NamirialSpa
Trust Service Provider

Trust Services

Practice Statement

*Protocol n. **18154** of **11/07/2016 – Official Register AOO AOO-AgID***

Category:	**Practice Statement**	Document No.:	**NAMTSP-TSPS-MO-v1.1.docx**
Written by:	**TSP Director**	Confidentiality notice:	**Public Document**
Verified by:	**Internal Auditor**	Version:	**1.1**
Approved by:	**CEO**	Issue date:	**08/07/2016**

Namirial S.p.A.

Chief Executive Officer

(Dr. Davide Ceccucci)

CECCUCCI DAV
2017.02.28 17:09:41

CN=CECCUCCI DAVIDE
C=IT
O=NON PRESENTE
2.5.4.4=CECCUCCI

RSA/2048 bits

– This page is intentionally left blank –

Table of Contents

History of changes

Version	1.0
Date	20/06/2016
Reasons	First release
Modifications	---

Version	1.1
Date	08/07/2016
Reasons	Corrections
Modifications	§ 5.5.2

1 Introduction

This document is the Namirial S.p.A. Trust Services Practice Statement (hereafter NAMIRIAL PS) and outlines the principles and practices common to all Namirial's trust services. This document applies to all entities participating in or using Namirial's trust services. This document describes the practices used to comply with the Regulation (EU) No 910/2014 (eIDAS).

Inspired by the ETSI EN 319 400 series, NAMIRIAL has divided its documentation into three parts:

- NAMIRIAL Trust Services Practice Statement (NAMIRIAL PS) describes general practices common to all trust services (this document);
- parts that are specific to the certification service (i.e. certificate policies or certification practices statement) are described within the service-based policy and/or practice statement (i.e. the operative manual for the certification service required for national laws);
- parts that are specific to the Time-Stamping service are described within the Time-Stamping Authority Practice Statement.

Pursuant to the IETF RFC 3647 [4] this document is divided into nine parts. To preserve the outline specified by RFC 3647 [4], section headings that do not apply have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them. Each first-level chapter includes reference to the corresponding chapter in ETSI EN 319 401 [2].

1.1 Overview

NAMIRIAL operates a Public Key infrastructure in order to provide Trust Services. NAMIRIAL is currently using different root certification authorities, one for each service. NAMIRIAL does not use Subordinate CA-s.

The Namirial S.p.A. Trust Services Practices Statement (NAMIRIAL PS) presents the criteria established by NAMIRIAL to provide electronic Trust Services, which enhance trust and confidence in electronic transactions. NAMIRIAL PS describes Namirial S.p.A. (NAMIRIAL) practices of providing Qualified Trust Services in conformity with the eIDAS regulation [1], legal acts of Italy, ETSI EN 319 401 General Policy Requirements for Trust Service Providers [2], and other related service-based standard requirements. Additionally NAMIRIAL follows CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [3].

This NAMIRIAL PS describes practices necessary for the achievement of the security level approved by the NAMIRIAL management. NAMIRIAL has achieved ISO/IEC 27001:2013 certification. The statement of applicability includes more detailed description of security measures.

In the event of conflict between the NAMIRIAL PS and the practice statements of specific services, the provisions of the practice statements of specific services shall prevail. In the event of conflict between the original document in English and the translated document in Italian, the original document in English shall prevail.

1.2 Document Name and Identification

This document is called "Namirial S.p.A. Trust Services Practice Statement".

1.3 PKI Participants

1.3.1 Trust Service Provider

NAMIRIAL is Trust Service Provider (TSP). The roles of NAMIRIAL as TSP are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of NAMIRIAL are described in the clause 9.6.1 of this NAMIRIAL PS.

1.3.2 Registration Authorities

Registration Authority (RA) and its roles are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of RA are described in the clause 9.6.2 of this NAMIRIAL PS.

1.3.3 Subscribers

Subscriber is specified in relevant service-based Policy and/or Practice Statement. Obligations and warranties of Subscriber are described in the clause 9.6.3 of this NAMIRIAL PS.

1.3.4 Relying Parties

Relying Party is defined in the clause 1.6.1 in this NAMIRIAL PS.

Obligations and warranties of Relying Party are described in the clause 9.6.4 of this NAMIRIAL PS.

1.3.5 Other Participants

Specified in relevant service-based Policy and/or Practice Statement.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Specified in relevant service-based Policy and/or Practice Statement.

1.4.2 Prohibited Certificate Uses

Specified in relevant service-based Policy and/or Practice Statement.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This NAMIRIAL PS is administered by NAMIRIAL. Namirial S.p.A.

Registry code IT02046570426
via Caduti sul lavoro, 4 - 60019 - SENIGALLIA (AN)
Italy
Tel (+39) 071.63494 (Mon-Fri 9.00-13.00, 15.00-19.00 GMT +01:00)
Fax (+39) 071.60910
E-mail: tsp@namirial.com
Homepage: http://www.namirialtsp.com/

1.5.2 Contact Person

TSP Director
E-mail: tsp@namirial.com

1.5.3 Person Determining NAMIRIAL PS Suitability for the Policy

Not applicable.

1.5.4 NAMIRIAL PS Approval Procedures

Amendments which do not change the meaning of the certification practice, such as corrections of misspellings, translation and updating of contact details, are documented in the versions and changes section of the present document and the fraction part of the document version number shall be enlarged.

In the case of substantial changes, the new Trust Service Practice Statement version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The NAMIRIAL PS is approved by the NAMIRIAL Chief Executive Officer and the TSP Director. NAMIRIAL ensures that the practices are properly implemented by conducting regular internal audits and conformity assessments.

The amended version of NAMIRIAL PS is published electronically on NAMIRIAL's website with *"Protocol n. <number> of <date> – Official Register AOO AOO-AgID"* wording.

1.6 Definitions and Acronyms

1.6.1 Terminology

Term	Meaning
Certificate Revocation List	a list of invalid (revoked, suspended) certificates.
Qualified e-Signature (i.e. Qualified Electronic Signature)	means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
Directory Service	certificate publication service
eIDAS Regulation	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
e-Signature (i.e. Electronic Signature)	data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign.
Policy	a set of rules that indicates the applicability of a Trust Service Token to a particular community and/or class of application with common security requirements.
Practice Statement	a statement of the practices that a TSP employs in providing a Trust Service.
Registration Authority	entity that is responsible for identification and authentication of subjects of certificates. Additionally, an RA accepts certificate applications, checks the applications and/or forwards the applications to the CA.
Relying Party	a recipient of a Trust Service token who acts in reliance on that Trust Service Token. NOTE: Relying Parties include parties verifying a Digital Signature using a public key certificate.
Private key	the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key	the key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify digital signatures created with the holder’s corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding private key.
Root CA	the top level Certification Authority whose certificate is distributed by application software suppliers and that issues subordinate NAMIRIAL CA certificates.
Sensitive Information	information which allows for simulation or replication of service, or also for the destruction or publication of the service private key. It also includes personal information.
NAMIRIAL CA	a Certification Authority of NAMIRIAL whose certificate is signed by the Root CA, or another subordinate CA
Subscriber	an entity subscribing with Trust Service Provider who is legally bound to any

	Subscriber obligations.
Subscriber 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.
Supervisory Body	the authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS [1] in the territory of that member state.
Time-Stamping Unit	a set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
Trust Service	described in eIDAS [1] as an electronic service which is normally provided in return for remuneration and which consists of: - the creation, verification, and validation of Electronic Signatures, electronic seals or electronic time-stamps, electronically registered delivery services and certificates related to these services or - the creation, verification and validation of certificates for website authentication or - -the preservation of Electronic Signatures, seals or certificates related to these services.
Trust Service Provider	an entity that provides one or more electronic Trust Services.
Trust Service Token	a physical or binary (logical) object generated or issued as a result of the use of a Trust Service (e.g. certificate).
Qualified Trust Service	means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.

1.6.2 Acronyms

Term/Acronym	Meaning
CA	Certification Authority
CRL	Certificate Revocation List
DMZ	Demilitarised Zone
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Modules
RA	Registration Authority
NAMIRIAL	Namirial S.p.A. Trust Service Provider
NAMIRIAL PS	Namirial S.p.A. Trust Service Provider Practice Statement
TSA	Time-Stamping Authority
TSP	Trust Service Provider

TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

2 Publication and Repository responsibilities

2.1 Repositories

NAMIRIAL 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.

2.2 Publication of Information

NAMIRIAL publishes in its public website 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 Pratice Statement (CPS),
  - conditions for insurance policy,
  - profiles,
  - 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.

2.2.1 Publication and Notification Policies

This NAMIRIAL PS is published in NAMIRIAL's public website at URL https://docs.namirialtsp.com in section “Trust Services Practice Statement”.

2.2.2 Items not Published in the Practice Statement

Refer to clause 9.3.1 of this NAMIRIAL PS.

2.3 Time or Frequency of Publication

Refer to clause 2.2.1 of NAMIRIAL PS.

Information on certification status is published in accordance with clauses 4.9.7 and 4.9.9 of this NAMIRIAL PS.

2.3.1 Directory Service

NAMIRIAL does not publish information on certificates via LDAP directory service.

2.4 Access Controls on Repositories

Information published in NAMIRIAL's repository is public and not considered confidential information.

NAMIRIAL has implemented security measures in order to prevent unauthorized access to add, delete, or modify entries into its repository. Publishing into NAMIRIAL's repository is restricted to authorized employees of NAMIRIAL.

3 Identification and Authentication

3.1 Naming

Specified in relevant service-based Policy and/or Practice Statement.

3.2 Initial Identity Validation

Specified in relevant service-based Policy and/or Practice Statement.

3.3 Identification and Authentication for Re-Key Requests

Specified in relevant service-based Policy and/or Practice Statement.

3.4 Identification and Authentication for Revocation Request

Specified in relevant service-based Policy and/or Practice Statement.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

Specified in relevant service-based Policy and/or Practice Statement.

4.2 Certificate Application Processing

Specified in relevant service-based Policy and/or Practice Statement.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Specified in relevant service-based Policy and/or Practice Statement.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Specified in relevant service-based Policy and/or Practice Statement.

4.4 Certificate Acceptance

Specified in relevant service-based Policy and/or Practice Statement.

4.5 Key Pair and Certificate Usage

Specified in relevant service-based Policy and/or Practice Statement.

4.6 Certificate Renewal

Specified in relevant service-based Policy and/or Practice Statement.

4.7 Certificate Re-Key

Specified in relevant service-based Policy and/or Practice Statement.

4.8 Certificate Modification

Specified in relevant service-based Policy and/or Practice Statement.

4.9 Certificate Revocation and Suspension

Specified in relevant service-based Policy and/or Practice Statement.

4.10 Certificate Status Services

Specified in relevant service-based Policy and/or Practice Statement.

4.11 End of Subscription

Specified in relevant service-based Policy and/or Practice Statement.

4.12 Key Escrow and Recovery

Specified in relevant service-based Policy and/or Practice Statement.

5 Facility, Management, and Operational controls

In the field of security management, NAMIRIAL guides itself by the generally recognised standards, e.g. ISO/IEC 27001 [5], and other standards required by regulations and law.

The NAMIRIAL's security management policy documents include the security controls and operating procedures for the NAMIRIAL facilities, systems and information assets providing the services. NAMIRIAL carries out and revises risk assessment regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures.

The NAMIRIAL management establishes the security policy, which forms a basis for consistency and completeness of information security and management support.

The NAMIRIAL Chief Executive Officer approves policies and practices related to information security for the overall NAMIRIAL services. The NAMIRIAL management communicates information security policies and procedures to employees and relevant external parties who are impacted by it. In addition, the NAMIRIAL management sets out the NAMIRIAL approach to manage information security objectives for Trust Services, including auditable procedures for internal control.

NAMIRIAL has achieved ISO/IEC 27001: 2013 certification.

5.1 Physical Controls

The NAMIRIAL services relies on secured premises to host its CA. NAMIRIAL is using physically separated space in server rooms specifically designed for data center operations.

5.1.1 Site Location and Construction

The NAMIRIAL services are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of Sensitive Information and systems whether covert or overt.

The protection provided is commensurate with the identified risks. The NAMIRIAL ensures that physical access to critical services is controlled and that physical risks to its assets are minimised.

5.1.2 Physical Access

The NAMIRIAL data centers are protected by a minimum of three tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Access to the highest tier requires the participation of two persons in Trusted Roles.

The employees of NAMIRIAL may gain access to the facilities concerned with Trust Services of NAMIRIAL only on the basis of an approved list. A log is kept for recording all entries to the data processing centre of NAMIRIAL.

The owner of the premises has no independent access to NAMIRIAL-s servers.

Any persons entering this physically secure area will not remain there without oversight by an authorised person.

5.1.3 Power and Air Conditioning

NAMIRIAL's secure facilities are equipped with:

- power systems to ensure continuous, uninterrupted access to electric power; and
- heating, ventilation, air conditioning systems to control the temperature and relative humidity.

5.1.4 Water Exposures

NAMIRIAL has taken reasonable precautions to minimise the impact of water exposure to the information systems.

5.1.5 Fire Prevention and Protection

NAMIRIAL has taken reasonable precautions to prevent and extinguish fires or other damaging exposure toflame or smoke. The fire prevention and protection measures of the NAMIRIAL have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

Portable media, appliances and software may be removed from the premises of the NAMIRIAL pursuant to the established procedure.

5.1.7 Waste Disposal

Media containing Sensitive Information are securely disposed of when no longer required. Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal. Any media with Sensitive Information removed from use (removable media, hard disks etc.) are sanitised when decommissioned or recycled for other use, to prevent data leaks.

5.1.8 Off-Site Backup

NAMIRIAL performs routine backups of critical system data, audit log data, and other Sensitive Information. The NAMIRIAL has dual data centres to ensure availability requirements. Databases in dual data centres are synchronised in real time. In addition, routine backups are performed. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage.

5.2 Procedural Controls

5.2.1 Trusted Roles

The employees of NAMIRIAL have job descriptions that specify the following Trusted Roles critical for security:

- *System Administrators*: they are responsible for the installation, configuration and maintenance of the information systems, including performing the system backup and recovery;
- *System Operators*: they are responsible for operating the trustworthy systems on a day-to-day basis and are authorized to perform system backup;
- *Security Officers*: they are responsible for the administration of and the implementation of the security practices;

- *Facility Officers:* they are involved in day-to-day operations, particularly in relation to buildings and premises. Likely areas of responsibility include for example: building and grounds maintenance, health and safety, physical security and space management.
- *System & Regulatory Auditors*: they are is responsible for carrying out regular comprehensive review of NAMIRIAL's adherence all applicable laws, regulations and standards; for that they have access to monitor the document archives and information system audit logs.
- *Data Privacy Officer*: oversees all the activities related to the development, implementation, maintenance and adherence to the organization's privacy policies and procedures. These policies cover the collection, use, disclosure and privacy of personal information in compliance with the Italian Privacy law (Legislative Decree no. 196/2003). This trusted role report directly to the Board of Directors.
- *Information Security & Risk Manager*: he/she is responsible for the management of information security and risk through the implementation of information security policies, procedures and guidelines. He/she is also responsible for conducting information security audits and carrying out periodical second-level internal controls. This trusted role report directly to the Board of Directors.
- *RA Administrator*: manages and controls the internal RA operators within the Registration Authority of NAMIRIAL and the external RA operators within the LRAs (Local Registration Authorities).
- *RA Operator*: on behalf of the Registration Authority (RA), they are responsible for carrying out the duties outlined in conformity with the NAMIRIAL policies and procedures specified for the identification and registration of subscribers.

NAMIRIAL has defined different type of System Administrators with internal regulation and the assignment is made person by person with a decree of the CEO. See clause 5.2.2 for details.

NAMIRIAL ensures that personnel have achieved trusted status, and departmental approval is given before such personnel are:

- Issued access devices and granted access to the required facilities; or
- Issued electronic credentials to access and perform specific functions on NAMIRIAL or other IT systems.

Security operations are managed by NAMIRIAL personnel in Trusted Roles, but may actually be performed by a non-specialist, operational personnel (under supervision).

The roles of RA Administrator and RA Operator are also considered security critical as they are responsible for identification and authentication of subjects of certificates and may be responsible for registration, certificate suspension, termination of suspension and revocation procedures.

5.2.2 Number of Persons Required per Task

The NAMIRIAL has established, maintains and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The following activities require a minimum of two different types of System Administrators in Trusted Roles:

- generation of certification keys;
- backup of the certification keys;
- restoration of the certification keys;
- management of HSM-s and CA core systems located in Secure Zone;
- physical visit to data centres.

5.2.3 Identification and Authentication for Each Role

All Trusted Roles are performed by persons assigned into this role by NAMIRIAL management and accepted by this person to fulfill this role.

The NAMIRIAL has implemented an access control system, which identifies authorities and registers all the NAMIRIAL information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use.

User accounts are locked as soon as possible when the role change dictates. Access rules are audited annually.

5.2.4 Roles Requiring Separation of Duties

The Trusted Roles of the Security Officer, System & Regulatory Auditor and System Administrators are completely separate and are staffed by different persons. A single person cannot have simultaneously types of System Administrator.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The employees of the NAMIRIAL have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

All the employees of the NAMIRIAL have signed a non-disclosure agreement (NDA) to maintain the secrecy of confidential information that has come to their knowledge in the course of their performance.

NAMIRIAL management has appropriate expertise, and is familiar with security procedures. Any person in a Trusted Role is informed of his responsibility through its job description and/or procedures related to system security and personnel control.

All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding NAMIRIAL operations.

5.3.2 Background Check Procedures

For all personnel seeking to become personnel in Trusted Roles, the verification of identity is performed through the personal (physical) presence of such personnel before the personnel in Trusted Roles can perform the NAMIRIAL operational or security functions. Furthermore, officially recognised documents of identification e.g., ID card or passports are checked. Suitability is further confirmed through background checking procedures.

Background verification checks are carried out in accordance with relevant laws, regulations and principles of ethics. The checks are proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. These checks are conducted on all candidates for employment and on contracted partners directly performing the Trust Service providing operations with access to production data.

5.3.3 Training Requirements

The employees of NAMIRIAL have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

NAMIRIAL ensures that all personnel performing managerial duties with respect to the operation of the NAMIRIAL receive comprehensive awareness training in:

- security principles and rules in NAMIRIAL;
- NAMIRIAL internal regulations and processes;
- duties they are expected to perform.

5.3.4 Retraining Frequency and Requirements

The requirements of this NAMIRIAL PS 5.3.3 will be kept current to accommodate changes in the NAMIRIAL system. Refresher training will be conducted as required, and the NAMIRIAL is testing security awareness of all personnel at least once a year.

5.3.5 Job Rotation Frequency and Sequence

No rotation used.

5.3.6 Sanctions for Unauthorized Actions

The NAMIRIAL adopts and further implement the organizational, management and control model in compliance with the Italian Legislative Decree 231/2001 as more precisely described hereafter.

Italian Legislative Decree n. 231 of 8 June 2001 introduced the administrative liability of legal entities and their respective bodies for specific types of criminal offences provided under the Italian Criminal Code (such as the crimes against the Italian public authorities, corporate crimes, market abuse etc.) and committed and prosecutable in Italy by subjects having the functions of representing, administering or directing the legal entity or one of its administrative units having a financial and functional autonomy or by part of their "staff' in the interest or to the benefit of the company.

In introducing these rules on corporate liability, the decree provides, however, for a specific form of exemption from liability if the company proves to have adopted and effectively implemented an appropriate Organizational, Management and Control Model (hereinafter the "Model") in order to prevent such crimes and that the responsibility for supervising the functioning and the observance of the Model and for updating it is being entrusted to a specific body ("Supervisory Committee") of the legal entity provided with autonomous powers of initiative and control.

On 1st September 2008 the Company adopted the Model serving to prevent the perpetration of crimes falling within the scope of Decree 231/2001. The adopted Model, however, goes beyond the mere application of the provisions of Legislative Decree 231/2001 and, by implementing fundamental principles of the Code of Ethics, provides a paradigm for the conduct of all those who act in the Company's name and on its behalf.

As result the employees are subject to disciplinary actions and measures up to and including termination and will be commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Independent Contractor Requirements

The NAMIRIAL does not use independent contractors in Trusted Roles.

5.3.8 Documentation Supplied to Personnel

The NAMIRIAL gives its personnel (including persons in Trusted Roles) the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

5.4.1 Types of events recorded

NAMIRIAL ensures that the following events are recorded:

- system events from the different components of the PKI (server start, net- work access, ...);
- technical events from the PKI softwares;
- functional events from the PKI softwares (certificate request, validation, re- vocation ...);
- operations including authentication action from people with a trusted role.

The NAMIRIAL CA is an off-line CA which events are stored in an exter- nal media after each operations. This media is stored in an environment with a sufficient security level. These journals allow to ensure the auditability and accountability of the actions (timestamp, person name).

Non-computerized event records are made for:

- production site access;
- maintenance actions and configuration changes;
- human resource changes;
- actions on media with store confidential information.

5.4.2 Frequency of processing log

The audit trail, hereafter GdC ("Giornale di Controllo" for Italian law), are always audited when an abnormal event occurs.

5.4.3 Retention period for audit log

The GdC are externalized every day and stored in a storage server inside NAMIRIAL premises. They are kept until the expiration of the last certificate issued the CA.

5.4.4 Protection of audit log

The GdC can be accessed only by authorized people of NAMIRIAL. Each modification must be authorized.

5.4.5 Audit log backup procedures

Audit logs are backups regularly on DR site.

5.4.6 Audit collection system

NAMIRIAL audit collection systems are internal.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

To properly secure NAMIRIAL's information technology assets, the information security & risk team assess the security stance periodically by conducting regular vulnerability assessments at least twice a year and penetration test at least once a year. With the outcomes of these activities NAMIRIAL can apply security fixes or other compensating controls to improve the security of the environments.

The techniques used during the security assessments aim to cover a range of methodologies and attack techniques as broad as possible in order to identify all the plausible cyber risks. For this purpose are used automated scanning tools as well as manual techniques.

5.5 Records Archival

5.5.1 Types of Records Archived

Specified in relevant service-based Policy and/or Practice Statement.

5.5.2 Retention Period for Archive

The retention period for archive is described in clause 5.4.3 of this NAMIRIAL PS and in relevant service-based Policy and/or Practice Statement.

5.5.3 Protection of Archive

Regardless of their storage media, archives are protected in integrity, and are only accessible by authorized personnel. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period required.

5.5.4 Archive Backup Procedures

Not applicable.

5.5.5 Requirements for Time-Stamping of Records

Database entries contain accurate time and date information. The time-stamps are not cryptography-based.

5.5.6 Archive Collection System (Internal or External)

The NAMIRIAL uses an internal archive collection system. LRA-s may use external archive collection system for physical archive records.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorised personnel in Trusted Roles are allowed access to the archive. The archives (paper and electronic) can be retrieved in at most two working days. These archives are kept and managed by NAMIRIAL personnel.

Records concerning the operation of services are made available to legal authorities and/or persons whose right of access to them arises from the law.

5.6 Key Changeover

Specified in relevant service-based Policy and/or Practice Statement.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

NAMIRIAL has implemented a business continuity plan, which covers procedures of risk assessment, incident handling (includes a response to incidents and disasters), recovery and recovery exercises.

NAMIRIAL carries out an annual risk assessment of NAMIRIAL's Trust Services to prevent possible danger to the availability of NAMIRIAL's operations and to minimise the risk of losing control of the Trust Services. The list of situations considered as emergency situations is determined by the risk assessment. The result of the risk assessment includes the requirements for recovery plans and recovery testing scenarios. The recovery plans and testing scenarios include at least the following threats:

- for NAMIRIAL CA and NAMIRIAL TSA, the private key used for the provisioning of the service is compromised or there is a serious suspicion thereof;
- for NAMIRIAL TSA, the loss of synchronisation of a time-stamping service clock.

The procedures for the handling of information security incidents, emergency situations and critical vulnerabilities are documented in the internal NAMIRIAL's Incident Reporting and Management Procedure. The objective of that regulation is the immediate response and recovery of availability and the continuous protection of NAMIRIAL services.

Recovery plans are tested annually.

In the event of an emergency, NAMIRIAL will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency situation and proposed solution through public information communication channels.

NAMIRIAL will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies as national CERT or Italian Data Protection Authority and partners such as Acrobat Adobe (for AATL) of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The event of the corruption of computer resources, software and data is handled according to the NAMIRIAL internal Security Incident Management Policy.

5.7.3 Entity Private Key Compromise Procedures

The compromise of a key of the CA will lead to the immediate revocation of all issued certificates. In such a case, the various participants will be notified that the CRL may not necessarily be fully trusted.

5.7.4 Business Continuity Capabilities After a Disaster

In order to ensure the business continuity capabilities after a disaster NAMIRIAL organises periodically crisis management trainings. The NAMIRIAL Incident Reporting and Management Procedure defines how crisis management and communication take place in emergency situations.

There is an internal agreement about priorities for systems and services recovery after the emergency situation or/and service interruption. NAMIRIAL maintains necessary back-up copies and archives to able to restore data after the emergency situation. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage.

NAMIRIAL has dual data centres to ensure the availability of services. NAMIRIAL office and data centres are independent of each other. In case of the emergency in data centres guidance's, source codes and other necessary materials are available from NAMIRIAL Office. In case of the emergency situation in NAMIRIAL office services in data centres will continue to work.

5.8 CA Termination

The Trust Service is terminated:

- with a decision of the NAMIRIAL Executive Management Committee;
- with a decision of the authority exercising supervision over the supply of the service;
- with a judicial decision;
- upon the liquidation or termination of the operations of NAMIRIAL.

NAMIRIAL ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation of NAMIRIAL's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of Trust Service Tokens.

Before NAMIRIAL terminates a Trust Service the following procedures will be executed:

- NAMIRIAL informs the following of the termination: all Subscribers and other entities with which the NAMIRIAL has agreements or other forms of established relations. In addition, this information will be made available to other Relying Parties;
- NAMIRIAL makes the best effort for doing arrangements with other Trust Service Provider to transfer the provision of services for its existing customers;
- NAMIRIAL destroys the CA and TSU private keys, including backup copies or keys withdrawn from use in such a manner that the private keys cannot be retrieved;
- NAMIRIAL reinitialises or destroys any hardware appliances related to this service depending on the security regulations;
- NAMIRIAL terminates authorisation of all subcontractors to act on behalf of NAMIRIAL in carrying out any functions relating to the process of issuing Trust Service Tokens for this service;
- NAMIRIAL maintains the documentation related to they supply of the Trust Service and information needed to verify the Trust Service Tokens if NAMIRIAL is not terminated according to the clause 5.4 and 5.5. In case NAMIRIAL will be terminated, NAMIRIAL hands over the aforementioned documentation related to the supply of the service and information needed to verify the Trust Service Tokens to the Supervisory Body pursuant to the established procedure.

In case of compromise the NAMIRIAL will additionally:

- Indicate that Trust Service Tokens and validity information issued using this CA or TSU key may no longer be valid;
- Revoke any CA and TSU certificate that has been issued for NAMIRIAL when NAMIRIAL is informed of the compromise of another CA or TSA.

In case of algorithm compromise NAMIRIAL will additionally:

- Schedule a revocation of any affected Trust Service Token.

The notice of termination of NAMIRIAL's Trust Service will be published in the public media.

NAMIRIAL does not assume liability for any loss or damage sustained by the user of the service as a result of such termination provided that NAMIRIAL has given the notice of termination through public information communication channels at least one month in advance.

NAMIRIAL has an arrangement with an insurer to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons, is unable to cover the costs by itself.

The requirements are applicable also in case of LRA-s termination. NAMIRIAL takes over the documentation and information related to the supply of the Trust Service and provides evidence of the operation for a time period defined in relevant service-based Policy and/or Practice Statement.

6 Technical security controls

6.1 Key Pair Generation and Installation

NAMIRIAL uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms.

6.1.1 Key Pair Generation

The signing keys of the NAMIRIAL Trust Services are created in accordance with the internal procedure for Creating the NAMIRIAL Root Key.

The Trust Service key pair generation and the private key storage occur in the HSM, which is used for providing keys, that are certified at the level EAL4+ of the Common Criteria and qualified by the ANSSI at the highest level. They meet the following requirements:

- Ensuring the confidentiality and the integrity of the CA private signing key during all their life cycle, as well as their safe destruction at the end of the life cycle;
- Being able to identify and authenticate its users;
- Limiting access to its services depending on the user and the role he has been assigned;
- Being able to perform a set of tests to verify it is operating properly and enter a safe state if an error is encountered;
- Allowing the creation of a digital signature to sign certificates generated by the AC, which does not reveal the CA private keys and cannot be forged without the knowledge of the private keys;
- Creating audit logs for every modification regarding security;
- If backup and restore of private keys is provided, ensuring the confidentiality and the integrity of the backuped data and require at a minimum dual control of backup and restore operations;
- Detecting physical disruption attempts and enter a safe state when such an attempt is detected.

The HSM protects the key from external compromise and operates in a physically secure environment.

NAMIRIAL has documented procedure for conducting NAMIRIAL CA key pair generation for all CA's. NAMIRIAL produces a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. Report is signed by the responsible for the certification service and the internal auditor. The procedures for key ceremony are documented in NAMIRIAL internal procedures.

The Subscriber Private Key generation is specified in relevant service-based Policy and/or Practice Statement.

6.1.2 Private Key Delivery to Subscriber

Specified in relevant service-based Policy and/or Practice Statement.

6.1.3 Public Key Delivery to Certificate Issuer

Specified in relevant service-based Policy and/or Practice Statement.

6.1.4 CA Public Key Delivery to Relying Parties

All NAMIRIAL Trust Services public keys are distributed in the form of X.509 certificates issued by the NAMIRIAL CA. The primary distribution mechanism for the NAMIRIAL Trust Service certificates is via the NAMIRIAL repository at https://docs.namirialtsp.com/certificates/. The NAMIRIAL takes obligation to provide the NAMIRIAL Trust Service certificates to Trusted List of Italy.

6.1.5 Key Sizes

Specified in relevant service-based Policy and/or Practice Statement.

6.1.6 Public Key Parameters Generation and Quality Checking

The key generation material uses parameters fulfilling the security requirements of the algorithm corresponding to the key pair. Further details are specified in relevant service-based Policy and/or Practice Statement.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Specified in relevant service-based Policy and/or Practice Statement.

6.2 Private Key Protection and Cryptographic Module

6.2.1 Cryptographic Module Standards and Controls

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.

Cryptographic module standards and controls for cryptographic devices which carry the Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.2 Private Key (n out of m) Multi-Person Control

The access to the NAMIRIAL CA keys is divided into six parts (2 out of 6) that are secured by different persons in Trusted Roles. For activation of the signing key of the NAMIRIAL the presence of at least two authorized persons is required in accordance with clause 5.2.2 of this PS.

6.2.3 Private Key Escrow

Private keys are not escrowed.

6.2.4 Private Key Backup

CA private keys are backuped 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.

The certification keys of the NAMIRIAL can be used only when they are activated.

For activation of the certification key of the NAMIRIAL the presence of at least two authorised persons is required as explained in clause 6.2.2 in this NAMIRIAL PS.

6.2.5 Private Key Archival

NAMIRIAL will not archive the NAMIRIAL CA private keys after it has expired. All copies of the NAMIRIAL CA private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All NAMIRIAL CA keys are generated by and in the a cryptographic module. The NAMIRIAL generates CA key pairs in the HSM in which the keys will be used.

6.2.7 Private Key Storage on Cryptographic Module

The HSM used by NAMIRIAL guarantee through the encryption of CA Private Keys that the keys can be deciphered and used only on the cryptographic module which has generated them.

6.2.8 Method of Activating Private Key

The NAMIRIAL CA private keys are activated according to the specifications of the cryptographic module manufacturer. For activation of the certification key of the NAMIRIAL the presence of at least two authorised persons is required as explained in clause 6.2.2 of this NAMIRIAL PS.

Method of activating Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.9 Method of Deactivating Private Key

The private key is deactivated when the HSM stops.

6.2.10 Method of Destroying Private Key

Method of the destroying NAMIRIAL CA private keys and internal control mechanisms depend from the options available to specific secure cryptographic module. When a key is destroyed, the CA ensures that all corresponding backup copies are also destroyed.

6.2.11 Cryptographic Module Rating

Refer to the clause 6.2.1 of this NAMIRIAL PS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA public keys are archived indefinitely after the expiry of the corresponding CA certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a certificate ends upon revocation. The operational period for key pairs is the same as the operational period for the certificates, except that they may continue to be used for signature verification.

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.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by the NAMIRIAL management.

For Subscriber certificates, the validity period is defined in relevant service-based Policy and/or Practice Statement.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The NAMIRIAL CA private key activation data generation and installation is performed according to the user manual of HSM.

The Subscriber's Private Key PINs generation and installation is specified in relevant service-based Policy and/or Practice Statement.

6.4.2 Activation Data Protection

HSM is kept in secure area and only authorized personnel in Trusted Roles can access to it.

The Subscriber's Private Key PINs protection is specified in relevant service-based Policy and/or Practice Statement.

6.4.3 Other Aspects of Activation Data

Specified in relevant service-based Policy and/or Practice Statement.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The NAMIRIAL ensures that the certification system components are secure and correctly operated, with an acceptable risk of failure.

The NAMIRIAL certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All critical software components of the NAMIRIAL are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorised software.

All critical systems are hardened following internal ad-hoc hardening procedures issued by the information security team.

All media containing production environment software and data, audit, archive, or backup information are stored within the NAMIRIAL with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media containing Sensitive Information are securely disposed of when no longer required. All removable media are used only for the intended period of the user (either by time or by number of uses).

NAMIRIAL has no defined capacity management process. The performance of NAMIRIAL services and IT systems is monitored by Service Managers and changes are done when necessary according to internal change management procedure.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

The NAMIRIAL security operations include: operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backups, network management, active monitoring of audit logs event analysis and follow-up, media handling and security, data and software exchange.

NAMIRIAL's personnel are authenticated before using critical applications related to the services.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

6.5.2 Computer Security Rating

NAMIRIAL uses standard computer systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the NAMIRIAL; or an analysis is carried out on behalf of the NAMIRIAL to ensure that security is built into the Information Technology's systems.

The software will be approved by the Service Managers and will originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures.

6.6.2 Security Management Controls

Measures are implemented in the information system of the NAMIRIAL, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread. Only the software directly used for performing the tasks is used in the information system.

6.6.3 Life Cycle Security Controls

The NAMIRIAL policies and assets for information security are reviewed at planned intervals, or should significant changes occur, they are reviewed to ensure their continuing suitability, adequacy and effectiveness.

The configurations of the NAMIRIAL systems are regularly checked for changes that violate the NAMIRIAL security policies. A review of configurations of the issuing systems, security support systems, and front-end/internal-support systems occurs at least on a weekly basis. The Security Officer approves changes that have an impact on the level security provided. The NAMIRIAL has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

The NAMIRIAL manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment. All NAMIRIAL policies and assets related to information security will be reviewed internally at planned intervals, or should significant changes occur, they will be reviewed to ensure their continuing suitability, adequacy and effectiveness.

6.7 Network Security Controls

The NAMIRIAL network is divided into zones by security requirements. Communication between the zones is restricted. Only the protocols needed for the NAMIRIAL services are allowed through the firewalls.

The front-end systems are in a DMZ protected by a firewall and TLS offload servers. Actual security-critical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

The root CA is in a high security zone and is air-gapped from all the other networks. The NAMIRIAL systems are configured with only these accounts, applications, services, protocols, and ports that are used in the Trust Service operations.

The NAMIRIAL ensures that only personnel in Trusted Roles have access to a secure zone and a high security zone.

The cabling and active equipment along with their configuration in the NAMIRIAL internal network are protected by physical and organisational measures.

The NAMIRIAL operates multiple data centres in separate sites for redundancy. Communication between sites is cryptographically secured.

All data centres are considered to be in a common internal secure network carrying the DMZ and secure zone. The transfer of Sensitive Information outside the NAMIRIAL internal network is encrypted.

The security of the NAMIRIAL internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

The NAMIRIAL performes a vulnerability scan twice a year on public and private IP addresses identified by NAMIRIAL.

The NAMIRIAL undergoes a penetration test on the certification systems annually at the set up and after the infrastructure or application upgrades or modifications determined significant by the NAMIRIAL.

The NAMIRIAL records evidence that each vulnerability scan and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8 Time-Stamping

NAMIRIAL is providing time-stamping service as qualifed Trust Service and is specified in Namirial S.p.A. Time-Stamping Authority Practice Statement [6].

The NAMIRIAL does not use time-stamping in relation to certification service. Database entries contain accurate time and date information. The time information is not cryptographic-based. The maximum allowed time variance in all parts of the certification system is 1 second. This is guaranteed by an internal Reference Clock service, according to which the chronologies of all parts of the certification system are synchronised. The Reference Clock uses GPS (Global Positioning System) as a primary time source which determines preciseness of the time in the NAMIRIAL's system.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.2 CRL Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.3 OCSP Profile

Specified in relevant service-based Policy and/or Practice Statement.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

Two kinds of compliance audit are made:

- an internal audit performed at least once a year
  - by an external provider specialized in PKI; or
  - by an internal auditor.
- a qualification audit performed by an accredited organization at least once a year.

An audit ensuring compliance to this CP is performed

- at least once a year for internal audit
- during annual renewal of qualification, as requested by the regulatory proceeding.
- after each major modification.

During the qualification process, a first compliance audit has been performed by an accredited organization as requested by the regulatory proceeding.

8.2 Identity/qualifications of assessor

The assessor must act with rigor in order to ensure that policies, statements and services are properly implemented and to detect the non-compliance items which might jeopardize the security of the service.

The TSP commits to hire assessors with a high level of expertise in system security, particularly in the field of the audited component.

8.3 Assessor’s relationship to assessed entity

The assessor is appointed by NAMIRIAL, and is allowed to audit the practices ruling the target component of the audit. He may be part of NAMIRIAL but is independant from the TSP.

8.4 Topics covered by assessment

The assessor operates compliance audits of the specified component, covering totally or partly the implementation of:

- the TSP PS;
- the CP and CPS;
- the TSA PS;
- the components of the PKI and TSS.

Prior to every audit, the assessors will provide the TSP Director with a list of components and procedures they wish to audit, and will subsequently prepare the detailed audit program.

8.5 Actions taken as a result of deficiency

Following the compliance audit, the assessment team gives the TSP the result which can be “success”, “failure” or “to be confirmed”.

In case of failure, the assessment team delivers recommendations to the TSP. The TSP then decides which actions to perform.

In case of result “to be confirmed”, the assessment team identifies the non-compliances and prioritizes them. The TSP then schedules the correction of these non-compliances. A validation audit then checks for their effective corrections.

In case of success, the TSP confirms that the audited component complies with the requirements of the CP.

8.6 Communication of results

The audit results are made available to the Executive Management Committee of NAMIRIAL and to the qualification organism in charge of the qualification of the TSP.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation or Status Information Access Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.4 Fees for Other Services

Fees for services are specified in NAMIRIAL’s price list or in the Subscriber’s or Relying Party’s agreement.

9.1.5 Refund Policy

NAMIRIAL handles refund requests case-by-case.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

In accordance with the relevant legislation, NAMIRIAL publishes the terms of the compulsory insurance policy on its website https://docs.namirialtsp.com/insurance/.

9.2.2 Other Assets

According to relevant agreements NAMIRIAL may give some additional warranties.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of this NAMIRIAL PS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to NAMIRIAL because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from NAMIRIAL about him/herself according to legal acts.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential or intended for internal use is public information. Information considered public in NAMIRIAL is listed in clause 2.2 of this NAMIRIAL PS.

Additionally, non-personalised statistical data about NAMIRIAL's services is also considered public information. NAMIRIAL may publish non-personalised statistical data about its services.

9.3.3 Responsibility to Protect Confidential Information

NAMIRIAL secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

9.4 Privacy of Personal Information

9.4.1 Personal Data Protection Principles

NAMIRIAL takes all the necessary measures so that personal data are protected and stored confidentially according to the Italian data protection code (Legislative Decree no. 196/2003).

9.4.2 Personal Information Processed by NAMIRIAL

The scope of personal information processed by NAMIRIAL is described in https://docs.namirialtsp.com/privacy/.

9.4.3 Responsibility to Protect Private Information

NAMIRIAL ensures protection of personal information by implementing security controls as described in chapter 5 of this NAMIRIAL PS.

9.4.4 Notice and Consent to Use Private Information

The exact terms under which the subscriber grants NAMIRIAL his/her notice and consent to use his/her personal information are described in https://docs.namirialtsp.com/privacy/.

9.4.5 Disclosure Pursuant to Judicial or Administrative Process

The circumstances under which NAMIRIAL may disclose the subscriber's personal information to third parties are described in https://docs.namirialtsp.com/privacy/.

9.4.6 Other Information Disclosure Circumstances

The circumstances under which NAMIRIAL may disclose the subscriber's personal information to third parties are described in https://docs.namirialtsp.com/privacy/.

9.5 Intellectual Property Rights

The products operated to provide the PKI belong to NAMIRIAL. Any use or reproduction, total or partial, of these elements and/or information within, by any means, is strictly prohibited and is a forgery punished, unless NAMIRIAL has previously given its written agreement.

9.6 Representations and Warranties

9.6.1 Trust Service Provider Representations and Warranties

NAMIRIAL is party to the mutual agreements and obligations between the TSP, Subscribers, and Relying Parties. This NAMIRIAL PS and service-based Practice Statements are integral parts of these agreements.

NAMIRIAL:

- provide its services consistent with the requirements and the procedures defined in this NAMIRIAL PS and service-based policies and practice statements;
- comply with eIDAS regulation [1] and related legal acts defined in this NAMIRIAL PS and service-based policies and practice statements;

- publish its NAMIRIAL PS and service-based policies and practice statements and guarantee their availability in a public data communications network;
- publish and meet its claims in terms and conditions for subscribers and guarantee their availability and access in a public data communications network;
- maintain confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- keep account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- inform the Supervisory Body of any changes to a public key used for the provision Trust Services;
- without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies as national CERT or Italian Data Protection Authority and partners such as Acrobat Adobe (for AATL) of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein;
- where the breach of security or loss of integrity is likely to adversely affect a natural or legalperson to whom the Trusted Service has been provided, notify the natural or legal person of the breach of security or loss of integrity without undue delay;
- preserve all the documentation, records and logs related to Trust Services according to the clauses 5.4 and 5.5;
- ensure a conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- has the financial stability and resources required to operate in conformity with this NAMIRIAL PS;
- publish the terms of the compulsory insurance policy and the conclusion of conformity assessment body or certificate in a public data communications network.

An employee of NAMIRIAL may not have been punished for an intentional crime.

9.6.2 RA Representations and Warranties

The LRA shall:

- provide its services consistent with the requirements and the procedures defined in the contract between NAMIRIAL and LRA, in this NAMIRIAL PS and service-based Policies and Practice statements;
- provide its employees with necessary training for supply of high-quality service;
- without undue delay after having become aware of it, will notify NAMIRIAL of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

An employee of LRA may not have been punished for an intentional crime.

9.6.3 Subscriber Representations and Warranties

The Subscriber shall:

- observe the requirements provided by NAMIRIAL in this NAMIRIAL PS and the respective service-based policies and/or practice statements;
- supply true and adequate information in the application for the services, and in the event of a change in the data submitted, he/she shall notify the correct data in accordance with the rules established in the service-based policies and practice statements;
- be aware of the fact that NAMIRIAL may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- be solely responsible for the maintenance of his/her private key and Trust Service Tokens. The Subscriber shall use his/her private key and Trust Service Tokens in accordance with this NAMIRIAL PS, service-based practice statements and service terms and conditions.

9.6.4 Relying Party Representations and Warranties

A Relying Party shall:

- study the risks and liabilities related to the acceptance of Trust Service Tokens. The risks and liabilities have been set out in this NAMIRIAL PS, in the appropriate service-based policies and practice statements and in the service terms and conditions.
- verify the validity of Trust Service Tokens on the basis of validation services offered by NAMIRIAL using:
  - published information on NAMIRIAL’s website https://docs.namirialtsp.com/ or
  - applicable validation service or
  - o appropriate cryptographic information.

9.6.5 Representations and Warranties of Other Participants

Specified in relevant service-based Policy and/or Practice Statement.

9.7 Disclaimers of Warranties

NAMIRIAL:

- is liable for the performance of all its obligations specified in clause 9.6.1 to the extent prescribed by the legislation of the Republic of Italy;
- has compulsory insurance contracts, which cover all NAMIRIAL Trust Services to ensure compensation for damage which is caused as a result of violation of the obligations of NAMIRIAL.

NAMIRIAL is not liable for:

- the secrecy of the private keys of the Subscribers, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service Token validation checks;
- the non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the Italian Data Protection Authority, Trusted List or any other public authority;
- non-fulfilment of the obligations arising from the NAMIRIAL PS if such non-fulfilment is occasioned by Force Majeure.

9.8 Limitations of Liability

The upper limit of the liability for any claim is established in the referred policy available at https://docs.namirialtsp.com/insurance/.

9.9 Indemnities

Indemnities between the Subscriber and NAMIRIAL are regulated in service based Terms and Conditions.

9.10 Term and Termination

9.10.1 Term

Refer to clause 2.2.1 of this NAMIRIAL PS.

9.10.2 Termination

This NAMIRIAL PS and/or service-based Practice Statements remain in force until they are replaced by a new version or when they are terminated due to Trust Service or NAMIRIAL’s termination.

Upon NAMIRIAL’s termination, NAMIRIAL is obliged to ensure the protection of personal and confidential information.

9.10.3 Effect of Termination and Survival

NAMIRIAL communicates the conditions and effect of this NAMIRIAL PS's and/or service-based Practice Statements termination via its public repository. The communication specifies which provisions survive termination.

At a minimum, all responsibilities related to protecting personal and confidential information, also maintenance of public information of repository, NAMIRIAL archives for determined period and logs survive termination. All Subscriber agreements remain effective until the certificate is revoked or expired, even if this NAMIRIAL PS and/or service-based Practice Statements terminate.

Termination of this NAMIRIAL PS and/or service-based Practice Statements cannot be done before termination actions described in clause 5.8 of this NAMIRIAL PS.

9.11 Individual Notices and Communications with Participants

In general, NAMIRIAL's website http://www.namirialtsp.com will be used to make any type of notification and communication. Other means of individual notices and communication is specified in relevant service-based Policy and/or Practice Statement.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to clause 1.5.4 of this NAMIRIAL PS.

9.12.2 Notification Mechanism and Period

Refer to clause 2.2.1 of this NAMIRIAL PS.

9.12.3 Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Procedures

All disputes between the parties will be settled by negotiations. If the parties fail to reach and amicable agreement, the dispute will be resolved at the court of the location of NAMIRIAL.

The other parties will be informed of any claim or compliant not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

The Subscriber or other party can submit their claim or complaint on the following email: info@namirialtsp.com.

9.14 Governing Law

This NAMIRIAL PS is governed by the jurisdictions of the European Union and the Republic of Italy.

9.15 Compliance with Applicable Law

NAMIRIAL ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];

- Italian Data Protection Code [7];
- related European Standards:
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [2];

  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [9];
  - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [9];
- CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [3].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

NAMIRIAL contractually obligates each LRA and other participants to comply with this NAMIRIAL PS and applicable industry guidelines. NAMIRIAL also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this NAMIRIAL PS, then the agreement with that party prevails, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this NAMIRIAL PS may not assign their rights or obligations without the prior written consent of NAMIRIAL. Unless specified otherwise in a contract with a party, NAMIRIAL does not provide notice of assignment.

9.16.3 Severability

If any provision of this NAMIRIAL PS is held invalid or unenforceable by a competent court or tribunal, the remainder of the NAMIRIAL PS remains valid and enforceable. Each provision of this NAMIRIAL PS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

NAMIRIAL may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. NAMIRIAL’s failure to enforce a provision of this NAMIRIAL PS does not waive NAMIRIAL’s right to enforce the same provision later or right to enforce any other provision of this NAMIRIAL PS. To be effective, waivers must be in writing and signed by NAMIRIAL.

9.16.5 Force Majeure

The subject of Force Majeure and other parties are responsible for any consequences caused by circumstances beyond his reasonable control, including but without limitation to war (whether declared or not), acts of government or the European Union, export or import prohibitions, breakdown or general unavailability of transport, general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Communication and performance in the case of Force Majeure are regulated between the parties with the agreements.

Non-fulfilment of the obligations arising from the NAMIRIAL PS and/or relevant service-related Policies and/or Practice Statements is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this NAMIRIAL PS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.

9.17 Other Provisions

Not applicable.

References

Numero	Descrizione
[I]	eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
[II]	ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
[III]	CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf;
[IV]	RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, https://www.ietf.org/rfc/rfc3647.txt;
[V]	ISO/IEC 27001: 2013 Information technology - Security techniques -Information security management systems – Requirements;
[VI]	Namirial S.p.A. Time-Stamping Authority Practice Statement, published: https://docs.namirialtsp.com/tsaps/;
[VII]	Italian Data Protection Code (Legislative Decree no. 196/2003).
[VIII]	Data Protection Disclaimer (Privacy), published: https://docs.namirialtsp.com/privacy/;
[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: Policy requirements for certification authorities issuing qualified certificates.