NamirialSpa
Trust Service Provider

Time-Stamping Authority

Practice Statement

Category:	**Practice Statement**	Document No.:	**NAMTSP-TSAPS-MO-v1.2.docx**
Written by:	**Service Manager TSA**	Confidentiality notice:	**Public document**
Verified by:	**TSP Director**	Version:	**1.2**
Approved by:	**CEO**	Issue date:	**07/07/2017**

Namirial S.p.A.
Chief Executive Officer
(Dr. Davide Ceccucci)

CECCUCCI DAV
2017.07.07 19:29:47
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	17/06/2016
Reasons	First release
Modifications	---

Version	1.1
Date	08/07/2016
Reasons	Update
Modifications	§4.3.1, §5.2

Version	1.2
Date	07/07/2017
Reasons	Update
Modifications	§ 6.5

1 Introduction

This document is the Namirial S.p.A. Time-Stamping Authority Practice Statement (NAMIRIAL TSA PS) that outlines the principles and practices related to Namirial's time-stamping services. This document applies to all entities participating in or using Namirial's time-stamping 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.
- parts that are specific to the certification service (ie. certificate policies or certification practices statement) are described within the "operative manual for the certification service" as required by national laws.
- parts that are specific to the Time-Stamping service are described within the Time-Stamping Authority Practice Statement (this document).

The NAMIRIAL Time-Stamping Authority (NAMIRIAL TSA) uses the public key infrastructure and trusted time sources to provide reliable, standards-based qualified time-stamps. NAMIRIAL time-stamps may be applied to any application requiring proof that datum existed before particular time.

This document states time-stamping specific practices of NAMIRIAL. In particular, the facility, management and operational controls such that Subscriber and Relaying Parties may evaluate their confidence in the operation of NAMIRIAL time-stamping services. This document should be read in conjunction with the NAMIRIAL Trust Services Practice Statement (NAMIRIAL PS), which describes overall NAMIRIAL trust services practices.

NAMIRIAL time-stamping service conforms to eIDAS regulation, legal acts of Italy and ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and other related standards.

1.1 Overview

NAMIRIAL issues Time-Stamping Tokens in accordance with ETSI EN 319 421 best practice for time-stamping policy.

EE Certification Centre Root CA has certified NAMIRIAL Time-Stamping Authority.

The Root CA certificates and other certificates necessary for PKI operation are available at https://docs.namirialtsp.com/certificates/.

The time-stamping service described in this NAMIRIAL TSA PS has qualified status in the Trusted List of Italy, https://eidas.agid.gov.it/TL/TSL-IT.xml.

In the case of conflict between NAMIRIAL TSA PS and NAMIRIAL PS the provisions of NAMIRIAL TSA PS shall prevail. In case of conflict between the English original document and the Italian translation, the English original shall prevail.

2 References

No.	Description
[I]	[eIDAS regulation] Regulation (EU) No 910/2014 of 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 319 421] ETSI EN 319 421 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
[III]	[DPCI] Data Protection Code of Italy (Legislative Decree no. 196/2003).

[IV]	[RFC 3161] RFC 3161: “Internet X.509 Public Key Infrastructure Time-stamp Protocol”.
[V]	[NAMIRIAL PS] Namirial S.p.A. Trust Service Provider Practice Statement.
[VI]	ITU-R Recommendation TF.460-6 (02/02): “Standard-frequency and time-signal emissions”. RFC 5905: “Network Time Protocol Version 4: Protocol and Algorithms Specification”

3 Definitions, symbols and abbreviations

3.1 Definitions

Term/Acronym	Meaning
Coordinated Universal Time (UTC)	The time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/02)
Network Time Protocol (NTP)	Protocol to synchronize system clocks among a set of distributed time servers and clients as defined in RFC 5905
Relying Party	The recipient of a Time-Stamp Token who relies on that Time- Stamp Token
Root CA	The top level certification authority whose certificate is distributed by application software suppliers and that issues subordinate NAMIRIAL CA and TSU certificates.
Subscriber	The entity which requires the services provided by a TSA and has entered into the Namirial S.p.A. Subscriber agreement
Time-Stamping Policy	A named set of rules that indicates the applicability of a Time- Stamp Token to a particular community and/or class of application with common security requirements applicable; the Time-Stamping Policy is defined in [ETSI 102023]
Time-Stamp Token (TST)	The data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Time-Stamping Authority (TSA)	The authority which issues Time-Stamp Tokens
Time-Stamping Unit (TSU)	A set of hardware and software which is managed as a unit and has a single Time-Stamp Token signing key active at a time (cluster of server nodes and hardware security modules (HSM) using common signing key)
TSA Disclosure Statement	A set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and Relying Parties, for example to meet regulatory requirements
TSA Practice Statement	Statement of the practices that a TSA employs in issuing Time-Stamp Tokens
TSA System	A composition of information technology products and components organized to support the provision of time- stamping

3.2 Abbreviations

Term/Acronym	Instead of
CA	Certification Authority
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
HSM	Hardware Security Modules
NTP	Network Time Protocol
NAMIRIAL	Namirial S.p.A. Trust Service Provider
NAMIRIAL PS	Namirial S.p.A. Trust Service Provider Practice Statement
NAMIRIAL TSA PS	Namirial S.p.A. Trust Service Provider Time-Stamping Authority Practice Statement
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4 General concepts

4.1 General Policy Requirements Concepts

The NAMIRIAL TSA PS references NAMIRIAL PS for common practices to all NAMIRIAL trust services.

4.2 Time-Stamping Services

NAMIRIAL takes overall responsibility for the provision of the time-stamping services, which include the following components:

- time-stamping provision - the service component that generates TSTs;
- time-stamping management;
- the service component that monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified in overall NAMIRIAL PS and in this NAMIRIAL TSA PS.

NAMIRIAL TSA adheres to the standards and regulations in section 2 of this document to keep trustworthiness of the time-stamping services for Subscribers and Relying Parties.

4.3 Time-Stamping Services Participants

4.3.1 Time-Stamping Authority

NAMIRIAL TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue TSTs. NAMIRIAL TSA has overall responsibility for the provision of the time-stamping services identified in section 5.2 NAMIRIAL TSA may operate several identifiable TSUs. NAMIRIAL has responsibility for the operation TSU that creates and signs on behalf of the TSA.

NAMIRIAL TSA is identified in the TSU certificate used to sign TST. NAMIRIAL substitutes the TSUs certificates every three months in accordance with the Italian laws. The TSU certificates have the OID 1.3.6.1.4.1.36203.2.1.2, the key usage is set to *digital signature* and the extended key usage is set to *timestamping* only.

Contact information:

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/

4.3.2 TSA Subscriber

The Subscribers are entities that hold a Subscriber agreement with NAMIRIAL time-stamping service. Subscriber may be an organization comprising several end-users or an individual end-user. Organizations that are Subscribers, are responsible for the correct fulfilment of the obligations from its end-users and therefore are expected to suitably inform its end-users about the correct use of time-stamps and the conditions of the NAMIRIAL PS and NAMIRIAL TSA PS.

4.3.3 TSA Relying Party

A Relying Party is an individual or entity that acts in reliance of a TST generated under [I] [II] policy by NAMIRIAL TSA. A Relying Party may, or may not also be a Subscriber.

4.4 Time-Stamping Policy and TSA Practice Statement

NAMIRIAL TSA Time-Stamping Policy is based on the Time-Stamping Policy specified in [I] [II] and is applied to TSAs issuing TSTs. This NAMIRIAL TSA Practice Statement is a form of NAMIRIAL Trust Services Practice Statement (NAMIRIAL PS) as specified in [I] [II] applicable to NAMIRIAL TSA issuing TSTs.

5 Time-Stamping Policies

5.1 General

NAMIRIAL TSA issues the TSTs in accordance with [ETSI EN 319 421] baseline Time-Stamping Policy.

The TSTs are issued with an accuracy of 1 second of UTC or better.

5.2 Identification

The object-identifier (OID) of the baseline Time-Stamping Policy is 0.4.0.2023.1.1.

This OID is referenced in every TST issued by NAMIRIAL TSA.

6 Policies and practices

6.1 Risk assessment

Refer to clause 5.7.1 of NAMIRIAL PS.

6.2 Trust Service Practice Statement

Refer to 1.5.4, 2.2 and 5.8 of NAMIRIAL PS.

6.3 Terms and conditions

The TSA Disclosure Statement is provided as a part of Terms and Conditions, which are available at https://docs.namirialtsp.com/terms/.

6.4 Information security policy

Refer to section 5 of NAMIRIAL PS.

6.5 TSA Obligations

NAMIRIAL TSA obligations towards Subscribers and Relying Parties specified in section 9.6.1 of NAMIRIAL PS apply.

In addition, Namirial is starting a plan to improve accessibility of the service for the disabled through Web Content Accessibility.

6.6 solutionsTSA Subscriber Obligations

The general obligations specified in section 9.6.3 of NAMIRIAL PS apply.

Subscriber is obligated to verify the signature of TSTs and ensure that the private key used to sign the TST has not been revoked.

Subscriber is obligated to use secure cryptographic functions for time-stamping requests. Subscriber is obligated to inform its end-users (e.g. Relying Parties) about correct use of time-stamps and the conditions of the NAMIRIAL PS and NAMIRIAL TSA PS. Subscriber obligations are also defined in the Subscriber agreement.

6.7 TSA Relying Party Obligations

The general obligations specified in section 9.6.4 of NAMIRIAL PS apply.

Relying Parties verify that TST has been correctly signed with the key corresponding to TSU certificate and that the private key used to sign the TST has not been compromised until the time of verification and take measures in order to ensure the validity of the TSTs beyond the life-time of the NAMIRIAL TSA certificates. Validity information has to be verified according to section 7.7.1 in this NAMIRIAL TSA PS.

6.8 Liability

The liability provisions in section 9.7, 9.8 and 9.9 of NAMIRIAL PS apply.

The liability of the NAMIRIAL to the Subscribers is stipulated in the Subscriber agreements to be signed with the Subscribers.

The liability of the NAMIRIAL to Relying Parties interested in the preservation of the proof value of the validity confirmations is regulated herein.

NAMIRIAL is not liable for the mistakes in the verification of the validity of time stamps or for the wrong conclusions conditioned by omissions or for the consequences of such wrong conclusions.

NAMIRIAL shall assume no liability for the loss of the proof value of validity confirmation due to Force Majeure.

7 TSA management and operation

7.1 Introduction

NAMIRIAL TSA implements all practices described in section 7.

The provision of a TST in response to a request is at the discretion of NAMIRIAL TSA depending on the Subscriber agreement.

7.2 Internal Organisation

The practices identified in section 9 of NAMIRIAL PS apply.

NAMIRIAL organisational structure, policies, procedures and controls apply to NAMIRIAL TSA. NAMIRIAL TSA organisational procedures comply with the standards and regulations referred in section 2.1 of this NAMIRIAL TSA PS.

7.3 Personnel Security

The practices identified in section 5.2 and 5.3 of NAMIRIAL PS apply.

In addition, NAMIRIAL has employed a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

7.4 Asset Management

The practices identified in section 5, 6.5 and 6.6.3 of NAMIRIAL PS apply.

7.5 Access Control

The practices identified in section 6.5 and 6.7 of NAMIRIAL PS apply.

7.6 Cryptographic Controls

7.6.1 TSU key generation

The practices of key generation described in section 6.1 and 6.2 of NAMIRIAL PS apply. Personnel restrictions are described in section 5.2 and 5.3 of NAMIRIAL PS.

NAMIRIAL TSU is using RSA key pair with 2048-bit modulus. This key pair is used only for signing TSTs.

All cryptographic modules are associated with the same public key certificate.

7.6.2 TSU Private Key Protection

The practices of TSU key protection, storage, backup and recovery described in section 6.2 and 6.3 of NAMIRIAL PS apply.

TSU private key will be backed up and securely stored for the unlikely event of key loss due to unexpected power interruption or hardware failure. Key backup will occur as part of key generation ceremony. Backed up private key remains secret and their integrity and authenticity is retained.

7.6.3 TSU Public Key Certificate

TSU public keys are made available to Relying Parties in a public key certificate.

The certificate for TSU public key is issued by NAMIRIAL Root CA and is distributed in X.509 form on NAMIRIAL public web site https://docs.namirialtsp.com/certificates/ and in the Italian Trusted List (TSL) https://eidas.agid.gov.it/TL/TSL-IT.xml. Validity information is available in periodically updated CRLs or OCSP service references located in the certificate.

Only one certificate is issued to any specific TSU key. TSU certificates are not renewed. NAMIRIAL TSU does not issue any TST before public key certificate is loaded into the TSU.

7.6.4 TSU Key Rekeying

TSU keys will have the expected lifetime of 10 years. A certificate is issued for the whole expected lifetime. TSU key lifetime is limited by NAMIRIAL Root CA certificate validity. With new Root CA certificate, a new TSU key will be generated.

7.6.5 Life cycle management of signing cryptographic hardware

The practices of HSM life cycle management are described in section 6.2 of NAMIRIAL PS apply.

7.6.6 End of TSU Key Life Cycle

NAMIRIAL takes measures to permanently disable access to the TSU private keys of after their expiry or revocation so that further use or derivation thereof is impossible.

7.7 Time-Stamping

7.7.1 Time-Stamp Issuance

NAMIRIAL TSA offers time-stamping services using RFC 3161 Time Stamp Protocol over HTTP transport. Service URL is specified in Subscriber agreements. Each TST contains Time- Stamping Policy identifier, unique serial number and TSU certificate containing NAMIRIAL TSA identification information.

NAMIRIAL TSU accepts SHA256, SHA384, SHA512 hash algorithms in time-stamp requests and uses SHA-512 cryptographic hash function in TST signatures.

NAMIRIAL TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

NAMIRIAL TSA logs all issued TSTs. TSTs will be logged for 20 years. NAMIRIAL can prove the existence of particular TST on the request of Relying Party. NAMIRIAL might ask the Relying Party to cover the costs of such service.

NAMIRIAL TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2 Clock Synchronisation with UTC

NAMIRIAL TSA ensures that its clock is synchronised with UTC within the declared accuracy of 1 second using the NTP.

NAMIRIAL TSA monitors its clock synchronisation and ensures that, if the time that would be indicated in a TST drifts or jumps out of synchronisation with UTC, this will be detected. In the case of a TST drift or jump out of synchronisation with UTC, NAMIRIAL TSA stops issuing time- stamps until the issue is corrected. Information about loss of clock synchronisation will be made available in public media.

Both local and remote NTP servers with GPS time sources are used for NTP reference. Monitoring of clock synchronisation is done by comparing the time sources.

Leap seconds are not considered and TSTs are issued as usual.

7.8 Physical and Environmental Security

The practices identified in section 5.1 and 6.7 of NAMIRIAL PS apply.

In addition, the access to TSA HSM's is allowed only for persons in the corresponding trusted roles.

7.9 Operation Security

The practices identified in section 6.5, 6.6 and 6.7 of NAMIRIAL PS apply.

7.10 Network Security

The practices identified in section 6.7 of NAMIRIAL PS apply.

TSU systems are configured with only these accounts, applications, services, protocols, and ports that are necessary in NAMIRIAL TSA’s operations.

7.11 Incident Management

The practices identified in section 5.7.1 of NAMIRIAL PS apply.

7.12 Collection of evidence

The practices identified in section 5.4.1 of NAMIRIAL PS apply.

7.13 Business Continuity Management

The practices identified in section 5.7 of NAMIRIAL PS apply.

Backups of the database of all issued TSTs by NAMIRIAL TSA are kept in off-site storage.

If TSU private key is compromised or suspected to be compromised, NAMIRIAL will inform Subscribers and Relying Parties and will stop using the compromised key. NAMIRIAL TSA will revoke the TSU certificate. The following actions will be carried out in accordance with the crisis commitee[1]s decision and recovery plan.

In case of loss of clock synchronisation, NAMIRIAL TSA suspends its operations to prevent further damage. Recovery plan is activated to restore the synchronisation and service.

7.14 TSA termination and termination plans

In case of NAMIRIAL TSA termination NAMIRIAL follows the procedures described in section 5.8 of NAMIRIAL PS.

Additionally, NAMIRIAL takes steps to have the TSU certificates revoked.

7.15 Compliance

NAMIRIAL TSA has implemented the security regulations. Validation of the compliance with these regulations is performed during the annual independent conformity assessment as described in section 8 of NAMIRIAL PS.

The NAMIRIAL TSA’s security regulations contain sensitive security information and are only available upon special agreement with NAMIRIAL.