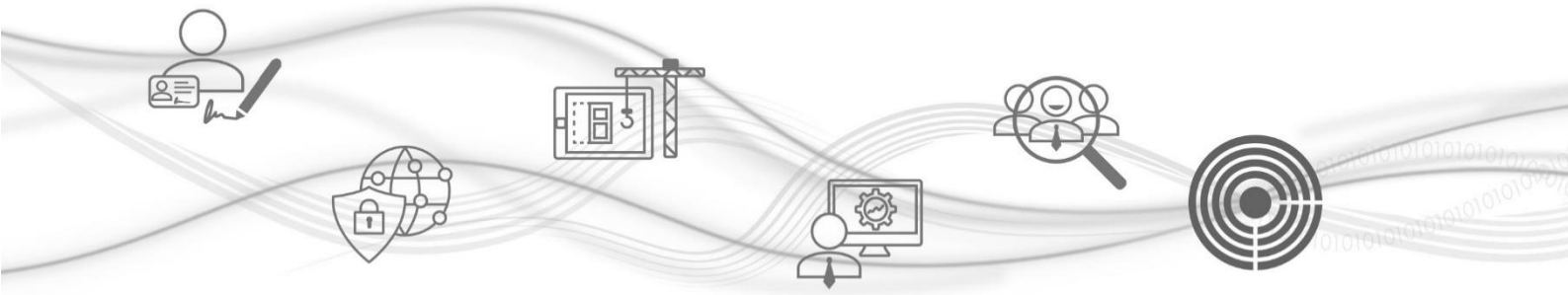
Long Term Archiving

Practice Statement



Category	**LTA**	Document Code	**NAM-LTA-MO**	**Namirial S.p.A.**
Edited by	**Eleonora Luzi**	Confidentiality note	**Public document**	CEO
Verified by	**Davide Coletto**	Version	**11.5**	**Massimiliano Pellegrini**
Approved by	**Massimiliano Pellegrini**	Issuing Date	**20/03/2026**	_____

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 01-04-2026 15:15:50
IP address: 151.0.245.62

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 8.256.361,60 i.v.

Index

Index 2
Version register 5
1 PURPOSE AND SCOPE OF THE DOCUMENT 8
2 TERMS AND DEFINITION 10
2.1 Glossary 10
2.2 Acronyms 16
3 REGULATIONS AND STANDARDS 17
3.1 Reference regulations 17
3.1.1 European Union 17
3.1.2 Italy 17
3.1.3 Romania 18
3.1.4 France 18
3.2 Reference Standard 19
4 ROLES AND RESPONSIBILITIES 21
4.1 Proxies 25
4.2 Obligations of external parties 25
5 ORGANISATIONAL STRUCTURE FOR THE LTA SERVICE 26
5.1 Organigram 26
5.2 Organisational structures 26
6 OBJECTS RELATED TO THE LTA PROCESS 30
6.1 Unique identifiers 31
6.2 Preservation objects 31
6.3 File Formats 32
6.3.1 Evaluation and interoperability index 33
6.3.2 Potential obsolescence of formats 34
6.4 Submission Information Package (SIP) 34
6.4.1 Pre-package 41
6.4.2 Revision Information Package 41
6.5 Archival Information Package (AIP) 41
6.6 Dissemination Information Package 45
7 LTA PROCESS 48

7.1 Ways of ingesting Submission Information Packages 49
7.2 Cheks on Submission Information Packages and objects contained within them 50
7.3 Signature Report 51
7.4 Acceptance of Submission Information Package and Generation of Submission Report 51
7.5 Rejection of the Submission Information Packages and Reports of anomalies 54
7.6 Antivirus Report 55
7.7 Creation and handling of the Archival Information Package 56
7.8 Encryption of objects 56
7.9 Management of documents containing sensitive data 56
7.10 Creation and handling of the Dissemination Information Package 57
7.11 Production of duplicated and digital copies and description of the possible intervention of a Public official 58
7.12 Preparation of measures to ensure interoperability and transferability to other providers 58
7.13 Interaction with the service 58
7.14 Deletion 59
7.14.1 Preservation Period 61
7.15 Use of Qualified Electronic Signatures and Seals Preservation Service 61
8 LTA SYSTEM 63
8.1 Logical components 65
8.2 Technological components 66
8.3 Physical components 67
8.3.1 Italy 68
8.3.2 France 68
8.3.3 Spain 68
8.3.4 Romania 68
8.3.5 LATAM 68
8.4 Software Components 69
8.5 Management and development procedures 69
8.5.1 Operation and Maintenance of the LTA System 69
8.5.2 Log 70
8.5.3 Change management 70
8.5.4 Periodic audit of compliance with relevant regulations and standards 70

8.5.5 Security management and risk assessment 71
9 MONITORING AND CONTROLS 72
9.1 Monitoring procedures 72
9.2 Verifying the integrity of archives 74
9.3 Solutions adopted in case of anomalies 74
10 ANNEXES 76

Version register

N°Ver/Rev/Draft	Date of issue	Description
1.0	28/11/2014	First issue of the document according to the AgID Practice Statement model for accreditation
2.0	22/01/2015	New issue for revisions
3.0	05/02/2015	Integration of the document for the accreditation with AgID
4.0	22/02/2016	Various revisions in all chapters of the document
5.0	26/09/2016	Review of the topology of service delivery sites, review of the organisational chart
6.0	26/10/2017	Various revisions in all chapters of the document. In particular: revision of the topology of the service delivery sites; restructuring and reformulation of the contents; updating of the technical specifications with respect to the latest version of the technical specifications
6.1	11/10/2018	Updating glossary and regulations; revising the organisational chart; updating the format table
7.0	19/09/2019	Updated definitions, updated Index of the SIP, AIP, DIP structure; specified submission mode for secure data transmission; added auxiliary site in case of unavailability of the Senigallia site
8.0	04/06/2020	Updating Roles and Responsibilities
9	04/08/2021	Revisions and adjustments in all paragraphs of the document. In particular: -Update of Terminology to comply with AgID Guidelines (par. 2) -Update of regulation to comply with AgID Guidelines (par. 3) -Updating Roles (par. 4) -Updating of draft tables on stored

		objects (par. 6.1) -Updating of Formats and addition of Interoperability Assessment to comply with AgID Guidelines (par. 6.2) - Adaptation of the Indexes related to the preservation process (SIP, AIP, DIP) (par. 6.3, 6.4., 6.5) -Inclusion of the paragraph on the encryption of digital objects (par. 7.6) - Update Physical Components (par. 8.3) - Correction of typos Monitoring procedures (par. 9.1)
10	09/05/2022	Revisions and adjustments in the following chapters of the document: -Glossary update (2.1) -Regulation and Standards Update (31, 3.2) -Updating of roles (4) -Updating the organisational structure (5.1, 5.2) -Update of supported formats with reference to Annex 2 of the AgID Guidelines (6.2) -Updating of monitoring procedures/ticketing platform (9.1) -Updated image numbering
10.1	27/06/2022	Revisions in the following par.: -Glossary update (2.1) - Inclusion of the paragraph on management of documents with sensitive data (7.7)
10.2	27/02/2023	Revisions in the following par: - Update physical components (8.3)
11	08/09/2023	Update of the entire document: -Document code update -Glossary update (2.1) -Acronyms update (2.2) - Update norms and standards (3) -Update roles (4) -Update terminology related to information packages (all paragraphs) -Added paragraph 6.3.1 "Pre-package -Added paragraph 6.3.2 "Revision Information Package" -Updated paragraph 7.7 -Updated paragraph 7.9 "Access to the System -Updated component 8 -Add paragraph 10 'Annex'.

		-Updated pics
11.1	15/05/2024	-Updated paragraph 1 -Added paragraph 4.2 "Obligations of external parties." -Updated paragraph 8.3 with maximum system configuration interval -Updated paragraph 6.1 "Unique identifiers" -Updated paragraph 7.11 "Discard" -Updated paragraph 7.13 "Use of Qualified Electronic Signature and Seal Preservation Service"
11.2	10/09/2024	Minor changes
11.3	20/12/2024	Not published in English
11.4	02/12/2025	- Updates to the section on regulatory references and standards; - Updated paragraph 2.1 "Glossary"; - Updated paragraph 4 "Roles and Responsabilities"; - DIP content update at paragraph 6.6 "Dissemination Information Package"; - Supported formats and extensions update at paragraph 6.3 "File format";
11.5	20/03/2026	– Updated paragraph 3.2 "Reference Standard" added HDS standard; – Updated paragraph 8.3 "Physical components" – Added paragraph 7.11 "Production of duplicates and digital copies and description of the possible intervention of a Public official"; – Updated paragraph 7.14 "Deletion"

1 PURPOSE AND SCOPE OF THE DOCUMENT

This document represents the Practice Statement for Long Term Archiving service provided and managed by Namirial Group, and it is adopted in accordance with the regulations on the generation, management, and archiving of digital documents.

The purpose of this document is to illustrate in detail the organisation, the subjects involved, and the roles played by them, the operating model, the description of the process, the description of the architectures and infrastructures used, the security measures adopted and any other information useful for the management and verification of the operation, over time, of the LTA system, in accordance with the Guidelines.

This document also describes all the procedures and practices followed by the Preservation Service Manager and by the Provider in managing the security of the service, documents and information processed in the LTA System.

This Practice Statement covers the LTA service and, in Annex 1, the Practice Statements for a Qualified Electronic Signatures and Seals Preservation service, which is used by the LTA service to ensure the integrity of the stored data and preserve qualified electronic signatures and seals. The Qualified Electronic Signatures and Seals Preservation service is designed to meet the requirements of Regulation (EU) No 910/2014 (eIDAS Regulation) as qualified preservation service for qualified electronic signatures and seals, i.e. compliant to articles 34 and 40 requirements, and is audited by an Accredited Conformity Assessment Body (CAB) and under supervision. The LTA Service implements a non-qualified electronic archiving service as defined in article 3(16)(m) of the eIDAS Regulation as revised by Regulation (EU) 2024/1183.

This document has been drawn up according to the following principles:

- **Compliance Principle**: the document aims to describe a LTA system and the archiving process in accordance with the valid regulation framework;
- **Transparency Principle**: the document aims to provide a clear explanation of the LTA System and the provided processes;
- **Process perspective**: the document aims to describe the steps of the archiving process according to the technical rules and reference models, including the OAIS (Open Archival Information System) standard ISO 14721;
- **Relevance Principle**: only relevant information is contained in this document, with a level of detail aimed at facilitating inspections, checks and controls, without specific and/or superfluous technical and procedural details;
- **Accuracy Principle**: information has been reviewed by several people, placed at different levels of the decision-making chain;
- **Concreteness Principle**: this document describes the LTA System with regard to all aspects related to the archiving and use of digital information assets, in accordance with the reference models;
- **Customisation Principle**: the description of any specific provision of the LTA service for a given designated community accessing the LTA System is performed on the basis of an analysis and preliminary study of the needs of the document owner and system users, in accordance with the OAIS

(Open Archival Information System) reference model standard ISO 14721 and is reported as a contractual annex.

This Practice Statement is also associated to the documents in the following table, which go into more detail on various aspects of the LTA Service.

Associated documents	***Description***
Service Data Sheet	This is the technical specification - annexed to the Contract - containing Contract specifics, in particular the essential requirements of the Service, the relative technical-functional and procedural specifications, as well as the timing of the archiving process. This document constitutes an integral and substantial part of the Customer Practice Statement drafted by the Customer and completes the LTA Practice Statement of Namirial in those aspects relating to the service such as the description of the document types activated by the Customer and the relative metadata, the submission rules, the authorised users, etc.
Application Form	Where applicable, it is the document proposed to the Customer by Namirial or the Distributor, which, together with the Service Data Sheet, contains certain specifics of the Contract.

Namirial LTA Practice Statement is identified by its revision level and date of issue. Namirial periodically performs a conformity check on the process of providing the LTA service and, where necessary, updates this document also in consideration of the evolution of regulations and technological standards.

This document is made available through publication on Namirial website and is generated in the PDF/A format, electronically signed, and archived in accordance with the regulations, to ensure the origin, certain date and integrity of the content from its issue and throughout the preservation period.

Back to Index

2 TERMS AND DEFINITION

2.1 Glossary

N.	Term	Definition
1.	Access	Operation enabling a specific user to search and retrieve a copy of documents
2.	Advanced electronic signature	A set of data in electronic form attached to or linked to a document which enables the identification of the signatory of the document and guarantees the unambiguous connection to the signatory, created by means over which the signatory can retain exclusive control, linked to the data to which this signature relates in such a way as to make it possible to detect whether the data have subsequently been modified
3.	AgID	Agenzia per l'Italia Digitale
4.	Analogue copy of a digital document	Analogue document having the same content as the digital document from which it is taken
5.	Analogue document	The non-electronic representation of legally relevant acts, facts or data
6.	Archival functions	Data archiving functions (acquisition, archiving, data management, access, dissemination)
7.	Archival Information Package (AIP)	Information package consisting of the transformation of one or more Submission Information Packages (SIP) in accordance with the OAIS standard
8.	Archival Manager	The natural person appointed as Archival Manager of Namirial
9.	Archive	Organic set of documents, folders and documental aggregations of any nature and format, produced or otherwise acquired by a Owner of the object in the course of its activity
10.	Archiving	Processing and management process of documents in current use and/or in the medium to long-term that enables their classification (indexing) for search and consultation purposes
11.	Attestation of conformity of digital image copies of an analogue document	Declaration issued by a notary public or other public official authorised to do so attached to the electronic document
12.	Authentication of document	The validation of the document by means of the association of data relating to the author or the circumstances, including time, of drafting
13.	Authenticity	Characteristic of a document that guarantees that it is what it claims to be, without having been altered or modified. Authenticity can be assessed by analysing the identity of the signer and the integrity of the electronic document

14.	Certification authority (CA)	It is the body, public or private, authorised to issue digital certificates through a certification procedure that follows international standards and complies with the relevant Italian and European regulations
15.	Customer Practice Statement	Document drawn up by the Owner of the object, detailing the specific procedures relating to the Service. This document may also indicate the activities of the LTA process entrusted to the LTA Provider, in accordance with the content of the LTA Practice Statement, and refer, for the parts within its competence, to the same
16.	DataBase	Collection of related and recorded data
17.	Designated community	A well-identified group of potential Users who should be able to understand the presered information, according to the OAIS standard. A designated community may also consist of several communities of Users
18.	Digital Archive	Archive consisting of digital documents, folders and digitized document aggregations managed and stored in a digital environment
19.	Digital copy of analogue document	An electronic document having the same content as the analogue document from which it is taken
20.	Digital copy of electronic document	A document having the same content as the document from which it is taken with a different sequence of binary values
21.	Digital folder	Structured and unambiguously identified aggregation of acts, documents, or data, produced and functional to the performance of a specific activity or a specific procedure. In the public administration, the file linked to the administrative procedure is created and managed in accordance with the provisions set out in Article 41 of the CAD
22.	Digital image copy of analogue document	An electronic document having the same content and form as the analogue document from which it is taken
23.	Digital signature	A particular type of advanced electronic signature based on a qualified certificate and on a system of cryptographic keys, one public and one private, interrelated, enabling the holder by means of the private key and the recipient by means of the public key, respectively, to make manifest and to verify the provenance and integrity of a document or set of documents
24.	Deletion	Operation by which, in accordance with current legislation, documents that have reached the end of their retention period are deleted.
25.	Deletion Package	Package generated by the service following the completion of an object deletion process.
26.	Dissemination Information Package (DIP)	Information package sent by the LTA System to the User in response to its request in accordance with the OAIS standard
27.	Dissemination session	Session for the delivery (dissemination) of one or more Dissemination Information Packages from the Provider to the Owner

28.	Document aggregation	Aggregation of documents or folders, grouped together by homogeneous characteristics, in relation to the nature and form of the documents or in relation to the subject matter or in relation to the functions of the owner of the object
29.	Document creation	The process of ensuring the authenticity of the origin and integrity of the content of documents, compliant as indicated in the Technical Rules
30.	Electronic document	The digital representation of legally relevant acts, facts, or data
31.	Electronic duplicate	Document obtained by storing, on the same device or on different devices, the same sequence of binary values as the original document
32.	Electronic signature	The set of data in electronic form, attached to or logically associated with other electronic data, used as a method of authentication
33.	Evidence	A sequence of binary symbols (bits) that can be processed by a digital procedure
34.	File Format	Mode of representing the sequence of bits that make up the document; commonly identified through the file extension
35.	FTP Server	Application for accepting incoming connections and secure communication with a client via the FTP protocol
36.	Guidelines on the formation, management, and preservation of digital documents (Guidelines) (Linee Guida)	Technical rules issued by AgID on the formation, protocol, management, and preservation of digital documents
37.	Hash function	A mathematical function that generates, from evidence, a print in such a way that it is effectively impossible, from this, to reconstruct the original evidence and generate identical prints from different evidence
38.	Identification	The validation of the set of data uniquely attributed to a subject, enabling its identification in information systems, carried out by appropriate technologies also to guarantee the security of access
39.	IDM	Tool for releasing the identification information of all parties seeking to interact with a System; this is achieved through an authentication module that verifies a security token as an alternative to explicitly authenticating a user within a security scope
40.	Immodifiability	A characteristic that makes the content of the document unalterable in form and content during the entire management cycle and guarantees its static preservation
41.	Imprint	The sequence of binary symbols (bits) of predefined length generated by applying an appropriate hash function to the former

42.	Index of the Archival Information Package	Structure of the data set supporting the archiving process, referring to the SInCRO standard (UNI 11386). It represents the preservation evidence.
43.	Index of the Deletion Information Package	Structure of the data set supporting the Deletion Package process and specifically defined by the LTA Provider
44.	Index of the Dissemination Information Package	Structure of the data set supporting the Dissemination Information Package process and specifically defined by the LTA Provider
45.	Index of the Submission Information Package	Structure of the data set supporting the Submission Information Package process and specifically defined by the LTA Provider
46.	Information Package	Container enclosing one or more objects to be archived, together with the metadata referring to the objects.
47.	Intake	Acceptance by the LTA System of a Submission Information Package as complying with the terms of the LTA Practice Statement
48.	Long Term Archiving System (LTA)	System for archiving data and documents for long-term and with legal evidences of the process
49.	LTA Practice Statement	The analytical document, relating to the LTA System, drawn up by the LTA Provider and published in its updated version on its website, in which the specific procedures relating to the Service are detailed, as well as the general policies of the LTA System
50.	Management Cycle	Time span of existence of the document, folders, document aggregation or archive from its formation to its deletion or preservation over time
51.	Metadata	Set of data associated with a document, or a folder, or a document aggregation to identify it and describe its context, content, and structure, and to allow its management over time in the LTA System
52.	Originals not unique	Documents whose content can be traced through other records or documents whose archiving is mandatory, even if in the possession of third parties
53.	Owner of the object (or Producer Subject)	Person who originally formed for his own use or commissioned another person or acquired the document in the course of his work or who has the availability of it
54.	Long-Term Archiving	Long-Term Archiving consists of all the activities aimed at defining and implementing the overall LTA system policies and governing its management in relation to the organizational model adopted. The purpose of LTA is to preserve in the long-term period the documents owned by the Customer as agreed at a contractual level in order to ensure the document integrity, authenticity, and legibility, maintaining their legal validity throughout the contractually established preservation period

55.	Preservation evidence	Evidence produced by the service that can be used to demonstrate that one or more preservation objectives have been achieved for a specific preservation object.
56.	Preservation profile	A preservation profile identifies a set of implementation details that specify how preservation evidence is generated and validated, and that are relevant to a preservation model and one or more preservation objectives.
57.	Preservation evidence augmentation	Augmentation of data to existing preservation evidence to extend the validity period of that evidence.
58.	Preservation Manager	Subject, identified by the Owner of the object of preservation responsible for the provision of the Service, who manages and implements the overall policies of the LTA System, ensuring compliance with the requirements of the standards
59.	Preservation process	Set of rules aimed at the preservation of documents
60.	Preservation Service Manager	The natural person appointed as Preservation Service Manager of Namirial
61.	Private key	The element of the asymmetric key pair, used by the holder, by means of which the digital signature is affixed to the document
62.	Producer	He is responsible for the generation of the SIP and its transmission to the LTA Provider
63.	Public key	The element of the asymmetric key pair intended to be made public, whereby the digital signature affixed to the document by the holder of the asymmetric keys is verified
64.	Qualification	Recognition by the relevant bodies that a public or private entity carrying out activities meets the requirements of the highest level, in terms of quality and security
65.	Qualified certificate	It is an electronic document certifying, with a digital signature, the association between a public key and the identity of a subject (natural person)
66.	Qualified electronic signature	A particular type of advanced electronic signature that is based on a qualified certificate and realised via a secure signature-creation device
67.	Qualified LTA Provider	Provider, public or private, carrying out activities that has been recognised as meeting the requirements of the highest level, in terms of quality and security
68.	Recipient	Identifies the subject/system to which the document is addressed
69.	Reliability	Characteristic expressing the level of trust the user places in the document
70.	Research session	A session started by a User of the LTA System, during which it is possible to retrieve and view the digital objects

71.	Revision Package	Information package sent to the LTA System according to a predefined format in order to make a revision to the data previously archived by the System
72.	Secure signature generation device	The secure devices for generating the qualified signature, which must have security certification according to Art. 35 of the CAD
73.	Security Copy	Backup copy of the archives of the LTA system
74.	Security Plan	The company document that analyses the context in which the company operates, reporting on the internal and external factors that influence it, and highlights the main critical issues related to the management of the security of the information managed
75.	Service Level Agreement (SLA)	It is the agreement between the owner of the object, the producer, the Preservation manager and the Provider on the service levels to be guaranteed
76.	Signature holder	The natural person to whom the electronic signature is assigned and who has access to the electronic signature creation devices
77.	Signature Report (or Validation Report)	Electronic document resulting from the verification of the qualified signature or qualified seal, containing data relating to the qualified certificate used to apply the signature/seal and preserved together with the preservation evidence as proof.
78.	Storing	Process of transposing analogue or electronic documents onto any suitable medium through an elaboration process
79.	Submission Information Package (SIP)	Information package sent by the Producer to the LTA System according to a predefined format
80.	Submission Report	Digital object certifying that the LTA System has taken over the SIPs sent by the Producer
81.	Submission session	Session for the sending (submission) of one or more SIPs from the Producer to the Provider, based on a format and content data model defined and agreed between the parties
82.	System log	Chronological recording of operations performed on a system for the purposes of controlling and verifying access, or logging and tracking changes that transactions introduce into a database
83.	Time Reference	Information containing the date and time with reference to Coordinated Universal Time (UTC), the affixing of which is the responsibility of the party forming the document
84.	Time validation	The result of the procedure by which one or more documents are assigned a date and time that can be enforced against third parties
85.	Unique identifier	Sequence of alphanumeric characters uniquely and persistently associated with the document, the folder, the document aggregation, to enable its identification

86.	User	Person, entity, or system that interacts with the system in order to use the information of interest
87.	Viewing	Operation to view a stored document and obtain a copy of it

Back to Index

2.2 Acronyms

N.	*Acronym*	*Description*
1.	AIP	Archival Information Package
2.	DIP	Dissemination Information Package
3.	LTA	Long Term Archiving
4.	OAIS	Open Archival Information System, ISO 14721
5.	SiNCRO	Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali (UNI 11386)
6.	SIP	Submission Information Package
7.	SR	Submission Report

Back to Index

3 REGULATIONS AND STANDARDS

3.1 Reference regulations

This section contains the main reference legislation for archiving activity at national and international level to which the activity of Namirial refers.

3.1.1 European Union

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - **GDPR**);
- **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 (**eIDAS**)
- **Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024** amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

3.1.2 Italy

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005, nelle disposizioni attualmente vigenti indicate nelle Linee Guida emanate da AgID;
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli

articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

- **AgID, Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, maggio 2021**;
- **AgID, Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici**, **dicembre 2021**

3.1.3 Romania

- **Lege nr. 135 din 15 mai 2007** privind arhivarea documentelor în formă electronică;
- **Ordin nr. 489 din 15 iunie 2009** privind normele metodologice de autorizare a centrelor de date;
- **Ordin nr. 493 din 15 iunie 2009** privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică;
- **Ordin nr. 585 din 9 mai 2011** pentru completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date;
- **Ordin nr. 1167 din 25 noiembrie 2011** pentru modificarea Anexei nr. 3 la Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date
- **Ordin nr. 20717 din 9 Mai 2024** pentru aprobarea Normelor tehnice privind procedura de acreditare a administratorilor de arhivă electronică și procedura de avizare a sistemelor electronice de arhivare și pentru abrogarea Ordinului ministrului comunicațiilor și societății informaționale nr. 493/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică.

3.1.4 France

- **Ordonnance n° 2004-178 du 20 février 2004** relative à la partie législative du code du patrimoine per la sua parte legislativa, con Décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres) Décret n° 2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI);
- **Arrêté du 4 décembre 2009** précisant les normes relatives aux prestations en archivage et gestion externalisée;
- **Décret n° 2020-733 du 15 juin 2020** relatif à la déconcentration des décisions administratives individuelles dans le domaine de la culture

3.2 Reference Standard

Below are the reference standards to which the Namirial LTA Service refers.

- **ISO 9001** Quality management systems - Requirements;
- **ISO/IEC 27001** Information technology - Security techniques - Information security management systems - Requirements;
- **ISO/IEC 27017** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- **ISO/IEC 27018** Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- **ISO/IEC 20000** Information technology — Service management — Part 1: Service management system requirements;
- **ISO 22301** Security and resilience — Business continuity management systems — Requirements;
- **ISO/IEC 22313** Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301;
- **ISO 14721** Space data and information transfer systems - Open archival information system (OAIS) Reference model;
- **ISO 14641** Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
- **ISO 16363** Space data and information transfer systems - Audit and certification of trustworthy digital repositories;
- **ISO/TS 7538** Functional requirements for disposition of records;
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 511** 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;
- **ETSI TS 119 172-4** Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists;
- **UNI 11386 Standard SInCRO** Support for Interoperability in Preservation and Recovery of Digital Objects;
- **NF 461** Système d'archivage électronique;
- **NF Z42-013** Archivage électronique - Recommandations et exigences ;

- **HDS (Hébergeur de Données de Santé)** Security standards and mandatory regulatory framework in France for any organization (public or private, including cloud providers) that hosts or processes personal health data on behalf of third parties

Back to Index

4 ROLES AND RESPONSIBILITIES

The LTA System described in this document defines and adopts a specific organisational model, involving subjects, structures and/or functions assigned to the submission, implementation, process delivery, management, and control of the LTA System. The reference organisational model is formally defined in terms of the roles and responsibilities of the various actors involved in the LTA process, as shown in the table below, in accordance with the roles and activities associated with them as indicated by the regulations and reference standards, including the OAIS.

The activities entrusted to the Preservation Service Manager are indicated in the Contract that the Customer signs upon activation of the service.

Role	*Name*	*Activities*	*Period*	*Possible proxies*
Preservation Service Manager	**Davide Coletto**	– definition and implementation of the overall policies of the LTA System, as well as the governance of the management of the LTA System; – definition of the characteristics and requirements of the LTA System in accordance with current legislation; - – proper delivery of the preservation service to the Producer; – management of conventions, definition of technical-operational aspects and validation of technical aspects specifying detailed aspects and operating procedures for the provision of preservation services	Since 22 January 2015	
	Luca Romagnoli	as above	24 November 2014 to 22 January 2015	
Security Officer	**Mario Veltini**	– compliance with and monitoring of the security requirements of the LTA System established by standards, regulations and internal security policies and procedures; – reporting any discrepancies to the Preservation Service Manager and	Since 5 July 2021	

		identifying and planning the necessary corrective actions.		
	Davide Coletto (interim)	as above	20 July 2018 to 5 July 2021	
	Andrea Lazzari	as above	24 November 2014 to 20 July 2018	
Archival Manager	**Eleonora Luzi**	– definition and management of the preservation process, including the methods of transfer by the Producer, acquisition, verification of integrity and archival description of the documents and document aggregations transferred, exhibition, access and use of the preserved documentary and information heritage; – definition of the preservation metadata set for documents and folders; – monitoring of the preservation process and archival analysis for the development of new LTA System functionalities; collaboration with the Producer for the purposes of transfer to preservation, selection and management of relations with the Ministry of Culture as far as it is concerned	Since 27 Nov 2025	
	Enrico Giunta	as above	26 May 2021 to 26 Nov 2025	already Archival delegate from 20 April 2020 to 25 May 2021
	Valeria Mocci	as above	24 October 2016 to 14 April 2021	

	Matteo Sisti	as above	24 November 2014 to 24 October 2016	
DPO	**Luca Santalucia**	– ensuring compliance with the applicable provisions on the processing of personal data; – guarantee that the data entrusted by Customers will be processed in accordance with the instructions given by the data controller, with security and confidentiality guaranteed.	Since 3 July 2023	
	Vanessa Cocca	as above	5 October 2021 to 2 July 2023	
	Serena Donegani	as above	20 July 2018 to 4 October 2021	
	Luca Romagnoli	as above	24 November 2014 to 20 July 2018	
Information System Manager	**Mario Veltini**	– management of the operation of the hardware and software components of the LTA System; – monitoring the maintenance of the SLA agreed with the Producer; – reporting any SLA discrepancies to the Preservation Service Manager and identifying and planning the necessary corrective actions; – planning the development of the technological infrastructure of the LTA System; – control and verification of service levels provided by third parties, with reporting of any discrepancies to the Preservation Service Manager.	Since 5 July 2021	

	Genesio Di Sabatino	as above	24 October 2016 to 5 July 2021	
	Giuseppe Benedetti	as above	24 November 2014 to 24 October 2016	
Development and Maintenance Manager	**Nicola Bruni**	– Coordination of the development and maintenance of the hardware and software components of the LTA System; – planning and monitoring of LTA System development projects; – monitoring of SLAs related to the maintenance of the LTA System; – relating with the Producer regarding the modalities of transfer documents and files concerning the electronic formats to be used, hardware and software technological evolution, and possible migrations to new technological platforms; – managing the development of websites and portals related to the preservation service.	3 September 2024	
	Fabio Didonè	as above	5 July 2021 – 15 May 2024	
	Davide Coletto (interim)	as above	24 October 2016 to 5 July 2021	
	Gianluca Cigliano	as above	24 November 2014 to 24 October 2016	
System and regulatory Auditor	**Luigi Enrico Tomasini**	– recurring and comprehensive review of the service adherence to all	Since 30 August 2025	

		applicable laws, regulations, and standards		
	Federica Marti	as above	Since 31 July 2023 to 29 August 2025	
	Margherita Menghini	as above	10 June 2022 to 31 July 2023	

4.1 Proxies

In Romania, Adrian Dinculescu, the assignee of all the tasks for the Preservation Service (except DPO and System and Regulatory Auditor), delegates his functions to the persons listed in the table above.

Back to Index

4.2 Obligations of external parties

Third-party obligations to support the services offered must provide, in general, the following assurances:

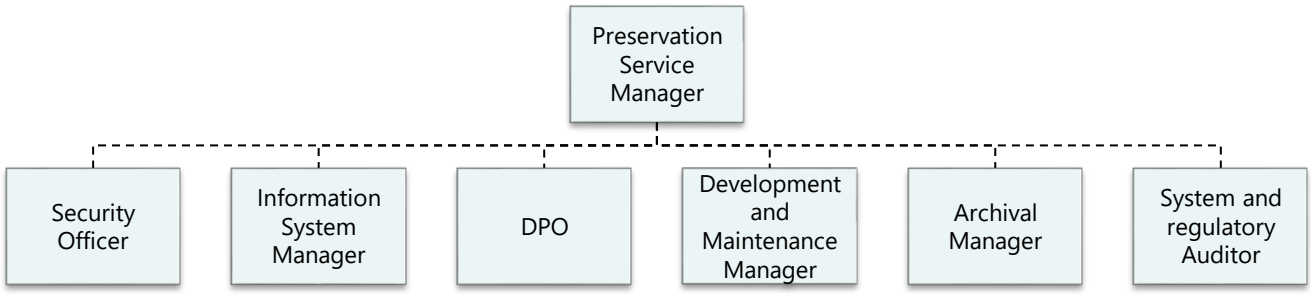
- know and comply with all that is stated in this document and in the preservation policies;
- observe and facilitate compliance with all that is stated in this document and in the preservation policies;
- inform of all changes that will be made to the infrastructure or procedures to ensure that the conditions set forth in the service certification requirements are maintained. In all cases, such changes must guarantee what is stipulated in this document and in the preservation policies;
- sign a contract with Namirial;
- use the services in accordance with the procedures established by Namirial;
- notify Namirial of any incident or event affecting the services

Back to Index

5 ORGANISATIONAL STRUCTURE FOR THE LTA SERVICE

5.1 Organigram

Below is the organisational chart adopted by the Namirial organisation for the management of the LTA service:



Organigram

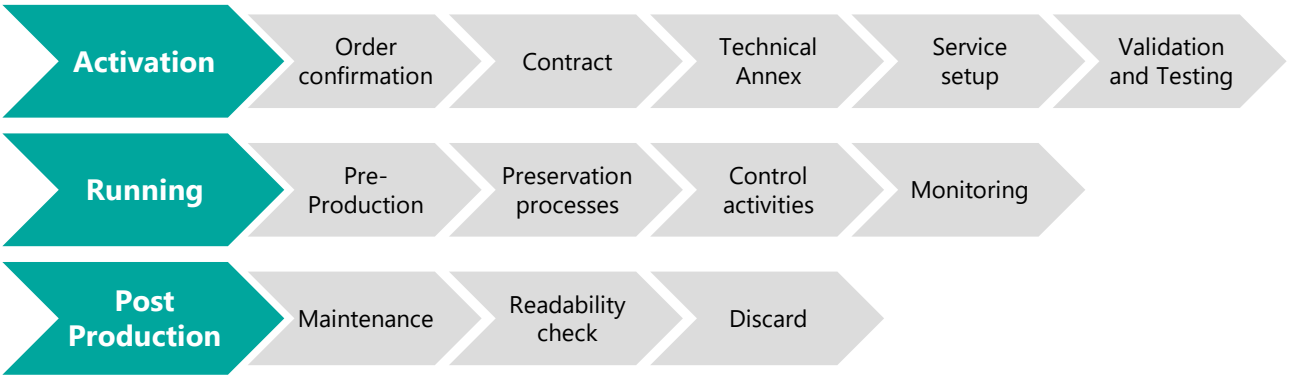
5.2 Organisational structures

Namirial considers the continuous improvement of the performance of its processes and services, as well as the Information Security System, one of the strategic tools through which to achieve the objectives of its business, consisting of the provision of resources and an organisational structure to support the design, development, management, delivery, and marketing of its services.

In particular, for the LTA service, Namirial has certified its information security management system in the logical, physical and organisational domain in which the LTA process is carried out (ISO/IEC 27001, 27017 and 27018 certifications) in the perimeter "Design and provision of services managed in Saas, Paas and on premise mode in the Enterprise Content Management and paperless business (Business Process Management, document acquisition and transmission, electronic invoicing, document formation, management of archiving and preservation of documents in compliance with the law)".

Corporate activities and coordination roles in relation to the LTA Service also consider the conceptual model relating to the ISO 14721 OAIS (Open Archival Information System) standard, in which are clearly distinguished the spheres of Producer (Producer/Customer), Management (LTA Provider) and Designated Community (Users enabled to use the archived documents, in order to make dissemination requests).

Namirial LTA Service has a life cycle characterised by three main phases: Activation, Running and Post-Production.



Service Life Cycle

In each phase of the service there are sub-phases.



Activation phase

The Service **Activation phase** takes place upon formal acceptance of the commercial offer and of the contractual conditions by the customer/owner of the object, including the appointment signed between the parties to perform the role of LTA Provider, Preservation Service Manager and Data Processor.

Once the **Commercial Area** receives the commercial offer, it notifies the activation to the administrative office, which then manages the entry of the customer's personal data in the information systems and the compilation of the **order confirmation** to be sent to the customer.

After the order confirmation has been sent to the customer, the internal information system activates the activities for the Support Area, which takes charge of the activity, contacts the customer, and initiates the preparation of the "Contract" and the Contract specifics document. The latter document is fundamental for the provision of the service to a specific Customer and is an integral part of the service contract.

Following the formal start-up phase of the order acquisition, the support area contacts the customer to define any pre-processes or additions necessary for the SIP submission by providing support to the customer.

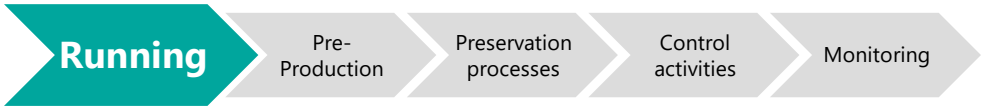
The preparation of the correct initial definition of the requirements and therefore compliance with current legislation on LTA Systems, with also the identification of related fulfilments, is ensured during the analysis phase by the preparation of the document Service Data Sheet, with control and supervision by the **Archival Manager**, the **DPO** (if necessary) and the **Preservation Service Manager**, who oversees final approval.

Subsequently, the process requires that each time there is a change in the Service (Change Process), the Contract Specification document must be updated and shared again between the parties.

Once the specificity of the Contract has been prepared and shared, validated by the **Preservation Service Manager** and the **Customer**, the Support Area engages the **Production Area**, which starts the service configuration activities in the platform.

First, an internal test is performed (internal verification by the **Production Area of the configurations performed** in accordance with what was agreed in the **specificity of Contract document**). Then, if required, testing is carried out with the customer.

The modalities of the testing, if any, are indicated in the specificities of the Contract; following the testing, if any, and its formal validation by the customer, the next phase is the production start-up.



Running phase

The **Production area** oversees managing the hardware and software components of the service and presiding over, controlling and monitoring the correct functioning of the systems for its delivery with the help of the **Nagios monitoring system and a QRadar SIEM** system under the supervision of the SOC.

In addition, the **Production Area** presides over and manages the infrastructure assets and the correct execution of the process, from the takein phase to the consistency check, from the generation of the Submission Report to the preparation and management of the Archival Information Packages, up to the preparation and management of the Dissemination Information Packages for the purposes of viewing and creation of duplicates and copies upon user request.

In particular, the **Information System Manager** has ownership of asset control activities and of monitoring the correct performance of the service. In case of incident, the incident management and resolution process is activated through the creation of an automatic ticket in order to trace the incident and resolve the anomaly. Any significant incidents and discrepancies are reported to the **Preservation Service Manager** through the procedure provided by the ISO/IEC 27001 standard.

Once the production process of document archiving has been successfully completed, the service must be maintained over time also in the post-production phase, for the entire contractually agreed duration, guaranteeing the documents and information packages integrity, authenticity of origin, readability, availability and retrievability, security and confidentiality.



Post-Production phase

The maintenance of the documents and packages generated in the LTA process is ensured by the activities of the Production Area (owner Information System Manager) and the Research and Development Area (owner Development and Maintenance Manager) that guarantee both from the infrastructural and application point of view the archiving and control of the service assets and therefore the correct maintenance of the documents and packages throughout the preservation period agreed with the producer of the documents.

During the post-production phase, the organizational structure of the LTA Provider, in particular with the activities of the **Support** and **Production Area**, supports the fulfillments required by the regulations.

In all these phases of the LTA service and in general in all the activities in charge of the Provider, it is necessary to guarantee the Management of Information Systems and Security in support of the service.

This objective is pursued by the Namirial organization through the definition of the tasks, roles and responsibilities described in this manual, through **periodic checks and audits**, and with tools for control and monitoring. Procedures defined within the safety management system (compliant with ISO/IEC 27001) and corporate quality management system (compliant with ISO 9001) are also the primary tools for risk analysis, planning and adoption of measures for prevention, maintenance, and continuous service improvement.

Primary actors in the implementation of Information Systems Management and Security are the managers defined in the organizational chart, who in concert must ensure the business objective and manage regulatory compliance and continuous improvement of service quality.

Back to Index

6 OBJECTS RELATED TO THE LTA PROCESS

The operation of the LTA System complies with the regulations on the formation, management and preservation of documents and the ISO 14721 OAIS (Open Archival Information System) standard, a reference model for the implementation and management of information systems for the archiving and preservation of digital objects.

Underlying the operation of the OAIS model, taken up by the current technical rules, is the concept of information to be archived (in the form of the so-called "Information Package").

In fact, the submission of packages (containing documents and/or data) to the LTA System by a Producer, as well as any dissemination of documents from the System to an authorized User, take place in the form of one or more separate sessions, through the exchange (submission or dissemination) of information packages.

Namirial Provider, in accordance with the OAIS standard, has implemented in the LTA System, for each of the key phases of the process, information packages as containers containing two types of information:

- Content information;
- Preservation Description Information - PDI.

Content information

It represents the set of information that constitutes the object of preservation; it is an Information Object composed of its Data Object and its Representation Information:

- Data Object: it is the digital object, composed of a set of bits sequences;
- Representation Information: these are information that represents a Data Object, i.e., associates it with more meaningful concepts (e.g., format). Includes Information properties, the meaningful information that must be maintained over time (e.g., formatting elements, etc.).

PDI - Preservation Description Information

They represent the information necessary for proper preservation of Content Information: they are provided by metadata and can be classified into:

- Provenance information: they document the history of the Content Information: e.g., provides information about the origin/source of the Content Information and who has cared for it since its origin;
- Identification Information: they identify and, if necessary, describe one or more mechanisms for assigning identifiers to the Content Information;
- Integrity Information: they ensure that the Content Information has not been altered without documentation of the event;
- Context information: they document the relationship of the Content Information to its environment, including why the Content Information was created, and how it relates to other Content Information;

- Access rights information: they may identify the limits of access to the Content Information, including license terms, legal restrictions, and control systems.

Content Information and Preservation Information are encapsulated and identifiable by Packaging information, which is information used to link and identify the components of an information package (Content Information and Preservation Information).

The Information Package can be searched within the LTA System by Descriptive Information, i.e., the set of information related to the Package description -necessary for the User to search, request, and retrieve the information archived by the System.

For the archiving of the information object the System is based, therefore, on a model for identifying and understanding the data object and its representation information, which contains information of both syntactic and semantic nature.

Back to Index

6.1 Unique identifiers

The LTA service is identified through appropriate identifiers shown below:

- **System OID** (unique system identifier): **1.3.6.1.4.1.36203.7.1.0**

- **Process OID WST** (preservation profile identifier based on the OAIS standard and WST model): **1.3.6.1.4.1.36203.7.1.1**

- **Process OID WTS** (preservation profile identifier based on the OAIS standard and WTS model): **1.3.6.1.4.1.36203.7.1.2**

6.2 Preservation objects

In the Service Data Sheet - a contractual annex agreed between the LTA Provider and the Customer, prepared based on the information shared in the analysis phase or prepared depending on the type of module to be activated - are listed and described the types of documents subjected to archiving for one specific Owner and the related archiving rules, which specify, for each Document Type:

- the kind of the document type;
- the list and description of metadata associated with the documents;
- the retention period;
- the timing of the LTA process;
- other rules that characterize the LTA process.

The Document Types of digital objects to be submitted into the LTA System are defined through the analysis and classification activities or based on the module to be activated.

6.3 File Formats

The System accepts all formats suitable for electronic archiving in accordance with **Annex 2** of the **AgID Guidelines on the formation, management, and preservation of electronic documents**:

- PDF. PDF/A (.pdf)
- Office Open XML (.dccx, .dotx, .xlsx, .pptx . . xltx . . ppsx, .potx)
- Open Document Format (.odt. .ods, .odp . . odg, .fods, .fodp, .fodg, .odi . . odf, .fodt)
- Markup Language (.html. .htm, .xhtml. .css, .md, .mml)
- XML (.xml. .xslt, .xsd . . xsl)
- TIFF (.tif . . tiff)
- JPG (.jpg ..j peg)
- PNG (.png)
- Scalable Vector Graphics (.svg, .svgz)
- MAIL (.emi, .mbox)
- TXT (.txt)
- Structured data (.csv, .json, .jsonld, .sql)
- Academy Color Encoding System (.exr, .mxf, .amf . . clf)
- Autodesk® (.dwg, .dwt, .fbx)
- Font (.otf, .ttf, .woff, .woff2)
- Audio (.wav, .bwf, .rf64, .flac . . pcm, .raw, .sam, .musicxml. .mid, .midi)
- Video (.mp4, .m4a, .m4v)
- Timed Text Markup Language (.ttml. .dfxp)
- Compress archive (.tar, .jar, .zip)
- ISO (.iso)
- VMDK (.vmdk)

Additional formats may be added in accordance with specific standards, guidelines, or requests from Producers with justified needs. In particular, the system also accepts:

- MP3 (.mp3)
- EDI (.edi)
- Digital model (ifc, .dwg, .dxf)

- XFIR (container based on asic standard)

The format and its interoperability must be properly assessed. If the request comes from the customer, the latter is responsible for this assessment.

Regarding the archiving of files in TXT format, which is not listed among the formats indicated in Annex 2, the Provider has carried out an interoperability assessment for its LTA System in accordance with paragraph 3.1 of Annex 2 of the Guidelines. The assessment and the related interoperability index are reported in the following paragraph.

In all cases, the Producer of the SIPs agreed to submit to the System documents **without executable codes or macro-instructions** that could alter their content.

On the documents, the Producer may add a digital signature in the standard signature formats CAdES (.p7m), PAdES (.pdf) and XAdES (.xml) and/or a time-stamp.

6.3.1 Evaluation and interoperability index

The LTA System supports the TXT format why it is a format that is widely used in many fields and recognised by most software. For archiving purposes, when using this format, it **is necessary to indicate** the specific Character Encoding adopted, on which the Customer is obliged to use standard interoperable fonts.

As indicated by AgID in paragraph 3.2 of Annex 2 of the Guidelines, **the** following is **the interoperability index for the TXT format**:

Feature	*Interval*	*Evaluation*	*Value*
Standardisation	0 a 3	The TXT format is a de facto and de jure standard. It is based on ASCII encoding; ASCII in its original 7-bit version (also called restricted ASCII, or US-ASCII) was recognised as a standard by ISO under ISO 646:1972. There is, however, a second, more recent version, which, being 8-bit, allows a wider range of characters (256 in total) and can therefore better suit the needs of languages where the alphabets are particularly vast: this second version is called extended ASCII and established itself first as a de facto standard (during the 1980s) and later as ISO/IEC 8859. There is, then, a third, enormously more extensive version (there are currently over a million possible characters), called UNICODE and developed in 1991, whose first 256 code points exactly match those of ISO 8859-1.	3
Apertura	0 a 3	The TXT format is an open format	3
Opening	0 a 4	The TXT format is not proprietary	2
Non-property	0 a 2	TXT is an extensible format	2
Extensibility	0 a 3	The TXT format does not allow the incorporation of any metadata within the file	0
Metadata level	0 a 2	The TXT format is non-binary. Being textual, it is among the most robust formats	2
Robustness	0 a 4	The TXT format is readable on any operating environment or device.	4
Device independence	not specified	The TXT format belongs to the text file category, and there are multiple word processing software packages that can be installed on Android, Linux, Mac OS, Windows, and Windows Phone system platforms to access and display files in TXT format.	2
Forward and backward compatibility	not specified	Unformatted format whose content is purely textual (ASCII)	2
Textual or binary		**TOTAL**	**20**

The values and scale used are those recommended in Section 3.2 of Annex 2 of the Guidelines:

- most interoperable format: total ≥ 20
- less interoperable format: total = 0
- minimum threshold: total = 12

6.3.2 Potential obsolescence of formats

The choice of suitable formats, as provided for and recommended by current legislation (e.g., PDF/A format), is recommended to minimize the risks associated with technological obsolescence. However, if technological developments or new standards and regulations give rise to the need to use new formats considered more suitable, a process aimed at adapting the document format may be considered. Following a preventive plan of checks aimed at performing the necessary verifications of integrity, legibility, and adequacy of the digital representation of the documents, an internal transfer process may be planned. This process transfers one or more archived documents by modifying their digital representation, while ensuring the integrity of the content.

Back to Index

6.4 Submission Information Package (SIP)

The Submission Information Package (SIP) is a zip file which include:

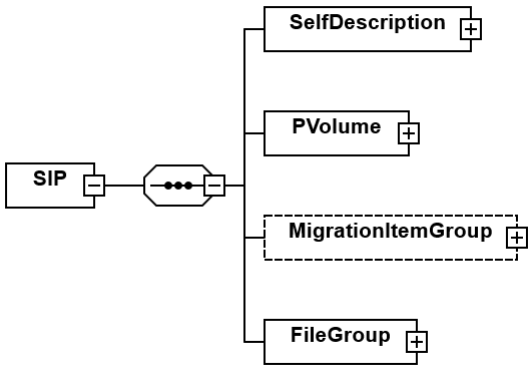
- documents subject to preservation (Content Information), possibly digitally signed (in the CAdES ".p7m" or PAdES or XAdES signing standard) or possibly time stamped (in the CAdES-T, or PAdES-T or XAdES-T time validation standard);
- a SIP Index file aimed at describing Preservation Description Information, i.e., describing information about the preservation object, identification of the Object Owner and the SIP Producer, descriptive and informational data about the packaging and each document in the package.

The SIP Index file is a file in the XML format, which ensures:

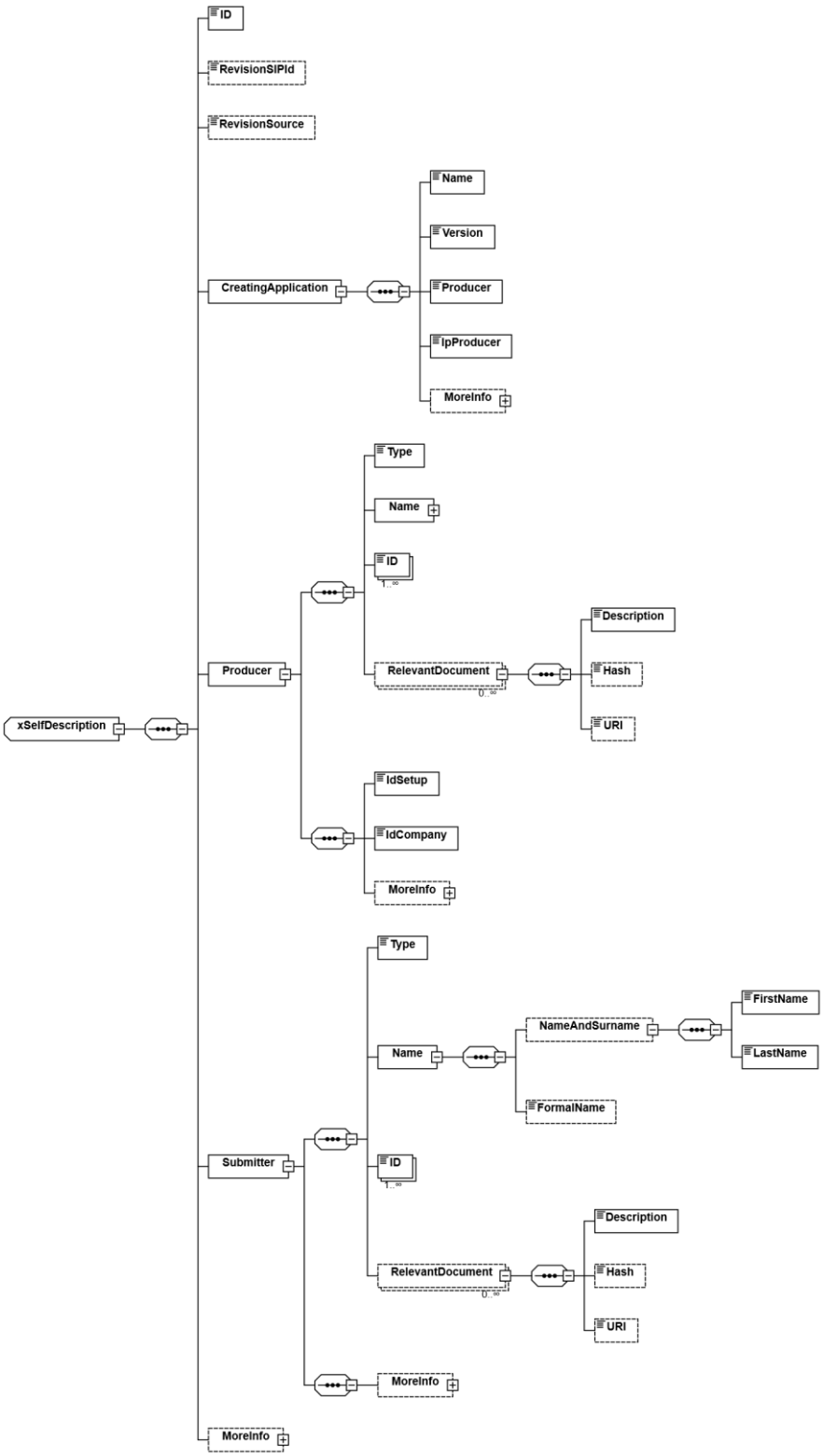
- the identification of the entity that produced the SIP (Producer);
- the identification of the application that produced it;
- the definition of the Document Type to which the documents included in the package belong and any messages from the Customer's Preservation Manager;
- the definition of the documents included in the package, with related information such as: file name, calculated hash, indexes (metadata) and their values, messages from the Preservation Manager, etc.

The SIP Index file can eventually be digitally signed by the Producer.

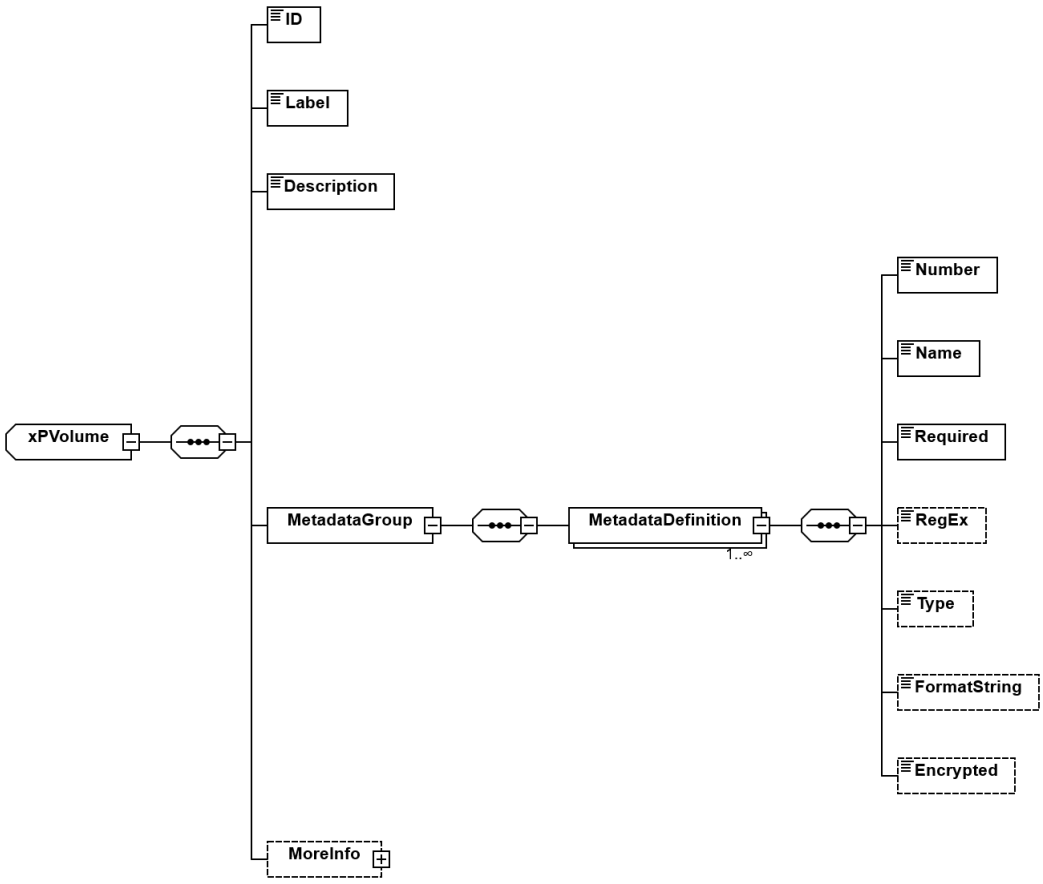
Below is the graphical representation of the XSD file of the Index of SIP:



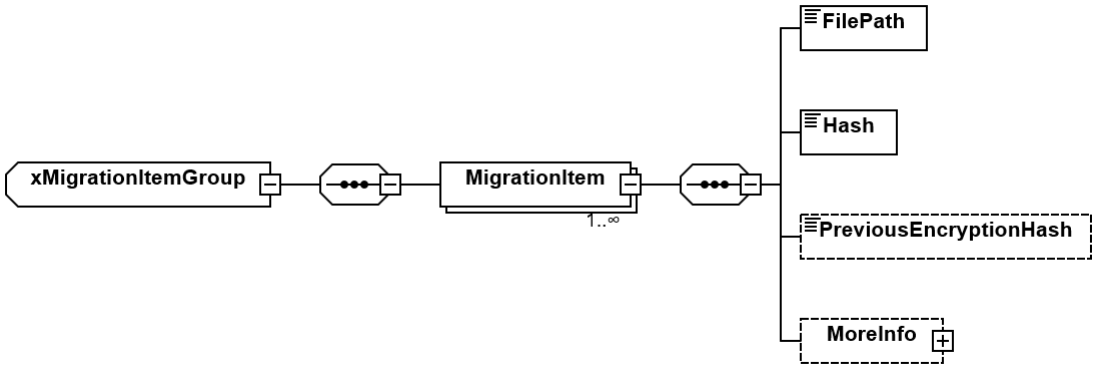
SIP Index Structure



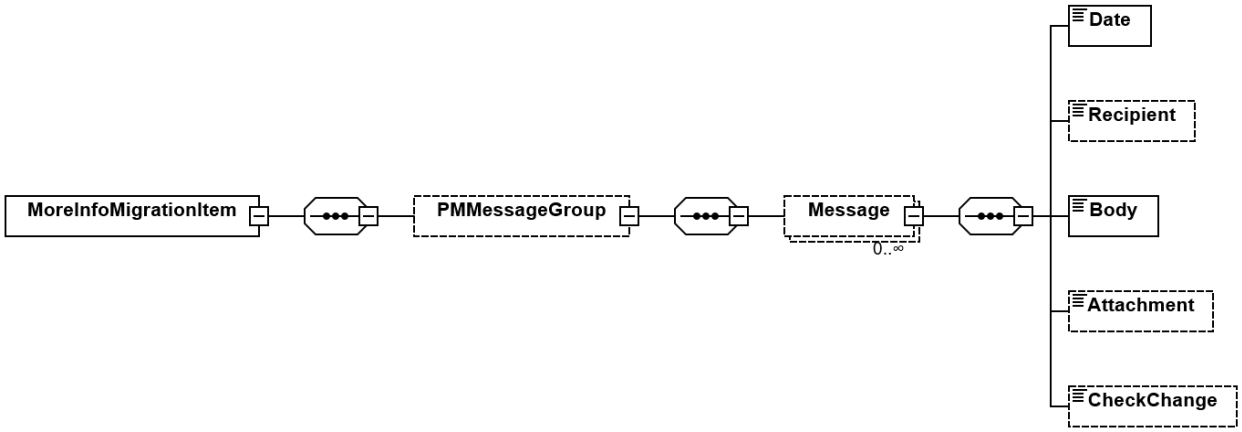
SelfDescription



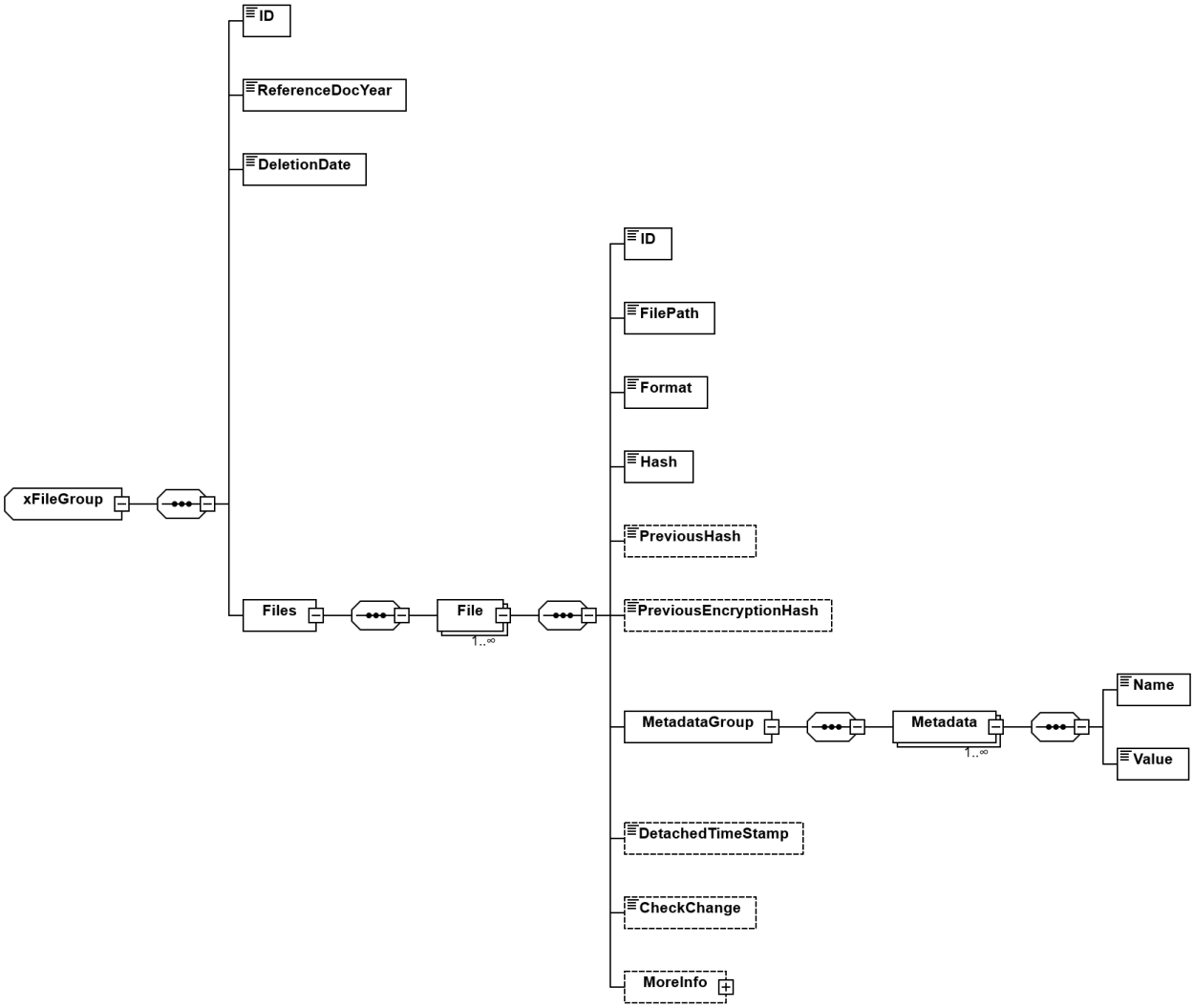
PVolume



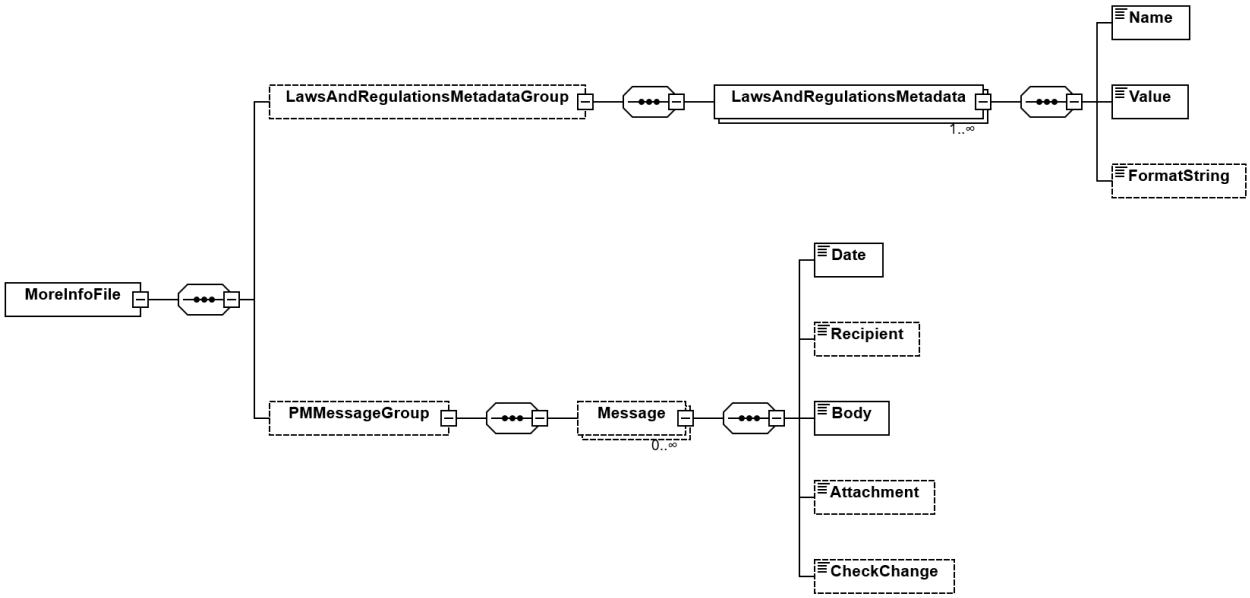
MigrationItem



MoreInfoMigrationItem


ID
ReferenceDocYear
DeletionDate
xFileGroup
Files
File
1..∞
ID
FilePath
Format
Hash
PreviousHash
PreviousEncryptionHash
MetadataGroup
Metadata
1..∞
Name
Value
DetachedTimeStamp
CheckChange
MoreInfo

FileGroup



MoreInfoFile

6.4.1 Pre-package

In the case of submission of unsigned or not time-stamped files and activation of an automatic affixition of certificate in the submission phase (optional mode), the Producer must submit to the System a pre-package (pSIP) containing index and unsigned documents to be archived.

If the checks are successful, the LTA Provider massively affixes the certificate to the Owner's documents identified by the Producer, completing the submission process with a SIP containing the signed documents and a new SIP Index, in which the hash of the unsigned document and the new hash of the signed document are listed.

Both the hash of the unsigned document (Previoushash) and the hash of the signed document are reported in the AIP Index generated by the LTA Provider at the end of the LTA process.

6.4.2 Revision Information Package

A revision package allows the user or system to update and add information to an object previously sent in archiving, by submitting a new SIP containing the unique reference (ID) of the original SIP to the service.

Once the new SIP has been acquired, the service creates a new preservation evidence - generating a new AIP - which contains a unique reference to the preservation evidence of the previous AIP.

To be accepted by the system, a revision package must contain the type of change requested, which can be:

- Rectification: intervention aimed at correcting elements present in the original SIP;
- Integration: intervention aimed at adding information to the original SIP;
- Annotation: intervention aimed at adding a summary record to the content of the original SIP.

Data augmentation with respect to existing preservation evidence (PIndex AIP) is performed using the Revision Package. Before the timestamp certificate applied to the AIP index expires, the system uses this process to extend the validity period of that evidence.

Back to Index

6.5 Archival Information Package (AIP)

The Archival Information Package (AIP) generated in the LTA process is a specialization of the information package and is composed of the transformation of one or more Submission Information Packages in the way outlined in this Practice Statement.

An AIP contains:

- the preservation objects (documents and/or document aggregations subject to the long-term archiving process);
- an Archival Information Package Index (AIPindex) representing Preservation Information and the Preservation Evidence.

The data structure of the AIP Index conforms to the national SInCRO standard (UNI 11386) regarding the structure of the data set supporting the LTA process.

The hash of the objects is computed using **SHA-256 (256-bit Secure Hash Algorithm) cryptographic algorithm** to generate irreversible and unique Hash.

The **AIP Index** is the preservation evidence produced in **XML format** associated with each AIP in which the data structure is detailed. A **qualified electronic signature** of the Namirial Preservation Service Manager and a **time stamp**, also generated with SHA-256 algorithm, are affixed to each AIP Index. The signature and time stamp are issued by Namirial as Certification Authority (CA) and Time Stamping Authority, respectively.

The following is the data structure of the AIP (PIndex – Preservation Index) complete with additional structures related to the various "MoreInfo" elements provided by the SInCRO (PIndex) standard.

- **SelfDescription (1)***: AIP description.
  - **ID (1)**: AIP unique identifier
  - **CreatingApplication (1)**:
    - **Name (1)**: Name of the application that created the AIP.
    - **Version (1)**: Application version
    - **Producer (1)**: Application producer
  - **MoreInfo (1)**
    - **EmbeddedMetadata (1)**: References of the Company to which the LTA process refers.
      - **MoreInfoSelfDescription (1)**
        - **IdSetup (1):** Activation Id of the Company
        - **IdCompany (1):** Id of the Company
        - **PIndexVersion (1):** Version of the PreservationIndex
        - **SystemOID (1):** Unique system identifier
        - **EnvironmentId (1)** Name and country of the environment
- **PVolume (1):**
  - **ID (1)**: AIP unique identifier
  - **MoreInfo (1)**
    - **EmbeddedMetadata**
      - **MoreInfoPVolume**
        - **SIPGroup (1)**
          - **SIP (1 -n)**
            - **SIPId (1):** Id of the Submission Information Package to which the AIP refers
            - **Hash (1):** Hash of the SIP
            - **SRId (1):** Id of the Submission Report
            - **SRHash (1):** Hash of the Submission Report
            - **SRCreationDate (1):** Date of generation of the SR
            - **MigrationItemGroup (1-n):** Info about migrated objects (if any)
- **FileGroup (1-n)**:
  - **ID (1)**: Id of the Document type to which the documents refer.

- **Label (0-1):** Document type name
- **Description (0-1):** Document type description
- **File (1-n)**:
  - **ID (1)**: Unique document identifier assigned by the System
  - **Path (1)**: Logical address of the file represented by a URI (locates the file within the storage).
  - **Hash (1)**: Hash function used, and value returned for the object
  - **PreviousHash (0-1)**: Hash function used, and value returned for the object (referring to a previous Preservation Index, if any) **MoreInfo**: info about PIndex XSD schema
    - **EmbeddedMetadata**
      - **MoreInfoFile:** Information about the document in the LTA System used to identify and describe the document
        - **File (1-n)**
          - **IdDoc**: Unique document identifier assigned by the Producer in the Submission phase
          - **SIPId**: Id of the Submission Information Package
          - **PreviousEncryptionHash**: hash of the unsigned object (only in case of pre-SIP)
          - **MetadataGroup:** list of the metadata associated with the object
            - **Metadata (0-n)**
              - **Name:** Name of the index
              - **Value:** Value of the index
          - **ReferenceDocYear:** Year to which the object refers
          - **LawsAndRegulationsMetadata:** metadata required by specific laws or regulations (if any)
        - **DeletionDate:** DeletionDate associated to the object
- **MoreInfoFileGroup (1)**
  - **PVolume**
    - **ID (1):** Id of the Document type to which the documents refer
    - **MetadataGroup:** list of the metadata associated with the object
      - **MetadataDefinition (0-n):** description of the structure of the metadata associated with the Document type
        - **Number:** Number of the index
        - **Name:** Name of the index
        - **Required:** Required index (true/false)
        - **RegEx:** RegularExpression
        - **Type:** Type of index (String, date, number, ..)
        - **FormatString:** Format of the string

➢ **Process (1)**

- **Submitter (1):** Information about the entity performing the physical transfer of digital objects into the LTA System.
  - **AgentID:** Submitter identifier
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the Submitter
    - **FormalName:** Formal Name of the Submitter

- **RelevantDocument (1-n):** Reference to a document from the entity involved in the LTA process that is relevant to understanding the process itself or the digital objects submitted for archiving.
- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoSubmitter**

- **Holder (1-n):** Information about the Preservation Object Owner or possessor, or holder of the digital objects transferred to the LTA System.
  - **AgentID:** Holder identifier
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the Holder
    - **FormalName:** Formal Name of the Holder
  - **RelevantDocument (1-n):** Reference to a document from the entity involved in the LTA process that is relevant to understanding the process itself or the digital objects submitted for LTA.
  - **MoreInfo**
    - **EmbeddedMetadata**
    - **MoreInfoHolder**
- **AuthorizedSigner (1-n):** Information about the person authorized to sign with an electronic signature (advanced or qualified) or with an electronic seal (advanced or qualified) the preservation index at the conclusion of the index creation process.
  - **AgentName**
    - **NameAndSurname:** Name and Surname of the **AuthorizedSigner**
    - **FormalName:** Formal Name of the **AuthorizedSigner**
  - **RelevantDocument (1-n):** Reference to a document from the entity involved in the LTA process that is relevant to understanding the process itself or the digital objects submitted for LTA.
  - **MoreInfo**
    - **EmbeddedMetadata**
    - **MoreInfo AuthorizedSigner**
      - **PreservationAgent**
        - **PreservationJobRole:** Job description related to the subject.
        - **CertificateIdentificationCode:** Identifier of the signing certificate used in closing the LTA process.
        - **Identifier (0-1):** Subject identifier assigned by the LTA System
- **TimeReference (1)**
  - **TimeInfo (1):** Date on which the Index file was produced. Corresponds within certain time limits (required by the file signing and time-stamping process) to the date the time stamp was apposed.
- **LawAndRegulations (1):** Reference standard for the generation of the PIndex.
- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoProcess:** Additional information related to the LTA process.
      - **PreservationAgent**
        - **AgentName (1)**
          - **NameAndSurname**

- **FirstName:** Name of the Agent
- **LastName:** Surname of the Agent

- **PreservationJobRole (1):** Job description related to the subject.
- **Identifier :** Subject identifier assigned by the LTA System

- **ProcessOID:** Preservation profile identifier based on the OAIS standard

*The number given in brackets specifies the number of occurrences that the element may take within the IAIP: e.g., '(1)' specifies that the element may occur only once; '(1-n)' specifies that it may occur 1 or more times.

Back to Index

6.6 Dissemination Information Package

The Dissemination Information Package (DIP) is generated by the LTA System to ensure interoperability and transferability to other LTA Providers in accordance with regulations and standards and can be requested by the user in the following ways:

- **Disseminated DIP as a result of searching a single document**, in response to the User's request;
- **Disseminated DIP as a result of searching multiple documents**, including those belonging to multiple AIPs, in response to the User's request. The package contains all the requested files and related index files of the AIPs of all packages;
- **Disseminated DIP in response to the request for termination of service**, in which case the DIP contains one or more AIPs, divided by Document Types and year of reference of the documents.

In all modes, the DIP consists of a zip archive containing the following elements:

- documents (digital objects stored in the system) requested by the User.
- Index of the SIP related to the documents.
- Submission Report (SR)
- Signature Report (only if the Qualified Electronic Signatures and Seals Preservation Service is active)
- One or more AIP Index files electronically signed by the Preservation Service Manager and time-stamped, associated with the documents requested by the User.
- DIP Index file: an XML file electronically signed by the Preservation Service Manager, which contains the hash of the AIP Index and the hash of each individual file (requested document or inside a requested package).

The DIP Index contains:

- **DIP Id**, as a result of saving to Data Base;
- **Date of the generation of the DIP** (in UTC format);
- **Owner** to whom the DIP refers (Company Name, Setup Id, Company Id, Tax Code, VAT Number);
- **SIP Id** related to the submitted documents;

- **User** who requested the DIP (First Name, Last Name, Tax Code and/or VAT Number);
- **Preservation Service Manager** (First and Last Name, Tax Code and/or VAT Number);
- **Operator** (First and Last Name/Company Name, Tax Code and/or VAT Number of the LTA Delegate/Provider);
- **Preservation Manager** (First and last name, Tax code and/or VAT number);
- **IP address** from which the generation request came;
- **AIP delivered** (AIP Id, Hash, Hash function used, File Url in the LTA System and DIP)
- **List of requested files** (Document Id, File Name, Reference Year, File Hash, Hash Function Used, File Url in the LTA System and DIP).

The data structure of the DIP is shown below. For terms already used previously, see the descriptive structure of the AIP:

- **Summary:** Info related to the DIP
  - **ID:** Identifier of the DIP assigned by the System.
  - **Producer**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **IdSetup**
    - **IdCompany**
    - **MoreInfo**
  - **Submitter**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **SIPGroup**
    - **MoreInfo**
  - **CreationDate:**
  - **IpAddressClient**
  - **Applicant:** Info related to the subject who requested the dip
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **MoreInfo**

- **Subjects:** Info related to the subjects involved in the process of the creation of the DIP
  - **Subject (0-n)**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **Role**
    - **MoreInfo**
- **Antivirus:** Name of the Antivirus software used in the process
- **LTA:** Info about the LTA System
  - **Name**
  - **Version**
  - **EnvironmentId**

- **AIPGroup:** Info related to the AIPs to which the DIP refers.
  - **AIP (1-n)**
    - **ID**
    - **Hash**
    - **FileUrl**
    - **InfectedFilesCount**
    - **FileGroup**
      - **File (1-n)**
        - **ID**
        - **IdDoc**
        - **PVolume**
          - **ID**
          - **Label**
        - **SIPId**
        - **FileType**
        - **FilePath**
        - **FileUrl**
        - **Hash**
        - **PreviousEncryptionHash**
        - **ReferenceDocYear**
        - **RevisionSIPIdOrigin**
        - **RevisionNumber**
        - **RevisionIsLast**
        - **CheckChange**
        - **VirusName**
        - **MoreInfo**
    - **MoreInfo**

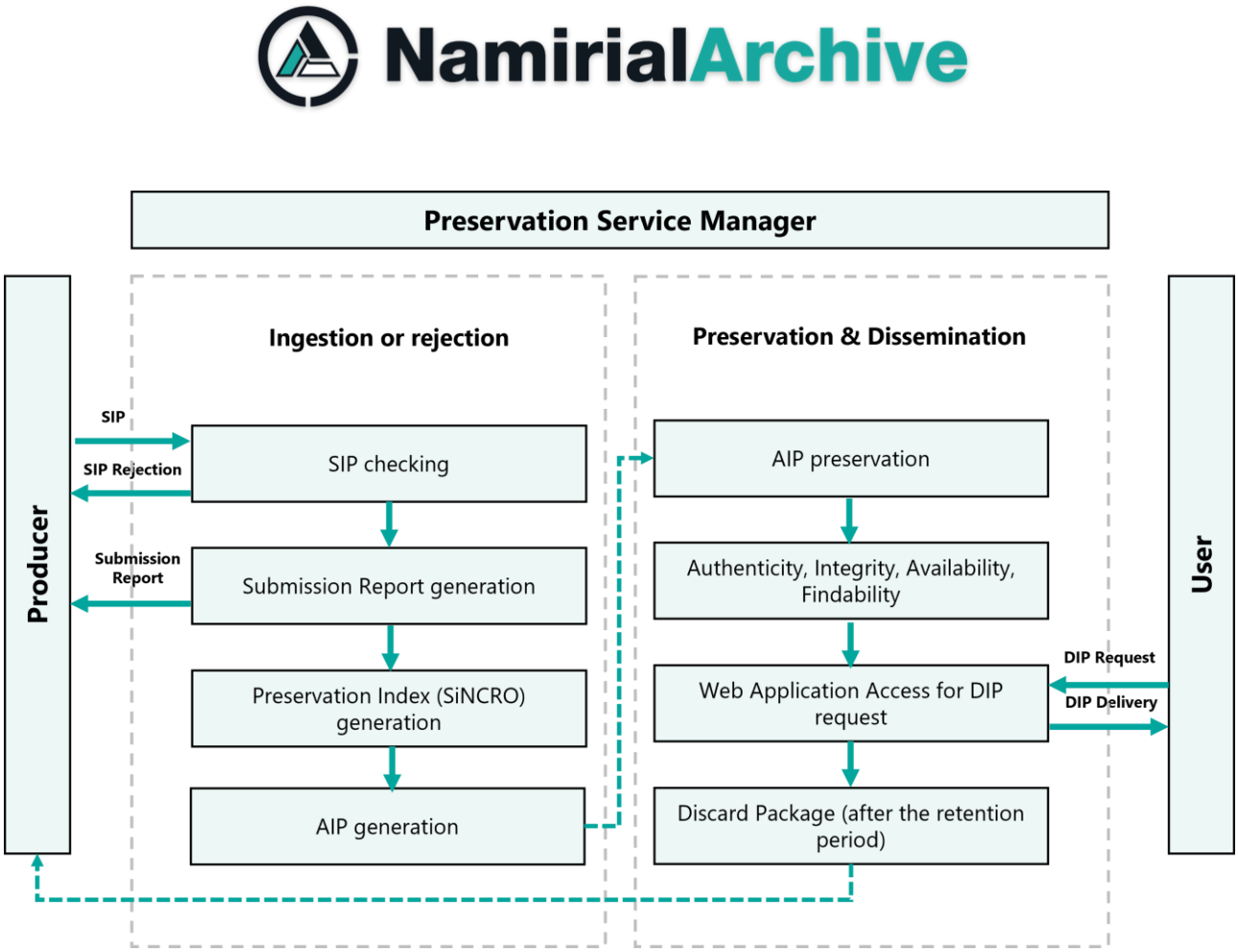
Back to Index

7 LTA PROCESS

The archiving process implemented by the System is governed in all its phases by the **LTA module**, which interacts with the several subjects of the System, the Owner of the objects, the SIP Producer, and the Users or User Groups (the Designated Communities defined by the OAIS standard).

The Owner of the objects, under his own responsibility, delegates the LTA Provider, as the service provider, entrusting the activities stipulated in the Contract to the Provider itself, which, through its Preservation Service Manager, ensures that the correct archiving process is carried out.

The following picture describes the archiving process.



Archiving Process

7.1 Ways of ingesting Submission Information Packages

The system provides the following ways for the Producer to submit SIPs to the Provider:

- Via Web Services (synchronous process)
    a. using web-services and integrating the platform through appropriate SDKs.
    b. through web page, by manual uploading of individual documents and archiving metadata;
2. Via sFTP and upload in the system (asynchronous process).

SIP intake can take place in two ways:

- Synchronous
    - Transfer via web services
    - Checks performed for the SIP in the intake phase.
    - Web services response (result of intake).
- Asynchronous
    - SIP transfer to dedicated SFTP folder
    - Intake triggered by Scheduled Job
    - Ingestion into the LTA System
    - Checks performed for the SIP in the intake phase
    - Creation of the "Intake outcome" file.

Both submission modes guarantee the security and confidentiality of the transmitted data thanks to the encryption of the adopted channel (HTTPS or sFTP).

The specifications and model-data adopted for SIP are the same, and the intake for both modes is concluded with the issuance of:

- an **Id identifier (GUID) assigned to the SIP** upon successful upload so that it is uniquely identified in the LTA System throughout the service lifecycle;
- an Exception if errors occurred during the upload.

Specifically, in sFTP mode, the outcome returned by the intake is a text file that is deposited in an output folder defined and agreed upon between Producer and Provider.

All individual SIP intake activities are tracked through the Log Management system built into the archiving system.

Back to Index

7.2 Cheks on Submission Information Packages and objects contained within them

In the process of SIPs intake in the LTA System, the service performs a series of consistency checks on each SIP and the objects it contains and generates an **intake outcome**.

- **(Blocker)** Checking that the Submission Information Package contains the SIP Index and files.
- **(Blocker)** Check validity of the SIP Index file with the XSD file.
- **(Blocker)** Check that the company defined in the SIP Index is present in the LTA System and that for this company a subject is set up in the LTA System for signing Submission Reports and AIPs.
- **(Blocker)** Check that the number of files in the SIP matches the number of files defined in the Index of the SIP, if BillList is NOT valued or set to False. While if the BillList field is set to True then the number of files in the package must match the number of documents that refer to single file names. The system checks that all documents indexed within the SIP Index, have a match with the files contained in the package.
- **(Blocker)** Check that the file names in the SIP match the files defined in the SIP Index.
- **(Blocker)** Check that the MIME type (MimeType) of the files defined in the SIP Index has been specified.
- **(Blocker)** Check that the names of the detached time stamps (DetachedTimeStamp) match the files (.tsr) in the folder where the preservation objects are also located.
- **(Blocker)** Check that the paths to the attachments imported from another LTA Provider present in the SIP match the attachments defined in the SIP Index (DIPPre).

The following checks are made for each document defined in the SIP Index:

- **(Blocker)** Verifies that the type defined for the document matches the type defined for the SIP Index.
- **(Blocker)** Verifies that the number of Metadata defined for the document matches those defined within the Document Type.
- **(Blocker)** Verifies that the name and order of the Metadata defined for the document matches those defined within the Document Type.
- **(Blocker)** Verification that the value for the mandatory Metadata is present, following the Metadata schema.
- **(Blocker)** Validation of the value for Metadata according to the defined regular expression, if any, following the metadata schema (entered into the SIP in the SourceVdA section).
- **(Blocker)** Verification that there are no documents with the same Document Id within the LTA System, for the Document Type associated with the company
- **(Blocker)** If the SIP Index has version less than 1.0.5 then verify that the filename meets the xs:anyURI standard
- **(Blocker)** Verifies the Hash of the files with the value entered in the SIP.

- **(Blocker)** Verification that the Hash of the files does not match the Hash of the 0-byte file.
- **(Blocker)** Verification of the Hash of attachments imported from other Provider.
- **(Blocker)** Verification of the validity of the signature on signed files.
- **(Blocker)** Document reference year verification.

If the consistency checks performed in the intake phase are positive, the SIP is acquired by the LTA System, otherwise the outcome shows final rejection.

In the consistency check phase of the SIP, the results of the checks are recorded in the Log Management System with time reference.

Back to Index

7.3 Signature Report

If the Qualified Electronic Signatures and Seals Preservation Service is active, the service performs a dedicated analysis of qualified certificates, generating a specific Signature Report as the result of the verification of qualified signatures and/or qualified seals. This report, in XML or JSON format, is digitally signed by the service (WST model) and also time-stamped (WST model). It contains data relating to the qualified certificates used to apply the signatures/seals and is kept together with the preservation evidence as proof. The Signature Report can be retrieved by the user by requesting the Dissemination Information Package (DIP).

For further information, please refer to Annex 1, which includes the Practice Statement for the Qualified Electronic Signatures and Seals Preservation Service.

Back to Index

7.4 Acceptance of Submission Information Package and Generation of Submission Report

In the case of takeover, the System generates the Submission Report as the outcome of all the checks performed on the SIP since its receipt. The purpose of the Submission Report is to formalize the acquisition of the objects to be archived. This report contains reference to one or more SIPs.

The generation of the Submission Report is done by scheduling a job within the scheduler integrated in the LTA System according to the scheduled timelines.

One or more Submission Reports can be generated for each Object Owner per scheduling:

- each Submission Report refers to only one Document Type;
- for each Owner it is possible to define the maximum number of SIPs to which a Submission Report refers.

The Submission Report is generated in XML format and contains the following information:

- LTA System version info;

- Info of the Object Owner with reference to the LTA System;
- References of the User who submitted the SIP;
- Date of generation of the Submission Report;
- Data of the Preservation Manager associated with the Object Owner;
- Data of the Delegate LTA Provider;
- Data of the Preservation Service Manager;
- Number of SIPs included in the Submission Report;
- Total number of files contained in the SIPs included within the Submission Report.
- Information on the type of SIP filled (first deposit, transfer from another system, or revision)
- Information on the version of the revision or origin SIP, if any.
- The Hash function by which the hash of the SIP Index was generated;
- Hash of the SIP Index(es) related to the Submission Report;
- The IP address of the machine where the SIP was generated.
- The list of messages from the Preservation Manager or his Delegate contained in the SIP related to the file;
- The outcome of the checks after the SIP has been ingested in the LTA System.

The structure of the Submission Report is shown below. For terms already used previously, see the descriptive structure of the packages.

- **Summary:** Info related to the SR
  - **Producer**
    - **Type**
    - **Name**
      - **NameAndSurname**
      - **FormalName**
    - **ID**
    - **IdSetup**
    - **IdCompany**
    - **MoreInfo**
  - **PVolume**
    - **ID**
    - **Label**
  - **CreationDate**
  - **Subjects:** Info related to the subjects involved in the process of the creation of the SR
    - **Subject**
      - **Type**
      - **Name**
        - **NameAndSurname**
        - **FormalName**
      - **ID**

- **Role**
- **MoreInfo**

- **LTA:** Info about the LTA System
  - **Name**
  - **Version**
  - **EnvironmentId**

- **SIPGroup:** Info related to the SIPs to which the SR refers.
  - **SIP (1-n)**
    - **ID**
    - **RevisionSIPId**
    - **RevisionSIPIdOrigin**
    - **RevisionNumber**
    - **RevisionSource**
    - **User**
    - **DocumentsCount**
    - **SubmitterIp**
    - **Type**
    - **MigrationItemsCount**
    - **Hash**
    - **DateFormat**
    - **Cancelled**
    - **PMMessageGroup:** Message of the Preservation Manager
      - **Message (1-n)**
        - **Date**
        - **Recipient**
        - **Body**
        - **Attachment**
        - **CheckChange**
    - **FileGroup**
      - **File (1-n)**
        - **IdDoc**
        - **FilePath**
        - **ReferenceDocYear**
        - **PMMessageGroup**
          - **Message (1-n)**
            - **Date**
            - **Recipient**
            - **Body**
            - **Attachment**
            - **CheckChange**
    - **CheckChange:** List of checks performed by the System on the SIPs
      - **Check (1-n)**
        - **Description:** Description of the type of check
        - **Result**
        - **Date**

MoreInfo

In addition, the Submission Report contains a time reference in UTC (Coordinated Universal Time) format and is digitally signed by the Preservation Service Manager.

Regarding time references, it should be noted that the system clock of all processors used in the service is synchronized with the NTP Time.nist.gov protocol.

Namirial LTA Provider allows the Producer to have Submission Reports available in the following ways:

- **through communication via certified or ordinary email**, according to the email address configured in the Data of the Owner of the object in the system (service configured at the request of the Customer and agreed at the contractual level). The email is automatically formatted by the System and attached is the Submission Report signed by the Preservation Service Manager and the unsigned file (for easier processing of the file by a possible third-party system). An XSLT file is also provided for easy viewing via browser;
- trough **request** to the LTA System **web service**;
- through **access** to the LTA System **web platform** by an authorized User.

All Submission Reports generated by the System, remain available throughout time for retrieving and viewing.

Back to Index

7.5 Rejection of the Submission Information Packages and Reports of anomalies

During consistency checks, the following anomalies may be encountered that generate rejection of SIPs:

- SIP does not contain SIP Index and documents;
- SIP Index file invalid with respect to XSD schema;
- Owner identification and mismatch with what is configured in the LTA System; absence of a Preservation Manager in the LTA System for the Owner of the documents to which the SIP refers;
- no Preservation Manager is configured in the LTA System for the Owner to whom the SIP refers;
- Number of files present in the SIP not matching the number of files declared in the SIP Index;
- File names present in the SIP not matching the file names defined in the SIP Index;
- Negative outcome of verification of MIME type declared in the SIP Index (MimeType among those allowed for LTA);
- Negative outcome of the verification of the formats declared in the SIP Index (formats among those allowed for LTA);
- Presence of files in the SIP Index with unspecified Document Id;
- Presence of files in the SIP Index with the same Document Id;
- Negative outcome of the verification of correspondence between the document type configured in the LTA System and the one declared in the SIP Index;

- Negative outcome of the correspondence verification between the metadata configured in the LTA System for a specific Document Type and the metadata declared in the SIP Index;
- Negative outcome of the verification of correspondence between the name and order of the metadata configured in the LTA System for a specific Document Type and those declared in the SIP Index;
- Esito negativo della verifica della presenza dei metadati dichiarati come obbligatori nell'Indice del SIP;
- Negative outcome of the verification of the presence of the metadata declared as mandatory in the SIP Index;
- Negative outcome of the verification of whether there is a regular expression of the metadata declared in the SIP Index;
- Negative outcome of verification that there are no documents with the same Document Id, within the LTA System, for the same Document Type associated with a given Owner;
- Negative outcome of the verification of correspondence between the hashes (imprints) of the documents calculated by the LTA Provider and the hash declared in the SIP Index by the Producer;
- Negative outcome of the signature validity check on the single document;
- Negative outcome of the digital signature validity check in the case of a signed SIP Index (optional).

The generation and delivery of intake outcomes are all actions recorded in the Log management System of the LTA System with a time reference.

Back to Index

7.6 Antivirus Report

The process includes a specific antivirus scanning function for objects sent to the system. This function notifies the user of any threats that may be hidden in a submitted SIP. The presence of any viruses does not block the arhiving process, guaranteeing the original content sent during submission.

The scan is performed after submission, and if a virus is detected, an antivirus report (AR) is generated with an XML structure based on the Submission Report.

Antivirus reports are generated by a scheduled process that considers each SIP package. After a scan is performed, the report is generated if the SIP package contains at least one virus.

An antivirus scan is also performed when a user requests a DIP.

Back to Index

7.7 Creation and handling of the Archival Information Package

The generation of the AIP Index is carried out in accordance with the relevant technical specifications, in particular to the data model defined by the SInCRO standard (UNI 11386).

The generation of the Index of the AIP corresponds to the final closure of the LTA process in accordance with the standard. This procedure takes place through the scheduling of a job within the scheduler integrated in the LTA System according to the timelines configured for the Object Owner. These rules allow one or more SIPs to be included in an AIP. AIPs are generated in such a way as to guarantee uniqueness and segregation of data for each Owner associated with a company. The nature of the AIP is described in the relevant paragraph.

The Preservation Service Manager's signature and time stamp of Provider are affixed to each Index of the AIP, making the SIPs included in the AIP unchangeable for the duration of the LTA of the digital objects.

The signature and time stamp are issued by Namirial as Certification Authority (CA) and Time Stamping Authority, respectively.

The system, also in the case of AIP generation, records logs for tracking the actions performed on the AIPs.

The recovery procedure in case of corruption or data loss of the AIPs provides for incident management with the highest priority level and recovery using the AIP backup copy.

Back to Index

7.8 Encryption of objects

The objects are encrypted with server-side encryption and keys managed by Amazon S3 (SSE-S3), a service provided by Amazon AWS, as a Namirial Datacenter (the section on physical components indicates any variations based on individual Regions).

When using server-side encryption, Amazon S3 encrypts an object before saving it to disk in its data centers and decrypts it upon request by the Customer.

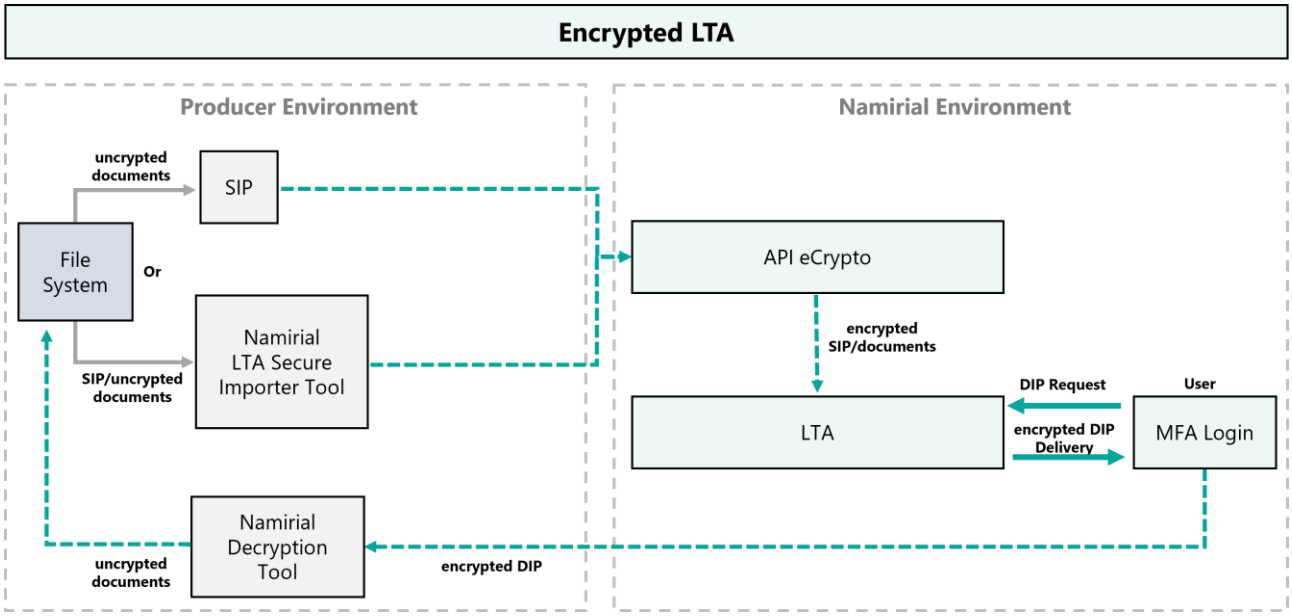
Server-side encryption protects the data at rest. Amazon S3 encrypts each object with a unique key. As further protection, it encrypts the key itself with a master key that rotates regularly. Amazon S3's server-side encryption uses one of the most powerful block ciphers available to encrypt data, namely 256-bit Advanced Encryption Standard (AES-256).

Back to Index

7.9 Management of documents containing sensitive data

In the case of objects containing sensitive data that may require specific security measures, the service implements additional security measures.

Specifically, the solution includes the use of advanced level encryption components, along with access control policies and user identity verification, as outlined below.



Management of documents containing sensitive data

Il The process consists of (a) the generation of SIPs by the Producer or - alternatively - (b) the deposit of already formed SIPs or documents with related metadata in the dedicated Tool installed in its own server. Through web service integration by the Producer (dedicated APIs eCrypto and LTA) or via tool with appropriate scheduling, data are sent in an encrypted tunnel. SIPs are encrypted and sent to the LTA System with the process described in the section on Archival Information Package management.

Access to the Web portal for viewing documents is protected by two-factor authentication; to view a specific encrypted document, it is necessary to download the document. The downloaded file can be viewed with a specific component that allows the files to be decrypted only to subjects authenticated using the assigned decryption key.

Every document access and request operation are tracked through logs.

Back to Index

7.10 Creation and handling of the Dissemination Information Package

The User can request a DIP during service lifetime or in case of termination of the service to migrate to another system. Upon request of the DIP, the system returns via encrypted channel (over HTTPS protocol) the package in the format of compressed zip folder consisting of the digital objects provided by the dissemination request.

The owner of the object is provided with a secure address for a web page dedicated to the return of objects stored in the generated DIPs. The user's interaction with the page is tracked for the purpose of recording the receipt operation. The page remains active to allow the user to retrieve the objects for a period specified in the contract.

Each DIP contains a DIP Index, signed by the Preservation Service Manager, which represents a report of the dissemination carried out.

At the end of the return operations and after the Owner has recovered the items, a declaration of receipt approved by the Owner is shared to confirm that the return has been successfully completed.

The User can request the generation of multiple DIPs, and each action of requesting and making available the DIP is tracked with a unique identifier within the Log Management System with the recording of a time reference.

The storage that maintains AIPs and DIPs consists of three replicas, two at the primary site and one at the DR site: this architecture ensures high reliability and data recovery following data corruption or loss if necessary.

Back to Index

7.11 Production of duplicated and digital copies and description of the possible intervention of a Public official

Upon the user's request, distribution packages may be issued in the form of an authenticated copy, corresponding exactly to the original stored within the system. This mode of issuance ensures the document's full legal validity, certifying the authenticity, integrity, and provenance of its content in accordance with applicable legislation.

In the event that the Producer requests the presence of a public official—as envisaged by Article 23-bis, paragraph 2 of the Digital Administration Code—Namirial shall provide all necessary personnel and resources required to perform the activities associated with such presentation. In this case, the decision to engage a public official shall rest solely with the Producer, who shall be fully responsible for all related expenses, which must be agreed upon in advance with Namirial in accordance with the provisions of the service agreement.

Back to Index

7.12 Preparation of measures to ensure interoperability and transferability to other providers

The main data structure guaranteeing interoperability for Namirial Provider is the Archival Information Package generated according to the SInCRO standard (UNI 11386).

Its dissemination through the request of one or more DIPs guarantees the correct transferability by the Owner of the object to another provider.

In the event of the return of all archived AIPs (e.g., due to the closure of the service or early termination of the service as contractually agreed), the Owner may request the system to disseminate them, via DIP, in the way agreed between the Provider and the Owner.

The system is able to acquire objects previously archived in the event of takeover/migration of archives managed by another providers.

Back to Index

7.13 Interaction with the service

Interaction with the service by the user can be via web integration and web access via interface. Depending on the required functionality, it is possible to:

- submit objects to the service;
- verify successful submission through the use of the Submission Report generated by the service;
- search the objects through unique keys (metadata);
- consult the archived objects;
- download the archived objects;
- download the Dissemination Information Packages (DIP) for the purpose of exhibiting preservation evidence.

The referencing organization of the users, within the contract, indicates the subjects qualified to access the platform (users), to whom Namirial provides unique credentials based on a double authentication factor (conforming to what is provided for the LoA substantial level). In the event of the need to add new users, the subjects indicated by the organization in the contract can request the activation of new users. Such subjects are also entitled to request revocation of credentials. In the case of the web interface, at the first access the user will have to change the password according to current data processing regulations. Each user is responsible for the exclusive control of his or her own access password, which is not recoverable or visible to Namirial staff as it is anonymized.

In addition, for security reasons, the service temporarily deactivates consultation users who have been inactive for more than six months. To reactivate the user, the user must proceed with the password renewal procedure accessible from the login page.

Activities related to access, consultation, and retrieval are tracked through the Log Management system integrated into the system.

Back to Index

7.14 Deletion

The deletion of objects consists of the operation by which their archiving is terminated, removing them from the service. This process is initiated:

- at the end of the archiving period for the objects;
- at the customer's request for specific packages/objects;
- in the event of termination of the service by the customer.

The user has the right to confirm the deletion proposal; if they do not confirm, they have the right to request an extension of the retention period.

In the event of termination, after the archived objects have been delivered to the user, the system proceeds with deletion.

These operations are managed automatically, through jobs and schedules that initiate the process of verifying the retention period, deletion proposals, authorizations, and deletion of items.

As a result of the successful deletion procedure, the service generates a Deletion package.

Mandatory Preliminary Requirements for Public Administrations

Prior to carrying out any disposal operations, Public Administrations are required to obtain clearance from the territorially competent Archival and Bibliographic Superintendency, pursuant to Articles 21 and 68 of Legislative Decree No. 42/2004 (Codice dei Beni Culturali e del Paesaggio) and in accordance with the provisions of the Ministry of the Interior circular of 1 March 1897, as well as subsequent regulations concerning the selection and disposal of archival documents. Such authorization constitutes a necessary and non-derogable condition for the initiation of the procedure: Namirial shall not proceed with any disposal operation in the absence of the corresponding authorization documentation provided by the User.

It is hereby specified that the obligation to obtain clearance from the Superintendency applies:

- to the archives of State administrations, public bodies, and private entities recognized as being of particular historical significance pursuant to Article 13 of Legislative Decree No. 42/2004;
- irrespective of the type of medium (paper or digital) and the preservation method employed.

Accordingly, the Data Controller shall be solely responsible for initiating the authorization procedure with the competent Superintendency in a timely manner, taking into full account the technical lead times required for the issuance of the clearance, which may extend over several months

The following is a list of the objects generated during the deletion process and their contents:

1. Deletion Request:
    - List of AIPs associated with the request
    - Subject who made the request
    - Reason for the requestDeletion
2. Provider Report:
    - List of documents associated with the request generated in CSV format for the Provider and containing minimal information about the files (document ID, document hash)
    - SIPs Indexes
3. Deletion Producer Report:
    - List of documents associated with the request generated in XML format and signed by the Provider, sent exclusively to the Owner as certification of the consistency of the objects to be deleted and containing information relating to the files (document ID, document hash, file name, metadata associated with the documents)
    - SIPs Indexes
4. Deletion Proposal:
    - Deletion Proposal Index
    - Deletion Provider Report

5. Deletion Package:
    - Deletion Proposal Index
    - Deletion Provider Report
    - Deletion Package
6. Any authorisation attachments
7. Deletion Report:
    - Notification of deletion

The Deletion Package contains:

- the deletion proposal;
- a report listing the objects, with minimal coding information such as their trace (object ID, hash), in accordance with data processing;
- the Deletion Package Index, containing, among other information, the outcome of the proposal's acceptance (approved or rejected) and the list of phases. This index is digitally signed by both the Preservation Service Manager and the user operating the deletion for approval.
- any attachments to the authorization process, such as authorizations from administrative bodies

The effective deletion of archived objects is notified to the Owner via the Deletion Report, which certifies the irreversible removal of documents from the system.

During the phases of the process, the Owner interacts with the system exclusively through the operator user who has been previously authorized to access the dedicated dashboard, and/or through an authorized technical user.

All phases of the process are tracked.

7.14.1 Preservation Period

The preservation period is the length of time during which the arching service archives the objects. The preservation period, within the service, is defined by associating a date (deletion date) with the SIP that indicates the end of the preservation period, after which the process of deleting the object and associated evidence is initiated. This date may:

- be provided by the user when generating and sending the SIP;
- be associated with objects archived automatically by the system.

During this period, the service creates and increases - if necessary - the preservation evidence to achieve the preservation objective.

Back to Index

7.15 Use of Qualified Electronic Signatures and Seals Preservation Service

Namirial's Long Term Archiving service provides the preservation evidence for a Qualified Electronic Signatures and Seals Preservation service that is compliant with TS 119 511 "Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques". Each preservation evidence, in compliance with the Italian standard UNI SInCRO, is protected with a qualified electronic signature or seal and a qualified time stamp to guarantee evidence integrity.

The Qualified Electronic Signatures and Seals Preservation service is a Qualified Trust Service that is compliant with Article 34 and 40 of the eIDAS Regulation. The compliance of Namirial as provider of said Qualified Trust Service and of the provided Qualified Trust Service to eIDAS requirements is confirmed by the audit of an accredited Conformity Assessment Body and the supervision of AGID, the Italian supervision body, as established by the eIDAS regulation for qualified trust services. The LTA service providing augmentation of preservation evidence complies with the requirements as an electronic archiving trust service according to Regulation (EU) 2024/1183.

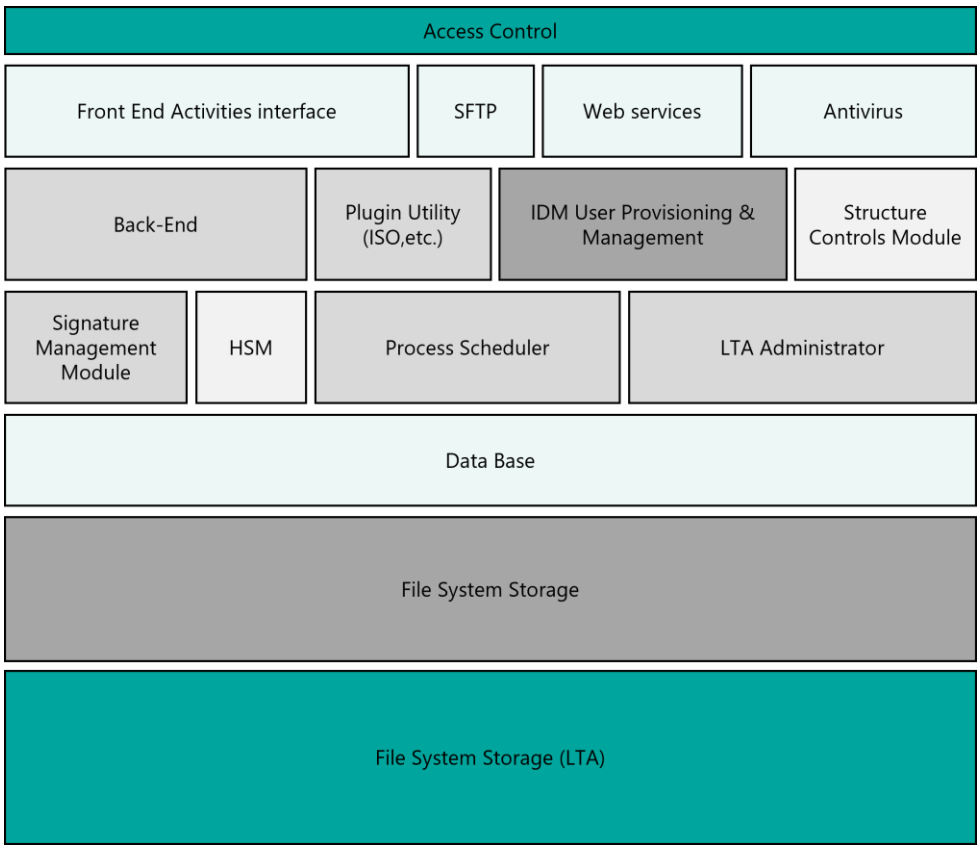
Annex 1 includes the Practice Statements for the Qualified Preservation Service of Qualified Electronic Signatures and Seals.

Back to Index

8 LTA SYSTEM

Namirial LTA Service infrastructure has been designed, organized, and developed to make the work steps atomic and the flow modular. High reliability components allow the system to be adapted according to the current load. Given the critical nature of the service, the IAC (Infrastructure as code), CI/CD (Continuous integration/Continuous deployment) and Business Continuity paradigms were followed from the design phase.

The main components of the solution can be schematized by the following graphical representation.



LTA System components

As depicted in the figure, the solution is developed in modules organized in stacks, in which there is a central core of the system that interfaces with the other logic-functional units.

The solution components are:

- User-accessible Interface front-end for: manual uploading of the documents, searching, requesting package dissemination, copy and duplicate documents creation, and other activities executable by administrators.
- Web Service module for package and document uploading and management activities.
- SFTP module for uploading of SIPs.
- Antivirus.

- Back-end module for interfacing activities with the DB and Filesystem.
- Utilities module (ISO creation, etc.).
- IDM - User Provisioning and Management module for access management.
- Process Scheduler. In the scheduler, jobs are managed for:
    - The intake of the SIP;
    - The start of consistency checks;
    - The generation of intake outcomes;
    - The generation and delivery of Submission Reports;
    - The generation of AIPs;
    - The generation and delivery of DIPs;
    - Deletion process.
- Module for controlling and planning the functionality of the entire service structure (also includes the Routing System that routes traffic to secondary DR sites in case of inaccessibility of the primary LTA System);
- Module for integration with signature devices (HSM).
- Storage management module.
- DB management module.
- Long Term Archiving (LTA) management module.

Based on the structure of the modules, each is expected to have three basic properties:

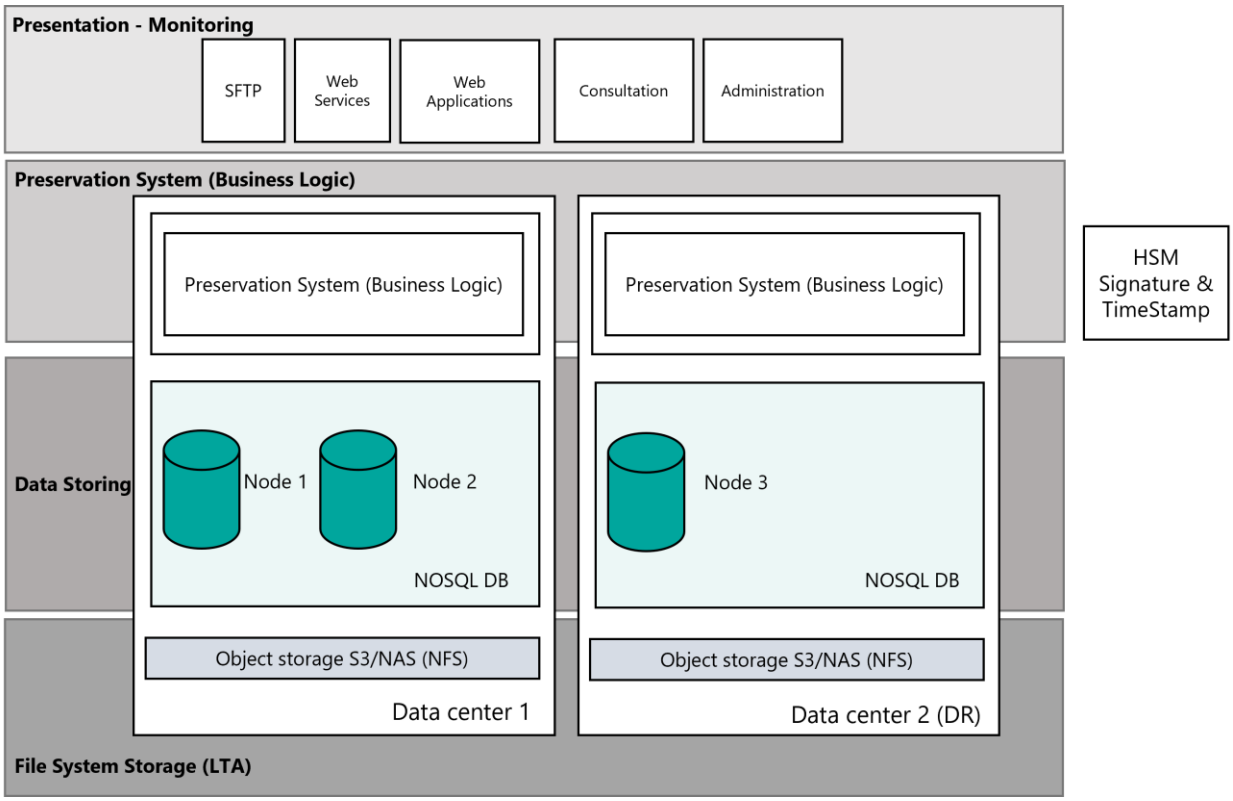
- Identification of the logical/physical person performing the activity;
- Control and management of the activity itself;
- Expandability of the module (activity load balancing, allocation, and clustered growth on available resources).

All module activities are tracked in the Log Management System.

Back to Index

8.1 Logical components

The logical components of the LTA System are described in more detail below.



System logical components

Application front-end (Web App front-end): is the administration and consultation portal of the LTA System. The web portal manages the authentication and profiling of users and allows to configure all the components of the LTA System, the master data of the Object Owner (Companies), the subjects involved in LTA with definition of Roles, Document Types, Users, administration rules for scheduling processes, etc.

DNS Router: the Routing system that in case of inaccessibility of the Primary LTA System, routes traffic to DR sites.

LTA System Web Service: the long term archiving service that exposes all the functions for application management of the LTA process. The APIs exposed are REST and SOAP.

SFTP Server: the service for the management of SIP receipt folders by the Owner.

Process Scheduler: its configuration allows the definition of the submission session, the preparation and management of AIPs, the dissemination session and the discard session. In addition, it allows defining the activation and scheduling of functions and services to continuously control the other functional entities of the LTA System; therefore, it interacts with the other entities of the system (archival planning, general services, acquisition, preservation, data management, accesses).

The logical entity of archival planning and controls works and interacts with the process scheduler and defines the functions and services to control the entire LTA System. This entity, managed by the administrator, defines the policies and jobs to maintain the integrity, availability, retrievability and readability of both archives and documents in the system, in accordance with current regulations and to protect against technological obsolescence. It also defines the data-models of the information packages (SIP, AIP, DIP, Deletion Package).

System Database: the system saves data to a NoSQL-type database with a configuration based on replication of sets of three nodes: two on the primary site and one on the DR site.

MMS Arbiter: the backup administration and data replication management module.

Long-Term File Storage (Object Storage S3): the system supports file storage on Object Storage S3 system and dedicated AWS buckets can be configured to simplify decommissioning/migration operations.

Back to Index

8.2 Technological components

The technological architecture of the LTA System can be divided into three levels:

- First level. Part of networking consisting of the network equipment (routers, switches), the firewall module to protect the system from unwanted access, the WAF (Web Application Firewall) and load balancers that stabilize the application and divide the load among the various machines that deliver the publicly reachable services. Specifically: dedicated VPCs (Virtual Private Clouds) are used at the network level, within which the various services organized into the different subnets required for scalability are built. Each subnetwork is built on one of the three available Availability Zones (AZs) to maximize resilience in the event of an incident on a single Availability Zone. Each VPC is dedicated to a specific service that is part of the system and is isolated from the others. The entry point of the system is a load balancer that distributes the work that the back-end machines perform after the passing of request checks on the WAF.
- Second level. Represents the Core of the LTA infrastructure and consists of physical servers that implement the functional modules and components, HSM devices or signature management libraries. In particular, the HSM devices are kept at the Namirial Certification Authority (CA) and comply with the security requirements of current regulations. To this level also belong all the antivirus control facilities of the packets sent by users (each document is checked and reported to the Producer in case of elements traceable to malware or viruses with a dedicated antivirus report).
- Third level. Represents the Datastore of the system and contains all documents and all AIPs.

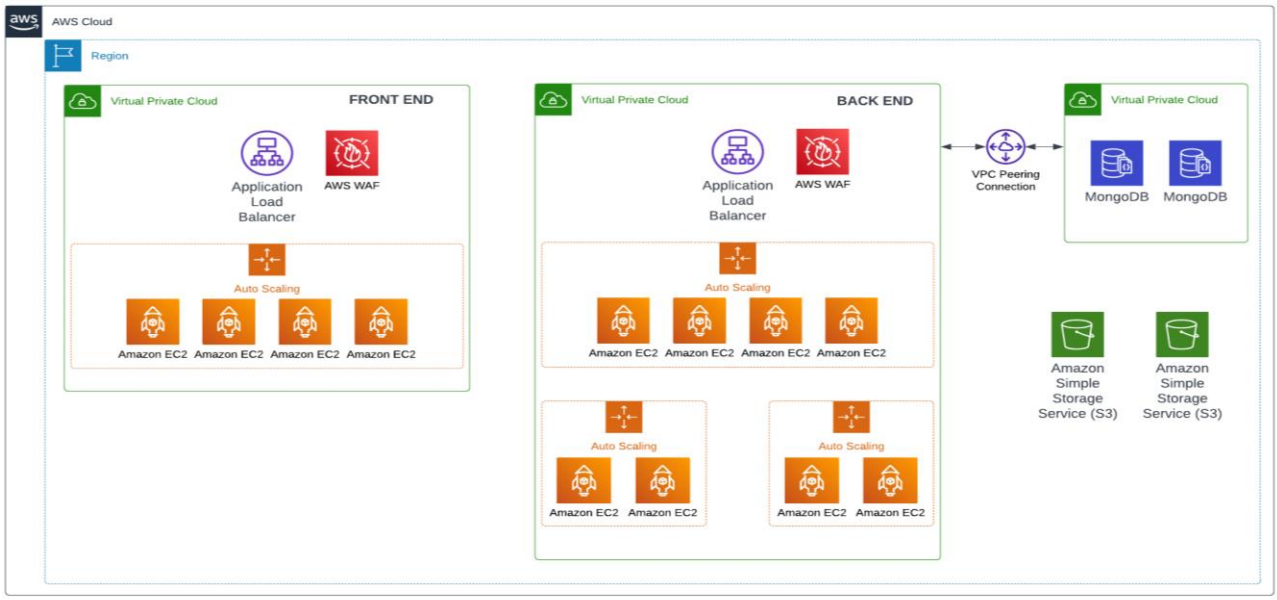
From the service delivery facility (primary facility), there is a direct, encrypted, private link to the Disaster Recovery facility. This facility is logically divided, as is the primary facility.

More details on the technology components can be found in the ISO/IEC 27001 certified Security Management System documentation.

Back to Index

8.3 Physical components

The LTA System provides services based on Amazon AWS data centers:



AWS service

- Primary Site, located on Amazon AWS, Outscale and GTS datacenter with all necessary components in HA and connected via connectivity described below.
- DR (Disaster Recovery) Site, located on Amazon AWS datacenter managed and administered via Amazon management interface.

Management and administration of the AWS cloud is the responsibility of Namirial's Cloud Operation team, which operates following best practices in terms of organization management. The team, which continues the training process continuously, is coordinated by the Head of IT Infrastructure.

Amazon AWS data centers comply with major international security standards and in particular implement an ISO/IEC 27001, 27017 and 27018 certified information security management system.

The network architecture enables handling large workloads and high traffic with low latency between workloads. Each Region is completely isolated and includes several availability zones, which are also completely isolated within the infrastructure. To better isolate any issues and achieve higher availability, the instances dedicated to the storage system workloads are spread across multiple availability zones within the same Region. In addition, the availability zones are at least 70 km apart.

The maximum interval between two checks (configuration of TSP systems) is performed every 24 hours.

8.3.1 Italy

LTA&QPres System provides services on AWS data center:

- Primary site: AWS Italian Region (Milan)
- Disaster Recovery: AWS Region EU-central-1 Frankfurt

8.3.2 France

LTA&QPres System provides services on AWS data center:

- Primary site: AWS French Region (Paris)
- Disaster Recovery: AWS Region EU-central-1 Frankfurt

LTA&QPres System also provides services on OutScale data centers in the cloudgouv-eu-west-1 region, which is redundant as follows:

- SEC1 (Pantin, France)
- SEC2 (Magny-les-Hameaux, France)
- SEC3 (Aubergenville, France)

8.3.3 Spain

LTA&QPres System provides services on AWS data center:

- Primary site: AWS Spanish Region (Aragon);
- Disaster Recovery: AWS Region EU-central-1 Frankfurt.

8.3.4 Romania

LTA System provides services on GTS Telecom SRL:

- Primary site in the datacenter of GTS Telecom SRL (Bucarest)
- Disaster Recovery in the datacenter of GTS Telecom SRL (Cluji)

8.3.5 LATAM

LTA System provides services on AWS data center:

- Primary site: AWS South America Region (Sao Paolo);
- Disaster Recovery: AWS US East (Northern Virginia) Region

*****

For insights and detail in relation to the physical components and business continuity, please refer to the ISO/IEC 27001-certified information security management system documentation.

8.4 Software Components

The following are the software components used in the LTA Service.

Function	*Operating System*	*License*	*Software Producer*
WAF	N.A.	AWS provided	AWS
Web service	Windows Server	Datacenter edition	Microsoft
Web Application	Windows Server	Datacenter edition	Microsoft
Scheduler	Windows Server	Datacenter edition	Microsoft
Antivirus	Ubuntu	Open source	Canonical
Server Signature	CentOS	Open source	CentOS
DB Server	Ubuntu	Open source	Canonical

Back to Index

8.5 Management and development procedures

Namirial, with the support of all corporate structures, each for the part of its competence, has taken steps to establish a system of service governance and oversight with the aim of:

- ensure the confidentiality, integrity, readability, retrievability and availability of documents and data in the system;
- formalize and ensure system requirements in accordance with applicable regulations;
- service maintenance;
- optimize incident management;
- assess risk and business continuity levels;
- monitor security levels;
- operationally manage security activities (incidents, fraud prevention, emergency communication management, etc.).

8.5.1 Operation and Maintenance of the LTA System

The security requirements (physical security, logical security, and organizational security) adopted in the operation and maintenance of the LTA System, incident management policies, and business continuity of the LTA service are specified and reported in the Security Plan and ISMS documentation.

Namirial LTA Provider maintains a chronological record of software platform components including all releases. These, along with the applications used throughout the LTA process over the years, are recorded to make documents and data related to the service available and usable over time.

The procedure of software releases follows the requirements imposed by ISO/IEC 27001 certification.

The preparation, verification and approval of documentation related to the LTA service are managed within the ISMS Procedures of the Namirial Organization.

Finally, Namirial makes available both internally and to external parties (customers, suppliers, etc.) a specific and expert support service, instantiated by the Authorized User through the ticketing system and structured as follows:

- Help Desk 1st Level: consists of the operators who receive the first contact from the User in case of need and are able to give support on issues related to platform usage, process, service, etc.
- Help Desk 2nd Level: depending on the cases, it can handle the technical requests of the first level and provides management and resolution of the issue.

8.5.2 Log

The events generated by the LTA System during the various phases of the process produce logs in order to track the various operations generated by the service during automatic processes and user interaction, and to facilitate the diagnosis of any anomalies and/or incidents.

Each log contains a time reference and a description that allows its nature and origin to be identified.

These files are maintained and archived by the system.

The nature of the data tracked, the types of logs, and the methods of sending them in archiving are detailed in the internal Security Plan document.

8.5.3 Change management

The change management process on the service is requested by the Customer through the ticketing platform and managed by dedicated teams through the eventual contractual update. The Contract transposes the service change specifications, and only if expressly accepted and shared via email by the Preservation Objects Owner, it allows to activate the subsequent implementation phase of the change (from testing to production deployment).

The change management of the service delivery infrastructure, on the other hand, is managed and described by the Provider according to the procedure defined by the ISO/IEC 27001 standard.

8.5.4 Periodic audit of compliance with relevant regulations and standards

The Preservation Service Manager periodically conducts a general review of the service together with the individuals assigned in the organizational chart for LTA, to ensure the compliance of the system with the expected level of service, analyze the causes of any incidents or disruptions, and promote prevention or improvement activities.

When necessary, a review meeting may be called in the case of particular events (e.g., changes in technology, regulatory or functional requirements, seasonality of processing load, etc.).

At least once a year, in agreement with internal functions, the Preservation Service Manager plans audit processes involving regulatory, process, organizational, technological, and logistical aspects, including the involvement of specific consultants.

The objective is to check the compliance of the system with laws, regulations, the contract with the Object Owner, the general documentation of the service, the principles that inspire the quality system and this Practice Statement.

Periodically, checks are also carried out on the functionality of the LTA system, mainly on:

- verification of the functionality of creating and maintaining Submission Reports, AIPs, etc;
- verification of the functionality of dissemination of packages and documents for the purposes of exhibition and production of copies;
- maintenance and availability of a software registry of the programs under management in the different versions, if any, to allow for restoration;
- verification of the correct configuration of the various data recorded (Subject Owner, Preservation Manager, other parties, Document Types, metadata, user privileges, etc.);
- verification of the proper operation of the security procedures used to ensure the affixation of digital signature and time validation;
- verification of the proper preparation and maintenance of Preservation Service documentation, including in case of changes in service conditions or events that must be kept track of, such as regulatory adjustments, technological evolutions, take-over of personnel in activities involved in LTA, technological and software evolutions, etc.

8.5.5 Security management and risk assessment

For the description of enterprise security management, risk analysis and business continuity, please refer to all documentation related to the ISO/IEC 27001-certified ISMS and for the specific Long Term Archiving (LTA) Service, to the Security Plan.

Back to Index

9 MONITORING AND CONTROLS

As part of the 27001 certifications and extensions, audits are conducted to check compliance with security implementation standards, as part of the continuous improvement process of the information security management system. Technical compliance audits involve testing operational systems to ensure that hardware and software checks and controls have been implemented correctly. Technical compliance audits also include **Vulnerability Assessment** and **Penetration Test**.

The strategy adopted by Namirial requires that the planning, supporting organizational structure, and business continuity tools developed include all the functional, technological, organizational, and infrastructural measures necessary to ensure quality, security, and reliability of the services provided for the Object Owner.

To achieve this goal, the monitoring and control procedures and tools described below are essential.

Back to Index

9.1 Monitoring procedures

The LTA service is constantly controlled by a monitoring system that detects malfunctions, anomalies, but also critical situations that risk causing problems in the system operation.

Namirial Production and Software Development organizational areas carry out online monitoring and control activities of the application and system components with which the services are delivered, through the indicators and controls identified on the ISMS Information Security Management System.

Specifically, Namirial performs control activities by making use of the **Nagios** platform (asset management system) and dedicated page for ticketing. Nagios upon the occurrence of an anomalous event related to hardware resources or application services notifies the SOC (Security Operations Center) of the anomaly, which, after checking, creates a ticket and assigns it to the Information Systems Manager or other deputy operator, who within a predetermined time (SLA - Service Level Agreement), must perform the appropriate maintenance to close the anomaly. The system also provides escalation policies to supervisors in case the ticket is not taken care of within the predetermined time. The ticket once processed is closed by the operator by entering the activities performed to resolve the incident. All tickets handled remain historicized in the system and form the basis for the creation of monitoring and control reports.

Namirial is also equipped with software for monitoring security and business continuity events on the essential services of the LTA System, this IBM **QRadar** software is used by the SOC operated by the company Yarix of Montebelluna, which monitors 24 hours a day 365 days a year and upon the occurrence of any critical events contacts the personnel in charge to mitigate any security and business continuity problems.

The Users of the LTA System can use the Namirial ServiceDesk ticketing platform accessible at servicedesk.namirial.com to request Level I help-desk support. The tickets generated carry the following information:

- assignment
- messages exchanged with the operator
- closing of the ticket

- activities performed.

Users can also independently monitor the status of the Service through Namirial Status page (status.namirial.com), which is constantly updated.

Users who are administrators of the LTA System can open tickets internally through the Jira platform if the request needs to be routed to higher levels of service than the first.

In addition, the ticketing system keeps track of the date and time of ticket handling. In particular, they are constantly monitored:

- processes and web services;
- service exposure to the user;
- document submission processes;
- sFTP service;
- scheduling services (e.g., Submission Report generation processes, AIP, DIP, etc.);
- support services (e.g., antivirus, signature service, time stamping service);
- storage occupancy, latency, and performance;
- DB processes, transactions, and performance;
- DB replication management system logs;
- web publishing service;
- web publishing service log;
- system logs and resource functionality;
- procedure and consistency logs;
- legal log rotation service;
- backup, geographic replication and DR processes;
- backup and DR system operation;
- HSM operation and performance;

The asset management and log management system detects the following data through the installation of an agent on the production machines of the LTA service:

- system administrator access;
- hardware and software installed on the server;
- CPU usage, RAM, disk SPACE monitored at 5-minute intervals.

Additional monitoring and control procedures required by the Customer shall be agreed upon between the LTA Provider and the Owner.

Back to Index

9.2 Verifying the integrity of archives

The process of verifying the integrity of information packages and documents includes:

- matching check on the number of documents (verification between the number of actual documents present in the LTA System and the number of records present within the DB structure for a specific Owner);
- integrity check of validation tools affixed to documents and Package Indexes (verification of the signature and time stamp on a chosen percentage of the total number of documents and XML indexes of the AIP present within the LTA System for a specific Owner).

Regarding the readability check, automatisms are in place in the LTA System that by the five-year deadline perform a series of checks on a sample basis extracted through a pseudo-random algorithm, considering the set of Id present in the totality of the archived documents:

- integrity check, carried out through the automatic calculation of the document hash and its comparison with the hash recorded during the creation of the AIP;
- readability check, on the set of documents extracted for integrity verification a subset of documents will be further created in order to verify their readability and following each control operation a report will be produced digitally signed by the Preservation Service Manager and archived in the System.

Back to Index

9.3 Solutions adopted in case of anomalies

The management of incidents in the service delivery and operation of the LTA System is governed by Namirial through the adoption of:

- appropriate detection tools;
- formalized systems for responding to unexpected events recognized as incidents;
- appropriate communication processes;
- efficient countermeasures for security and restoration of LTA System functionality or in case of data loss.

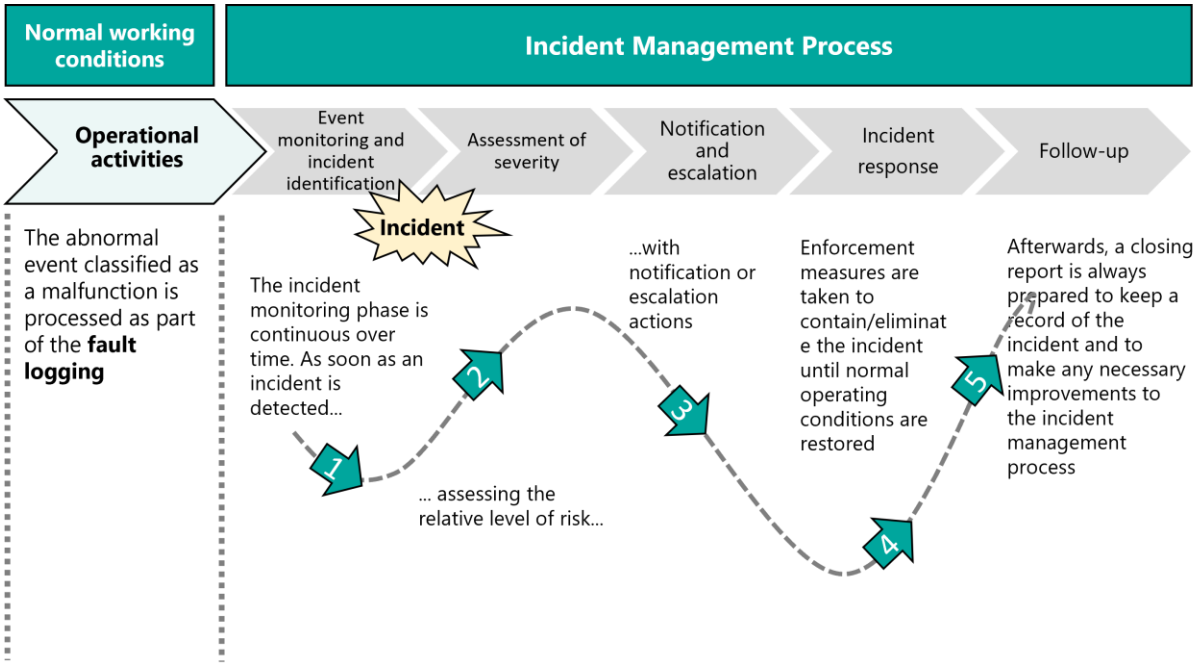
The system uses automatic controls to ensure the integrity and consistency of data processed by the system; automatic controls require the intervention of the organizational structure supporting the LTA service only when anomalies occur that cannot be handled automatically.

In case a system or process incident occur, operations to detect and restore functionality follow a defined and documented procedure, as also required by the ISO/IEC 27001-certified ISMS management system.

In the incident management framework, Namirial follows a procedure that complies with the following steps:

- Phase 1: Monitoring and identification of the incident;

- Step 2: Tracking the incident;
- Phase 3: Classification of the incident;
- Phase 4: Notification and escalation;
- Step 5: Incident response;
- Phase 6: Follow-up.



Incident Management

When malfunctions or critical situations occur, the monitoring system generates email notifications to available staff who will take action to resolve the problem in accordance with the SLAs agreed with the Owner and in accordance with internal incident management procedures.

For a more detailed discussion of this topic, please refer to the specific business documents in Incident management subject to ISO/IEC 27001 certification.

Back to Index

10 ANNEXES

Complementing this LTA Practice Statement there are several corporate documents relating to specific aspects concerning to Namirial LTA Service - Long Term Archiving (LTA).

The following is a list of these documents available for consultation if they are public.

Within the documents listed, references to additional Namirial group documents and policies can be found.

N.	*Name*	*Confidentiality note*
Annex 1.	Namirial - LTA - Policy and practice statement for the preservation of qualified signatures and seals	Public document
Annex 2.	Namirial - LTA and QPres- Security Plan	Internal document
Annex 3.	Namirial - LTA and QPres - Termination Plan	Internal document
Annex 4.	Namirial - LTA and QPres - Risk Assessment	Internal document

Back to Index