Certification Authority

PKI Disclosure Statement

Category	**CA**	Docuement ID	**NAM-CA-PDS**	**Namirial S.p.A.**
Written by	**Simone Baldini**	Confidentiality note	**Public Document**	Legal Representative
Verified by	**Giuseppe Benedetti**	Version	**1.0**	**Davide Ceccucci**
Approved by	**Davide Ceccucci**	Issuance date	**26/05/2017**	CECCUCCI DAV 2017.06.05 15:36:44 CN=CECCUCCI DAVIDE C=IT O=NON PRESENTE 2.5.4.4=CECCUCCI RSA/2048 bits

Namirial S.p.A.

Sede legale, direzione e amministrazione 60019 Senigallia (AN) - via Caduti sul Lavoro, 4
C.F./ISCR. REG. IMPR. ANCONA N.02046570426 - P.I. IT02046570426 - CAP. SOC. € 6.500.000,00 i.v.
Tel. 07163494 s.a. - Fax 199.418016 - info@namirial.com - www.namirial.com

– This page is intentionally left blank –

INDEX

HISTORY OF CHANGES

VERSION	1.0
Date	26/05/2017
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]	Addendum Manuale Operativo – Certificati di Firma Disposable

1 INTRODUCTION

This document is the PKI Disclosure Statement, as required by European standard ETSI EN 319 411-1, related to the certification service offered by the Trust Service Provider Namirial S.p.A..
In the following, the certification service is also referred to by "CA service" (Certification Authority). The 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" is referred to by "eIDAS Regulation".
This document does not substitute or replace the Terms and Conditions of the CA service nor the Certification Practice Statement (CPS) published on the CA website (see further on).

2 CA CONTACT INFORMATION

The CA can be contacted at the following address:

VIA CADUTI SUL LAVORO, 4
60019 - SENIGALLIA (AN)
TEL: 071.63494
FAX: 071.60910

Web site: https:// http://www.namirialtsp.com
Info mail: firmacerta@namirial.com
Tel. +39 071.63494
Fax +39 071.60910

For any queries regarding this PKI Disclosure Statement or other documents of the Namirial S.p.A. CA service, please send an email to firmacerta@sicurezzapostale.it.

To request revocation of a certificate, follow the on-line procedure described in the CPS (requires the credentials provided at certificate issuance time). Alternatively, contact the Namirial S.p.A. customer support team at fax number +39.071.60910 or send an email to firmacerta@namirial.com. For further information, refer to the CPS published on the CA website.

3 CERTIFICATE TYPES, VALIDATION PROCEDURES AND USAGE

Namirial S.p.A. issues qualified certificates according to European standard ETSI EN 319 411 , EN 319 412 and other related standards. Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), at the conditions published on the CA website.

All certificates are signed with hashing function SHA-256. For further information on the supported certificate policies (e.g. their respective OIDs and other features) see the documentation published on the CA website at https://docs.namirialtsp.com/.

The issuing CAs certificates of Namirial S.p.A. are published on the CA website and on the website of AgID (Agenzia per l'Italia Digitale) at www.agid.gov.it (see the List of Trust Service Providers).

To allow validation of certificates, the CA makes available both the Certificate Revocations List (CRL) and an on-line status checking service based on the OCSP standard. The URLs of both are included in all certificates, respectively in the CRLDistributionPoints and AuthorityInformationAccess extensions.

4 RELIANCE LIMITS

Certificates are issued for advanced and qualified electronic signatures and electronic seals.
Limitations on the use of certificates may be specified within certificates themselves, in the UserNotice attribute of the CertificatePolicies extension.
Limitations on the value of transactions in which the certificate can be used may be specified in certificates, within the qCStatements certificate extension, by means of the QcEuLimitValue item.
All records pertaining to the life-cycle of certificates, as well as all the CA service audit logs, are retained by Namirial S.p.A. for 20 years.

5 OBLIGATIONS OF SUBSCRIBERS

The certificate subscriber must:

- provide complete, accurate and truthful information to the CA at the time of certificate request;
- use its private keys only for the purposes and in the ways allowed by the CPS;
- adopt suitable measures to prevent any non-authorized use of its private keys;
- (for certificates that require use of a signature device) if it generates its private key by itself, generate it within a signature device approved by the CA;
- up to the date of certificate expiration, promptly inform the CA in the following cases:
    - its signature device gets lost, is stolen or gets damaged;
    - it has lost the exclusive control of its private key, e.g. because of compromise of the activation data (e.g. PIN) of its signature device;
    - some information contained in its certificate is inaccurate or no longer valid:
- in the case of compromise of its private key (e.g. because the PIN of its signature device gets lost or disclosed to non-authorized people), immediately cease any use of such private key and make sure that it will no longer be used.

For further information, please refer to the CPS.

6 CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

All those who rely on the information contained in certificates (in short, "Relying Parties") must verify that certificates are not suspended or revoked. Such verification can be performed by consulting the list of revoked certificates (CRL) published by the CA or by querying the OCSP service provided by the CA, at the addresses (URLs) contained in certificate themselves.

7 LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

For warranty and liability limitations, please refer to the Terms and Conditions of the Qualified CA service published on the Namirial website at https://docs.namirialtsp.com/.

8 APPLICABLE AGREEMENTS, CPS, CP

The agreements and conditions applying to the CA service are found in the following documents, published on the Namirial S.p.A. website at https://docs.namirialtsp.com/:

- Certification Practice Statement (CPS) of the Qualified CA service
- General Terms and Conditions of the Qualified CA service

The supported Certificate Policies (CP) are described in the CPS; see also section 3 above.

9 PRIVACY POLICY

Namirial complies with Italian law on privacy (D.Lgs. 196/2003), with EU Regulation No. 679/2016, and with the recommendations and provisions of the Italian Data Protection Authority. For further information, refer to the general Terms and Conditions of the Qualified CA Service published on the Namirial S.p.A. website at h https://docs.namirialtsp.com/.

All records relating to qualified certificates issued by Namirial S.p.A. (e.g. evidence of the identity of subscribers; certificate issuance requests, including acceptance of the Terms and Conditions; certificate revocation re- quests; etc.) are retained by Namirial S.p.A. for 20 years.

10 REFUND POLICY

For the refund policy, please refer to the general Terms and Conditions of the Qualified CA service published on the Namirial S.p.A. website at https://docs.namirialtsp.com/.

11 APPLICABLE LAWS, COMPLAINTS AND DISPUTE RESOLUTION

The CA service provided by Namirial S.p.A. is subject to Italian and European law. The applicability, execution, interpretation and validity of the CPS are governed by Italian law and by directly applicable European laws, irrespective of the contract or other choice of legal provisions and without the need to establish a commercial contact point in Italy. This choice is intended to ensure uniformity of procedures and interpretations for all users, regardless of where they reside or use the service.

For all legal disputes related to the Namirial S.p.A. CA service, where Namirial S.p.A. is plaintiff or defendant, the Court of Ancona shall have exclusive jurisdiction, with the exclusion of any other court and excluding any hypothesis wherein the law provides for the competence of Consumer's court.

12 TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

Since November 3, 2010, Namirial S.p.A. is a Certification Service Provided (Certification Authority) enlisted in the public registry of accredited CAs maintained by Agenzia per l'Italia Digitale (AgID).

As of July 1st, 2016, Namirial S.p.A. is a Trust Service Provider of certification and electronic time-stamping services according to the eIDAS Regulation, and therefore enlisted in the Italian List of Trust Service Providers (TSL) published by AgID.

Namirial S.p.A.' CA service is subject to conformity assessment every two years, according to European norms ETSI EN 319 411-1 and ETSI 319 411-2, by an independent, qualified and accredited auditor, as required by the eIDAS Regulation.