Carrying out random actions.

The procedure will perform the face match for biometric check between the filming and the photo of the identity document. In any case, a back office operator will have to check the evidence acquired.
If the check is successful, the Certification Authority is authorised to issue the Certificate and can release it.
If not, the Subscriber will have to carry out the procedure again.

3.3.4 Identification by Qualified Signature Certificate

This procedure requires the Subscriber to complete the application form envisaged for issuing digital signature, to sign it using a Qualified Electronic Signature and to submit the signed document to the system. An automated procedure performs makes sure that:

- the signature is valid;
- the signer of the form coincides with the Subscriber;
- a copy of the same application document has not already been used to obtain another digital signature certificate.

3.3.5 Identification using Electronic Authentication Tools

This method requires the Subscriber to have a pre-existing means of electronic identification:

- Notified by the Member State in accordance with Article 9 of the eIDAS Regulation, high level;
- Notified by the Member State in accordance with Article 9 of the eIDAS Regulation, significant level, provided that it gives a guarantee equivalent to physical presence in terms of reliability;
- Not notified and issued by a public authority or a private entity provided that it gives a guarantee equivalent to physical presence in terms of reliability and this is confirmed by a conformity assessment body.

Specifically, with regard to the Italian state, the following are recognised as suitable means of electronic identification:

a) the CNS (National Service Card);
b) the TS-CNS (Health insurance card – National Service Card);
c) the CIE (Electronic ID Card)
d) the CRS (Regional Service Card)
e) Digital identities issued in the context of the SPID level 2 system or higher.
f) Digital identities issued in the context of electronic identification recognised by an EU member state pursuant to Art. 8 and 24 eIDAS.

In cases a, b, c, d above, the Subscriber, after entering the PIN, carries out authentication on the portal of the Certification Authority or the CIE ID Server (CIE case).

The system retrieves the personal information entered in the Digital Certificate and associates it with the Subscription Certificate being requested.
In case e, the Subscriber, using SPID level 2 or higher credentials, is called upon to carry out an authentication at the portal of the Certification Authority or one of its LRAs by means of tools made available by the SPID circuit.
Access to the Certificate request function is via level 2 authentication or higher after using SPID credentials issued by the Identity Manager.
If the digital identity used was issued by a Manager other than Namirial, the request and issue of the Certificate will take place in accordance with AgID's Notice No. 17 of 24 January 2019 on *"Use of SPID digital identities for the purpose of issuing Qualified Certificates"*. In particular, the Certificate will contain the OID 1.3.76.16.5, registered by the Agency, with the following description: "Certificate issued through the Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity".
Registration data is stored in these cases exclusively in electronic form.

3.3.6 Identification through PSD2-compliant processes

Banking or financial institutions can offer their customers the possibility of issuing a Qualified Electronic Signature at the same time and for the purpose of using their services. The identification of Subscribers can in such cases take place via LRAs registered and operating on behalf of the Certification Authority. The identification takes place according to one of the methods identified in point 3.3 through processes external to Namirial that are authorised by AgID and compliant with Article 24 eIDAS. The processes in question must meet an authentication level that is at least equal to the *significant* level in accordance with Art. 8 of the Regulation and operate in accordance with local AML regulations, as well as in accordance with Directive (EU) 2015/2366 as amended of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2).
This regulation envisages that the Subscriber can be identified by the attributes related to his/her bank account, trusted through authentication at his/her online banking service.
Once identification is complete, the Certification Authority in possession of the necessary dataset can issue a Qualified Signature Certificate.

3.3.7 AgID-certified solutions

A number of solutions have already been certified and recognised by AgID in accordance with both Art. 24 eIDAS and the German Geldwäschegesetz (GwG).
These include:

- Check24;
- Autoident by IDNow;

- NECT;
- SignID;
- WebID;
- UMB.

3.4 Qualified Certificates for Legal Entities

In the process of issuing Qualified Certificates to Legal Entities, the Subject is the legal entity to which the Qualified Certificate of Seal will be registered, the Subscriber is the natural person who submits the request to the Certification Authority and carries out the identification phase. Identification takes place "in person" or by means of a Qualified Signature Certificate.
The user identification and registration procedure basically consists of the following steps:

- identifying "in person" or by means of a Qualified Signature Certificate;
- submitting the request, together with the necessary documentation;
- verifying the information provided, and accepting or rejecting the request.

The identification in person or by means of a Qualified Signature Certificate is carried out as described in paragraphs 3.3.1 and 3.3.4, respectively.

3.5 Identification and Authentication for the renewal of keys and Certificates

The renewal of Certificates must comply with the following conditions:

- the Certificates must not have expired,
- the request for renewal must be submitted within the last 90 days of validity.

The Certificates that fulfil these conditions and are issued on physical devices can only be renewed once.
Ninety days before the deadline, subjects will receive an email reminding them of the deadline and explaining the procedures to be followed. In case of non-renewal, further alerts will be sent 30 and 10 days before expiry.
The subjects access an online procedure that identifies the Subscriber and validates his or her identity by performing digital signatures with the Certificate whose duration is about to expire (more details are described in the relevant user guide available at https://support.namirial.com)
If the request is made after the expiry of the Certificate, a new registration and issue will be carried out.

3.6 Identification and Authentication for suspension and revocation requests

Subscriber, Subjects and Third Parties can request suspension or revocation of the Certificate. The procedures for such requests are:

- **on-line procedure**: online revocation service accessed via the device serial number and a special revocation code. This option is only available to the Subject because he/she is the only one who knows his/her personal codes. The request for revocation or suspension of the Qualified Certificate is submitted to the Certification Authority by filling out in full the appropriate form made available on the website (https://support.namirial.com);
- **physical application procedure**: This option is available to all users (Subscriber, Subject and Third Party) and is carried out by means of a paper application form that the user must download from the CA's website and submit completed and signed accordingly.

For both procedures, the request for revocation contains the date from which the Certificate will be revoked.
The request for suspension contains the start and end date.
The Certification Authority checks the authenticity of the request and revokes the Certificate by entering it in the list of revoked and suspended Certificates (CRL) it manages.

4. Operational life cycle requirements for Certificates

This section describes how the Certification Authority operates and, in particular, the organisation and functions of the personnel assigned to the certification service, how to apply for the Certificate and how to communicate with the Certificate Subscriber or Subject of the Certificate.
Unless otherwise indicated in this document and in accordance with ETSI standard 319-411, the following operational requirements are applied to the Certificate's life cycle. All entities included in the Namirial domain (RA, LRA, Subscribers, Subjects or other participants) must notify Namirial CA of all changes to the information on a Certificate during its period of validity and until its expiry or revocation. The Namirial CA will only issue, revoke or suspend Certificates in response to authenticated and approved requests.

4.1 Subjects who can apply for the issue of a Certificate

The Certification Authority issues certificates for

Natural persons:

- independent (personal certificates);
- belonging to organisations;
- members of Professional Associations.

Legal entities:

- Certificate issued to the Organisation or Association (Electronic Seal);

The Certificates issued can be related to:

- subscription keys generated for use through remote signature applications
- subscription keys generated for use through "disposable" remote signature applications with limited time availability (see relevant addendum)
- subscription keys generated for signing via physical signature devices;
- subscription keys generated for signing by automatic subscription applications;
- subscription keys generated for the Electronic Seal application

In all cases, Subscribers and Subjects are subject to a registration process that requires the following:

- Filling in a special form;
- Accepting the General conditions

4.1.1 Requesting the Certificate

The conditions for identification and authentication are described in detail in Chapter 3.

4.2 Registration of users

The procedures for registering the Subscriber (and Subject if he/she is not the Subscriber) and issuing the Certificate envisage:

- that the Subscriber and the Subject must be identified with certainty by the Certification Authority in one of the ways described in the previous paragraphs.
- that the Subscriber and Subject have read the privacy policy referred to in Article 13 of the GDPR
- that the Subscriber and Subject have given their consent to video recording and data processing, in the case of video identification;
- that the Subscriber and Subject have read the General Contract Conditions and this Operating Manual;
- that the Subscriber and Subject have signed the Qualified Certificate Issue Application Form (available from the "Documents" section of https://docs.namirialtsp.com website), duly completed in all its parts;

If inclusion of the Role and the Interested Third Party in the Qualified Certificate is required, the following must also be provided:

- a document of the Organisation on headed paper, bearing the date and protocol number, authorising the inclusion of the data in the Qualified Certificate of the Subscriber, not earlier than 30 (thirty) days from the date of the request for registration;
- certification that the organisation has received the privacy policy referred to in Art. 13 of the GDPR.

If the Position and/or Professional Qualification is required to be included in the Qualified Certificate, the following must also be provided:

- a document issued by the Professional Association/Register/Board certifying actual membership, not earlier than 30 (thirty) days from the date of application for registration.

Only if the Subscriber matches the data in the Subject field of the Certificate, he/she assumes the status of Subject.

4.3 Registration Process

The participants in the registration process (Subjects, Subscribers, LRAs, RAOs, IRs) contribute to the successful issuing of the Certificate, each fulfilling their responsibilities.

The Certification Authority, having completed the identification phase, performs the registration operation of the Subscriber/Subject through the web portal of the digital certification service, which registers the data provided in its database. The Certification

Authority then issues the Qualified Certificate and, where applicable, delivers the signature device.
The registration activities, in addition to being carried out directly by the authorised personnel of the Certification Authority, can be performed by the personnel of the LRAs, the RAOs, or by the personnel designated as IRs, after appropriate training.

4.4 Processing the request

Natural person attributes

The Certificates issued to a natural person can be:

- Personal, in which case Subscriber and Subject coincide
- The Subject belongs to an Organisation
- The Subject belongs to a Professional Association

The attributes acquired by the CA for the purpose of issuing Certificates and referring to the Subject are:

- Name and surname
- Date of birth
- Place of birth

Tax code if the Subject is an Italian citizen. If the Subject is a foreign national, the data specified in the appropriate section 3.1.3 Uniqueness of names is acquired

- Identity document details
- Address of residence and email address
- Certified Email Address if it corresponds to the procedure identified for the transmission of the password required for opening the blind envelope
- Mobile address if it corresponds to the procedure identified for the transmission of the password required for opening the blind envelope

Legal entity attributes

The Certificates issued to the legal entity consist of Electronic Seals (QES)

The attributes acquired by the CA for the purpose of issuing Certificates are:

- Tax code
- Vat number
- Company name
- Registered offices
- Email address
- Certified email address
- Mobile address

4.5 Issuing the Certificate

If the result of the checks on the attributes referred to in the previous paragraphs is positive, a request is sent to the CA to issue the certificate for the natural person or legal entity.
Otherwise, the Certification Authority can refuse to complete the issue of the Certificate, e.g. if the information is missing, incomplete or inconsistent, if there are doubts as to the identity of the Subject or Subscriber, or if the documentation provided does not comply with the Certificate Authority's instructions.

4.6 Key generation procedure

The key generation procedure involves the following steps:

- assigning the Subject a unique identification code as part of the Certification Authority's users (CUC), different for each Certificate issued;
- generating the Certificate containing the public key and the expected data by signing with the CA's certification key;
- entering the Certificate in the Certificate directory;
- recording in the audit log that the generation has taken place;
- sending the Certificate from the CA to the LRA;
- entering the Certificate in the signature device;
- checking the entry of the Certificate in the signature device;
- deleting from the DB of the encrypted record of the blind envelope associated with the Subject;
- recording in the audit log that the signature device has been customised.

4.7 Acceptance of the Certificate

The Certification Authority does not expect any conclusive behaviour when issuing the Certificate. The latter is deemed to be accepted when issued.

4.8 Key pair and use of certificate

The owner of the Certificate must safeguard its private key, taking care to avoid its disclosure to third parties. Namirial will provide a special subscription contract that outlines the owner's obligations regarding the protection of the private key. Private keys must only be used as specified in the "keyUsage" and "extendedkeyUsage" fields, as stated within the relevant Certificate. The responsibilities regarding the use of keys and Certificates include those addressed below in paragraph 9.8.3. The Certificates are to be used only as prescribed in the Certificate Policy and the General Conditions. Any other use is prohibited.

4.9 Delivery methods of personal signature devices and secret codes

Any physical signature devices are handed over to the Subject by the RAO or IR, following identification and registration of the Subject.
The following user codes are related to the Certificate and the physical signature device, if any:

- Virtual device PIN (Remote Signature Certificate, Disposable Remote Signature, Automatic Signature or Seal)
- PIN and PUK of the physical device (smartcard/token usb)
- Software Certificate Password (Software Electronic Seal)

These codes are delivered to the Subject after the Certificate has been issued in secure mode.

4.9.1 Changing the Codes of the Subject

At any time following the generation of the Certificate, the Subject may change the *CodicePIN*.

4.9.1.1 Changing the PIN

The PIN can be changed by the Subject either within the Certification Authority's service portal, by accessing its reserved area, or via the standalone FirmaCerta software.

4.10 Restrictions on use

Without prejudice to the Certification Authority's responsibility pursuant to Italian Legislative Decree 82/2005 (Digital Administration Code, Art. 30 paragraph 1 letter a), it is the responsibility of the Subject to check compliance with the restrictions on use included in the Certificate.
The request to insert other specific restrictions on use, the text of which may not exceed 200 characters in any case, will be assessed by the Certification Authority for legal, technical and interoperability aspects and enhanced accordingly.
In consideration of the aforesaid restrictions, the Certification Authority adopts the restrictions on use indicated by the users, pursuant to Article 12, paragraph 6, letter c) of CNIPA Resolution 45/2009 as amended, and inserts, at the request of the Subject or the legal entity that requested the Certificate, at least the following restrictions on use:

- The Subjects use the certificate only for the purposes for which it is issued.
- This certificate may only be used for unattended/automated digital signatures.
- The certificate may be used only for relations with the (declare the subject).

4.11 Renewing the Certificate

The renewal must necessarily be carried out before the expiry of the Certificate. The procedure can be used to renew a previous Certificate issued by the Certification Authority in cases where the Subscriber has a valid Qualified Certificate and the corresponding SSCD/QSCD provided by the Certification Authority. The CA provides a software application that can generate the key pair within the Q/SSCD and the request for the PKCS # 10 Certificate.

The procedure for re-issuing keys requires at least the following steps:

- Update of certain data of the Subject (e.g. Qualification, Organisation, etc.) if there is a request from an entity with which the Subject is associated. In this scenario, the entity will provide new information;
- Make sure that the Subscriber has exclusive control of the Q/SSCD by signing with the previous Certificate;
- Generation of a new key pair in the Q/SSCD and issue of a new Certificate;
- Recording of events relevant to the entry in the CA audit log

4.12 Changing the Certificate

A Certificate signed by the issuing CA cannot be modified. In order to remedy potential inaccuracies incurred during the generation process, a new Certificate must be issued and, for security reasons, the previous one must be revoked. If the issued Certificate contains incorrect information due to errors made by the CA or RA, the incorrect Certificate will be revoked and a new one will be promptly issued at no additional cost to the customer and without requiring any further information from the customer. On the other hand, if the Certificate issued contains incorrect information due to errors made by the Subscriber (e.g. incorrect filling in of one or more fields in the application form), the incorrect Certificate will be revoked.

4.13 Revocation and suspension of the Qualified Certificate

The suspension or revocation of the Certificate takes place in compliance with Articles 22 to 29 of the Italian Prime Ministerial Decree of 22 February 2013, determines the end of its validity before its natural expiry date and invalidates any signatures affixed after the publication of the revocation list containing the reference to such Certificate. The publication of the list is attested by an appropriate time reference affixed by the Certification Authority.
The revocation and suspension lists (CRLs) are published in the Certificates directory with the frequency established by Art. 18, paragraph 4, of CNIPA Resolution no. 45 of 21 May 2009, as amended.
The Certification Authority can anticipate the issue of the CRL in special circumstances.

The date of publication of the list, certified by a time reference, is recorded in the Certification Authority's Audit Log, where suspensions, revocations and reactivations of Certificates are noted.
The suspension of the Certificate entails the invalidity of signatures generated during the period of suspension. If a Certificate in a suspended state is revoked, the revocation will take effect from date on which the suspension started.

4.13.1 Grounds for revocation or suspension of the Certificate

The maintenance of the Qualified Certificate is always the responsibility of the Certification Authority, which must:

- revoke it in case of termination of the Certification Authority's activity, without prejudice to the indication of a replacement Certification Authority pursuant to Art. 37, paragraph 2, of Italian Legislative Decree 82/2005 (Digital Administration Code);
- revoke or suspend it in response to an order by the authorities;
- revoke or suspend it at the request of the Subject or of the Interested Third Party from whom the Subject derives his/her powers, in cases where:
- the physical device has been lost,
- the secrecy of the private key or of the access credentials to the signature generation device has ceased to exist,
- the physical device has been damaged,
- any event has occurred that has compromised the reliability of the key,
- the Subject's reference data indicated in the Certificate, including those relating to the Role, have changed,
- abuse or falsification has been established,
- the relationship between the Subject and the Certification Authority has ended.

Suspension may occur as a result of the following circumstances:

- request for revocation whose authenticity cannot be ascertained in time;
- interruption of the validity of the Certificate for temporary non-use.

The Subject is entitled to request revocation or suspension of the Certificate for any reason it deems valid and at any time.
The request for revocation or suspension of the Qualified Certificate is made in writing to the Certification Authority, by filling in all parts of the form made available on the CA's website.
The request for revocation will contain the date from which the Certificate will be revoked. The authenticity of this request is checked by the Certification Authority, which carries out the revocation by entering the Certificate in the list of revoked and suspended Certificates (CRL) managed by it.

4.13.2 Emergency Suspension

In case of loss/compromise of the private key or of the codes enabling its use, the Subject will promptly request the Certification Authority to suspend the Certificate.
The request can be sent:

- by phone[3] to the Help Desk;
- via the Web [4] by entering the emergency code or OTP.

The Certification Authority promptly enters the Qualified Certificate in the list of revoked and suspended Certificates (CRL).
Thereafter, the Subject/Interested Third Party will request in writing from the Certification Authority the revocation or suspension or reactivation of the Certificate, stating the reasons therefor.
If the Subject/Interested Third Party does not make a written request within 60 (sixty) days of the suspension, the Certificate shall be revoked.
The Certification Authority shall notify the Subject of the expiry of the suspension period by email 10 (ten) days before the deadline, which must not be later than the expiry date of the Certificate.
The revocation takes effect from the date on which the suspension starts.

4.13.3 How to submit requests

The revocation, suspension or reactivation of the Certificate can be requested as follows:

- **Website**, the Subject/Interested Third Party connects to the Certification Authority's website, filling in the appropriate electronic form. To guarantee the authenticity of the request, the Subject must authenticate himself/herself to the Certification Authority's services with his/her credentials and OTP code before accessing the system.
- **On paper**, the Subject/Interested Third Party downloads the appropriate form from the Certification Authority's website, fills in the form in its entirety, goes to the Certification Authority with a valid identity document or forwards the form by fax with a copy of a valid identity document.

The Certification Authority checks the authenticity of the request as follows:
in case of Subject:

- makes sure that the request is filled in completely,
- makes sure that the identity document is valid;

in case of Interested Third Party

- makes sure that the request is filled in completely,

[3] The customer will be asked for some personal data to ensure the lawfulness of the request.
[4] The website is accessible 24 hours a day, seven days a week.

- checks the existence of the stamp or other equivalent marking,
- makes sure that the Subscriber is the "Contact Person" indicated in the Agreement,
- makes sure that the identity document is valid.

4.13.4 Time frame for handling requests

The requests for revocation, suspension and reactivation of Qualified Certificates will be handled within one working day of receipt of the request, it being understood that the Certification Authority will promptly publish the new list (CRL) in case of a request for an emergency suspension.
The time of publication is attested by a time reference and noted in the audit log.

4.13.5 Notification of revocation or suspension

After checking the authenticity of the request, the Certification Authority shall promptly notify the Subject and/or the Interested Third Party as follows:

- if the request is on the Subject's initiative, the Certification Authority checks whether the Certificate contains information relating to the organisation. In that case, it shall notify the Third Party by email of the revocation or suspension;
- if the request is at the initiative of the Interested Third Party, the Certification Authority shall notify the Subject and the Interested Third Party by email of the revocation or suspension of its Certificate;
- if the request is at the Certification Authority's initiative, the Certification Authority shall notify the Subject by email of its intention to revoke or suspend the Certificate, stating the reason and the effective date and time; if the Organisation is present in the Certificate, it informs the Interested Third Party by email if it had signed the Convention of the change in the status of the Certificate.

4.14 Certificate status verification service

The Namirial CA provides control services to check the status of the certificate, such as CRL and OCSP. The status of the Certificate (which could be active, suspended or revoked) is made available to all entities involved by publishing the Certificate Revocation List (CRL). The CA also makes an OCSP (On-line Certificate Status Provider) available at the following link: https://sws.firmacerta.it/. The CRL is signed when it is issued, with the CA's Certificate.
Both the CRL and OCSP are available 24 hours a day, 7 days a week.

4.15 How to replace keys

4.15.1 Replacing user subscription keys

The maximum duration of a Qualified Certificate is six (6) years. The key renewal request must be made before the expiry of the Certificate (from the 45th day before the expiry date).
The renewal of the Certificate can only be done by the Qualified Certification Authority that issued it and the Subject can do so by means of the remote procedure available in the "FirmaCerta" software made available by the Certification Authority.

The renewal procedure includes:

- updating of the data relevant to the Subject with the information provided by the Interested Third Party (if any);
- verifying possession of the signature device containing the expiring Certificate by means of a remote procedure;
- generating a new key pair on the secure signature device and issuing a new Certificate, by remote procedure;
- recording the successful operation in the Audit Log.

If the Qualified Certificate also contains information relating to the Role and Organisation, the Certification Authority shall include it in the new Certificate, verifying, at the time of renewal, that no revocation of the Certificate has been received from the Interested Third Party.
If the information relating to the Role and Organisation contained in the Certificate to be renewed is no longer valid at the time of renewal, a Certificate without such information will be issued to the Subject wishing to renew through the remote procedure.
In case of a request made after the expiry of the Certificate, it will be re-registered and issued.
Should it become necessary to replace the Qualified Certificate, due to changes in the information contained therein, the Certificate shall be revoked and/or reissued.

4.15.2 Replacing Time Stamping Keys

Time Stamping keys are replaced after no more than 3 (three) months of use, regardless of the duration of their validity period and without revoking the corresponding Certificate, in accordance with Article 49, paragraph 2 of the Italian Prime Ministerial Decree of 22 February 2013.
Time Stamping Key Certificates have a maximum duration of 11 (eleven) years.

4.15.3 Replacing certification keys

It takes place in compliance with Art. 30 of the Italian Prime Ministerial Decree of 22 February 2013. The CA's "Root" Certificate used by the Certification Authority to sign the Qualified Certificates of the Subject lasts 20 years and is replaced every 8 years to ensure the usability of all issued Certificates until their natural expiry date.

4.16 Termination of subscription

The service contract, signed by the CA and the customer, is deemed to be terminated on the following dates:

- date of expiry of the Certificate;
- date of revocation of the Certificate.

4.17 Key escrow and key recovery

Key escrow is not permitted for CA keys. The CA's private keys are not kept but are encrypted within files that can only be used within the specific HSM and within its own Security World.
The use of keys within HSMs is only permitted with an adequate quorum of OCS cards (2/6), whereas for the Security World setting, the quorum is satisfied with the use of 3/6 cards.

5. Controls and security measures

Policies, responsibilities and operating procedures are defined for access to Namirial's protected areas and for access to information and the application system. Physical protection devices are implemented in these areas to minimise the risks of unauthorised access. Protection is implemented by access control systems and video surveillance systems positioned at the most critical points and indicated by appropriate signs. A Disaster Recovery site is located in Milan with a level of physical security at least similar to that of the primary site.

5.1 Physical controls

The work areas are subject to different control measures depending on the risks, the value of the assets and the information to be protected. An organised authorisation process related to the type of area manages all accesses.

5.1.1 Location of the site

Namirial runs its CA operations from secure data centres equipped with logical and physical controls that make Namirial CA operations inaccessible to unauthorised personnel. Namirial operates in accordance with a security policy designed to detect, deter and prevent unauthorised access to the organisation's operations.

5.1.2 Physical accesses

Namirial protects its equipment from unauthorised access and implements physical controls to reduce the risk of equipment tampering. The secure parts of Namirial CA's hosting facilities are protected by physical access controls that make them accessible only to duly authorised persons. Access to secure areas of buildings requires the use of a secure device. The buildings are under constant video surveillance.
Access to the Datacenter room requires a strong authentication system. Rules of access and behaviour to be kept inside the Data Centre are posted outside the Data Centre.

5.1.3 Electric energy and air conditioning

Data centres have primary and secondary power supplies that ensure continuous and uninterrupted access to electricity. Uninterruptible power supplies (UPSs) and electric generators provide redundant backup power. Namirial's data centre facilities use multiple systems for heating, cooling and air ventilation.

5.1.4 Exposure to water

A detection system detects the presence of liquid via sensors and triggers an alarm in case of flooding.

5.1.5 Fire Prevention

Data centres are equipped with fire suppression mechanisms.

5.1.6 Media storage

Namirial protects its assets from accidental damage and unauthorised physical access.

5.2 Procedural controls

5.2.1 Trusted roles

The personnel appointed according to the trusted roles in the ETSI EN 319-401 standard include the CA and RA system administration operators. The functions and tasks performed by trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and reliability of PKI operations. All personnel appointed according to trusted roles must be free from conflicts of interest that could be detrimental to impartiality in the operations of PKI Namirial.
Trusted roles are appointed by the management. A list of personnel appointed to such roles is maintained and reviewed by the organisation. The responsibilities of trusted roles are as follows:

- Security Officers: Responsibility for defining security policies.
- System administrators: Authorised to install, configure and maintain Namirial trust systems for the management of the service
- System operators: Responsible for the day-to-day operation of the Namirial trust systems. They are authorised to back up the system.
- System auditors: Authorised to view archives and audit logs of Namirial trust systems.

5.2.2 Number of persons involved in the activities

In case of tasks relating to critical functions, Namirial requires at least two persons to act in a trusted role to prevent one person from acting independently. When this mechanism is active, two authorised persons are required to apply it where appropriate.

5.2.3 Identification and authentication for each role

The personnel in charge of these services are required to authenticate themselves to the CA and RA systems before accessing the environments necessary to perform their trusted roles.

5.2.4 Activities requiring segregation of duties

The activities that require segregation of duties are as follows:

- The verification of information in the generation of CA Certificates (root and intermediate, where applicable);
- The approval of CA Certificate applications;
- Most tasks related to CA key management or CA administration.

For these activities, Namirial identifies from among its employees figures appropriate to the trusted roles defined above, who can only be assigned one role between director or auditor, but both can also play the role of operator.

5.3 Controls on personnel

These figures have adequate experience in the definition, development and management of PKI services and have received the necessary level of training on procedures and tools that can be used in various operational phases.
The Namirial personnel in charge of these activities must:

- have the competence, reliability, experience and qualifications required, and have received training in security and personal data protection regulations appropriate to the services offered and their job function;
- be able to fulfil the requirement of "knowledge, experience and qualifications" through training or actual experience, or a combination of both;
- be updated on new threats and the latest applicable security practices.

5.3.1 Qualifications, experience and authorisation requirements

Namirial hires personnel with the highest levels of integrity and competence. There is no citizenship requirement for personnel performing trusted roles associated with the issue of other types of Certificates.

5.3.2 Checking past experience

Namirial checks the identity and performs a background check on each employee in order to assign one of the trusted roles envisaged and indicated above.

5.3.3 Training requirements

All new Namirial personnel receive basic security awareness training during the company-wide onboarding process. In addition to this, dedicated on-the-job training is provided to all Namirial personnel involved in specific tasks, as described in this document.

5.3.4 Training update frequency and requirements

The personnel are required to maintain high levels of competence through industry-relevant training sessions in order to continue to act in accordance with the requirements of trusted roles. Namirial informs all those in these roles of any changes in normal operations.

5.3.5 Job rotation frequency

In case of job rotation, Namirial carries out a security check including a credential check at the level of networks, systems, applications or other resources used, as well as access authorisations to facilities and areas.

5.3.6 Penalties for unauthorised actions

Namirial personnel who do not follow the organisation's internal policies and provisions, both through negligence and malicious intent, are subject to administrative or disciplinary sanctions, including termination of employment or collaboration and, in the most serious cases, penal sanctions.

5.3.7 Requirements for non-employee personnel

Non-employee personnel who have been assigned a trusted role are subject to the requirements and duties specific to that role as well as any sanctions.

5.3.8 Documentation provided to personnel

The personnel, upon onboarding, are provided with the necessary information to perform their duties, including a copy of this document and the necessary operational documentation to maintain the integrity of Namirial's CA operations.

5.4 Procedures for managing the audit log

Namirial records all relevant information relating to data issued and received by it and keeps the records accessible for a period of 20 years for the purpose of providing adequate evidence in legal proceedings and ensuring continuity of service.

5.4.1 How often the audit log is saved

The audit log must be saved on a daily basis.
The exact time of significant environmental, key management and Namirial clock synchronisation events are recorded. The time used to record events as required in the audit log must be synchronised with UTC at least once a day.

5.4.2 Retention of audit log records

The procedure put in place by the Certification Authority envisages that the events detected and available on the database are extracted and inserted into text files managed in such a way as to guarantee their integrity and availability.
The records of the operation of the services are available to the court in case of legal proceedings and internally for the purposes of audits and periodic system checks.

5.4.3 Backup of the audit log

The synchronisation of events with the repository on the Disaster Recovery site takes place at least daily.

5.5 Archiving the records

Namirial produces and maintains accessible records that include all activities and all relevant information relating to data issued and received by Namirial.
The CA keeps the records accessible for a period of 20 years in order to provide adequate evidence in legal proceedings and ensure continuity of service. These records remain accessible even if Namirial has ceased its activities.
The main evidence gathered is:

- Issue requests;
- Documents provided by Subscribers;
- CSR (Certificate Signing Request) provided by Subscribers;
- Personal data of the Subscriber and the Subject (if they are different entities);
- Requests for revocation or suspension;
- All the Certificates issued;
- Audit log for 20 years.

5.6 Replacing the key

If the end user (Subject) decides to use a new key, he/she must necessarily apply for a new Certificate.

5.7 Compromised key and disaster recovery

Namirial documents the procedures for reporting and handling incidents, as well as the facts related to them.
Namirial documents the recovery procedures used if IT resources, software and/or data are damaged or suspected to be damaged. Namirial establishes the measures required to ensure the complete restoration of the service, within an appropriate time frame depending on the type of interruption in the event of a disaster or compromised servers, software or data.

The measures taken by the Certification Authority comply with the requirements of ISO 27001 certification.

5.8 Termination plan

Namirial established an updated termination plan. In particular, according to this internal procedure, Namirial shall:

- inform at least 60 days before termination the following subjects: all Subscribers and other subjects with whom Namirial has agreements or relations, including the Relying parties and the competent authorities (AgID and the certification body). Furthermore, this information must be made available to other relying parties;
- terminate the authorisation of all subcontractors to act on behalf of Namirial in the performance of any function relating to the process of issuing Certificates;
- transfer obligations to a reliable party for the maintenance of all information necessary to provide evidence of Namirial's operation for a reasonable period unless it can be proved that Namirial does not hold any information;
- private keys must be destroyed or withdrawn to ensure that they cannot be recovered;
- make arrangements to transfer the provision of trust services for its existing customers to another Trust Service Provider.

The Certification Authority has drawn up its "Termination Plan" for the exclusive use of the Certification Authority and in accordance with Art. 24 eIDAS.

6. Technical safety checks

6.1 Key pair generation

The CA issues the Qualified Certificate in accordance with Regulation (EU) no. 910/2014. The certification keys used to sign the Certificates are generated by means of devices and procedures that guarantee the uniqueness, secrecy and resilience of the private key.
The CA uses a cryptographic key pair of at least 4096 bits generated within HSM (Hardware Secure Module).

The HSMs and procedures ensure that:

- key pairs are generated individually, always in a single copy;
- key pairs meet the requirements imposed by RSA generation algorithms and verifications because HSMs have an internal engine for generating RSA and DSA key pairs;
- the generation of all possible key pairs is equiprobable;
- the person activating the generation procedures is always identified;
- the generation of key pairs takes place exclusively within the HSM;
- if devices are prepared or operated by a third party, Namirial checks that this third party has the appropriate requirements.

In its certification activities, Namirial uses the RSA algorithm.
The generation of certification key pairs by the CA is under double control, according to the Key Ceremony procedure.

6.2 How keys are generated

The asymmetric key pair (public and private) is generated using devices and procedures that ensure, in relation to the state of scientific and technological knowledge, the uniqueness and robustness of the generated keys, as well as the secrecy of the private key. The key generation system ensures:

- that the pair meets the requirements of the generation and verification algorithms used;
- the equiprobability of generating all possible pairs;
- the identification of the person activating the generation procedure.

The keys belonging to one of the types listed in Art. 5, paragraph 4, of the Italian Prime Ministerial Decree of 22 February 2013 are generated (Art. 6 and 7), stored (Art. 8) and used (Art. 11, paragraph 1) within the same electronic device having the security features referred to in Art. 12 of the Italian Prime Ministerial Decree mentioned above.
The keys are generated within the secure signature generation device.

If the generation takes place outside this device, the generation system complies with the provisions of Art. 9 of the Italian Prime Ministerial Decree of 22 February 2013.
In case of a Certificate coupled with a CNS, the generation of signature keys can take place centrally and also outside the CNS itself; moreover, it can be carried out at the Certification Authority in accordance with the specific agreements in place with the issuing PA, in any case in compliance with the RFC 3161 standard (X.509 Public Key Infrastructure Time Stamp Protocol) and Art. 9 of the Italian Prime Ministerial Decree of 22 February 2013.
The keys corresponding to Qualified Certificates for Electronic Seals are generated using the same procedures adopted for the generation of keys corresponding to Qualified Certificates for Electronic Signatures.

6.2 How certification keys are generated

The generation of the keys within the signature devices takes place in the presence of the Party Responsible of the Certification Service, as envisaged by Art. 7 of the Italian Prime Ministerial Decree of 22 February 2013, and is preceded by the initialisation of the signature devices for the Certificate generation system with which the Certificates of the Subjects and those of the time validation system are signed.
In general, the following criteria are complied with:

- the procedure takes place in the presence of a number of business managers deemed adequate and sufficient to prevent unlawful transactions;
- once the key pairs have been generated, the private ones are divided into several parts, each of which is transcribed onto two sets of smart cards;
- the smart cards in each set are each assigned to one of the designated company persons, who will associate their own password with them, which they will keep secret;

6.2.1 How user subscription keys are generated

Once the registration phase has been completed, during which the Subscriber's and Subject's data is stored in the Certification Authority's database, it is possible to generate the subscription keys. This can be done in two different ways:

- Keys generated by the Certification Authority (or LRA).
- Keys generated by the Subscriber.

In any case, since the signature device is at the disposal of the Subject or of the RA/RAO operators, they may generate a new key pair using the asymmetric key generation function of the same device.
The signature devices used meet the security requirements of the regulations.
Keys corresponding to Qualified Electronic Seal Certificates can only be generated by the Certification Authority.

6.2.1.1 Keys generated by the Certification Authority

This procedure is carried out by the RA operators of the Certification Authority at its premises or by the RAOs of the LRAs.

The following operations are carried out:

- the operator logs in to the Certification Authority's services, selects the Subscriber's registration data and activates the Certificate request procedure;
- the application accesses the signature device with the default PIN and generates the key pair.

6.2.1.2 Keys generated by the Subscriber

Self-enroll release

This procedure requires the customisation of the signature device to be carried out under the control of the user, or at least in his/her presence, and is based on secure electronic interactions with the Certification Authority (generally connections via the Internet protected by protocols guaranteeing an adequate level of security).

At this stage, the signature keys are generated by the Subscriber itself by activating with the CA-approved application the secure signature generation device envisaged or indicated by the Certification Authority itself.

The Subscriber is:

- recognised by the Certification Authority by means of a confidential personal code or password;
- authenticated by the secure signature generation device by entering the PIN contained in the blind envelope (scratch-card) delivered following identification by the IR/RAO

Renewal

This procedure can be used for renewal operations of a previous Certificate generated by the Certification Authority in cases where the Subscriber has a valid Subscription Certificate and the corresponding signature device provided by the Certification Authority. For this purpose, the Certification Authority provides the "FirmaCerta" client application capable of generating the key pair within the signature device and the Certificate request in PKCS#10 format.

The hardware and software prerequisites as well as all installation instructions for the "FirmaCerta" product can be found in the software's "Quick Start Guide" available at the URL:

https://support.namirial.com/

The document, which is an integral part of this Operating Manual, contains the operating procedures for the renewal of signature Certificates.

Keys corresponding to Qualified Certificates for Electronic Seals do not fall into this category.

6.2.3 How Time Stamping Keys are Generated

Key generation takes place in compliance with Articles 49 and 50 of the Italian Prime Ministerial Decree of 22 February 2013; in particular:

- The Certification and Time Stamping keys, pursuant to Art. 49, paragraph 4, of the Italian Prime Ministerial Decree of 22 February 2013, are generated in the presence of the person in charge of the certification and time validation service.
- The key pair used for time validation is 2048 bits in length and is uniquely associated with the time validation system at the time of generation.

In order to limit the number of time stamps generated with the same pair, the Time Stamping keys are replaced and a new Certificate is issued after no more than 3 (three) months of use, irrespective of the duration of their validity period and without revoking the corresponding Certificate.
The profile of Time Stamping Certificates complies with CNIPA Resolution no. 45 of 21 May 2009.

6.2.4 Delivery of the private key to the Subscriber

The private key is contained within the device: HSM in the case of remote signature, physical media in the case of tokens or smart cards. The Subject, upon receiving the Certificate, becomes responsible for it, as well as for the private key that can only be used with the delivered PIN, which must be kept exclusively.

6.3 Private key protection and engineering controls on the cryptographic module

The key pairs used by the CA to sign the Certificates and CRLs are stored in a high-quality HSM (Hardware Security Module).
The HSM used by Namirial is certified at EAL4+ Common Criteria level and qualified ANSSI at the highest level.

6.3.1 Cryptographic algorithms and key length

Pursuant to Art. 3 of CNIPA Resolution no. 45 of 21 May 2009:

- the RSA (Rivest-Shamir-Adleman) algorithm is used in signing operations;
- the keys used by the Certification Authority to sign the Certificates are at least 4096 bits long;
- the length of the subscription key of the Subjects is at least 2048 bits.

6.3.2 HASH functions

The SHA-256 hash function is used to generate the fingerprint.

6.4 Other aspects of key pair management

Namirial uses the CA's private signature keys appropriately and does not use them beyond the end of their life cycle.

In particular:

- The CA's signature key used for generating Certificates and/or issuing revocation status information is not used for any other purpose;
- Certificate signature keys are only used within physically secure premises;
- The use of the CA's private key is compatible with the hashing algorithm, the signature algorithm and the length of the signature key used to generate the Certificates, in line with Section 6.3;
- All copies of the CA's private signature keys will be destroyed at the end of their life cycle.

6.5 Activation data

Activation data consists of the set required for the activation of the Subscription Certificate delivery process; the activities are described in paragraph 4.4

6.6 IT security checks

The operating systems used by the CA to manage the Certificates have a high level of security and follow the hardening procedures established by Namirial. Tasks and areas of responsibility are segregated in order to minimise the possibility of unauthorised or inadvertent changes or misuse of Namirial assets.
System access events are recorded, as described in Section 5.1.
Both physical and logical local network components are maintained in a secure environment and configurations are periodically checked for compliance with the requirements specified by Namirial.
The control over attempts to add or delete certificates and change other associated information (e.g. revocation status information) is implemented.
Continuous monitoring and alerting facilities are in place to enable Namirial to detect, record and promptly react to any unauthorised and/or irregular attempt to access its resources.

6.7 Process life cycle safety checks

6.7.1 Controlling the assets

Namirial uses reliable systems and products that are protected against modifications and that guarantee the technical safety and reliability of the processes they support.

In particular:

- The security requirements are analysed during the design and requirements identification phase of any system development project undertaken by Namirial;
- Change management procedures are applied to emergency releases, modifications and patches of any operating software as well as configuration-level changes to which the information security policy applies.
- The integrity of Namirial systems and assets is protected against viruses, malicious and unauthorised software.
- Media management procedures are defined and implemented in order to protect media from damage, theft, unauthorised access, obsolescence and deterioration during the period of time the records are to be kept.
- Organisational procedures are defined and implemented to manage all trust and administrative roles that have an impact on service delivery.

6.7.2 Controlling the private key

In order to securely issue and manage CA keys, Namirial uses HSM (Hardware Security Module) that:

- is tamper-proof and guarantees key protection according to regulatory security levels and high technological standards;
- prevents any unauthorised attempt to read, duplicate, extract the private key
- retains the Private Key to ensure its protection, privacy and secure storage throughout its life cycle;
- identifies the operators.

6.8 Network security controls

Namirial's network architecture is structured on several levels in order to create separate network environments, directed to hosts related to different functions and characterised by different levels of criticality.
The security of network access and traffic is ensured through the application of protection policies implemented on firewall systems located on different network layers.
The requests to implement new rules on the firewall are handled through a change request.
The activation of rules causing a high level of impact is dealt with the Security Officer.
The security of the CA private network is realised not only by the perimeter protection

systems described above, but also by a specific configuration that keeps internal addresses as reserved. The communications between the management stations and the systems are protected by means that ensure authentication between the parties and their privacy.
The potential remote connections take place over an encrypted VPN channel and require authentication via Username, Password and an authentication token (OTP).
The communication between the application modules of Namirial's PKI platform takes place via cryptographic channels.
The communication among users accessing online services takes place via TLS/SSL connections with SHA -256 algorithm.
The system implemented to manage user access provides both AAA (authentication, authorisation, access) and profiling mechanisms and encryption of the communication channel with TLS/SSL protocol.
The system should also manage access from consultants working on Namirial's internal network.

6.9 Timestamping

All systems used by the CA during the flow are aligned with UTC time references and synchronised via a reliable source such as NTP servers.

7. Policy, restrictions on use and management of Certificates

7.1 Certificate Profiles

The Certificates comply with the following regulatory requirements:

- international standard ISO/IEC 9594-8:2005 [X.509 version 3];
- public specifications IETF RFC 5280 Management of Reliable Public Certificates;
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles (Part 1, 2, 3, 5).

The CA fills in the issuer and subject fields of each Certificate issued following the adoption of the requirements defined above in accordance with what is stated in this document. By issuing the Certificate, the CA declares that it has followed the procedure described in the document to prove that on the date of issue of the Certificate all information relating to the subject was accurate.
The following sections describe the main attributes normally included in each Qualified Certificate issued by Namirial. Should the Subscriber request a new type of attributes not included below, Namirial will set them accordingly provided that the new set of attributes complies with the above specifications.
As required by Italian law, Qualified Signature Certificates or Time Stamps are issued directly using the following CA root certificates:

CA Root name	Purpose	Notes
Namirial Qualified eSignature	Issuing certificates for digital signatures	CA Root certificate
Namirial CA Qualified Signature	Issuing certificates for digital signatures	CA Root certificate
Namirial EU Qualified eSignature	Issue of qualified certificates for electronic signature	CA Root certificate
Namirial EU Qualified CA	Issue of qualified certificates for electronic signature and electronic seal	CA Root certificate
Namirial Time Stamping Authority	Issue of time stamp certificates	CA Root certificate
Namirial CA TSA	Issue of time stamp certificates	CA Root certificate

Table 4: Profile certificate

7.1.1 Namirial EU Qualified e-Signature

Version	Version 3
Serial Number	21 0d 6c b1 7c 11 0b 9b
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." **organizationalUnit:** "Namirial Trust Service Provider" **organizationIdentifier**: "VATIT- 02046570426" **commonName**: "Namirial EU Qualified eSignature"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extensions	
Subject Key Identifier	30 45 db 26 02 3d bf 0d 9a d8 b8 10 ea 7c cd a4 ae 8e 5c 27
Authority Key Identifier	30 45 db 26 02 3d bf 0d 9a d8 b8 10 ea 7c cd a4 ae 8e 5c 27
Certificate Policies	Not critical Policy OID, 1.3.6.1.4.1.36203.1.1 Cp: URL: https://docs.namirialtsp.com/
crlDistributionPoint	Not critical http://crl.namirialtsp.com/QES4K.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 1 - Namirial EU qualified e-signature

7.1.2 Namirial Qualified Signature

Version	Version 3
Serial Number	6E E8 2F B2 FF 76 2F 06
Signature	sha256, RSA

Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." organizationalUnit: "Namirial Trust Service Provider" **commonName**: " Namirial Qualified e-Signature"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extensions	
Subject Key Identifier	0b a4 b2 bb 27 39 c1 e1 09 d3 77 6c b8 75 e1 67 8d e3 22 fe
Authority Key Identifier	0b a4 b2 bb 27 39 c1 e1 09 d3 77 6c b8 75 e1 67 8d e3 22 fe
Certificate Policies	Not critical Policy OID, 1.3.6.1.4.1.36203.1.1 Cp: URL: https://docs.namirialtsp.com/
crlDistributionPoint	Not critical http://crl.namirialtsp.com/QES.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 2 - Namirial qualified e-signature

7.1.3 Namirial CA Qualified Signature

Version	Version 3
Serial Number	41 58 c1 3a 49 d2 98 19
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A./02046570426" organizationalUnit: "Certification Authority" **commonName**: " Namirial CA Qualified Signature"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer

SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extensions	
Subject Key Identifier	63 fd ed e6 8c 62 47 48 cf ea 09 41 73 76 11 e2 64 62 7b 10
Authority Key Identifier	63 fd ed e6 8c 62 47 48 cf ea 09 41 73 76 11 e2 64 62 7b 10
Certificate Policies	Not critical Policy OID, 2.5.29.32.0
crlDistributionPoint	Not critical http://crl.firmacerta.it/FirmaCertaQualificata1.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 3 - Namirial CA qualified signature

7.1.4 Namirial EU Qualified CA

Version	Version 3
Serial Number	39 61 62 D9 E5 04 83 A3
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." organizationalUnit: "Trust Service Provider" **commonName**: " Namirial EU Qualified CA"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extensions	
Subject Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Authority Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Certificate Policies	Not critical Policy OID, 1.3.6.1.4.1.36203.1.1

crlDistributionPoint	Not critical http://crl.namirialtsp.com/CA4K.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 4 - Namirial EU Qualified CA

7.2 Certificate Directory

The Certificate directory contains:

- all the Certificates issued by the Certification Authority;
- the list of suspended and revoked Certificates (CRLs).

7.3 CRL Profile

The CRL conforms to the RFC 5280 public specifications.

Version	2
signature	sha256withRSA
Issuer	CA DN
Thisupdate	This field indicates the issue date of this CRL.
Nextupdate	The date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date.
reevokedCertificate	List of revoked certificates' serial numbers
CRL.Extensions	CRLNumber, ExpiredCertsOnCRL and Authority Key Identifier
signatureAlgorithm	sha256withRSA
Signature Value	Signature computed on the hash of the DER encoding of CertList.

Table 5 - CRL profile

7.4 OCSP Profile

The OCSP protocol conforms to the RFC 6960 public specifications.
The detailed list of fields contained within the OCSP responses provided by the Namirial OCSP Responder is set below.

responseStatus	Choice of Successful (0), malformed (1), internalError (2), tryLater (3), sigRequired (5), unauthorized (6) Related to state and/or configuration of the Service (as for Rfc 6960)
Basic Response	
Version	1 (0x0)
Responder ID	SHA-1 of the Responder's Public Key (excluding the tag and length fields)
ProducedAt	GeneralizedTime of production of the response (UTC). The time at which the OCSP responder signed this response.
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Responses	Only one response per certificate
CertID.hashAlgorithm	SHA-1 160 bit
CertID.issuerNameHash	Hash (SHA-1) of issuer's DN
CertID.issuerKeyHash	Hash (SHA-1) of issuer's public key
CertID.serialNumber	CertificateSerialNumber
Cert Status	Choose from: Good[0], Revoked[1], Unknown[2]
Cert Status.RevokedInfo	revocationTime = The time at which the certificate was revoked or placed on hold. revocationReason = The reason for revocation of certificate
thisUpdate	The most recent time at which the status being indicated is known by the responder to have been correct.
Response.Extensions	OCSP nonce
signatureAlgorithm	sha256withRSA
Signature	Signature computed on the hash of the DER encoding of ResponseData.
Certs	OCSP Responder's Certificate CA's Certificate

Table 6 - OCSP profile

7.5 Accessing the Certificate directory

The reference copy of the Certificate directory can only be accessed from the Certificate generation system. Only the Certification Authority is permitted to publish information on operational copies of the Certificate directory. This information is publicly accessible in read-only mode and via the http protocol.
To avoid having CRLs that are too large, when each Certificate is issued, the Certification Authority associates a specific CRL with it the full download address of which is included in the CRL Distribution Point extension.
When issuing revocation lists, the Certification Authority shall ensure that the set of all CRLs necessary to cover all the Certificates issued in their entirety up to that time by the Certification Authority is published.
Partitioned certificates and CRLs are issued in compliance with the RFC 5280 technical specification, with a special reference to the extensions required for partitioning CRLs described here.
Pursuant to Art. 42, paragraph 3 of the Italian Prime Ministerial Decree of 22 February 2013, the Certification Authority also makes accessible at the following URL a copy of the list, signed by the Agency, of the Certificates relating to the certification keys set forth in Article 43, paragraph 1, letter e) of the Italian Prime Ministerial Decree referred to above:

https://cms.firmacerta.it/Certificatori/Certificatori.zip.p7m

7.6 Managing the Certificate directory

The reference copy of the Certificate directory is managed by the Certification Authority, is not accessible from the outside and contains all Qualified Certificates and revocation lists issued by the Certification Authority.
All operations that change data within the directory are automatically reported in the Audit Log.
The directory is updated when each Qualified Certificate is issued and when the revocation list (CRL) is published.
Certificate revocation lists (CRLs) are publicly accessible in read-only mode and contain revoked or suspended subscription Certificates. The publication of revocation lists is updated synchronously with each update of the directory of revoked or suspended Certificates.

7.7 Archiving of Qualified and Time Stamping Certificates

Qualified Certificates and those relating to Time Stamping keys are archived and retained for 20 (twenty) years after issue.

Private signature keys whose Certificate has expired can no longer be used.

8. Audit and compliance

Namirial is a Trust Service Provider responsible for issuing the Qualified Signature and accredited by a certification body, which in turn is accredited by Accredia. The conformity assessment report is sent to AgID.
Consequently, Namirial is subject to a conformity assessment ("supervision") by the Agency itself and is required to carry out regular internal inspections.

8.1 Frequency and circumstances of conformity assessment

Namirial's audit function is responsible for internal audits of Digital Signature services. It verifies that processes comply with legal requirements and company regulations and procedures. The internal audit is carried out at least once a year. On the other hand, the third-party audit performed by an Accredia-accredited certification body is carried out annually.

8.2 Identity and qualification of the person carrying out the control

Compliance audits are carried out by Bureau Veritas Italy.
On the other hand, internal audits are the responsibility of the relevant corporate function using suitably qualified employees.

8.3 Relations between Namirial and the certification body

There is no relationship between Namirial and the certification body that could in any way influence the audit results in Namirial's favour.

8.4 Area being assessed

The certification body performs conformity assessment of Namirial's activities, supervised by AgID, which operate in compliance with Regulation (EU) 910/2014, known as "eIDAS-Electronic Identification Authentication and Signature".
The main purpose of the internal audit is to check the integrity of the Audit Log and compliance with the Certification Authority's operating procedures.

8.5 Actions resulting from non-compliance

In case of non-compliance, Namirial takes the necessary corrective actions tracked and measured until resolution.

8.6 Reporting results

The results of the audit, carried out by the certification body, are shared with the Certification Authority through a conformity assessment report. The result of the internal audit is reported to the Management and the organisational structure manager in charge of providing the service.

9. Other legal and business aspects

9.1 Rates

The maximum rates for the service are published on the Certification Authority's Shop.
Different conditions can be negotiated on a customised basis depending on the volumes required.

9.2 Financial liability

Namirial has taken out adequate insurance to cover the risks of the activity and any damages resulting from the certification service.

9.3 Responsibility of the Subject

The Subject is responsible for providing information that is certain, true and traceable to his/her identity. He/she is also called upon to comply with the procedures laid down for the issue and safekeeping of credentials, and to carefully read the information material made available by the CA, of which this manual is a part. This person is also obliged to scrupulously follow the instructions provided by the Certification Authority.
The Subscriber, if any, must provide the CA with information that is certain, true and traceable to the identity on whose behalf it is requesting the Certificate. He/she shall also be responsible for informing the Subject of his/her obligations regarding the safekeeping of credentials,

9.4 Responsibility of the CA and restrictions on damage

9.4.1 Limitations of liability of the Certification Authority

The Certification Authority is responsible to the Subjects for compliance with legal obligations arising from the activities envisaged by the CNIPA Circular of 6 September 2005, the Italian Prime Ministerial Decree of 22 February 2013, the eIDAS Regulation, Italian Presidential Decree 445/2000, CNIPA Resolution 45/2009 and DigitPA Commissioner's decision no. 69/2010 as amended.

The Certification Authority, where applicable, provides the Subject with a special kit configured in two alternative ways:

- Secure signature device (smart card, USB SIM Token or Micro SD) complete with Signature Certificate and the thoroughly tested software for affixing and checking qualified signatures.
- Secure signature device (smart card, USB SIM Token or Micro SD) not customised (without subscription keys), device customisation procedure and software, for affixing and checking qualified signatures (Art. 7 -11)

The Certification Authority accepts no responsibility:

- for improper use of the certificates issued;
- for the consequences arising from the Subject being unaware of, or failing to comply with, the procedures and operating methods indicated in this document;
- for the failure to comply with its obligations for reasons not attributable to it;

9.4.1.1. Limitations and Damages

Pursuant to Art. 57, paragraph 2 of the Italian Prime Ministerial Decree of 22 February 2013, the Certification Authority has taken out an insurance policy to cover the risks of the activity and damages to all parties (Subjects, Interested Third Parties, Relying parties) not exceeding the limits indicated below:

- 150,000 euro per individual claim for a total of 1,500,000 euro per insurance year for all capital losses arising from all claims brought against the Certification Authority for all insurance covers combined.

9.5 Confidentiality and processing of personal data

9.5.1 Protection of personal data

The following is a description of the procedures and operating methods that Namirial S.p.A., as Data Controller, adopts in carrying out its activities. Personal information concerning the Subjects of the Certificates and, more generally, customers of the service provided is processed, stored and protected in accordance with the provisions of European Personal Data Protection Regulation 679/2016.

9.5.2 Protection and rights of data subjects

Namirial S.p.A. guarantees the protection of data subjects in compliance with European Regulation 679/2016 on the protection of personal data. In particular, it provides data subjects with all necessary information in relation to the right of access to personal data and the uses of such data permitted by law.

Access to their data by data subjects is permitted by means of a written request, using the format downloadable from the Namirial website ww.namirial.com, to be sent to the data protection officer, also by email to dpo@namirial.com, who will process the request without undue delay.

Data subjects must give written consent to the processing of their data by Namirial S.p.A.

9.5.3 Processing methods

All personal information acquired during the provision of services is processed by Namirial, which adopts the security measures described in this manual in order to prevent its loss, illicit use or access by unauthorised personnel.
Data in electronic format is stored on dedicated data servers and on optical media in protected cabinets.
Namirial S.p.A. reserves the right to store paper data at its headquarters, in paper archives to which only expressly authorised persons have access.

9.5.4 Purpose of processing

Personal data is acquired in accordance with the purposes set out in the privacy policy provided to the Subscriber during the Certificate application phases. The privacy policy is also published at https://docs.namirialtsp.com/privacy/.
The purposes of the processing are listed below.

- management of the contractual relationship;
- any checks on the quality of service and security of the system;
- commercial activities carried out by sending privacy policies related to the issue of products and/or services similar to or directly related to the Certification and Time Stamp services.

The data subject has the possibility of objecting to the processing of personal data concerning this type of communication.

9.5.5 Other forms of data use

Personal data can be used for purposes other than the provision of the services described in this manual and can be disclosed to public entities such as police, public authorities and judicial authorities if the same entities request it for reasons of public order and in compliance with law provisions for the security and defence of the State, the prevention, investigation and/or prosecution of criminal offences.

9.5.6 Data security

In compliance with current regulations, Namirial S.p.A. takes all necessary safety measures in order to minimise:

- the risks of destruction or loss, accidental or otherwise, of data;
- the risks of damage to hardware resources on which data is stored;
- the risk of damage to the premises where the data is stored;
- unauthorised access to data;
- processing activities not permitted by law or company regulations

The security measures taken by Namirial also guarantee:

- the integrity and safeguarding of data against tampering or modification by unauthorised parties
- data availability and its consequent usability;
- data confidentiality or the guarantee that only authorised persons have access to the information.

9.6 Archives containing personal data

The archive containing personal data is the registration database.
The archives listed above are managed by the registration manager and are adequately protected against unauthorised access, in accordance with the GDPR as amended

9.7 Rights of intellectual property

This document is the property of Namirial, to which all rights are reserved. The owner of the Certificate retains all rights to its brand name and domain name. In relation to the ownership of other data and information, the applicable law applies.

9.8 Obligations and guarantees

9.8.1 Certification Authority

The CA is obliged to:

- operate in accordance with this document;
- identify Subscribers and Subjects as described in this document;
- issue and manage Certificates as described in this document;
- provide an efficient Certificate suspension or revocation service;
- ensure that the owner has the corresponding private key at the time the certificate is issued;
- promptly report any compromise of the private key;
- provide clear and complete information on procedures and service requirements;
- provide a copy of this document to anyone who requests it;
- ensure that the provision of digital signature services is accessible to persons with disabilities;
- ensure that personal data is processed in accordance with current regulations;
- guarantee the availability of the service, except in the case of scheduled maintenance activities, which are communicated in advance;
- provide an efficient and reliable information service on the status of Certificates.

9.8.2 Registration Authority

The Registration Authority deals with the personal data of the data subject with the utmost confidentiality and in accordance with the GDPR.

9.8.3 Subscribers or Subjects

The Subscriber or Subject is obliged to:

- read, understand and fully accept this document;
- apply for the Certificate provided by this document;
- securely generate the public and private key pair using a trusted system;
- provide the CA with accurate and truthful information during registration;
- take technical and organisational measures to prevent the private key from being compromised;
- guarantee the privacy of confidential codes received by the CA;
- request immediate suspension of the Certificate in the event of suspected or confirmed compromise of the private key;
- immediately request revocation of the Certificate if one or more information contained in the Certificate is no longer valid;
- following the issue and until the expiry or revocation of the Certificate, promptly notify the CA of any changes to the information provided in the application;

9.8.4 End users

End users, i.e. all entities (other than the Subscriber or the Subject) relying on
Certificates issued hereunder, are obliged to:

- ensure that they obtain sufficient information on the functioning of the Certificates and the PKI;
- check the status of the Certificates issued by Namirial on the basis of this document;
- rely on a Certificate only if it is not expired, suspended or revoked.

9.9 Guarantee limitations

What is described in the Trust Service Practice Statement applies.

9.10 Damage limitations

What is described in the Trust Service Practice Statement applies.

9.11 Damages

What is described in the Trust Service Practice Statement applies.

9.12 Terms and termination

What is described in the Trust Service Practice Statement applies.

9.13 Notifications

What is described in the Trust Service Practice Statement applies.

9.14 Dispute settlement procedures

What is described in the Trust Service Practice Statement applies.

9.15 Competent Court

What is described in the Trust Service Practice Statement applies.

9.16 Applicable law

What is described in the Trust Service Practice Statement applies.

APPENDIX A: Tools and methods for affixing and checking digital signatures

The tools made available by the Certification Authority allow for PAdES, CAdES and XAdES type signatures. More information on the types of signatures that can be used can be found at http://www.agid.gov.it/.

There are two ways to affix a digital signature:

- signature with personal signature device (e.g. smartcard, USB token or similar),
- signature with automatic/remote procedure based on the use of HSM.

The following paragraphs set out the operating procedures for both cases.

Signature with personal signature device

Namirial makes available to users free of charge a software called "FirmaCerta", which allows them to easily perform all operations relating to digital signatures. Specifically, the software enables, for each individual file:

- digital signature;
- time stamping;
- signature and time stamp check;
- countersigning a file (validation);
- handwritten digital signature.

The functions offered by the "FirmaCerta" product also include the possibility of:

- signing large volumes of digital documents at once, such as invoices, policies, payment receipts, bank transfers and any other type of digital document;
- signing PDF documents while retaining the original format;
- choose the hardware device with which the signature is to be affixed (Smart Card - Token);
- associating/placing a time stamp or signature (handwritten digital signature) on a document;
- selecting files by dragging and dropping them within the same signing window with the Drag & Drop feature;
- signing password-protected PDF documents.

The hardware and software prerequisites as well as all installation instructions for the "FirmaCerta" product can be found in the software's "Quick Start Guide" available at the URL:

http://www.firmacerta.it/manuali.php

The document, which is an integral part of this Operating Manual, contains the operating procedures for generating and checking digital signatures.
Some document formats make it possible to insert executable code (macros or commands) within the document without altering its binary structure, and such as to activate functions that can modify the acts, facts or data represented in the document. Note that digitally signed files containing such structures do not produce the effects referred to in Article 21, paragraph 2, of the CAD, and it is the responsibility of the Subject to ensure, by means of the typical functions of each product, the absence of such executable codes.
Appendix C provides operating procedures, with reference to certain widely used formats, to ensure that the document does not contain macro-instructions or executable code.

Signature with automatic signature applications

The user uses a signature "client" application provided by the Certification Authority or the Customer (e.g. company, bank, public body, etc.) that provides application services to internal or external users. Therefore, the specific methods for signing depend on the particular client application used by the users and are described on a case-by-case basis by the addendum to the operating manual.
The solution provided by the Certification Authority consists of two components:

- **HSM and the SignEngine server (hereinafter SE) that controls and drives it.** SE is responsible for the low-level signing of document hashes.
- **The SignWebServices server (hereinafter SWS).** It is the component capable of affixing and checking signatures at a high level of abstraction. It integrates with customer systems (custom or legacy). It needs to communicate with the SE component but can be located elsewhere. SWS performs the enveloping in the various supported formats and calculates the hashes to be signed by SE.

Therefore, there are two different usage scenarios:

- **HSM at the customer's CED.** This configuration is preferable if a considerable number of signatures have to be produced and guarantees greater performance results as the HSM is dedicated and there are no appreciable network delays as all communication takes place over the LAN. In this scenario, both the SE and SWS components are installed at the customer's premises.
- **HSM at Namirial.** With this configuration, the customer merely carries out the integration between its systems and the SWS component, disregarding the purchase and operation of the HSM. In this scenario, the customer only needs the SWS component or the remote signature application provided by the Certification Authority.

Therefore, the automatic signature system, based on HSM, can be hosted at the Certification Authority's data centre or at the Customer's data centre; in the second case, the Customer must comply with the physical, logical, operational and management security requirements indicated by the Certification Authority, which will carry out periodic checks on compliance with these requirements in accordance with Article 3, paragraph 5, of the Italian Prime Ministerial Decree.
The SE and SWS components independently establish secure connections that are always protected by TLS/SSL protocols, with server authentication and session encryption with symmetric keys of at least 128 bits and, in accordance with Art. 42, paragraph 6 of the Italian Prime Ministerial Decree, do not allow the Certification Authority to know the acts or facts represented in the electronic document that is the subject matter of the subscription or checking process.
The signing request from the client is authenticated with username and password. Users access the server exclusively via a local area network (LAN) that cannot be reached from the internet, and the Signature Certificate contains appropriate restrictions on use.

Signature with remote signature applications

For signing remotely, it will be possible to use applications distributed by the Certification Authority or by the Customer (e.g. company, bank, public body, etc.) providing application services to internal or external users. Therefore, the specific methods for signing depend on the particular application used by the users and are described on a case-by-case basis by the addendum to the operating manual. The signing request from the user is always two-factor authenticated. The standard mode is based on the use of a static PIN (first factor) accompanied by a dynamic OTP (One-Time Password) that can be, depending on the case:

- mobile token
- SMS token
- physical token

The tools provided by the Certification Authority are as follows:

- FirmaCerta
- FirmaCertaMobile
- FirmaCertaWeb

FirmaCerta is a desktop application that can be installed on workstations equipped with the Microsoft Windows operating system. The hardware and software prerequisites as well as all installation instructions for the "FirmaCerta" product can be found in the software's "Quick Start Guide" available at the URL:

http://www.firmacerta.it/manuali.php

The document, which is an integral part of this Operating Manual, contains the operating procedures for generating and checking digital signatures.

FirmaCertaMobile is a mobile application, developed by the Certification Authority, which can be installed on devices equipped with the Android and IOS operating systems;

FirmaCertaWeb is a web application that can be used to sign and check signatures using commonly used browsers and is available at the following URL:

https://sws.firmacerta.it/SignEngineWeb/

In any case, signing will require the user to enter the following codes:

- Virtual Device Code5
- PIN6
- OTP

The Certification Authority cannot in any way gain knowledge of or have the possibility of changing the PIN code. It will be the Subject's responsibility to manage this code, without which the associated Certificate cannot be used to affix new signatures.
If the *PIN* code is no longer available, the Subject is advised to immediately suspend the associated Certificate, in accordance with the procedure described in Section 4.13.2.

Note also that the server applications used as part of the remote signature service adopt specific security measures, in accordance with Art. 42, paragraph 6 of the Italian Prime Ministerial Decree, and do not allow the Certification Authority to know the acts or facts represented in the electronic document subject to the subscription or checking process.

How to affix and define the Time Reference

The issue of the time stamp, requested by the Subject of the Qualified Certificate, is obtained by means of a software programme provided by the Certification Authority and installed on the Subject's computer, and the web service is accessible via the internet using a secure protocol.
The stamping process is as follows:

- the Subject, using the software supplied with the kit, produces and signs the time stamping request for the electronic document,
- The request is forwarded to the Certification Authority using a secure protocol

[5] This information is contained in the form signed by the Subject.
[6] Set by the Subject during key generation.

(HTTPS),
- the Certification Authority checks the request and the credentials of the Subject,
- the Certification Authority generates the time stamp with a high reliability system that coincides with the time of its generation with a difference of no more than one second from the UTC time scale (IEN).
- the stamping is handed over to the Subject in a secure manner for use.

The fingerprint of the electronic evidence is calculated using the SHA-256 hash function. If the time-stamping system (TSA) receives a non-compliant request, an error message is returned.

Archiving and Validity of Time Stamps

All time stamps issued by the validation system are stored in a special digital archive that cannot be modified.
Brands are retained for 20 (twenty) years from the date of issue and are valid for the entire period of retention.

Time Reference Accuracy

When generating the time stamp, the TSA server uses the date and time from the system clock, which is kept aligned with UTC (Coordinated Universal Time) time by means of two synchronisation systems:
- an external probe connected to the GPS satellite network system,
- the NTP service made available by INRIM.

The accuracy of the time reference system is 1 second. The tolerance, as required by the regulations in force, is never more than one second in relation to the UTC time scale (IEN).

Appendix B – Namirial Certificate Policy

Certificate Policies

The Certification Authority uses the following Object Identifiers, (OIDs) pertaining to its Private Enterprise Number:

1.3.6.1.4.1.36203	Namirial S.p.A.
1.3.6.1.4.1.36203.1	CA FirmaQualificata
1.3.6.1.4.1.36203.1.1	Policy CA FirmaQualificata
1.3.6.1.4.1.36203.2	CA TSA
1.3.6.1.4.1.36203.2.1	Policy CA TSA
1.3.6.1.4.1.36203.4	CA Autenticazione
1.3.6.1.4.1.36203.4.1	Policy CA Autenticazione

Table 5: Namirial CA Object Identifier

The Certificates issued according to the rules of this document are identified with the following Object Identifiers, (OIDs):

1.3.6.1.4.1.36203.1.1.1	Policy for certificates associated with time stamping servers (used until January 2014). The policy identifies time stamp issues in compliance with RFC 3161
1.3.6.1.4.1.36203.1.1.2	Policy for qualified certificates associated with secure device for signature creation by manual procedure.
1.3.6.1.4.1.36203.1.1.3	Policy for qualified certificates associated with secure equipment for signature creation by means of an automatic procedure. User Notice: This certificate is only valid for automatic signatures. This certificate may only be used for unattended/automated digital signatures.
1.3.6.1.4.1.36203.1.1.4	Policy for certificates associated with OCSP servers related to Subscription certificates.
1.3.6.1.4.1.36203.1.1.5	Policy for qualified certificates associated with secure equipment for signature creation by means of a remote procedure.
1.3.6.1.4.1.36203.1.2.1	Policy for qualified certificates issued to legal entities whose private key does not reside in a Qualified Seal Creation Device
1.3.6.1.4.1.36203.1.2.3	Policy for qualified certificates issued to legal entities whose private key resides in a Qualified Seal Creation

	Device
1.3.6.1.4.1.36203.2.1.1	Policy for certificates associated with time stamping servers (used as from January 2014). The policy identifies time stamp issues that comply with RFC 3161, the eIDAS Regulation and the ETSI EN 319 401 standard as amended.
1.3.6.1.4.1.36203.2.1.2	Policy for certificates used to issue qualified time stamps. The policy identifies time stamp issues that comply with RFC 3161, the eIDAS Regulation, ETSI EN 319 401 and ETSI EN 319 421 as amended.
1.3.6.1.4.1.36203.4.1.2	Policy for authentication Certificates.
1.3.6.1.4.1.36203.4.1.4	Policy for certificates associated with OCSP servers relating to authentication certificates.

Table 6: Object Identifier of Certificates issued by Namirial CA

QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key related to the certificated public key resides in a QSCD

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject (legal entity) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal entity).* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1 and 3): *organizationIdentifier contains an identification of the subject organization different from the organization name*

	VAT or NTR || Code country || - || identifier **commonName (OID 2.5.4.3):** *commonName contains name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name* **givenName (OID 2.5.4.42)**: Optional *EXTENDED NAME OF THE LEGAL REPRESENTATIVE* **Surname (OID 2.5.4.4)**: Optional *EXTENDED SURNAME OF THE LEGAL REPRESENTATIVE* **Dn_Qualifier (OID: 2.5.4.46):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key

Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Certificate Policies	Not critical • QCP-l-qcsd (0.4.0.194112.1.3) • Policy OID 1.3.6.1.4.1.36203.1.2.3 Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 7 - QCP-L-QSCD policy for EU qualified certificate issued to a legal person where the private key related to the certificated public key reside in a QSCD

QCP-l Policy for EU qualified certificate issued to a legal person

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject (legal entity) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal entity).*

	organizationIdentifier (2.5.4.97) (ETSI 319 412 part 1 and 3): *organizationIdentifier contains an identification of the subject organization different from the organization name VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name* **givenName (OID 2.5.4.42)**: Optional *EXTENDED NAME OF THE LEGAL REPRESENTATIVE* **Surname (OID 2.5.4.4)**: Optional *EXTENDED SURNAME OF THE LEGAL REPRESENTATIVE* **Dn_Qualifier (OID: 2.5.4.46):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-calssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt -4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key

Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Certificate Policies	Not critical • QCP-l (0.4.0.194112.1.1) • Policy OID 1.3.6.1.4.1.36203.1.2.1 Cp: URL: https://docs.namirialtsp.com/ • NCP (0.4.0.2042.1.1)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 8 - QCP-L policy for EU qualified certificate issued to a legal person

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm)

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL**

	organizationName contains full registered name of the organization associated with the subject. **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which cannot be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Identification Number of the Subject.* *In the event that this information is not available it is possible to use identification document serial number.* *If it is not possible to use id document's serial number it is possible to use other identification numbers assigned by a government o civil authority. In such a case it is possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional

	Dn_Qualifier contains a unique identification code assigned to the Subject by the CA **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt -4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.2 (smart card)

	Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2) Or • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.5 (HSM) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 9 - QCP-N-QSCD policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key reside in a QSCD (smart card or HSM)

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm) with etsi en 319 412-2 type 'B' or TYPE 'D' OR type 'f' key usage

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the*

	organization identified in organizationName attribute. *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which cannot be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Identification Number of the Subject.* *In the event that this information is not available it is possible to use identification document serial number.* *If it is not possible to use id document's serial number it is possible to use other identification numbers assigned by a government o civil authority. In such a case it is possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*

SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.2 (smart card) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2) Or • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.5 (HSM) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)

	All the Qualified Certificates issued under this profile bring the following limitation of usage: *"The use of the certificate is limited to relations with public sector bodies"*
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical One value among ETSI EN 319 412-2 TYPE B or TYPE D or TYPE F values

Table 10 - QCP-N-QSCD policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or HSM) with ETSI EN 319 412-2 TYPE 'B' or TYPE 'D' or TYPE 'F' KEY USAGE

QCP-n-qscd-A - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for automatic signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier*

	commonName (OID 2.5.4.3): *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which cannot be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Identification Number of the Subject.* *In the event that this information is not available it is possible to use identification document serial number.* *If it is not possible to use id document's serial number it is possible to use other identification numbers assigned by a government o civil authority. In such a case it is possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	

Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit
Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.3 (HSM Automatica) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 11 - QCP-N-QSCD-A - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for automatic signature

QCP-n-qscd-D - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for disposable signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 30 days
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)**

	as an alternative respect to GivenName and SurName: *pseudonym contains a unique string suitable to identify the subject within CA environment and which cannot be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Identification Number of the Subject.* *In the event that this information is not available it is possible to use identification document serial number.* *If it is not possible to use id document's serial number it is possible to use other identification numbers assigned by a government o civil authority. In such a case it is possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-calssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit

Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6.1) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.6 (HSM Disposable) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 12 - QCP-N-QSCD-D - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for disposable signature

QCP-n-qscd-LD - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for Long-Lived disposable signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	30 days
Subject	**countryName (OID 2.5.4.6):**

(ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	*countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which cannot be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Identification Number of the Subject.* *In the event that this information is not available it is possible to use identification document serial number.* *If it is not possible to use id document's serial number it is possible to use other identification numbers assigned by a*

	government o civil authority. In such a case it is possible to use a code derived by one of the previous ones. **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains a unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extensions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit
Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code)

	https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6.1) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.7 (HSM Long-Lived Disposable) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 13 - QCP-N-QSCD-LD - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for long-lived disposable signature

Appendix C: macros and controls

Macro instructions or executable codes within the document that modify the acts and facts represented in the document invalidate the signature (Art. 4, paragraph 3, of the Italian Prime Ministerial Decree). It is the Subject's responsibility to ensure, by means of the typical functions of each product, the absence of such executable codes.
The steps to disable macro instructions or executable codes for the most popular products are outlined below. For details, please refer to the user manuals supplied with the applications.

MS Word® 2003 and MS Excel® 2003
To deactivate macros, follow the steps below:

- select all text and then press Ctrl+Shift+F9 simultaneously.

MS Word® 2007 and MS Excel® 2007
To deactivate macros, follow the steps below:

- click on the Office button,
- click on Options,
- click on Protection Centre,
- go to Protection Centre Settings,
- click on Deactivate all macros with notification.

MS Word® 2010/2013 and MS Excel® 2010/2013
To deactivate macros, follow the steps below:

- click on the File button,
- click on Options,
- click on Protection Centre,
- go to the Protection Centre Settings button,
- click on Deactivate all macros with notification.

Adobe Acrobat®
To deactivate the JavaScript code execution functions, follow the steps:

- click on Edit,
- click on Preferences,
- JavaScript,
- remove the JavaScript enable flag.