Qualified electronic signatures and seals preservation policy

Annex 1 - LTA Practice statement

Category	**LTA**	Document ID	**NAM_LTA_PO**	**Namirial S.p.A.**
Written by	**Federica Marti**	Confidentiality note	**Public document**	**CTO**
Verified by	**Enrico Giunta**	Version	**1.0**	**Davide Coletto**
Approved by	**Davide Coletto**	Issue date	**08/09/2023**	—

Signed by: COLETTO DAVIDE
Issued by: Namirial CA Firma Qualificata
Signing time: 12-09-2023 09:35:44
IP address: 93.46.20.169

Namirial
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494 | www.namirial.com

Table of Content

History of changes

V.1	
Date	08/09/2023
Reason	First release
Changes	-

1 Purpose and scope of the document

This document constitutes the Annex 1 of the Long-term archiving (LTA) service practice statement and includes Namirial qualified electronic signature and seal preservation policy.

This preservation service policy describes what Namirial offers regarding its Qualified electronic signatures and seals preservation service, deepening the measures carried out and the methods for extending the reliability of signatures and seals beyond their technological validity period, and indicates the applicability of the service.

The present policy is addressed to all customers who have subscribed to the Namirial preservation service and, more widely, to all those who are interested in it.

1.1 Policy identification and updates

This policy is referenced as follows:

Reference Identifier	OID : 1.3.6.1.4.1.36203.0.0.19511.1.1

The document is kept up to date together with the LTA Practice statement, in order to reflect regulatory changes and developments in the service.

2. References

Law references are already listed in § 3 of the LTA Practice Statement.
The present document, in particular, is defined to explain the service in compliance with the following standard:

Number	Reference
[I]	ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

3 Definitions and acronyms

The fundamental definitions to understand how the service works are already clarified in § 2 Terms and definitions of the LTA Practice Statement and in § Definitions and acronyms of the Operating Manual - Certificate Policy & Certificate Practice Statement for Certification and Time Stamping Services.

The following definitions add to the existing ones:

Terms	Definitions
Preservation evidence	evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object
Preservation evidence policy	set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence
Preservation goal	one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmenting externally provided preservation evidences
Preservation model	Three preservation storage models for the preservation service are distinguished: 1) Preservation services with storage [WST]. In this case, the data to be preserved is stored by the preservation service while the evidences and the preserved data are delivered upon request by the preservation service to the preservation client. The preservation service stores the submitted data object(s) (SubDO(s)) and the preservation object(s) (PO(s)) and the associated preservation evidences. The PO(s) are derived from the SubDo(s) by augmentation or by building a Preservation Object Container (POC). 2) Preservation services with temporary storage [WTS]. In this case, the data to be preserved is stored on the client side. The preservation service keeps the data or a hash of the data to be preserved only temporarily at latest until the evidence is produced. Evidence is produced asynchronously. Once they are produced, the evidence is stored during some time period to allow the client to retrieve them. 3) Preservation services without storage [WOS]. In this case, the data to be preserved is stored on the client side. The preservation service neither stores the SubDO nor the preservation evidence. Evidence is produced synchronously and is included in the response. The preservation service only keeps traces of its actions to be able to provide records of its activities.
Preservation profile	A preservation profile identifies a set of implementation details specifying how preservation evidences are generated and validated and which are pertinent to a preservation storage model and one or more preservation goals.
Preservation scheme	A preservation scheme is a generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated. It can be supported by one or more preservation profiles.
Signature validation policy	In case of preservation of digital signatures where the preservation service collects the validation data needed to determine the status of the digital signature, the signature validation policy is referenced in the preservation

	profile. In this case, the validation policy describes the rules followed to obtain the validation data.
Unique identifier	Unique and permanent reference given to all objects operating in the perimeter of the LTA Service (i.e. Preservation Objects, Preservation evidence, Information packages, Document types, accounts etc)

4. Preservation profile

Namirial applies one preservation profile thoroughly described in the LTA Practice statement, publicly available online - along with the present document - on Namirial S.p.A. website. The preservation profile adopted by Namirial applies during the whole preservation period of the stored objects and during the whole preservation evidence retention period.

The actual preservation profile is active since 2014 and will be used until the termination of the service. Given Italian laws, which place mandatory constraints on the implementations, the profile, in general, does not change: all allowed dynamic aspects are specified and tracked in the LTA Practice statement (the newest version is always available online and all the previous versions, dated and numbered, are stored in the LTA system; thus, it is possible to identify which version applied at which time).

The profile, as per LTA Practice statement, is based on the OAIS schema (see LTA Practice statement references), used to implement a preservation storage model with storage (WST), developed using in the process digital signature techniques (automatic signatures and time-stamps) provided by Namirial itself, given its eIDAS Qualified Trust Service Provider status.

The preservation goals pursued are:

1. the provision of proofs of existence over long periods of time of general data whether this data is signed or not;

2. the preservation over long periods of time of the ability to validate a digital signature, to maintain its validity status and to get a proof of existence of the associated signed data.

This second scenario guarantees the:

1. extension over long periods of time the ability to validate a digital signature and to maintain its validity status (regardless of the signature provider, because Namirial accepts all kind of digital signatures);
2. provision of proofs of existence of data over long periods of time.

To be able to extend over long periods of time the validity status of a digital signature the preservation service provides a proof of existence of:

1. the signature;
2. the signed data; and
3. the validation data (certificate paths, revocation information).

The Namirial LTA system preserves these objects as a whole: through the Packages mechanism outlined in the LTA Practice statement, the digitally signed documents are stored with their signatures, with the associated metadata and validation data.

The supported input formats, supported digital signature formats, output formats and supported evidence formats are defined in the LTA Practice statement.

All objects in the system are identifiable through a unique identifier.

5. Preservation evidence policy

The preservation evidence policy applied is thoroughly described in the LTA Practice statement.

It is based on the Italian standard UNI 11386 (SInCRO) (Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali), that defines the structure of the Preservation Index as a strategic component of the long-term preservation process.

This technical standard defines an XML schema that identifies the structure of the data set to support the preservation and retrieval process of digital objects. This data set is called the Preservation Index (PIndex) and it is a file to be associated with the objects submitted for preservation.

This XML Index file is signed and time-stamped by Namirial and its validation is possible by opening the Preservation Index and validating the signature and the time-stamp through a certificate validation tool. Moreover, reading the XML, it's possible to verify the integrity of the HASH of the documents submitted by the Producer and all the data related to the Preservation object's owner.

If the preservation evidence needs an update or an augmentation, the Namirial LTA system provides the Revision Information Package (a specification of the Submission Information Package - SIP - outlined in the LTA Practice statement).

6. Signature validation policy

As highlighted in § 4. Preservation profile, Namirial LTA System preserve the whole signed document: LTA Practice statement describes how the submitted objects are checked before becoming preserved objects.

Preserved signed objects, maintaining all their properties, can be validated through every validation tool available (Namirial also provides its own free softwares to perform this operation).