Digital Signature Certification Authority

Certification Practice Statement and Certificate Policy

Category	**Certification Authority**	Document ID	**NAM-CA-CPS-CP**	**Namirial S.p.A.**
Written by	**Simone Baldini**	Confidentiality note	**Public Document**	Legal Representative
Verified by	**Giuseppe Benedetti**	Version	**1.3**	**Davide Ceccucci**
Approved by	**Davide Ceccucci**	Issuance date	**29/06/2017**	CECCUCCI DAV 2017.06.30 10:47:43 CN=CECCUCCI DAVIDE C=IT O=NON PRESENTE 2.5.4.4=CECCUCCI RSA/2048 bits

Namirial S.p.A.

Registered office, management and administration 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
Tax Code/REG. REGISTER OF COMPANIES OF ANCONA no. 02046570426 - VAT no. IT02046570426
SHARE CAPITAL. € 6.500.000,00 fully paid-up
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

– This page is intentionally left blank –

TABLE OF CONTENTS

HISTORY OF CHANGES

VERSION	**1.3**
Date	29/06/2017
Reason	Content update
Changes	added new CA Root profile certificate.

VERSION	**1.2**
Date	20/06/2017
Reason	Content update
Changes	typo correction; added CA Browser Forum statements added LRA in PKI participants 3.4 added cross reference for suspension/revocation procedure 4.4 added time representation in accord to RFC 5280 4.9 updated the suspension/revocation carrying out 7.2 updated CRL Profile 7.3 updated OCSP Profile 7.1.7, 7.1.8 added Long-lived Disposable certificates profile other updating

VERSION	**1.1**
Date	05/06/2017
Reason	Content update
Changes	Updates to documents references and certificate profiles; typo correction

VERSION	**1.0**
Date	23/05/2017
Reason	First document issuance
Changes	---

REFERENCES

Number	Description
[I]	Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.
[II]	Decreto del Presidente del Consiglio (DPCM) 22 febbraio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71."
[III]	Decreto Legislativo (DLGS 196) 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n. 123 della Gazzetta Ufficiale n. 174, 29 luglio 2003
[IV]	Decreto Legislativo (CAD) 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale", pubblicato nella Gazzetta Ufficiale n.112 del 16 maggio 2005 con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
[V]	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
[VI]	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
[VII]	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
[VIII]	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
[IX]	ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[X]	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
[XI]	ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[XII]	ISO EN UNI 9001:2008 – Quality management system
[XIII]	ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework
[XIV]	Deliberazione CNIPA n. 45/2009 e s.m.i.
[XV]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[XVI]	ISMS-DOC-A16-Security breaches reporting procedure-V1 Final

[XVII]	20170428-NAM_CA_Struttura_Organizzativa_v3.0
[XVIII]	Manuale Operativo Servizi di Certificazione e Marcatura Temporale ver 2.2
[XIX]	IISMS-DOC-08-Regolamento sicurezza delle informazioni aziendali
[XX]	HR001 Job Profiles TSP
[XXI]	ISMS Governance Manual
[XXII]	ISMS-DOC-06-Information Risk Management & Control Manual
[XXIII]	ISMS-DOC-A17-Business Continuity Policy
[XXIV]	ISMS-DOC-A16-Incident Management Policy
[XXV]	ISMS-FORM-08-Risk Assessment and treatment plan Document-V1 Final
[XXVI]	Proposal for Article 19 Incident Reporting- Annex A
[XXVII]	Trust Services Practice Statement
[XXVIII]	ISMS-DOC-08-Information Security Operational Policy.23.02.2017-V1
[XXIX]	Firma Elettronica Qualificata Remota - Richiesta autorizzazione all'uso di apparati Thales ai sensi dell'art. 35 comma 5 del CAD
[XXX]	ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[XXXI]	ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[XXXII]	ETSI EN 319 412-4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[XXXIII]	ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[XXXIV]	Request for Comments 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[XXXV]	CNIPA Limiti d'uso nei CQ - Limiti d'uso garantiti agli utenti ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45
[XXXVI]	Rfc 5280 - Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[XXXVII]	ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[XXXVIII]	ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[XXXIX]	Operating Manual Addendum Disposable Signature Certificates / Addendum Manuale Operativo – Certificati di Firma Disposable
[XL]	Manuale Operativo Certificati di Firma Remota
[XLI]	Directive 2005/60/EC issued by the European Parliament and Council dated October 26, 2005**,** *on preventing the use of the financial system for the purpose of money laundering and terrorist financing*
[XLII]	Directive 2006/70/EC dated August 1, 2006 containing implementing measures for the Directive 2005/60/EC of the European Parliament and Council regarding the *definition of "persons politically exposed " and the technical criteria for simplified procedures for the adequate verification of the clientèle and for exemption in case of financial activity conducted on an occasional or very limited basis*

[XLIII]	Directive (EU) 2015/849 of the European Parliament and of the Council dated May 20, 2015**,** *concerning the prevention of use of the financial system for money laundering or terrorist financing, amending (EU) Regulations No. 648/2012 of the European Parliament and Council and repealing Directive 2005/60/EC of the European Parliament and Council and Commission Directive 2006/70/EC.*

Table 1 - References

INDEX OF TABLES

1 INTRODUCTION

1.1 OVERVIEW

This document describes the Digital Signature service provided by Namirial S.p.A. The procedures adopted to issue the Digital Certificates are reported on the website https://docs.namirialtsp.com.

This document represents the CPS and CP adopted by Namirial to manage the certificates and the encryption keys related to Digital Signature.

This Document describes techniques, policies and procedures of the CA personnel in some services and in the entire life cycle of certificate solutions that are issued by Namirial S.p.A. The structure and contents of this CPS and CP are based on the guidelines specified by the RFC 3647 standard.

In addition, Namirial S.p.A. ensures its compliance with the requirements identified in the documents: 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 on the website http://www.etsi.org)

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the Certification Practice Statement (CPS) being applied to Qualified Certificates issued by Namirial S.p.A. Version and time of last revision are indicated on the first page. This document is published on Namirial's web site in two languages: Italian and English. In the event of any inconsistency between the two versions, the English version takes precedence.

Namirial S.p.A. ensures compliance of its certificates with the Root ASN.1 OID laid down in this document.

The Private Enterprise Number OID for Namirial S.p.A. is iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

This CPS is reported on the certificates with the following OID: **1.3.6.1.4.1.36203.1**.

1.3 PKI PARTICIPANTS

1.3.1 CERTIFICATION AUTHORITY

The Certification Authority is a third and trusted party that issues the certificates and signs them with its private key (CA key). In addition to that, the CA manages the certificates status. The role of the CA, regarding the service described, is performed by Namirial S.p.A., a company that can be identified as follows:

Company Name:	**Namirial S.p.A.**
Registered office:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) ITALIA (IT)
VAT Number:	IT02046570426
Phone and Fax numbers	TEL: +39 071.63494 FAX: +39 071.60910
Digital Signature web site:	http://www.namirialtsp.com
Web Site:	http://www.namirial.com
Certified email address:	firmacerta@sicurezzapostale.it
Email address	firmacerta@namirial.com

Table 2 - Contact information Registration Authority

The Registration Authority (RA) is the person, the structure or the organization that performs the following activities:

- Acceptance and validation of requests related to certificates issuance and management;
- Registration of the Subscriber and the related organization;
- Authorize the CA to issue the requested certificates;
- Certificate provision and subsequent notification to the client.

The RA activity is performed by Namirial employees as indicated in Internal Organization and Responsibility Procedures.

1.3.1.1 LOCAL REGISTRATION AUTHORITY

The LRA is the natural or legal person authorized by the Certification Authority to carry out operations needed to issue Certificates, according to the procedures identified and described in this document. The LRA must have previously signed a service agreements with the Certification Authority. The LRA may rely on RAO for operations of identification, registration and issuance. In general the LRA performs the same activities as the Registration Authority but in locations that are external and distributed across the territory.

1.3.2 SUBJECT

Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

The subject can be:

a) a natural person;
b) a natural person identified in association with a legal person;
c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization); or
d) a device or system operated by or on behalf of a natural or legal person.

NOTE: Relationship between subscriber and subject is described as follows and in clauses 1.3.3.

1.3.3 SUBSCRIBER

The Subscriber is a natural person or a legal person that requires a certificate:

1. The Subscriber can be the subject
2. The Subscriber can act on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company).

The link between the subscriber and the subject is one of the following:

a) To request a certificate for natural person the **subscriber** is:
   i. the natural person itself;
   ii. a natural person mandated to represent the subject; or
   NOTE: The local legal dispositions can address the handover of responsibility to a third person.
   iii. any entity with which the natural person is associated (such as the company employing the natural person or a non-profit legal person the natural person is member of).

b) To request a certificate for legal person the **subscriber** is:
   i. any entity as allowed under the relevant legal system to represent the legal person; or
   ii. a legal representative of a legal person subscribing for its subsidiaries or units or departments.

c) To request a certificate for a device or system operated by or on behalf of a natural or legal person the **subscriber** is:
   i. the natural or legal person operating the device or system;
   ii. any entity as allowed under the relevant legal system to represent the legal person; or
   iii. a legal representative of a legal person subscribing for its subsidiaries or units or departments.

1.3.4 RELYING PARTIES

Relying parties are natural or legal persons that rely on a certificate and/or on a digital signature, that is verifiable with reference to a public key listed in a subject's certificate. In order to verify the validity of a digital certificate, relying parties must always refer to Namirial CA revocation information such as a Certificate Revocation List (CRL). Relying parties meet specific obligations as described in this document.

1.4 CERTIFICATE USAGE

Certificates issued by Namirial are valid in order to apply Digital Signatures on electronic documents enforceable against third parties (i.e. such as electronic mail and retail transactions).
It is forbidden any misuse of the certificates issued by Namirial in relation to this document and PKI Disclosure Statement.
If Namirial gains knowledge of any misuse, the certificate is immediately revoked.
It is assumed that the client has the competence and the necessary knowledge to properly use the certificate.

1.5 CPS AND CP ADMINISTRATIONS

This document is edited, published and updated by Namirial. Any change to this document is submitted to the internal review process, is approved by the Top Management and notified to Italian Digital Agency (AgID) and to the certification body. Any question or clarification concerning this document may be forwarded by mail to firmacerta@sicurezzapostale.it or firmacerta@namirial.com.
Namirial S.p.A. develop, implement, enforce, and annually update this document according to the relevant and latest versions of standards and guidelines required.
Following that, Namirial S.p.A. develop, implement, enforce, display prominently on its Website, and periodically update as necessary its own auditable public documentation (such CPS and CP and other relevant documents).

1.6 DEFINITIONS AND ACRONYMS

TERM	MEANING
AgID	Agenzia per l'Italia Digitale (National Digital Agency), the Supervisory Body in Italy.
Certification Authority (CA)	Authority trusted by one or more users to create and assign certificates
Certification Body	Third party auditor, part of national supervisory body's processes.
Certificate	Public key of a user, together with some other information, rendered un- forgeable by encipherment with the private key of the certification authority which issued it.
Certificate Policy (CP)	Named set of rules that indicates the applicability of a certificate to a community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates.
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. Digital Signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
Hardware Security Module (HSM)	An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.

OID	Object Identifier: In computing, object identifiers or OIDs are an identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name
Public Key Infrastructure (PKI)	Set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public- key encryption
PKI Disclosure Statement (PDS)	A supplemental instrument of disclosure and notice by a Certification Authority.
Qualified electronic Signature/Seal Creation Device (QSCD)	Device responsible for qualifying a digital signature
Registration Authority (RA):	Entity that is responsible for identification and authentication of subjects of certificates.
Relying party:	Person or organization acting upon a Certificate, typically to verify signatures by the Subscriber or to perform encryption towards the Subscriber. The Relying Party relies upon the accuracy of the binding between the Subscriber public key distributed via that Certificate and the identity and/or other attributes of the Subscriber contained in that Certificate.
Subject:	Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.
Subscriber:	Person or organization contracting with the Certification Authority, for being issued one or more Certificates.

Table 3 - Definition and acronyms

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORY MANAGEMENT

Namirial "repository" consists in the CA services website https://docs.namirialtsp.com/ in the Italian and English version.
The CA manages the repository independently and it is directly responsible for it.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The CA publishes at least the following documentation on its website:

- Trust Service Practice Statement (TSPS)
- Certification Practice Statement (CPS) and Certificate Policy (CP);
- Root CA certificates under which certificates for subscribers are issued;

Namirial S.p.A conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

2.3 TIME AND FREQUENCY OF PUBLICATIONS

This Document and the attached documents are published on the CA's website every time they are updated.

2.4 ACCESS CONTROL ON PUBLISHED INFORMATION

This Document and the attached documents are publicly available in the "pdf" format.
Namirial SpA ensures that its repository is available 24 hours a day, 7 days a week with a minimum of 99,44% availability overall per year with a scheduled down-time that does not exceed 0,28% annually.
Namirial SpA publishes in its public website at least the following information:

- The document "Operative Manual for the Certification Service" (as required by national laws), which represents the service-based policy and practice statement for the Certification Service and contains:
- Certificate Policy (CP),
- Certification Practice Statement (CPS)
- Profiles
- Conditions for insurance policy,
- Conditions for use of certificates,
- The URLs of Certificate Revocation Lists
- Trust Services Practices Statement

- The Time-Stamping Authority Practice Statement, which represents the service-based policy and practice statement for the Time-Stamping Service
- General Terms and Conditions
- Terms and Conditions for Use of Time-Stamping Service
- Audit results;
- Root CA certificates under which certificates for subscribers are issued
- Data Protection Disclaimer (Privacy)
- Insurance Policy

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 319 412-1 - 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 persons
- ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

The certificates report the value "no repudiation" for the key Usage extension. The field "subject" on the certificate reports understandable information which may allow to identify the certificate owner (legal or natural person).
In case of certificates for natural person, the field "subject" contains, at least:

- countryName;
- givenName and surname
- commonName

In case of certificates for legal person, the field "subject" contains, at least:

- countryName;
- organization Name
- organizationIdentifier
- commonName

3.2 INITIAL IDENTITY VALIDATION

The identity validation process involves the verification by Namirial of the identity of the Subscriber and of the identity of the Subject in case this one is different from the former (i.e. the Subscriber is acting on behalf of one or more distinct Subjects to whom it is linked). Namirial will ask the Subscriber and the Subject to provide identity information and supporting documents as required to perform the identification. The procedures to release a qualified certificate are:

- Registration
- Identification

The employees of the Registration Authority or a delegate office conduct the registration and identification which is under Namirial control and responsibility. The delegate office can be conducted:

- By the Namirial employees;
- By the entity to which Namirial delegates the identification activities.

The identification is based on documents that are applicable in the local country, such as a valid personal identification document. Namirial stores the identification documents or an attestation from an appropriate and authorized source, and retains this information for the required period (20 years).
Namirial can issues certificates to itself, according to ETSI EN 319 411-1 clause 6.2.2 q, because the organization runs all the RA tasks.

3.3 I&A FOR RE-KEY REQUESTS

The renewal of the certificates must respect 3 conditions: the certificates must not be expired, the certificates are issued on physical devices (smartcard, token USB, micro SD) and the renewal request must be presented within the last 90 days of validity. The certificates that meet these conditions can only be renewed once. For the other certificates the renewal features is disabled.
Subjects, 90 days before the expiration date, will receive an e-mail, which will remind them the deadline, and will explain the procedures to follow. If no renewal is made, additional 30 and 10 days' notice will be sent before expiration.
Subjects access to an online procedure that identifies the applicant, and validates its identity, by mean of performing digital signatures with certificate for which the lifetime is nearing to expiry (more details are described in relevant user guide available in https://docs.namirialtsp.com)
If the request is made after the expiration of the certificate, a new registration and issuance will be performed.

3.4 I&A FOR REVOCATION REQUESTS

Subscribers, Subjects, Third Parties may request the certificate revocation; the procedures for the revocation requests are:

- **on-line procedure**: online revocation service that is accessed through the device serial and an appropriate revocation code. This option is only available to the Subject because it is the only one who is expected to know the confidential personal codes. The request for the revocation or suspension of the qualified certificate is submitted to the Certification Authority by filling out in all its parts the special form made available on the Certification Authority's site (https://cms.firmacerta.it/areaPrivata/).

- **Physical request procedure:** This option is available to all users (Subscriber, Subject and Third Party) and it's performed through and application paper form which user has to download from the CA web site and submit compiled and signed accordingly.

For both modalities, the revocation request contains the date from which the certificate will be revoked.
The suspension request contains the start date and end date.
The Certification Authority verifies the authenticity of the request and proceeds to revoke the certificate by entering the same in the list of revoked and suspended certificates (CRLs) it manages.

Please refere to §4.9 of this document for more details.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Unless differently stated in this document and in accordance with the ETSI 319-411, the following operational requirements are applied to certificate's lifecycle. All the entities included in the Namirial domain (RA, LRA, Subscribers, Subjects or other participants) must notify to Namirial CA all the changes to the information reported on a certificate during its operational period and until it expires or it is revoked. Namirial CA will issue, revoke or suspend the certificates only in response to authenticated and approved requests.

4.1 CERTIFICATE APPLICATION FOR NATURAL PERSON

In this scenario, the Certificate Requests may be submitted in different ways:

- by authorized personnel of the Certification Authority or LRA Registration Offices, through RAO;
- by Third Party who signed an Agreement;
- by a notary or other public officer;
- by a person established by the Certification Authority of the role of IR (Registration appointee).
- through its electronic ID associated with a digital signature certificate already under its sole control.
- through the recognition already carried out by a financial broker or other party exercising financial activity;
- Additional identification means can be find in [XXXIX]and [XL].

4.2 CERTIFICATE APPLICATION FOR LEGAL PERSON

In this scenario, the Certificate Requests may be submitted only to authorized personnel of the Certification Authority or LRA Registration Offices, through RAO. Presence of a duly mandated Subscriber is required.

The user identification and registration procedure is essentially based on the following steps:

- physical presence or electronic identification;
- Submission of the request, with the necessary documentation;
- Validation of the provided information in order to accept or reject the request.

The following paragraphs show the details of these ways of identification.

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

- Filling out an application form;
- Acceptance of the Terms and Conditions

4.3 CERTIFICATE APPLICATION PROCESSING

Upon receipt of a request for certification, Namirial (or its delegate) carries out appropriate verification activities, such as verifying the registration and the identity of the Subject and the Subscriber.
For the registration, the subscriber shall provide all the documents required for the identification and contractual and registration documentation. Additional documentation is also required in relation to the type of Certificate. The registration operator (RAO or IR) receives the documentation submitted by the subscriber and verifies the validity of the document.

4.3.1 IDENTIFICATION CARRIED OUT BY CA OR LRA REGISTRATION OPERATOR (RAO)

Subject or Subscriber may be identified by the Certification Authority (or an LRA Registration Office) with a valid identity document or an equivalent Recognition Document pursuant to national regulation (Id document, etc..) or international regulation (Passport).

Subject or Subscriber may also be identified by electronic means through the Remote Video Identification System of the Certification Authority; In order to be identified, Subscriber has to use a personal computer with webcam and working pc audio system.

To ensure the protection and management of your personal data in full compliance with Data Protection regulation, each subscriber will be provided in advance with the privacy statement and, in the case of identification via a video conference system, will be required to consent to the video recording and processing of data by the Certifying Officer.

Once obtained the applicant's consent the registration of the video conference can start, which will begin with the repetition of the consent request procedure.

The specific telematic identification and registration procedures studied by the Certification Authority and implemented by its agents in that location are not made public for security reasons.

In detail, recording data, consisting of video audio files and structured electronic metadata, are kept in a secure form for a period of twenty years at the Certification Authority. This procedure satisfies the requirements of Art. 32, paragraph 3, letter a) of the CAD.

The person who identifies the Subject, perform identification by checking the claimed identity against valid document, provided that it contains a recent and recognizable photograph of the owner, his signature and the Stamp, issued by an Government Authority.

It is the right of the person performing the identification to exclude the admissibility of the document used by the Holder if it is deemed unsuitable to provide unambiguous identification.

The method of identification and registration may be used for the issue of Qualified Certificates to natural persons (§ 4.1) and legal person (§ 4.2).

4.3.2 IDENTIFICATION CARRIED OUT BY THE INTERESTED THIRD PARTY WHO SIGNED AN AGREEMENT

The Third Interested Person, in the person of the representative, collects and submits to the Certification Authority the following signed documents:

A) Certificate Issuance Application Form
B) Copy of a valid identity document or of an equivalent valid recognition document accepted under national or international regulation.

These documents can be signed by mean advanced, qualified, digital or autographed electronic signatures.

4.3.3 IDENTIFICATION CARRIED OUT BY A NOTARY OR OTHER PUBLIC OFFICER;

Whereas Subscriber is the same of the Subject, it's possible to compile the request for issuing certificates and other application form (available from "Documents" section of the website https://docs.namirialtsp.com/ in presence of a Public Officer (Notary or equivalent). The Subscriber will compile and sign all application forms in presence of a Public Officer and ask for a validation of the applied data and signatures

The subscriber sends to the Certification Authority:

(A) the Certificate Issuance Form (in original);
(B) the Declaration of the notary officer (in original);
(C) Copy of a valid identity document or of an equivalent valid recognition document accepted under national or international regulation.

4.3.4 IDENTIFICATION CARRIED OUT BY AN OPERATOR ENDORSED OF THE IDENTIFICATION AND REGISTRATION ACTIVITIES (IR)

In this scenario, the identification is carried out by a person qualified as Registration Appointee (IR) belonging to a third party, and it's required the physical presence of the Subscriber (which shall be the same of the Subject). These entities (IRs) may operate after the subscription of a contract between the Certification Authority and the Third Company. The latter indicates his / her staff, who is identified as a Registration Appointees (IR) and who has to act under the procedures established and contained in this CPS concerning: identification and registration of the applicant's data, verifying that the registration form and certificate request are correctly filled in, signing of the contract and, when provided, direct delivery of the device.
The Subscriber has to provide:

- the Registration Form and Request for the Certificate containing Subscriber's data, hopefully already provided in electronic mode (eg by web pre-registration procedure);
- Identification document;
- Term and conditions
- Privacy Statement
- Signature device, if required

In order to identify correctly the Subscriber, the IR has to adopt identification procedure provided in Section 4.1. It' required that the document provided is the same of the one loaded during web pre-registration procedure.

Certificate Issuance Application Form shall be signed by the Subscriber in presence of the IR.

In any case, the responsibility for the registration, identification and validation operations is the Certification Authority.

4.3.5 IDENTIFICATION THROUGH THE RECOGNITION ALREADY CARRIED OUT BY A FINANCIAL BROKER OR OTHER PARTY PERFORMING FINANCIAL ACTIVITY

According to this method, the Certification Authority makes use of the recognition already carried out by a financial broker or other party performing financial activities, which, under the anti-money laundering regulations from time to time in force, is obligated to identify its customers.

The data used for the recognition of the Applicant are issued by the financial party in accordance with specific national regulation according to the Directives [XLI], [XLII] and [XLIII].

4.4 CERTIFICATE ISSUANCE

If the results of the verifications reported on the previous section are positive, the Registration operator will send to the CA a certificate issuance request. The process of generating key occurs inside the signature device.

The Certification Authority issues certificates for

Natural persons:

- independent (standard certificates);
- associated (belonging) to Organizations;
- associated (belonging) to Professional Orders.

Legal person:

- for use as Electronic Seal (standard certificates);

Certificates may be associated to:

1. Signing keys generated for signing through personal signature devices (refer to section 5.4.5 of [XXVIII] for more details);
2. Signing keys generated for signature through automated subscription applications (refer to section 5.4.6 of [XXVIII] for more details);
3. Signing keys generated for use through remote signature applications (refer to section 5.4.7 of [XXVIII] for more details);
4. Signing keys generated for use through Electronic Seal (refer to section 5.4.8 of [XXVIII] for more details)
5. Signing keys generate for disposable certificate (refer to [XXXIX] for more details)

For representation of dates and time, Namirial use the UTCTime declared in RFC 5280 with a precision of one (1) minute. For more details about key pair generation modalities, refer to section 5.3 of [XXVIII].

4.5 CERTIFICATE ACCEPTANCE

By using the certificate generation activation described in internal procedure (Certificate Life Cycle Management), the Certificate is automatically generated and accepted.

4.6 KEY PAIR AND CERTIFICATE USAGE

The certificate Owner must safeguard its private key, paying attention to avoid its disclosure to third parties. Namirial will provide an appropriate subscription agreement (Terms and Condition), which highlights the owner's duties regarding the private key protection. The private keys must be used only as specified in the fields "keyUsage" and "extendedkeyUsage", as reported on the related digital certificate. The responsibilities related to the use of keys and certificates include the ones addressed below. Certificates shall be only used as prescribed by the CP and Terms and Conditions. Any different usage is forbidden. Specifically, they may not be used for infringing rights or for violations of any kind of laws or regulations.

4.7 CERTIFICATE RENEWAL

The renewal must be made, necessarily, before the certificate is expired. The procedure can be used for the renewal of a previous certificate issued by the Certification Authority in cases where the Applicant 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 PKCS # 10 certificate request.

The rekeying procedure requires at least following steps:

- Updating of some Subject's data (i.e. Title, Organization, etc..) if the there is a request by an entity with which the Subject is associated. In this scenario, the entity will provide new information;
- Take assurance that applicant has the sole control of the Q/SSCD by mean to perform signature with previous certificate
- Generation of a new key pair in Q/SSCD and issuing of a new certificate
- Registration of the enrollment relevant events inside CA event logging and audit system

4.8 CERTIFICATE MODIFICATION

A certificate being signed by the issuer CA cannot be modified. In order to remediate to potential inaccuracies incurred during the generation process, it is necessary to issue a new certificate and, for security reasons, revoke the previous one. In case of the issued certificate reports incorrect information, due to mistakes made by the CA or the RA, the wrong certificate will be revoked and a new one will be promptly issued without any additional charge for the client and without requesting further information to the client. On the other hand, if the issued certificate reports incorrect information due to mistakes made by the Subscriber (e.g. incorrect compilation of one or more fields on the application form), the wrong certificate will be revoked.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The suspension of a certificate causes a temporary block of its validity, starting from a given time (date/time).
The revocation of a certificate causes the anticipated expiration of its validity, starting from a given time (date/time). The revocation of the certificate is irreversible and not backdated. The suspension and the revocation of a certificate are carried out by generating and publishing a new CRL (Certificate Revocation List) which includes the serial number of the

suspended/revoked certificate. The CRL is freely available to anyone who needs to verify the certificate state. The publication of CRL takes place, however, at maximum every 1 hour.

The Certificate Suspension / Revocation can be performed in the following ways:

1. directly by the holder using the Private Area on the site www.firmacerta.it
2. by the LRA or Namirial Registration Authority

In case no. 2. the Holder shall submit the request to the RA/LRA in person or send a written request to the Certification Authority.
In the first case, the RAO will perform the requested operation after verifying the identity of the applicant, according to §3.
In the second case, the Holder is required to sign the request Revocation, whit a photocopy of an identity document in validity, and attached to the request, and delivered directly to the Certification Authority. For address information please refer to §1.3.1
As an alternative, the request can be submitted via certified mail to Certification Authority certified e-mail address (see §1.3.1)

4.10 CIRCUMSTANCES FOR REVOCATION

The following conditions may cause the revocation of a digital certificate:

- loss, theft, modification, not authorized disclosure or any other damages of the certificate subject's private key;
- alteration of information reported on the certificate and related to the certificate subject;
- errors during registration process;
- existence of judicial proceedings (e.g. following illegal activities committed by the certificate owner entity);
- cessation of business by the certificate owner entity;
- specific request made by the owner (e.g. due to end of use of the certificate);
- breach of contract by the client (e.g. failure to pay).
- Namirial can revoke the certificates in case of non-compliant suspect uses, upon notice to the relying parties, except in urgent cases.

4.10.1 CIRCUMSTANCES FOR SUSPENSION

The following conditions may cause the suspension of a digital certificate:

- The subject or the legal person associated with the subject in identification process (e.g. subscriber), , for any reasons and in any moment, may request the certificate suspension.
- Namirial can suspend the certificates in case of non-compliant suspect uses, upon notice to the relying parties, except in urgent cases.

4.11 CERTIFICATE STATUS SERVICES

Namirial CA provides control services to verify the state 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 the involved entities by publishing the Certificate

Revocation List (CRL). The CA makes also available an OCSP (On-line Certificate Status Provider) at following link: https://sws.firmacerta.it/. The CRL is signed at the moment of its issuance, with the CA certificate.

4.12 END OF SUBSCRIPTION

The service contract, subscribed by the CA and the client, is considered terminated at the following dates:

- certificate expiration date;
- certificate revocation date.

4.13 KEY ESCROW AND RECOVERY

Key escrow is not allowed for the CA key. CA private keys are backed up for recovery purposes, outside of HSMs, and confidentiality and integrity controls are guaranteed by the HSM itself. All private key backups of the CA are stored inside a backup storage.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Policies, responsibilities and operating procedures are defined to access in protected areas of Namirial and to access to information and application system. In these areas, physical protection devices are implemented to minimize risks related to unauthorized accesses. The protection is implemented by access control systems and video surveillance systems located in the most critical points and marked by specific signs. A Disaster Recovery Site is placed in Milan with a level of physical security at least similar respect to the primary site.

5.1 PHYSICAL CONTROLS

The working areas are under different control measures, related to risks, goods' value and information in the environment. An organized authorization process, related to the kind of accessed area, manages all the accesses.

5.1.1 SITE LOCATION AND CONSTRUCTION

Namirial performs its CA operations from secure, commercial data center that are equipped with logical and physical controls that make Namirial CA operations inaccessible to non-trusted personnel. Namirial operates under a security policy designed to detect, deter, and prevent unauthorized access to Namirial operations.

5.1.2 PHYSICAL ACCESS

Namirial protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of Namirial CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of the buildings requires the use of a secure device. The buildings are under constant video surveillance.
The access to Datacenter's room requires strong authentication system. Externally to the Data Center the regulations for access and behavioral standards to be kept within the Data Center are affixed.

5.1.3 POWER AND AIR CONDITIONING

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and electrical generators provide redundant backup power. Namirial's Datacenter facilities use multiple systems for heating, cooling and air ventilation.

5.1.4 WATER EXPOSURES

A detection system that detects the presence of liquid through sensors and alarms in case of flooding.

5.1.5 FIRE PREVENTION AND PROTECTION

The data centers are equipped with fire suppression mechanisms.

5.1.6 MEDIA STORAGE

Namirial protects its media from accidental damage and unauthorized physical access.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel related to identity vetting and the issuance and revocation of certificates. The functions and duties performed by persons in trusted roles are distributed to allow that just a person cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations by himself. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the Namirial PKI's operations.
Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually. Trusted roles include roles that involve the following responsibilities:

- Security Officers (Security Practicers): Overall responsibility for defining security practices. Security Officers ensure the confidentiality, integrity and availability of data and business applications related to the Digital Signature.
- Security Officers (Authorization): Overall responsibility for authorizing System Administrator and System Operators in the implementation of the security practices
- System administrators: Authorized to install, configure and maintain the Namirial trustworthy systems for service management
- System operators: Responsible for operating the Namirial trustworthy systems on a day-to-day basis. Authorized to perform system backup.
- System Auditors: Authorized to view archives and audit logs of the Namirial trustworthy systems.
- Registration and revocation officers: Responsible for keys management life cycle with reference to revocation and suspension services of certificates for digital signature keys.
- Service Responsible Officer: Overall responsibility for Digital Signature Service, operating manual and the processes for the life cycle management, in according with specific regulatory aspects.

More specific information can be found in internal policies.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

In case of tasks related to critical functions, Namirial requires that at least two people acting in a trusted role to avoid that a person can act by himself. When this mechanism is active, two authorized persons are required to apply it where appropriate. More information can be found in internal policies.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All personnel are required to authenticate themselves to CA and RA systems before accessing to systems necessary to perform their trusted roles.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

Roles requiring a separation of duties, that include:

1) The verification of information in CA certificate generation (root and intermediated ones, when applicable);
2) The approval of CA certificate applications;
3) Most duties related to CA key management or CA administration.

Namirial specifically designates individuals to the trusted roles defined above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. Namirial's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 PERSONNEL CONTROLS

The employees have many years of experience in definition, development and management of PKI services and have received an adequate level of training on procedures and tools, that can be used in various operational phases.
Namirial employees and contractors:

- possess the necessary expertise, reliability, experience, and qualifications and have received training regarding security and personal data protection rules as appropriate as the offered services and their job function;
- are able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of both;
- are updated on new threats and current security practices.

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Namirial hires personnel with the highest levels of integrity and competence. A comprehensive set of personnel screening activities and related evaluation criteria has been defined to be able to detect risks in this matter. There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of certificates.

5.3.2 BACKGROUND CHECK PROCEDURES

Namirial verifies the identities and performs a background check of each person to schedule someone for a trusted role. Namirial, also, requires that each person must appear in -person in front of a human resources employee who is responsible to verify identities. The human resources employee verifies the identities using the required forms of government -issued

photo identification. The Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background.

5.3.3 TRAINING REQUIREMENTS

All new Namirial personnel receive basic security awareness training during their introduction process. On top of that, a dedicated on-the-job training is provided to all Namirial personnel involved in specific tasks asdescribed throughout this Certification Practice Statement.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Personnel must maintain high skill levels through industry-relevant training sessions and performance programs in order to continue acting in trusted roles. Namirial updates all individuals acting in trusted roles about any changes to Namirial's operations. If Namirial operations change, Namirial will provide documented training, in accordance with an executed training plan, to all personnel acting in trusted roles.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

In case of job rotation, Namirial performs a security check, including a verification of credentials at level of networks, systems, applications or other assets used as well as the facility and zone access authorizations.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Namirial employees and agents, who don't comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Independent contractors, who are assigned to perform trusted roles, are subject to specific duties and requirements for each role and are subject to sanctions as specified in this section.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the present document and operational documentation needed to maintain the integrity of Namirial CA operations. Personnel have also access to information on internal systems and to security documentation, identity vetting policies and procedures, discipline -specific books, treatises and periodicals, and other information.

5.4 AUDIT LOGGING PROCEDURES

Namirial records all relevant information concerning data issued and received by Namirial and keeps the records accessible for an appropriate period, with the purpose of providing evidence in legal proceedings and ensuring service continuity. In particular:

- The confidentiality and the integrity of current and archived records concerning operation of services are maintained;
- Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices;
- Records concerning the operation of services are made available if required for the purposes of providing evidence of the services correct operation and for the purpose of legal proceedings;
- The exact time of significant Namirial environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log shall be synchronized with UTC at least once per day;
- Records concerning services are held for an appropriate period in order to provide necessary legal evidence as notified in the Namirial terms and conditions;
- The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period in that they are required to be held.

5.5 RECORDS ARCHIVAL

Namirial does and keep accessible records including all the activities and all relevant information concerning data issued and received by Namirial.
The CA keeps the records accessible for an appropriate period, with the purpose of providing evidence in legal proceedings and ensuring service continuity. These records are accessible even in the case in which Namirial have ceased its activities.
The main evidence collected are:

- Issuance requests;
- The documentation provided by Subscribers;
- The CSR (Certificate Signing Request) provided by Subscribers;
- Subscribers and Subject personal data (if they are different entities);
- Requests for revocation or suspension;
- All certificates issued;
- Audit logs for at least 20 years.

More information can be found in internal policies.

5.6 KEY CHANGEOVER

In case of the end user (owner) decides to use a new key, he must necessarily request a corresponding new certificate.

5.7 COMPROMISE AND DISASTER RECOVERY

Namirial documents applicable incident, compromise reporting and handling procedures. Namirial documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted. Namirial establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.
More information can be found in internal policies.

5.8 CA OR RA TERMINATION

Namirial defined an up-to-date termination plan. In particular, according to the internal procedure, Namirial shall:

- inform at least 60 days before the termination the following entities about the termination: all subscribers and other entities with which Narmirial has agreements or other form of established relations, among which relying parties, Namirial and relevant authorities (the National Supervisory Body AgID, and the certification body). In addition, this information shall be made available to other relying parties;
- terminate all subcontractors' authorization to act on behalf of Namirial in carrying out any functions related to the process of issuing trust service tokens;
- transfer obligations to a reliable party for maintaining all the necessary information to provide evidence of Namirial operation for a reasonable period, unless it can be demonstrated that Namirial does not hold any information;
- private keys, including backup copies, shall be destroyed, or withdrawn, to assure that the private keys cannot be retrieved;
- make arrangements to transfer provision of trust services for its existing customers to another Trust Service Provider.

More information can be found in internal procedure "Termination Plan".

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION

The CA issues the qualified certificate in according with the Regulation (EU) No 910/2014. The certification keys used for signing certificates are generated by means of devices and procedures that ensure uniqueness, secrecy and resilience of the private key. The CA uses at least 4096-bit cryptographic key pair generated within HSM (Hardware Secure Module).
The HSMs and procedures ensure that:

- the key pairs are generated individually, always in single copy;
- the key pairs meet requirements imposed by generation algorithms and RSA verifications because the HSMs have a key pair generation internal engine of RSA and DSA;
- the generation of all possible key pairs is equiprobable;
- the person who activates generation procedures is always identified;
- the generation of key pairs occurs exclusively inside the HSM, that is responsible for preservation of private keys;
- if the devices are prepared or managed by a third party, Namirial verifies that this third party is meeting the appropriate requirements.

In the certificate activities, Namirial uses the RSA algorithm.
The generation of key pairs of certification by CA is under dual control, in according to Key Ceremony procedure.
In addition, the NAMIRIAL stops issuing new certificates at an appropriate date prior to the expiration of the CA's certificate such that no Subscriber certificate expires after the expiration of the CA certificate.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

The key pairs used by the CA to sign certificates and CRLs are stored in a HSM (Hardware Security Module) of high quality, provided with safety certification in accordance with FIPS 140-2.
The HSM used by the NAMIRIAL is certified at the level EAL4+of the Common Criteria and qualified by the ANSSI at the highest level.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

Namirial uses appropriately the CA private signing keys and doesn't use them beyond the end of their life cycle.
In particular:

- CA signing key used for generating certificates and/or issuing revocation status information, is not used for any other purpose;
- The certificate signing keys are only used within physically secure premises;

- The use of the CA's private key is compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with section 6.1;
- All copies of the CA private signing keys will be destroyed at the end of their life cycle.

6.4 ACTIVATION DATA

Activation Data consists in activation of all systems involved in delivering of digital signature; these activities are managed by Operative Guide.

6.5 COMPUTER SECURITY CONTROLS

The operating systems used by the CA to manage certificates have a level of security appropriate and shall follow the hardening procedures set out by Namirial. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuses of Namirial assets.
The access events to systems are recorded, as described in section 5.4 and 5.5.
Local network components are kept in a physically and logically secure environment and their configurations are periodically checked for compliance with the requirements specified by Namirial.
Multi-factor authentication are implemented for all accounts capable of directly causing certificate issuance.
Access control on attempts to add or delete certificates and modify other associated information (e.g. revocation status information) are implemented.
Continuous monitoring and alarm facilities are provided to enable Namirial to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.6 LIFE CYCLE SECURITY CONTROLS

Namirial uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
In particular:

- An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by Namirial;
- Change control procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the Information security policy.
- The integrity of Namirial systems and information are protected against viruses, malicious and unauthorized software.
- Media management procedures are defined and implemented in order to protect media from damage, theft, unauthorized access, obsolescence and deterioration of media within the period of time that records are required to be retained.
- Organizational Procedures are defined and implemented in order to manage all trusted and administrative roles that impact on the provision of services.

In order to issue and manage CA keys in a secure way, Namirial use HSM (Hardware Security Module), which:

- Are tamper-proof and guarantee the protection of the Keys According to the Security Levels expected from the Regulation and the high technological standard;
- prevents any unauthorized attempt of Reading, duplication, extraction of the private key;
- keeps the Private Key to ensure its protection, privacy and safe storage for the whole Life Cycle;
- identifies operators;

6.7 NETWORK SECURITY CONTROLS

Namirial's network architecture is structured on several levels in order to create separated network environments, addressed to host systems related to different functions and characterized by different levels of criticality.

The access and the network traffic security is realized by the application of protection policies implemented on the firewall systems located on different network levels.

The implementation requests of new rules on the firewall, are managed through a change request.

The activation of rules that cause a high impact level, is dealt with the Security Officer. The CA private network security is realized not just by the perimeter protection systems described backwards, but also by a specific configuration, which maintains the internal addresses as reserved. The communication between the management stations and the systems are protected by means of tools which assure the authentication among the parts and their privacy.

Potential remote links take place on an encrypted VPN channel and request the authentication through Username, Password and an authentication token (OTP).

The communication among application forms of Namirial's PKI platform occurs through cryptographic channels.

The communication among users who access to the online services takes place through TLS/SSL connections with SHA - 256 algorithm.

The system implemented to manage users' accesses gives both AAA (authentication, authorization, access) and profiling mechanisms and the communication channel encryption with TLS/SSL protocol.

The system is also supposed to manage the accesses that come from the consultants who work on the internal Namirial Network.

6.8 TIMESTAMPING

All processing systems used by the CA are aligned with the UTC time and synchronized with a reliable source (through NTP server).

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The certificates are compliant with:

- international standard ISO/IEC 9594-8:2005 [X.509 version 3];
- public specification 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 issuing CA fills the issuer and the subject fields of each certificate issued after the adoption of requirements, defined above, in accordance with what is stated in the Certificate Policy. With the issuance of the certificate, the CA declares to have followed the procedure described in its CP to prove that, at the date of certificate issuance, all information related to the subject were accurate.

7.1.1 QUALIFIED CERTIFICATES CAS

7.1.1.1 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
Extentions	
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 4 - Namirial EU qualified e-signature

7.1.1.2 NAMIRIAL QUALIFIED E-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
Extentions	
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 5 - Namirial qualified e-signature

7.1.1.3 NAMIRIAL CA FIRMA QUALIFICATA

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 Firma Qualificata"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extentions	
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 6 - Namirial CA firma qualificata

7.1.1.4 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
Extentions	
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 7 - Namirial EU Qualified CA

7.1.2 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

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 person) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal person).* **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):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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:` http://crl.namirialtsp.com/CA4K.crl 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 8 - 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

7.1.3 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 person) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal person).* **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):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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`: http://crl.namirialtsp.com/CA4K.crl 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 9 - QCP-L policy for EU qualified certificate issued to a legal person

7.1.4 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)

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 can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** *Title contain an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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:` http://crl.namirialtsp.com/CA4K.crl 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 10 - 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)

7.1.5 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

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 can't be used to retrieve Subject's Identity*

	serialnumber (OID 2.5.4.65): *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** *Title contain an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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:` http://crl.namirialtsp.com/CA4K.crl 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

7.1.6 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

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	60 min
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 can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** *Title contain an unique identification code assigned to the Subject by the CA*

SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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`: http://crl.namirialtsp.com/CA4K.crl 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

7.1.7 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

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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 can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** *Dn_Qualifier contain an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** *Title contain an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces 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`: http://crl.namirialtsp.com/CA4K.crl 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

7.2 CRL PROFILE

The CRLs is compliant with the public specification RFC 5280.

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 Valure	Signature computed on the hash of the DER encoding of CertList.

Table 14 - CRL profile

7.3 OCSP PROFILE

The OCSP protocol is compliant to the public specification RFC 6960.
More in details, here below, follow the list of fields contained in OCSP Responses provided by Namirial OCSP Responder

responseStatus	Choise 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 Reponder'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	Choise between: 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	sha1WithRSAEncryption
Signature	Signature computed on the hash of the DER encoding of ResponseData.
Certs	OCSP Responder's Certificate CA's Certificate

Table 15 - OCSP profile

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Namirial is a Trusted Service Provider for the qualified digital signature, accredited by a certification body, accredited by Accredia. The conformity assessment report is sent to the AgID. As a result, Namirial is subject to a compliance assessment ("surveillance") by AgID and is required to carry out periodic internal inspections.

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Namirial auditor is responsible for internal audits on Digital Signature services, verifying that the processes compliance in according to requirements of legislation and regulations of the corporate procedures. The internal audit is taken at least once a year. Third party audit performed by a certification body, accredited by Accredia, is carried out with annual periodicity.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSORS

Internal audit are carried out by Namirial auditors, qualified as a security auditors in accordance with the international standard ISO 27001 and ISO 9001.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

There is no relationship between Namirial and the certification body that may in any way influence audit results in favor of Namirial. Namirial auditors are employees who reports directly to the Management and are independent structure responsible in comparison with Service Responsible.

8.4 TOPICS COVERED BY ASSESSMENT

The certification body carries out conformity assessment of Namirial activities, supervised by AgID, that operate in respect of EU Regulation 910/2014, known as "eIDAS-Electronic Identification Authentication and Signature".
Internal audit is mainly aimed at verifying the integrity of the "Journal of Control" (Audit log), and the respect of CA's operating procedures.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In case of compliance deficiencies, Namirial adopts the necessary corrective measures that are tracked until resolution.

8.6 COMMUNICATION OF RESULTS

Audit results, carried out by the certificatory auditor, are shared with the interested CA through a conformity assessment report. The internal audit result is communicated to the Management and to the Responsible of the organizational structure in charge for providing the CA service.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The maximum fees of the service are published on the website: https://shop.namirial.com. Different conditions can be negotiated on a custom basis, depending on the required volumes.

9.2 FINANCIAL RESPONSIBILITY

Namirial has signed an appropriate insurance to cover the risks of the activity and any damage deriving from the certification service.

9.3 PROTECTION OF CONFIDENTIALITY AND PROCESSING OF PERSONAL INFORMATION

Namirial is the owner of personal information collected in the process of identification and registration of Entities who request certificates. Therefore the information is treated with the maximum confidence and in accordance with the provisions of the requirements identified in ETSI EN 319 411-1 [2], clause 6.8.4. In case of the identification and registration activity of users is obtained from a delegated structure (RA), the latter is described as a "processor".

9.3.1 ARCHIVES CONTAINING PERSONAL INFORMATION

The file containing personal data is the registration database.
The archives listed above are managed by the manager of registration and are adequately protected against unauthorized access, in accordance with the provisions of the Italian legislative Decree no. 196 dated June 30, 2003 [DLGS196] and subsequent updates

9.4 INTELLECTUAL PROPERTY RIGHTS

This Document is property of Namirial, which reserves to itself all the rights related to it. The certificate owner maintains all the rights over the own trademark (brand name) and on his domain name. In relation to the properties of other data and information it is applied the law in force.

9.5 OBLIGATIONS AND GUARANTEES

9.5.1 CERTIFICATION AUTHORITY

The CA is committed 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 service of suspension or revocation of certificates;
- Ensure that the owner held, at the time of the certificate issuance, the corresponding private key;
- Promptly report the possible compromise of the private key;
- Provide clear and complete information on the procedures and requirement of the service;
- Provide a copy of this document to anyone who requests;
- Ensure that the provision of digital signature services are accessible for persons with disabilities;
- Ensure the treatment of personal data compliant with current legislation;
- Ensure the availability of the service except in the case of programmed maintenance activity, that is previously notified to the subscribers;
- Provide an efficient and reliable information service on the status of certificates.

9.5.2 REGISTRATION AUTHORITY

The Registration Authority treats personal data of the subject with the maximum confidence and in accordance with the provisions of the Italian legislative Decree no. 196 dated June 30, 2003 [DLGS196] and subsequent updates.
Namirial is starting a plan to improve accessibility of the service for the disabled through Web Content Accessibility solutions.

9.5.3 SUBSCRIBER OR OWNER

The Subscriber or owner has the obligation to:

- Read, understand and fully accept this document;
- Request the certificate provided by this document;
- Generate in a safe way the public-private key pair, using a trustworthy system;
- Provide to CA accurate and truthful information in the registration phase;
- Adopt technical and organizational measures designed to prevent the impairment of the private key;
- Ensure the privacy of reserved codes received from the CA;
- Demand immediate suspension of the certificate in case of suspected or confirmed impairment of the private key;
- Immediately request the revocation of the certificate in the event that one or more information contained in the certificate lose validity;
- Following the issue and until the expiration or the revocation of the certificate, promptly notify the CA of any changes to the information provided in the application phase;

9.5.4 END USER

The end users, so all the entities (different from the Subscriber or the Subject) that rely on certificates issued under this document, have an obligation to:

- perform a reasonable effort to obtain sufficient information on the functioning of certificates and PKI;
- check the status of certificates issued by Namirial on the basis of this CP;
- rely on a certificate only if it has not expired, suspended or revoked.

9.6 DISCLAIMERS OF WARRANTIES

The explanations identified in Trust Service Practice Statement document is applied.

9.7 LIMITATIONS OF LIABILITY

The explanations identified in Trust Service Practice Statement document is applied.

9.8 INDEMNITIES

The explanations identified in Trust Service Practice Statement document is applied.

9.9 TERM AND TERMINATION

The explanations identified in Trust Service Practice Statement document is applied.

9.10 COMMUNICATIONS

The explanations identified in Trust Service Practice Statement document is applied.

9.11 DISPUTE RESOLUTION PROCEDURES

The explanations identified in Trust Service Practice Statement document is applied.

9.12 GOVERNING LAW

The explanations identified in Trust Service Practice Statement document is applied.

9.13 COMPLIANCE WITH APPLICABLE LAW

The explanations identified in Trust Service Practice Statement document is applied.