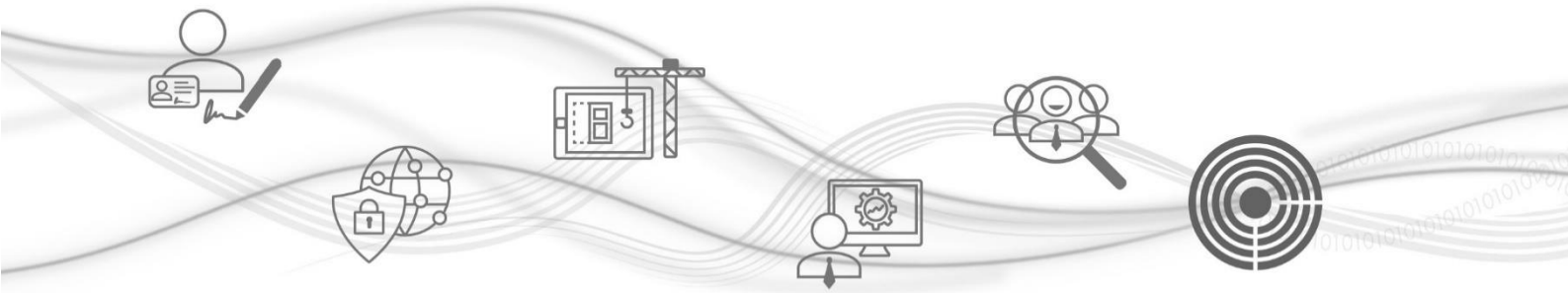
Long Term Archiving

Practice Statement



Category	**LTA**	Document Code	**NAM-LTA-MO**	**Namirial S.p.A.**
Edited by	**Enrico Giunta**	Confidentiality note	**Public document**	CEO
Verified by	**Davide Coletto**	Version	**11**	**Massimiliano Pellegrini**
Approved by	**Massimiliano Pellegrini**	Issuing Date	**08/09/2023**	_____

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 € 8.238.145,00 i.v.

Index

Issue of the document

Action	*Date*	*Name*	*Role*
Editing	06/09/2023	Enrico Giunta	Archival Manager
Verification	07/09/2023	Davide Coletto	Preservation Service Manager
Approval	08/09/2023	Massimiliano Pellegrini	CEO

Version register

N°Ver/Rev/Draft	*Date of issue*	*Description*	*Comments*
1.0	28/11/2014	First issue of the document according to the AgID Practice Statement model for accreditation	First version according to the AgID (Agenzia per l'Italia Digitale) model
2.0	22/01/2015	New issue for revisions	Changes to paragraphs 2.1, 6.1, 6.2, 6.3, 7.1, 7.2, 7.4 and 7.6
3.0	05/02/2015	Integration of the document for the accreditation with AgID	Changes to paragraphs 2.1, 6.2, 7, 7.3, 7.4 and 7.6
4.0	22/02/2016	Various revisions in all chapters of the document	Changes in all paragraphs
5.0	26/09/2016	Review of the topology of service delivery sites, review of the organisational chart	Changes to paragraphs 5.1, 8.3
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	Changes in all paragraphs

6.1	11/10/2018	Updating glossary and regulations; revising the organisational chart; updating the format table	Changes to paragraphs 2.1, 3.1, 5.1, 6.1
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	Changes to paragraphs 2.2, 6.2, 6.3, 6.4, 7.1, 8.3
8.0	04/06/2020	Updating Roles and Responsibilities	Changes to paragraphs 4, 6.4, 7.9, 9.1
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)	Changes to paragraphs: 2 3 4 6.1 6.2 6.3 6.4 6.5 7.6 8.3 9.1
10	09/05/2022	Revisions and adjustments in the following chapters of the document: -Glossary update (2.1) -Regulation and	Changes to paragraphs: 2.1 3.1 3.2

		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	4 5.1 5.2 6.2 9.1
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)	Changes to paragraphs: 2.2 7.7
10.2	27/02/2023	Revisions in the following par: - Update physical components (8.3)	Changes to paragraphs: 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	Changes to paragraphs: 2.1 2.2 3 4 6.3.1 6.3.2 7.7 7.9 8 10

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 preservation 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 preservation 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 Preservation System.

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

- **Compliance Principle**: the document aims to describe a preservation system and the preservation process in accordance with the valid regulation framework;
- **Transparency Principle**: the document aims to provide a clear explanation of the Preservation System and the provided processes;
- **Process perspective**: the document aims to describe the steps of the preservation 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 Preservation System with regard to all aspects related to the preservation and use of digital information assets, in accordance with the reference models;
- **Customisation Principle**: the description of any specific provision of the preservation service for a given designated community accessing the Preservation 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 Preservation 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 preservation 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 preservation 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 preserved 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	The Agenzia per l'Italia Digitale (Digital Italy Agency) is the technical agency of the Presidency of the Council of Ministers of Italy whose task is to ensure the achievement of the objectives of the Italian Digital Agenda and to contribute to the dissemination of the use of information and communication technologies, fostering innovation and economic growth
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 preservation functions (acquisition, preservation, 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 in accordance with current laws and regulations
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 of preservation 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 of preservation, detailing the specific procedures relating to the Service. This document may also indicate the activities of the preservation 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.	Discard	Operation by which documents of no administrative value and of historical and cultural interest are eliminated in accordance with current legislation

25.	Discard Information Package	Information package containing the documents to be discarded by the preservation system once the preservation time limit has been reached
26.	Dissemination Information Package (DIP)	Information package sent by the Preservation 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 of preservation
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 preservation process, referring to the SInCRO standard (UNI 11386)
43.	Index of the Discard Information Package	Structure of the data set supporting the Discard Information 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 preserved (digital documents, folders, aggregations), or even just the metadata referring to the objects to be preserved in accordance with the OAIS standard, which provides for information packages of different kinds interacting with the Preservation System (SIP, AIP, DIP, etc.)
47.	Intake	Acceptance by the Preservation System of a Submission Information Package as complying with the terms of the LTA Practice Statement
48.	Long Term Archiving System (LTA)	Digital documents Preservation System
49.	LTA Practice Statement	The analytical document, relating to the Preservation 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 Preservation 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 Preservation System
52.	Originals not unique	Documents whose content can be traced through other records or documents whose preservation is mandatory, even if in the possession of third parties
53.	Owner of the preservation 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.	*Pacchetto di Archiviazione (PdA)*	Name of the AIP according to the Italian legal framework on the formation, management, preservation of digital documents
55.	*Pacchetto di Distribuzione (PdD)*	Name of the DIP according to the Italian legal framework on the formation, management, preservation of digital documents
56.	*Pacchetto di Versamento (PdV)*	Name of the SIP according to the Italian legal framework on the formation, management, preservation of digital documents
57.	Preservation	Digital Preservation Service consists of all the activities aimed at defining and implementing the overall preservation system policies and governing its management in relation to the organizational model adopted. The purpose of preservation 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
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 Preservation 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 in accordance with current laws and regulations
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 preservation 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 preservation activities that has been recognised as meeting the requirements of the highest level, in terms of quality and security

68.	*Rapporto di Versamento (RdV)*	Name of the Submission Report according to the Italian legal framework on the formation, management, preservation of digital documents
69.	Recipient	Identifies the subject/system to which the document is addressed
70.	Reliability	Characteristic expressing the level of trust the user places in the document
71.	Research session	A session started by a User of the Preservation System, during which it is possible to retrieve and view the digital objects
72.	Revision Package	Information package sent by the Producer to the Preservation System according to a predefined format in order to make a revision to the data previously preserved by the System
73.	Secure signature generation device	The secure devices for generating the qualified signature, which must have security certification according to Art. 35 of the CAD
74.	Security Copy	Backup copy of the archives of the preservation system
75.	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
76.	Service Level Agreement (SLA)	It is the agreement between the owner of the object of preservation, the producer, the preservation manager and the Provider on the service levels to be guaranteed
77.	Signature holder	The natural person to whom the electronic signature is assigned and who has access to the electronic signature creation devices
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 Preservation System according to a predefined format and in compliance with the OAIS standard
80.	Submission Report	Digital object certifying that the Preservation 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.	AgID	Agenzia per l'Italia Digitale - Digital Italy Agency
2.	AIP	Archival Information Package
3.	DIP	Dissemination Information Package
4.	LTA	Long Term Archiving
5.	OAIS	Open Archival Information System, ISO 14721
6.	SiNCRO	Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali (UNI 11386)
7.	SIP	Submission Information Package
8.	SR	Submission Report

Back to Index

3 REGULATIONS AND STANDARDS

3.1 Reference regulations

This section contains the main reference legislation for preservation activity at national and international level to which the preservation 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**)

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**, **giugno 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

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 Preservation 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 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;
- **NF 461** Système d'archivage électronique;
- **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;
- **UNI 11386 Standard SInCRO** Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali;
- **ISO 16363** Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

Back to Index

4 ROLES AND RESPONSIBILITIES

The Preservation 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 Preservation System. The reference organisational model is formally defined in terms of the roles and responsibilities of the various actors involved in the preservation 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 Preservation System, as well as the governance of the management of the Preservation System; – definition of the characteristics and requirements of the Preservation 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 preservation 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	**Enrico Giunta**	– 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 preservation 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 26 May 2021	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 Preservation 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 Preservation 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	**Fabio Didonè**	– Coordination of the development and maintenance of the hardware and software components of the Preservation System; – planning and monitoring of preservation system development projects; – monitoring of SLAs related to the maintenance of the Preservation 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.	Since 5 July 2021	
	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	Federica Marti	– recurring and comprehensive review of the service adherence to all applicable laws, regulations, and standards	Since 31 July 2023	
	Margherita Menghini	as above	10 June 2022 to 31 July 2023	

4.1 Proxies

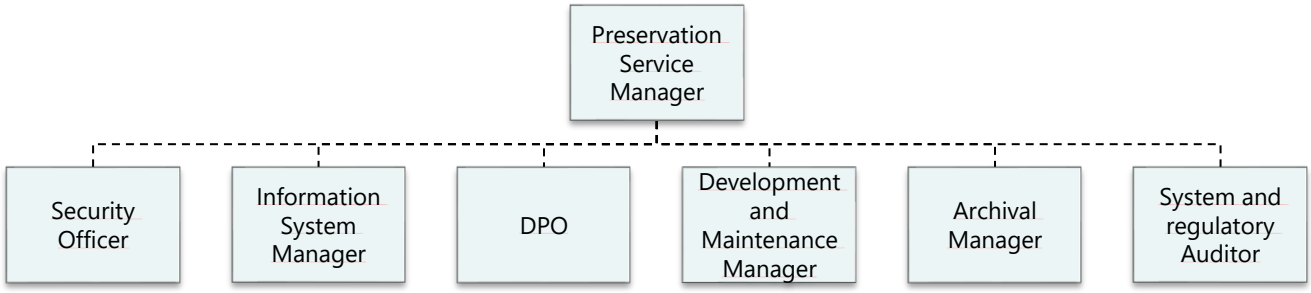
In Romania, Adrian Dinculescu, the assignee of all the tasks for the Preservation Service (except DPO and System and Regulatory Auditor), delegates his functions to the persons listed in the table above.

Back to Index

5 ORGANISATIONAL STRUCTURE FOR THE PRESERVATION SERVICE

5.1 Organigram

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



Pic 1 Organigram

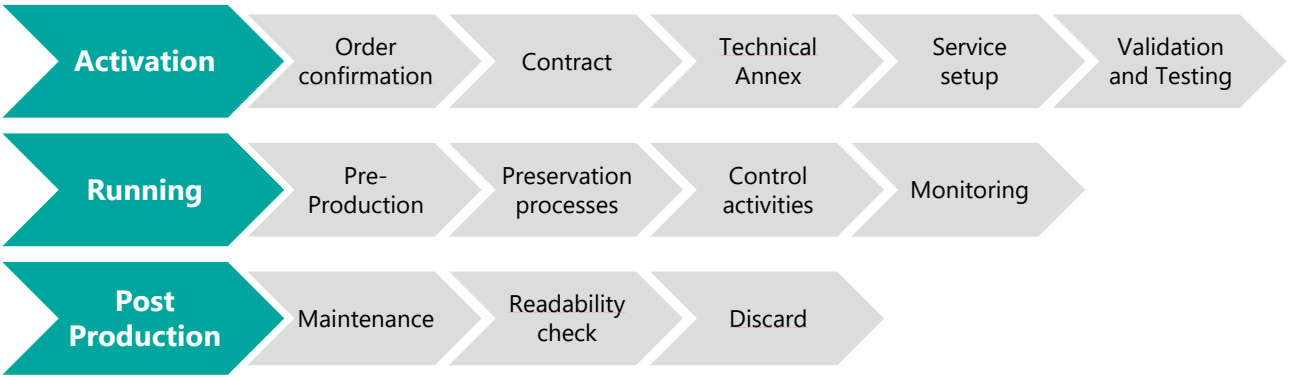
5.2 Organisational structures

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 preservation service, Namirial has certified its information security management system in the logical, physical and organisational domain in which the preservation 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 Preservation 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 preserved documents, in order to make dissemination/distribution requests).

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



Pic 2 Preservation Service Life Cycle

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

Pic 3 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 preservation 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.

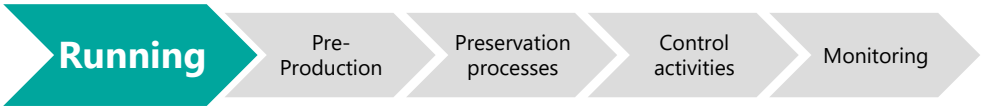
The preparation of the correct initial definition of the requirements and therefore compliance with current legislation on preservation systems, with also the identification of related fulfilments, is ensured during the analysis phase by the preparation of the document Service Data Sheet, with control 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.



Pic 4 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 preservation 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.

Pic 5 Post-Production phase

The maintenance of the documents and packages generated in the preservation 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 preservation 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.

Finally, after the expiration of the preservation period, contractually agreed upon between the producer, the Preservation Manager and the Preservation Service Manager, the Discard procedure is initiated, the notification of the discard and the closure of the service. Owners of these activities are the Support and Production Area.

In all these phases of the preservation 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 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 PRESERVATION PROCESS

The operation of the Preservation 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 preserved (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 Preservation 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 Preservation 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 preserved by the System.

For the preservation 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 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 service to be activated - are listed and described the types of documents subjected to preservation for one specific Owner and the related preservation 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 preservation process agreed upon with the Owner;
- other rules that characterize the preservation process.

The Document Types of digital objects to be submitted into the Preservation System are defined through the analysis and classification activities or based on the standard service to be activated

6.2 File Formats

The Preservation System accepts formats that conform to the list of formats suitable for preservation indicated in **Annex 2** of the **AgID Guidelines on the formation, management, and preservation of electronic documents**. Files with non-compliant formats will be discarded during takein.

About the preservation of files in TXT format, which is not listed among the formats indicated by AgID, the Provider has carried out the interoperability assessment for its preservation system as indicated in paragraph 3.1 of Annex 2 of the Guidelines. The assessment and the related of interoperability index are given in the next paragraph.

The following is a list of the **most common formats** used for preservation of digital documents; **for the complete list of supported formats please refer to Annex 2 of the Guidelines**.

File format	Owner	Extension	Mime Type	Viewer	Viewer manufacturer
PDF	Adobe Systems - www.adobe.com For preservation purposes, when using this format, documents must be formed exclusively with interoperable typefaces, which are considered 'standard' by various sector bodies, as further specified in paragraph 2.8 Typefaces of Annex 2 of the AgID Guidelines	.pdf	application/pdf	Adobe Reader	Adobe Systems www.adobe.com
PDF/A	Adobe Systems - www.adobe.com	.pdf	application/pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems www.adobe.com
XML	W3C For preservation purposes, when using this format, it is mandatory for the Holder to also maintain the XML Schema .xsd file over time.	.xml	application/xml text/xml	Mozilla -Chrome - Internet Explorer	Firefox - Google - Microsoft -
TXT	For the purposes of preservation in the use of this format, it is important to specify the character encoding adopted.	.txt		Mozilla -Chrome - Internet Explorer	Firefox - Google - Microsoft -
TIFF	Aldus Corporation later acquired by Adobe	.tif, .tiff	image/tiff	Various image viewers	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	image/jpeg	Various image viewers	For more information on the format www.jpeg.org
EML	Various	.eml		E-mail clients support the display of eml files	Various
OOXML	Microsoft This format must guarantee certain characteristics that make it suitable for long-term preservation, among them the embedding of fonts, the presence of indications of presentation of the document, and	.docx, .xlsx, .pptx			

	the possibility of applying an XML digital signature to the document. It is advisable to use the *Strict* profile, which eliminates certain 'proprietary' extensions that may reduce the interoperability of the format itself				
ODF	OASIS OpenOffice.org Consortium	.ods, .odp, .odg, .odt	application/vnd.oasis.opendocument.text		www.oasis-open.org

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.

6.2.1 Evaluation and interoperability index

The Preservation System supports the TXT format, even though it is not listed among the formats indicated in Annex 2 of the Guidelines issued by AgID, why it is a format that is widely used in many fields and recognised by most software. For preservation 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

Back to Index

6.3 Submission Information Package (SIP)

The Submission Information Package (SIP) is an uncompressed zip archive consisting of:

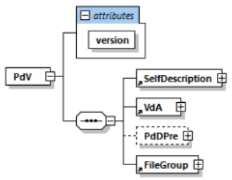
- documents subject to preservation (Content Information), possibly digitally signed (in the CAdES ".p7m" or PAdES or XAdES signing standard) or possibly time stamped (in the CAdES-T, or PAdES-T or XAdES-T time validation standard);
- a SIP Index file aimed at describing Preservation Description Information, 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:

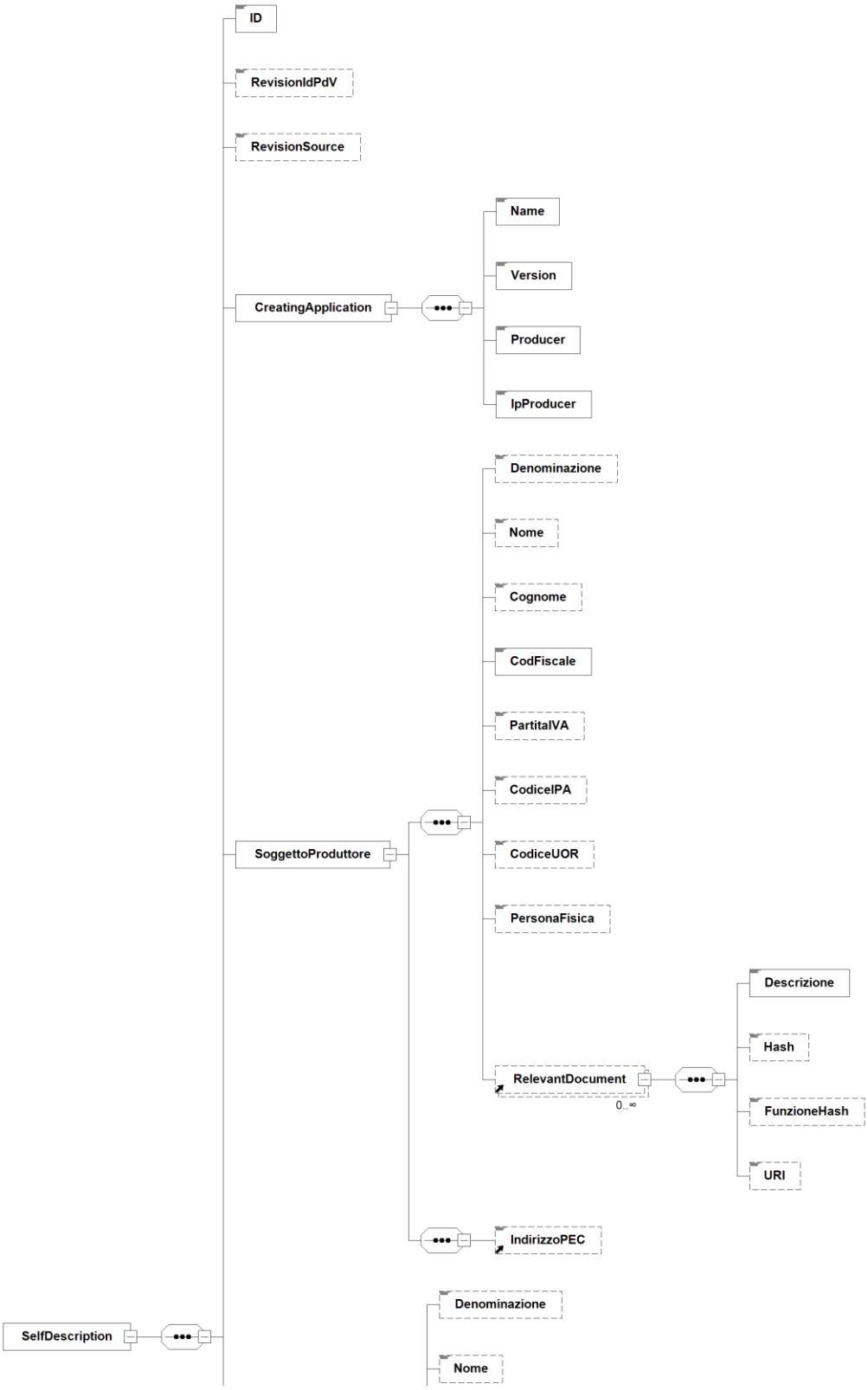
- the identification of the entity that produced the SIP (Producer);
- the identification of the application that produced it;
- the definition of the Document Type to which the documents included in the package belong and any messages from the Customer's Preservation Manager;
- the definition of the 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.

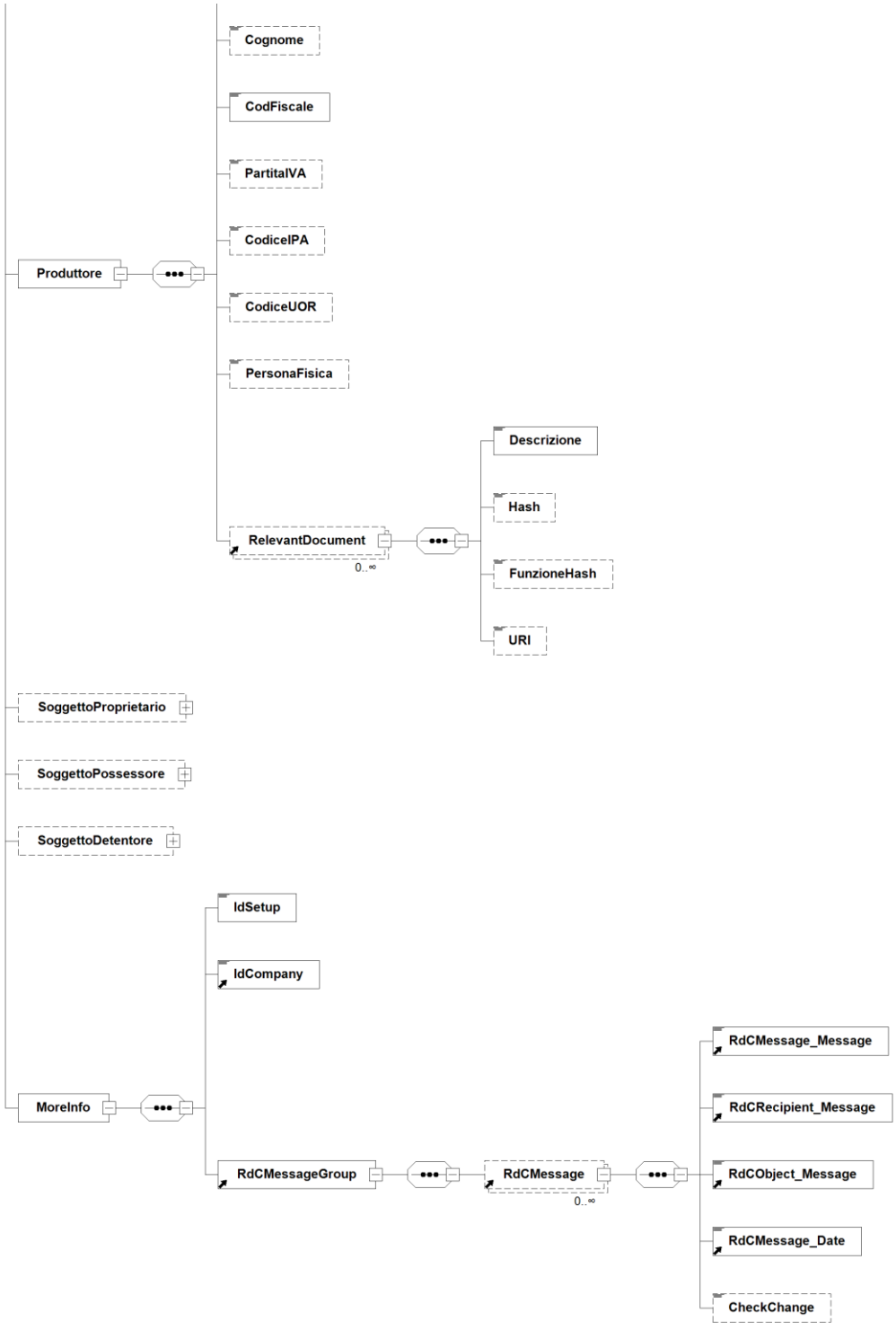
The SIP Index file can eventually be digitally signed by the Producer.

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

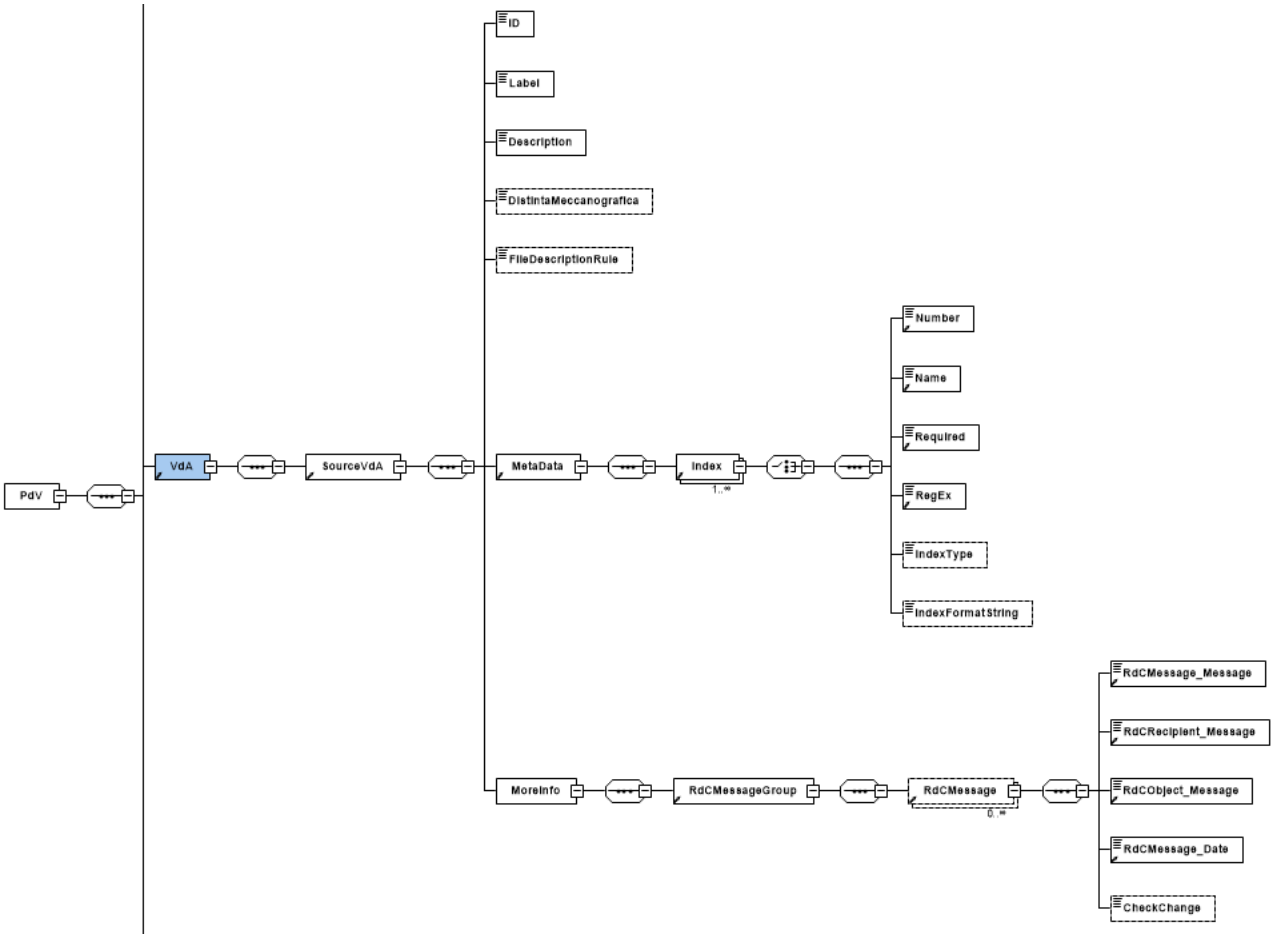


Pic 6 SIP Index structure with the main components

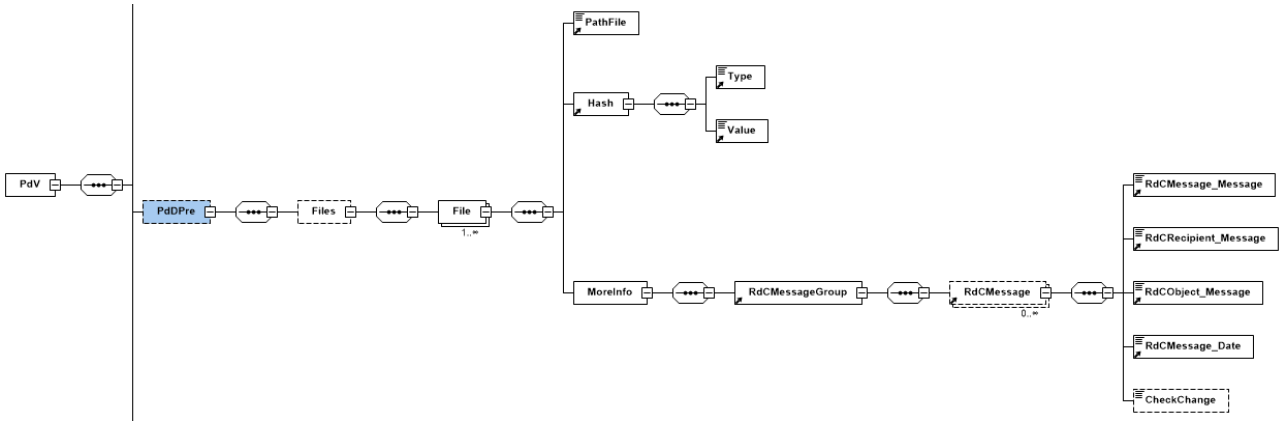

ID
RevisionIdPdV
RevisionSource
CreatingApplication
Name
Version
Producer
IpProducer
SoggettoProduttore
Denominazione
Nome
Cognome
CodFiscale
PartitaIVA
CodiceIPA
CodiceUOR
PersonaFisica
RelevantDocument
0..∞
Descrizione
Hash
FunzioneHash
URI
IndirizzoPEC
SelfDescription
Denominazione
Nome



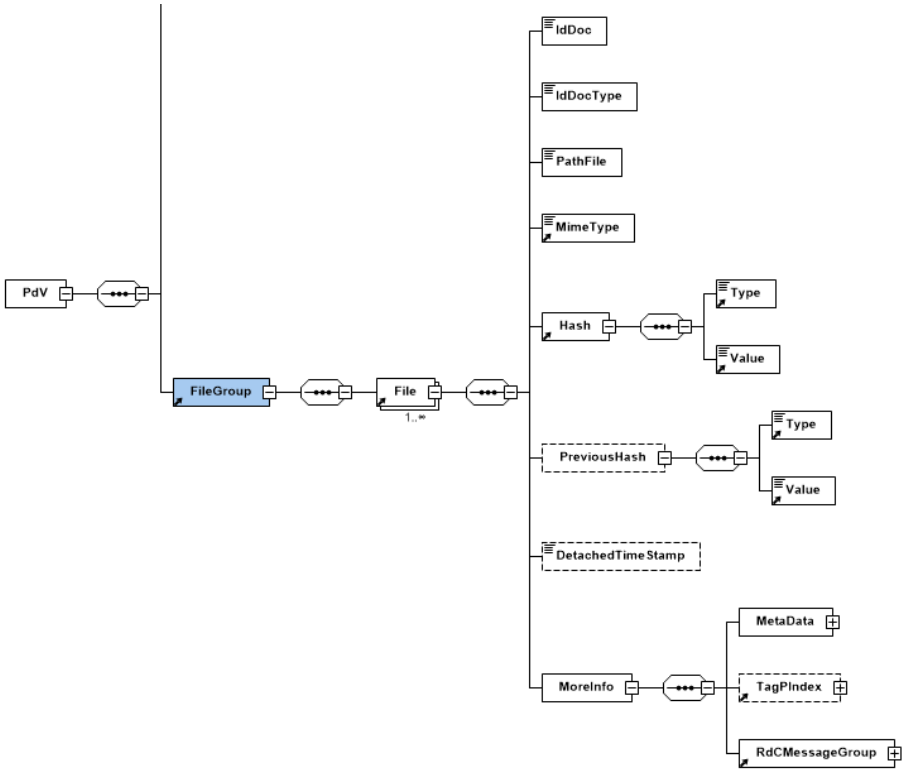
Pic 7 SIP Index Structure (SelfDescription Section)



Pic 8 SIP Index Structure (VdA Section)



Pic 9 SIP Index Structure (DIPPre Section)



Pic 10 SIP Index Structure (FileGroup Section)

6.3.1 Pre-package

In the case of submission 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 preserved.

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 preservation process.

6.3.2 Revisione Information Package

A revision package allows changes to an already submitted SIP by creating a new SIP containing the unique reference Id of the original SIP to be revised.

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

- Correction: Intervention aimed at correcting or modifying a previous act or condition
- Supplementing: Intervention to add a previous act or condition

- Note: Summary note for administrative, disciplinary, etc. purposes

The use of the revision package is also used in cases where a new certificate needs to be affixed in relation to preservation evidences.

Back to Index

6.4 Archival Information Package (AIP)

The Archival Information Package (AIP) generated in the preservation 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 preservation 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 preservation 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 complete with additional structures related to the various "MoreInfo" elements provided by the SInCRO (PIndex) standard.

- **SelfDescription (1)***: General description of the package.
  - **ID (1)**: Unique ID of the AIP generated by the Storage System (database-generated AIP ID).
  - **CreatingApplication (1):**
    - **Name (1)**: Preservation System.
    - **Version (1)**: Version obtained from the Web Service.
    - **Producer (1)**: Preservation System Producer
  - **PIndexSource (0-n)**
    - **ID (1):** Id of the previous Archival Information Package (AIP), if any.
    - **Path (1):** Path relative to the IAIP (SInCRO) of the previous package (if any).
    - **Hash (1):** Value returned by the function by applying it to the IndexAIP file of any previous packet; contains the 'hashFunction' attribute identifying the hash function used for the calculation.
  - **MoreInfo (1)**

- **EmbeddedMetadata (1)**: References of the owner subject of the documents to which the preservation process refers.
  - **MoreInfoSelfDescription (1)**
    - **IdSetup (1):** Setup id for the document owner within the system.
    - **IdCompany (1):** Id of the entity holding the documents within the system.
    - **VersionIPdA (1):** Version of the AIP index defined by the LTA Provider.

➢ **PVolume (1):**

- **ID (1)**: Unique ID of the AIP generated by the Preservation System (database-generated AIP ID).
- **Label (0-1):** Name of aggregation.
- **Description (0-1):** Description of aggregation.
- **PVolumeSource (0-n):** Information on a preservation volume from which the one in question originated.
  - **ID (1):** Identifier of the aggregation.
  - **PIndexID (1):** Preservation index identifier associated with the previous preservation volume.
- **PVolumeGroup (0-1):** Information on an aggregation to which the preservation volume belongs.
  - **ID (1):** Identifier of the aggregation.
  - **Label (0-1):** Name of aggregation.
  - **Description (0-1):** Description of aggregation.
- **MoreInfo (1)**
  - **EmbeddedMetadata (1)**: List of SIP included within the AIP
    - **MoreInfoVolume (1)**
      - **PdVGroup (1)**
        - **PdV (0-n)**
          - **IdSIP(1)**: Id of the SIP returned by the Preservation System at the end of take-over.
          - **RevisionIdSIP (0-1)**: Id of the revised SIP (may be either the source SIP or the last published version for the source SIP). The node is only present if the SIP represents a revision.
          - **RevisionIdSIPOrigin (0-1):** Id of the source SIP (initial SIP from which all revisions originate). The node is only present if the SIP represents a revision.
          - **RevisionNumber (0-1):** Revision number required to order the sequence of revisions relating to the source MoU. The node is only present if the SIP represents a revision.
          - **RevisionSource (0-1):** Defines the source of the revision package. Allowed values: RequestProducer or Internal. The node is only present if the SIP represents a revision.
          - **FunctionHash (1)**: Hash function used to calculate the hash of the IndexSIP.

- **Hash (1)**: Value returned by the hash function applied to the IndexSIP file.
- **IdSubmission Report (1)**: Id of the Submission Report returned by the Preservation System upon generation.
- **FunctionHashSubmission Report (1):** Hash function used to calculate the hash of the SR.
- **HashSubmission Report (1):** Value returned by the hash function applied to the SR.
- **Data Submission Report (1):** Date of generation of the SIR.
- **Submission Report MessageGroup (1)**: Any communication between the producer and the Preservation Manager or his Delegate relating to the SR.
    - **PMMessage (0-n)**
        - **PMMessage_Message:** Text of the message.
        - PMRecipient_Message**:** Text of the message for the recipient of the Submission Information Package.
        - **PMObject_Message:** Any attached file referring to the communication.
        - PMMessage_Date**:** Date on which the message was entered.
        - **CheckChange:** Additional metadata allowing the verification of document modification to be specified. Allowed values: Correction; Integration; Annotation.

- **DIPPre (0-1)**
    - **Files (1)**
        - **Files (0-n)**
            - **PathFile (1):** Uri of the file relating to a DIPPre attachment (reversal from previous LTA Provider). Necessary to better identify the attachment and to be able to understand in which SIP the file is located.
            - **Hash (1)**
                - **Type (1):** Hash function applied to the DIPPre attachment.
                - **Value (1):** Value returned by the hash function applied to the DIPPre attachment.
        - **PMMessageGroup (1)**
            - **PMMessage (0-n):**
                - **PMMessage_Message:** Text of the message.

- PMRecipient_Message**:** Text of the message for the recipient of the Submission Information Package.
- **PMObject_Message:** Any attached file referring to the communication.
- PMMessage_Date**:** Date on which the message was entered.
- **CheckChange:** Additional metadata allowing verification of document modification to be specified. Allowed values: Correction; Integration; Note.

- **FileGroup (1-n)**:
  - **ID (1)**: Id of the document type to which the documents refer.
  - **Label (0-1):** Name of the document type to which the documents refer.
  - **Description (0-1):** Description of the document type to which the documents refer.
  - **File (1-n)**: File definition including encoding, extension and format (MimeType)
    - **ID (1)**: Id of the document assigned by the Preservation System (unique within the Preservation 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 by the function when applied to the file being stored.
    - **PreviousHash (1)**: hash function used and value returned by the function by applying it to the file subject of the Preservation (referring to a previous Preservation index).
    - **MoreInfo**:
      - **EmbeddedMetadata:**
        - **MoreInfoFile:** Information about the document in the preservation system used to identify and describe the document within the archive.
          - **File (1)**
            - **IdDoc**: Unique file identifier assigned by the Producer (unique within the document type defined for the company).
            - **IdSIP**: Id of the SIP associated with the document.
            - **Indexes (1)**
              - **Index (1-n)**
                - **Name**: Name of the index (metadata) field.
                - **Value**: Value of the index field (metadata).
            - **YearReferenceDoc**: Document Reference Year (e.g. year of tax period)
            - **Subject**: Metadata used to briefly summarise the content of the document or in any case to clarify its

nature. It is calculated automatically by the system, according to the rules defined at the time of submision.

- **CheckChange:** Additional metadata allowing the verification of document modification to be specified. Allowed values: Correction; Integration; Note
- **PMMessageGroup (1)**: Any communication between the producer and the preservation manager or his delegate relating to the file.
  - **PMMessage (0-n)**
    - **PMMessage_Message:** Text of the message.
    - PMRecipient_Message**:** Text of the message for the recipient of the Submission Information Package.
    - **PMObject_Message:** Any attached file referring to the communication.
    - PMMessage_Date**:** Date of Message Entry
- DetachedTimeStamp**:** References to any detached time stamp associated with the document.
- **AdditionalMetaData:** Additional metadata required by AgID guidelines.

- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoFileGroup (1):** Definition of the Document Type to which the document belongs.
      - **Typology (1)**
        - **IdTypology (1)**: Id of the Document Type to which the document belongs.
        - **Indexes (1)**
          - **Index (1-n)**
            - **Number**: Index number. Position of the index field (metadata) within the definition of the Type.
            - **Name**: Name of index field (metadata)
            - **Required**: Indicates whether the value of the index (metadata) is mandatory (possible values: True, False).
            - **RegEx**: Possible validation expression for the index value (metadata).
            - **IndexType**: Metadata data type (possible values: string, integer, date)
            - **IndexFormatString**: Format of the data type.

- **Process (1)**
  - **Submitter (1):** Information relating to the party performing the physical transfer of digital objects into the preservation system.

- **AgentID:** Identifier of the subject based on one of the identification types predefined by the ETSI standard**.**
- **AgentName: Name of** the subject (NameAndSurname or FormalName).
  - **NameAndSurname**
    - FirstName: Name of the subject.
    - LastName: Last name of the subject.
  - **FormalName: Name** or company name of the subject.
- **RelevantDocument (1-n):** Reference to a document of the party involved in the preservation process, relevant to the understanding of the process itself or of the digital objects undergoing preservation.
- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoSubmitter**
      - **IPA Code (0-1):** IPA code defined if the entity is a Public Administration.
      - UOR code **(0-1):** UOR code defined if the entity is a public administration.
      - **VAT number (0-1):** VAT number valued (if present) if the person is a natural person.

- **Holder (1-n):** Information on the Holder of the preservation object (producing party) or the owner, possessor or holder of the digital objects transferred into the preservation system.
  - **AgentID:** Identifier of the subject based on one of the identification types predefined by the ETSI standard.
  - **AgentName: Name of** the subject (NameAndSurname or FormalName).
    - **NameAndSurname**
      - FirstName**:** Name of the subject.
      - **LastName:** Last name of the subject.
    - **FormalName: Name** or company name of the subject.
  - **RelevantDocument (1-n):** Reference to a document of the party involved in the preservation process, relevant to the understanding of the process itself or of the digital objects undergoing preservation.
  - **MoreInfo**
    - **EmbeddedMetadata**
      - **MoreInfoHolder**
        - **IPA Code (0-1):** IPA code defined if the entity is a Public Administration.
        - UOR code **(0-1):** UOR code defined if the entity is a public administration.
        - **AgentIdPdV (1):**
          - **IdPdV (1-n):** List of Id SIPs transferred by the subject.
        - **VAT number (0-1):** VAT number valued (if present) if the person is a natural person.
- **AuthorizedSigner (1-n):** Information on the person authorised to append the electronic signature (advanced or qualified) or the electronic seal (advanced or qualified) on the storage index, at the conclusion of the index creation process.
  - **AgentID:** Identifier of the subject based on one of the identification types predefined by the ETSI standard.

- **AgentName: Name of** the subject (NameAndSurname or FormalName).
  - **NameAndSurname**
    - FirstName**:** Name of the subject.
    - **LastName:** Last name of the subject.
  - **FormalName: Name** or company name of the subject.
- **RelevantDocument (1-n):** Reference to a document of the party involved in the preservation process, relevant to the understanding of the process itself or of the digital objects undergoing preservation.
- **MoreInfo**
  - **EmbeddedMetadata (1)**
    - **MoreInfoAuthorizedSigner (1):** Additional information regarding the designated signatory for the closure of the Preservation process.
      - **PreservationAgent**
        - **PreservationJobRole:** Job description referring to the subject.
        - **CertificateIdentificationCode:** Identifier of the signing certificate used in closing the Preservation process.
        - **VATNumberNaturalPerson:** VAT number valued (if present) if the person is a natural person.
        - Identifier **(0-1):** Identifier of the subject assigned by the Preservation System when defining the subject.

- **TimeReference (1)**
  - **TimeInfo (1):** Date on which the index file was produced. It corresponds within certain time limits (required by the file signing and marking process) to the date on which the time stamp was issued.
- **LawAndRegulations (1):** Reference to the reference standard: *Technical rules on the storage system pursuant to Articles 20(3) and (5-bis), 23-ter(4), 43(1) and (3), 44 and 71(1) of the Digital Administration Code referred to in Legislative Decree No 82 of 2005.*
- **MoreInfo**
  - **EmbeddedMetadata**
    - **MoreInfoProcess:** Additional information related to the Preservation process.
      - **PreservationAgent (0-n)**
        - **AgentID (0-n):** Identifier of the subject based on one of the identification types predefined by the ETSI standard.
        - **AgentName (1):** Name of the subject (NameAndSurname or FormalName).
          - **NameAndSurname**
            - FirstName**:** Name of the subject.
            - **LastName:** Last name of the subject.
          - **FormalName:** Name or company name
        - **PreservationJobRole (1):** Job description referring to the subject.
        - **Identifier (0-1):** Identifier of the subject assigned by the Preservation System when defining the subject.

*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

6.5 Dissemination Information Package

The Dissemination Information Package (DIP) is generated by the preservation system to ensure interoperability and transferability to other Preservation 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:

- The documents (digital objects stored in the system) requested by the User.
- The Index of the SIP related to the documents.
- 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 Preservation 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 Preservation System and DIP)
- **List of requested files** (Document Id, File Name, Reference Year, File Hash, Hash Function Used, File Url in the Preservation System and DIP).

The data structure of the DIP is shown below:

- **DescGeneral**: Information on the User, the Preservation manager and the Preservation system.
  - **ID**: Id of the Dissemination Information Package (DIP) assigned by the Preservation System.
  - **IdSetup**: Customer Code associated with the Owner of the preservation object.
  - **Company Id**: Id of the reference company in the document system.
  - **SubjectProducer**
    - **Name:** Name of the Owner of the object.
    - **Tax Code:** Tax code of the Owner
    - **VAT No.:** VAT No. of the Owner
    - **IPA Code:** IPA code of the Owner (in the case of Public Administration).
    - **PhysicalPerson:** Indicates whether the Owner is a natural person (true, false).
  - **Producers:** List of entities that have physically transferred digital objects into the Preservation System.
    - **Producer:** entity that physically transfers digital objects into the Preservation System.
      - **Name:** Name of Producer.
      - **Fiscal Code:** Manufacturer's fiscal code.
      - **VAT No.:** VAT No. of the Producer. IPA
      - **IPA Code:** IPA Code of the Producer (in the case of Public Administration).
      - **PhysicalPerson:** Indicates whether the Producer is a physical person (true, false).
      - **SIP Id submitted**
        - **SIP Id:** Id of the SIP submitted in the Preservation System.
  - **DateGeneration**: The date in UTC format referring to the production of the DIP.
  - **IpAdressClient:** IP address from which the DIP extraction request arrived
  - **Applicant**: Biographical data of the DIP applicant.
    - **Name**: Name of the applicant.
    - **Surname**: Applicant's surname.
    - **CodiceFiscale**: Tax code of the applicant.
    - **VAT number**: VAT number of the applicant.
  - **SubjectsProcess**, Data of Preservation Manager, Preservation Operator (Provider) and Preservation Service Manager.
    - **PM**: data of the Preservation Manager (name and surname or company name, role, tax code or VAT number).
    - **Operator**: Provider data (name and surname or company name, role, tax code or VAT number).
    - **PSM**: Personal data of the Preservation Service Manager (name and surname or company name, role, tax code or VAT number).

- **AntiVirus:** Antivirus software name and date/time of last update.
- **LTA**: Data of the Preservation System.
  - **Name**: Name of the Preservation System.
  - **Version**: Version of the Preservation System.

- **AIPGroup**: Description of the extracted AIP.
  - **AIP**: Description of the Archival Information Package.
    - **Id**: Id of the Archival Information Package (unique identifier assigned by the Preservation System).
    - **FunctionHash**: Type of hash function used to calculate the value.
    - **Hash**: Value obtained by applying the hash function to the file associated with the index of the AIP.
    - **UrlFile:** URI of the file in the package.
    - **NumInfectedFiles:** Possible number of infected files contained in the DIP.
    - **FileGroup**: List of extracted files.
      - **Files**
        - **Id**: Id of the document assigned by the Preservation System
        - **IdDoc**: Id of the document in the document system or other system
        - **IdTypology:** Id of the reference type within the preservation system
        - **Typology:** Name of the Document Type referred to.
        - **SIP Id:** Id of the SIP in which the document is contained.
        - **PathFile**: Name of the file associated with the document.
        - **TypeFile:** type of file (depending on the origin of the SIP).
        - **YearReferenceDoc**: Reference year of the stored object.
        - **FunctionHash**: Type of hash function used to calculate the value.
        - **Hash**: Value obtained by applying the hash function to the file associated with the document.
        - **UrlFile:** URI of the file in the DIP.
        - **RevisionSIPId**: Id of the revised SIP (may correspond with the source SIP or with the last published revision for the source SIP). The node is only present if the SIP represents a revision.
        - **RevisionSIPIdOrigin**: Id of the source SIP (initial SIP from which all revisions originate). The node is only present if the SIP represents a revision.
        - **RevisionNumber**: Revision number required to order the sequence of revisions relating to the origin SIP. The node is only present if the SIP represents a revision.
          RevisionIsLast: Identifies the last version of the file within a sequence of revisions (true or false).

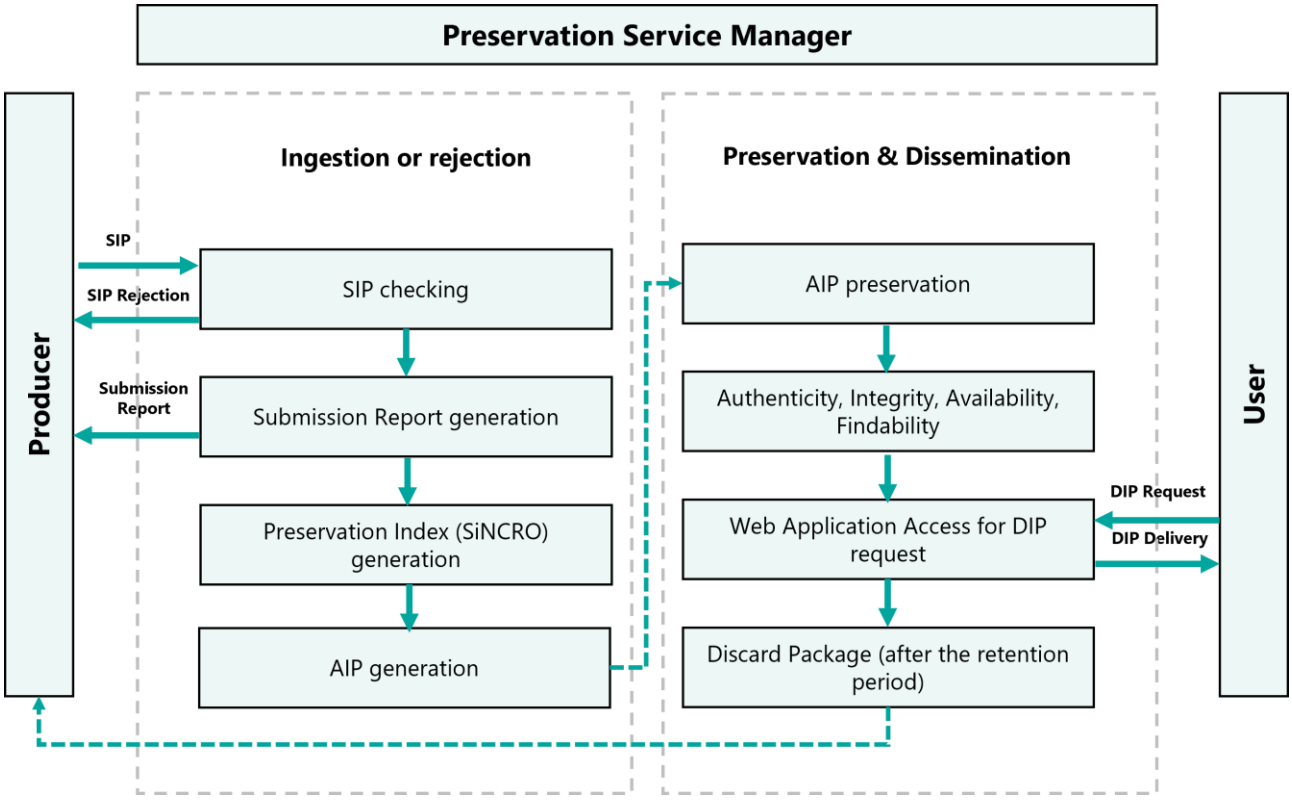
Back to Index

7 THE PRESERVATION PROCESS

The preservation process implemented by the Preservation System is governed in all its phases by the **System Administration entity**, which interacts with the other entities 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 Preservation Manager, 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, will carry out the activities.

The following picture describes the preservation process in accordance with the regulations on the formation, management and preservation of digital documents.



Pic 11 Preservation 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 preservation 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 Preservation 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 HTTPS channel integrates Transport Layer Security (SSL/TLS) type encryption on the HTTP base protocol; this technique increases the level of protection against attacks.

The digital certificate used for the HTTPS connection is provided and guaranteed by GeoTrust.

The sFTP protocol provides for data transfer using the SSH-2 protocol, which guarantees encryption of the transmitted information.

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 Preservation 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.

Namirial Preservation system for SIP intake is all in high availability ensuring data redundancy.

In addition, procedures for generating backups of SIPs submitted by the Producer are active in the preservation service. Storage and backup policies can be defined at the document class level, this setting allows the user to specify how long the backup copy of the SIP should be maintained in the storage dedicated to SIPs.

The storage that maintains backup copies consists of three replicas, two on the primary site and one on the DR site; this architecture ensures high reliability and recovery following a disaster.

All individual SIP intake activities are tracked through the Log Management system built into the preservation system. Logs are maintained throughout the retention period of the submitted objects.

Therefore, if there is a need for data retrieval of SIPs that have not yet been transformed into AIPs by the system, the retrieval in agreement with the Object Owner can be triggered through a request ticket to the Support area. The request sorted to the technical-operational area of Namirial allows to activate the restore of the copies of the SIPs maintained in the dedicated storage area, to recreate the process of SIP acquisition and thus initiate a new takeover process.

Back to Index

7.2 Cheks on Submission Information Packages and objects contained within them

In the process of SIPs intake in the Preservation 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 Preservation System and that for this company a subject is set up in the preservation 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 (within the DIPPre reserved folder) 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 (SourceVdA section).
- **(Blocker)** Verifies that the number of Metadata defined for the document matches those defined within the Document Type (defined in the SIP Index in the SourceVdA section).
- **(Blocker)** Verifies that the name and order of the Metadata defined for the document matches those defined within the Document Type (defined in the SIP Index in the SourceVdA section).
- **(Blocker)** Verification that the value for the mandatory Metadata is present, following the Metadata schema (entered in the SIP in the SourceVdA section).
- **(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 Preservation 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 with the value entered within the DIPPre section.
- **(Blocker)** Verification of the validity of the signature on the file. Optional verification checks on signed files.
- **(Blocker)** Document reference year verification: must be the same for all documents (defined of the SIP Index in the FileGroup/File/MoreInfo/MetaData/ReferenceDocYear section).
- **(Blocker)** Verification of additional metadata valuing using the tags defined for the document (defined in the Index of the SIP in the section: FileGroup/File/MoreInfo/TagPIndex)

If the consistency checks performed in the intake phase are positive, the SIP is acquired by the Preservation 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 an attached time stamp (time reference).

Back to Index

7.3 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 preserved. 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 Preservation 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 be included within a Submission Report.

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

- Preservation System version info;
- Info of the Object Owner with reference to the Preservation 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 Preservation System.

The structure of the Submission Report is shown below:

GeneralDescr

- **IdSetup**, the customer code of the Company.
- **Company Id**, the unique identifier assigned to the owner/producer
- **CompanyName**, The comapny name/designation of the producing entity.
- **Fiscal Code**, The tax code of the Producer.
- **VAT No.**, The VAT No. of the producing entity represented by the Country Code and the VAT No. separated by ":" e.g. IT:04030410288.
- **IdTypology**, The code of the Document Type/class referring to the related SIP.
- **Typology**, Description of the Document Type referring to the related SIP.

- **GenerationDate**, The date of generation of the Submission Report in UTC format.
- **PM**, Data of the Preservation Manager.
    - **Name and Surname,** the name of the Preservation Manager.
    - **Fiscal Code** of the Preservation Manager.
    - **VAT number** of the Preservation Manager.
- **Operator**, Data of the Preservation Delegate.
    - **Name and Surname/Company** Name of the Preservation Delegate.
    - **Fiscal Code** of the Preservation Delegate.
    - **VAT number** of the Preservation Delegate.
- **PSM** Data of the Preservation Service Manager.
    - **Name and Surname,** the name of the Preservation Service Manager.
    - **Fiscal Code** of the Preservation Service Manager.
    - **VAT number** of the Preservation Service Manager.
- **LTA**, Indications of the Preservation System that created the Submission Report
    - **Name**, Commercial name of the Preservation System.
    - **Version**, Version of the Preservation system.

SIPGroup (1-n), Constitutes the group of SIPs considered by the Submission Report.

- **SIP**
- **Id**, Id of the SIP included in the Report.
- **RevisionIdSIP**, Id of the revised SIP. (Can be either the origin SIP or the last published revision for the origin SIP). The node is only present if the SIP represents a revision.
- **RevisionIdSIPOrigin**, Id of the origin SIP (initial SIP from which all revisions originate). The node is only present if the SIP represents a revision.
- **RevisionNumber**, Revision number required to order the sequence of revisions related to the origin SIP. The node is only present if the SIP represents a revision.
- **RevisionSource**, Define the source of the Revision package. Allowed values: RequestProducer, Internal. The node is only present if the SIP represents a revision.
- **User**, data of the Producer submit the SIP.
    - **Name,** Producer Name.
    - **Surname,** Producer's Surname.
    - **Fiscal Code** of the Producer.
    - **VAT number** of the Producer.
- **NumFiles**, Number of Files Included in the Submission Information Package.
- **IpProducer**, Ip of the server/pc where the SIP was formed.
- **Type**, File type depending on the origin of the SIP.
- **AttachmentsDIPImportCounter**
- **Hash** Description of the hash function used to generate the fingerprint.
    - **Type,** Algorithm type (e.g. SHA256).
    - **Value,** The HASH value of the ISIP obtained at intake.
- **FormatDate**, Description of date format e.g. yyyy-MM-ddTHH:mm:ssK
- **Cancelled**, Indicates whether the Submission Information Package was cancelled.
- **PMMessageGroup**, This section collects all messages from the Preservation Manager entered on the SIPs, or derived from the anomaly log.
- **FileGroup** (1-n), The group of files included in the SIP.
    - **IdDoc,** Document Id in the document system.
    - **PathFile,** Object file name to be preserved.
    - **YearReferenceDoc,** The year to which the object to be preserved refers.
    - **PMMessageGroup,** Messages from the Preservation Manager referring to the file under consideration.

- **CheckGroup** (1-n)
  - **Description,** Description of the type of Check performed and the description of the outcome.
  - **Outcome,** may be OK or KO.
  - **Date,** The date the check was executed.

In addition, the Submission Report contains the Tag "<DataGeneration>" as 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 Preservation System **web service**;
- through **access** to the Preservation 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

7.4 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 Preservation System; absence of a Preservation Manager in the Preservation System for the Owner of the documents to which the SIP refers;
- no Preservation Manager is configured in the Preservation 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 file preservation);

- Negative outcome of the verification of the formats declared in the SIP Index (formats among those allowed for file preservation);
- 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 digital signature validity check (only if the SIP Index is signed);
- Negative outcome of the verification of correspondence between the document type configured in the Preservation System and the one declared in the SIP Index (field: SourceVdA);
- Negative outcome of the correspondence verification between the metadata configured in the Preservation System for a specific Document Type and the metadata declared in the SIP Index (field: SourceVdA);
- Negative outcome of the verification of correspondence between the name and order of the metadata configured in the Preservation System for a specific Document Type and those declared in the SIP Index (field: SourceVdA);
- Esito negativo della verifica della presenza dei metadati dichiarati come obbligatori nell'Indice del SIP (campo: SourceVdA);
- Negative outcome of the verification of the presence of the metadata declared as mandatory in the SIP Index (field: SourceVdA);
- Negative outcome of the verification of whether there is a regular expression of the metadata declared in the SIP Index (field: SourceVdA);
- Negative outcome of verification that there are no documents with the same Document Id, within the Preservation 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. Verification checks on signed documents is optional and can be activated only on signed documents.

It should be noted that in the Preservation System there is a procedure to allow the Provider to cancel SIPs that have already ingested only if they are not part of a preservation process that has already been completed (SIP already included in a signed and marked AIP).

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

Back to Index

7.5 Creation and handling of the Archival Information Package

The generation of the Index of the AIP is carried out according to the specifications of the regulations on the formation, management, and preservation of digital documents and according 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 preservation process in accordance with the standard. This procedure takes place through the scheduling of a job within the scheduler integrated in the Preservation System according to the timelines configured for the Object Owner. These rules allow one or more SIPs to be included in an AIP. The nature of the AIP is described in the appropriate section.

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 preservation 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

7.6 Encryption of preservation 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.

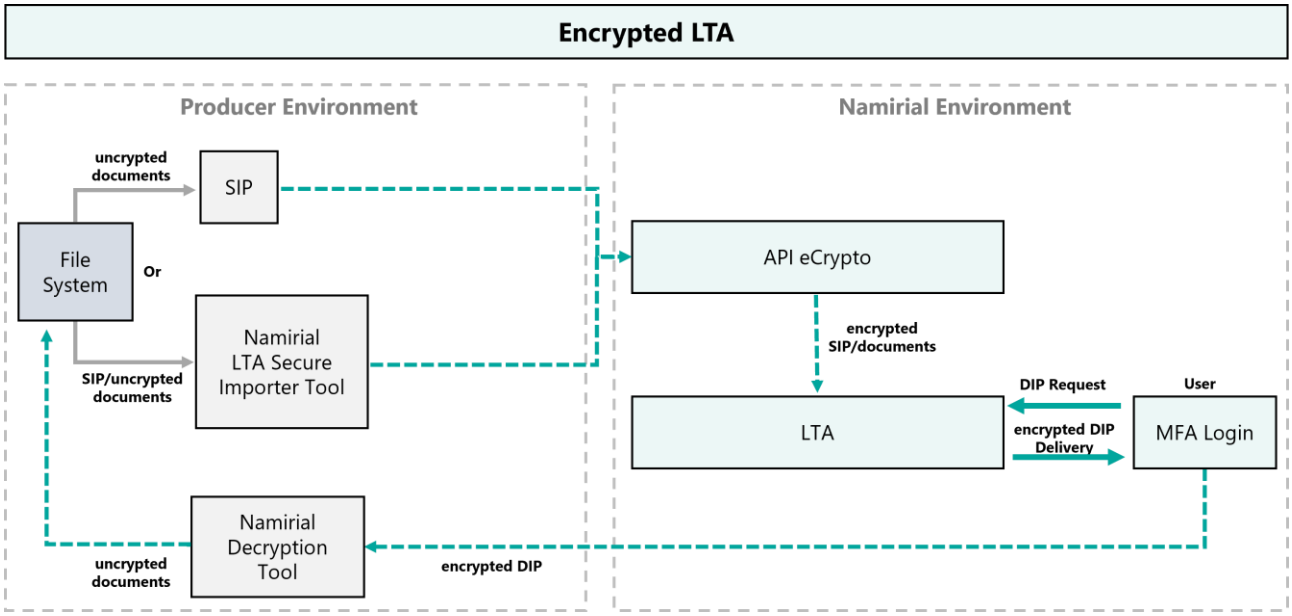
Server-side encryption protects the data at rest. Amazon S3 encrypts each object with a unique key. As further protection, it encrypts the key itself with a master key that rotates regularly. Amazon S3's server-side encryption uses one of the most powerful block ciphers available to encrypt data, namely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

Back to Index

7.7 Management of documents containing sensitive data

In the case of objects containing sensitive data that, according to the regulations, require special handling, 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.



Pic 12 Management of documents containing sensitive data phases

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 Preservation 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. Every document access and request operation are tracked through logs.

Back to Index

7.8 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 types of DIPs and data-models are described in the appropriate section of this document.

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.

Back to Index

7.9 System Access

Web access via interface allows the user to:

- search documents through unique keys (preservation metadata);
- verify the positive outcome of the submission through the download of the Submission Report generated by the System;
- view the preserved documents;
- download duplicates of the preserved documents, by single document or by range of documents;
- download Dissemination Information Packages (DIPs) for the purpose of having preservation evidence.

The user authenticates himself by entering the credentials (username and password) previously communicated to him by Namirial. On first access, the user must change the password in accordance with current data processing regulations. Each user is responsible for the exclusive control of his own access password, which is not recoverable or visible to Namirial personnel as it is anonymized.

In addition, for security reasons, the Preservation System temporarily deactivates consultation users that have been inactive for more than six months.

In the case of objects containing specific sensitive data, the access to the web portal to consult the documents is protected by strong authentication (as indicated in the section "Management of documents containing sensitive data"), which guarantees a higher standard of security. To consult a specific encrypted document, it is necessary to download the document. The downloaded file can be viewed through the specific Namirial component that allows decrypting files only to those authenticated by the assigned decryption key.

All authentication, search, consultation and download operations of digital objects so far indicated are implementable through integration by calling the preservation system web service.

Activities related to access, consultation and exhibition are tracked through the Log Management system built into the preservation system. Logs are maintained throughout the contract period.

Back to Index

7.10 Creation of duplicates and electronic copies and description of the possible intervention of the public official

There are cases where the production of an electronic copy with attestation of conformity by a public official is required:

1. to update the file format of the document to technological evolution by activating a replacement reversion process due to checks by the Preservation Service Manager

2. at the express request of the User.

In the first case, the ownership of the activity is in the hands of the LTA Provider and the Preservation Service Manager who, according to a preventive plan of controls, performs the verifications of integrity, readability and adequacy of the digital representation of the documents to the technological evolution.

The process, fully traced in the Log Management Systems, requires the management of a replacement reversion, i.e., the process that transfers one or more preserved documents by changing their digital representation and ensuring the integrity of the content.

In cases where the intervention of the public official is involved, the procedure involves making the original and copy documents available to the person in charge, who, once he or she has verified the immodifiability of the content, affixes the digital signature on a file called "attestation of conformity."

This document is preserved in the system as an integrative attachment (linking by hash between Archival Information Packages) along with the conforming copy document and then both are preserved. All evidence of the operation performed is maintained over time.

It should be noted that the choice of suitable formats provided for and recommended by current regulations (e.g., PDF/A format) is indicated to minimize risks related to technological obsolescence.

Back to Index

7.11 Discard

Once the retention period for packages and documents agreed between the LTA Provider and the Customer has passed, the preservation system must implement the Archival Information Package discard procedure.

The system notifies (via email/certified mail) the Owner of the start of the discard process for certain AIPs, thus giving notice and providing the information necessary for the Owner to evaluate the possible request for extension of the retention period.

If the preset deadline is exceeded and no request for extension is made, the discard procedure job is triggered and produces Discard Information Packages in relation to the AIPs subject to the procedure. The operation is tracked in the system and an Index file of the Discard Information Package is produced, digitally signed by the Preservation Service Manager, which thanks to the XSLT file can be viewed by the Owner of the documents or other interested parties, for verification of the correct procedure performed.

Finally, it is recorded in the system if the management of the discard procedure is related to public or private archives that are of particularly important historical interest; in this case, an alert is triggered and the discard procedure of the Archival Information Package takes place only after authorization from the Ministry of Culture, issued to the Owner in accordance with the provisions of the relevant regulations.

Back to Index

7.12 Measures to ensure interoperability and transferability to another LTA Provider

The main data-structure guaranteeing interoperability for Namirial LTA Provider is the Archival Information Package generated according to the technical rules on the Preservation System and according to the SInCRO standard (UNI 11386).

Its dissemination through the request of one or more DIPs through different modalities (web interface, web service) guarantees the correct transferability by the Owner of the object to another LTA Provider.

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

Each DIP contains a DIP Index, signed by the Preservation Service Manager, which is a report of the dissemination performed. The DIP also contains the XSLT file for the correct display of the DIP Index.

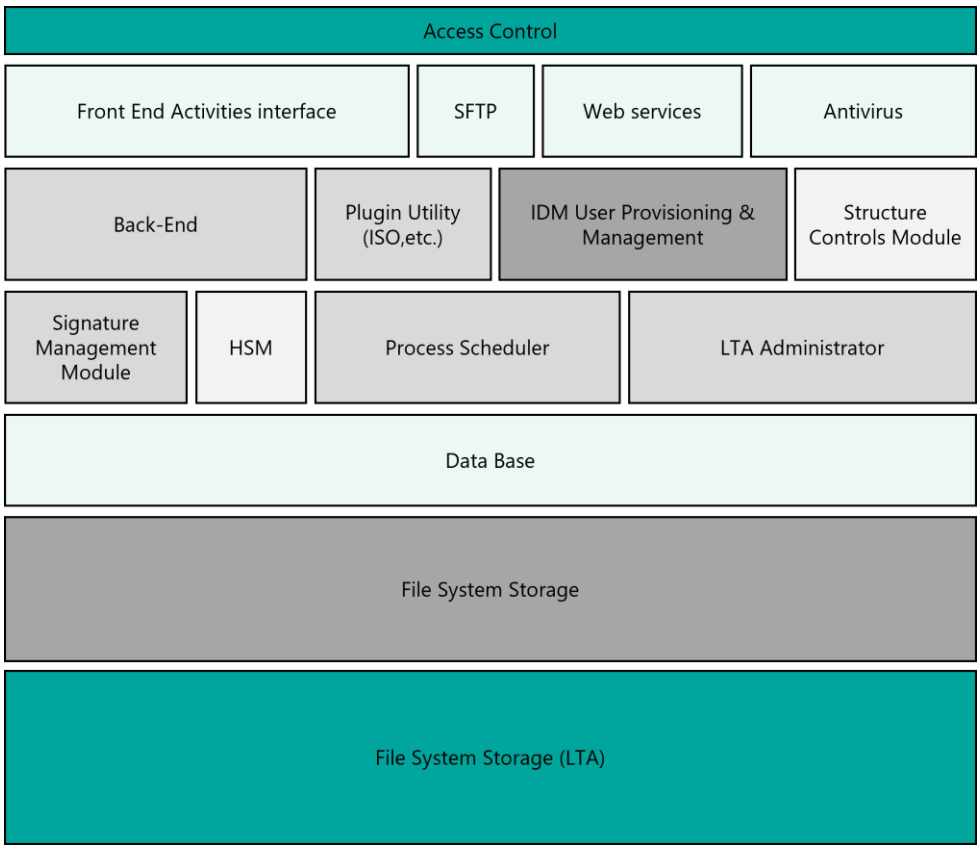
The system can ingest SIP/AIP compliant with the SInCRO structure (UNI 11386) in the case of way-in/migration of archives managed by another LTA Provider that has adopted this standard for generating the Index of the AIP.

Back to Index

8 PRESERVATION SYSTEM

Namirial Preservation Service infrastructure has been designed, organized, and developed to make the work steps atomic and the flow modular. High reliability components also 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.



Pic 13 Preservation 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 bulk uploading of SIPs.
- Antivirus.

- Back-end module for all interface 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;
    - The generation of Discard Information Packages.
- 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 Preservation 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:

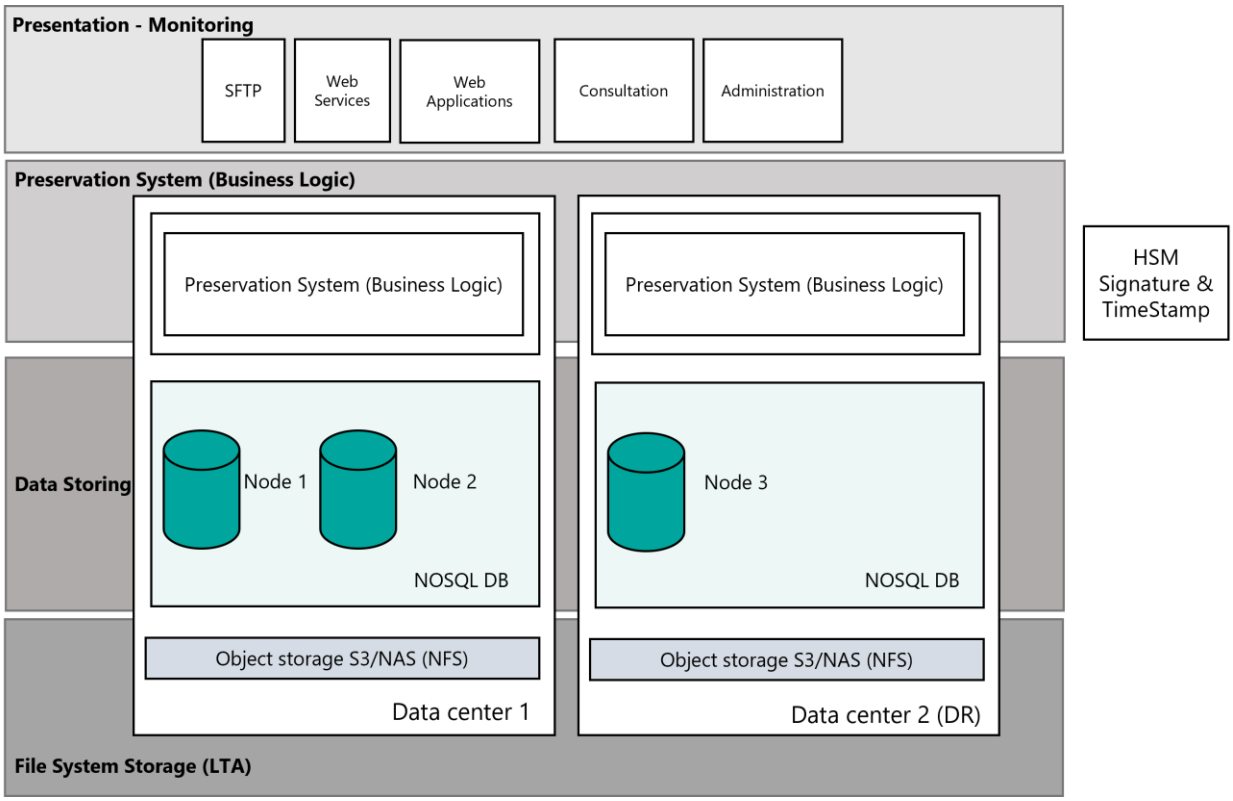
- Identification of the logical/physical person performing the activity;
- Control and management of the activity itself;
- Expandability of the module (activity load balancing, allocation, and clustered growth on available resources).

All module activities are tracked in the Log Management System, described in the following paragraphs.

Back to Index

8.1 Logical components

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



Pic 14 Preservation System logical components

Application front-end (Web App front-end): is the administration and consultation portal of the Preservation System. The web portal manages the authentication and profiling of users and allows to configure all the components of the Preservation System, the master data of the Object Owner (Companies), the subjects involved in preservation 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 Preservation System, routes traffic to DR sites.

Preservation System Web Service: the computer document preservation service that exposes all the functions for application management of the preservation 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 Preservation System; therefore, it interacts with the other entities of the system (preservation planning, general services, acquisition, preservation, data management, accesses).

The logical entity of preservation planning and controls works and interacts with the process scheduler and defines the functions and services to control the entire Preservation 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, Discard Information Package).

Preservation 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 Preservation 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 preservation 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.

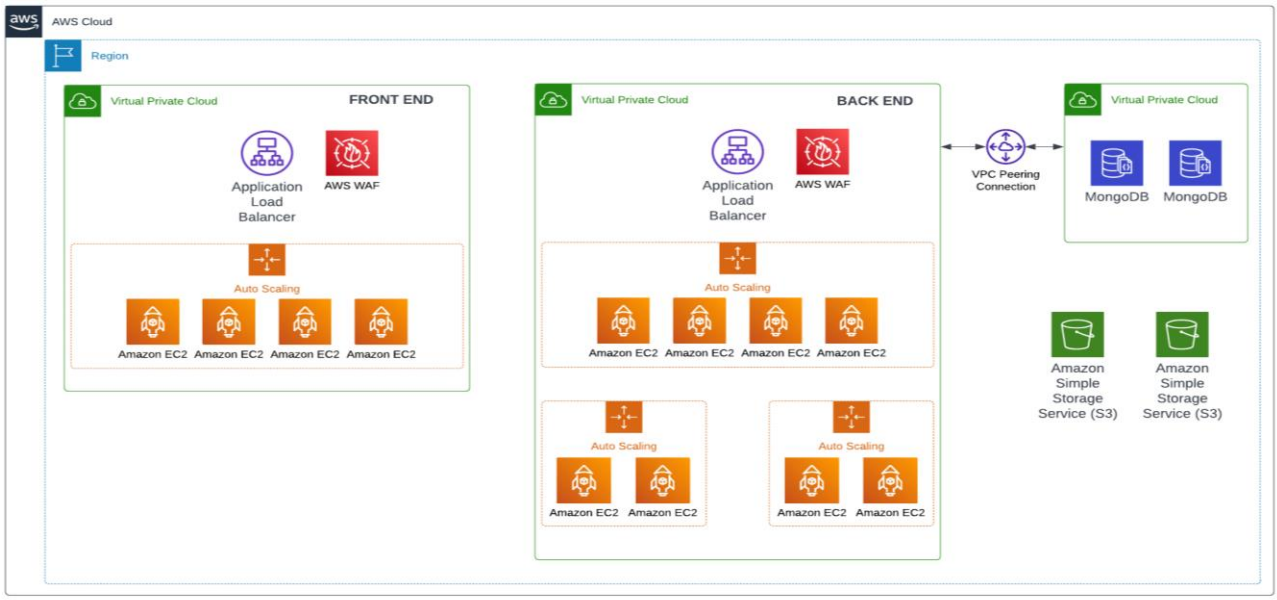
From the service delivery facility (primary facility), there is a direct, encrypted, private link to the Disaster Recovery facility. This facility is logically divided, as is the primary facility.

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

Back to Index

8.1 Physical components

The preservation system provides services based on Amazon AWS data centers:



Pic 15 Physical components

- Primary Site, located on Amazon AWS 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 Cloud Ops Manager.

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

Amazon's network architecture enables it to handle 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 Amazon AWS 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.

8.1.1 Italy

The distance of the Primary and Site DR regions are:

- Sito Primario: AWS Region Italiana (Milano) -> AWS Region Tedesca (Francoforte) – 600 Km
- Sito Disaster Recovery AWS Region EU-central-1 Francoforte - Distanza in linea d'aria maggiore di 600km.

- Primary Site: AWS Italian Region (Milan) -> AWS German Region (Frankfurt) - 600km
- Disaster Recovery Site AWS Region EU-central-1 Frankfurt – Linear distance greater than 600km.

8.1.2 France

- Primary Site: AWS French Region -> AWS Italian Region (Milan) - 851km
- Disaster Recovery Site AWS Region EU-central-1 Frankfurt - Linear distance greater than 600km.

8.1.3 Romania

The Preservation System provides services on data center of GTS Telecom SRL.

- Primary site, located in GTS Telecom SRL's datacenter with all necessary components in HA and connected via connectivity
- Disaster Recovery site, located in the datacenter of GTS Telecom SRL

*****

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.

Back to Index

8.2 Software Components

The following are the software components used in the Preservation 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

8.3 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.).

8.3.1 Operation and Maintenance of the Preservation System

The security requirements (physical security, logical security, and organizational security) adopted in the operation and maintenance of the Preservation System, incident management policies, and business continuity of the preservation 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 preservation 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 preservation 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.

8.3.2 Log management and maintenance

The Preservation System applicatively integrates tracking via a log system of all calls/events on the system. The data tracked are:

- LOG Level: indicates the type of information tracked, Debug, Warning, Info.
- Message: descriptive information about the operation performed.
- Notes: the application parameters sent for the considered operation.
- Operation: the description of the executed application event.
- User: the name of the User who requested the operation.
- IP Address: the IP address, if any, from where the request originated.
- Creation Date: the date the Log was created.

Logs are maintained in accordance with applicable regulations by implementing mechanisms and controls to protect against unauthorized changes or operational problems in order to avoid:

- the deactivation of logging tools;
- alterations to logged messages;
- editing and modifications to log records;
- running out of available space resulting in loss of records;
- the loss of confidentiality of information.

A daily backup is made, and logs are kept in the Preservation System for the period related to the retention of the retained objects.

8.3.3 Preservation System monitoring

All operations performed by each system component are tracked via logs to maintain evidence of activities and facilitate the diagnosis of any anomalies and/or incidents.

The monitoring system adopted is described in more detail in the chapter on monitoring and controls.

8.3.4 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.

8.3.5 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 preservation, 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.

Periodic audits are, in addition, carried out on the functionality of the Preservation 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 preservation, technological and software evolutions, etc.

8.3.6 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 Preservation Service-Long Term Archiving (LTA) to the LTA 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 Preservation 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 Preservation 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 preservation 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 Preservation 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 Preservation 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 preservation 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 Preservation 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 Preservation System for a specific Owner).

Regarding the readability check, automatisms are in place in the Preservation 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 preserved 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 preserved 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 Preservation System is governed by Namirial through the adoption of:

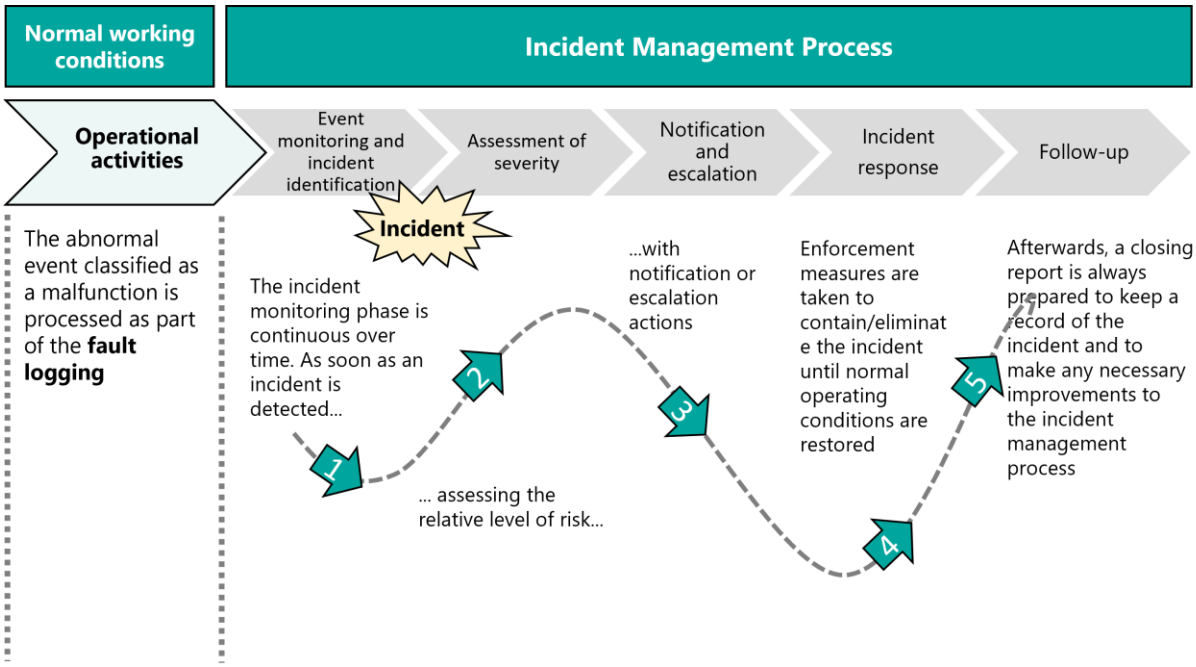
- appropriate detection tools;
- formalized systems for responding to unexpected events recognized as incidents;
- appropriate communication processes;
- efficient countermeasures for security and restoration of Preservation System functionality or in case of data loss.

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 preservation 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.



Pic 16 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 ANNEX

Complementing this LTA Practice Statement there are several corporate documents relating to specific aspects concerning to Namirial Preservation 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*
1.	Namirial - LTA - Qualified electronic signatures and seals preservation policy	Public document
2.	Namirial - LTA - Security Plan	Internal document
3.	Namirial - LTA - Termination Plan	Internal document
4.	Namirial - LTA - Risk Assessment	Internal document

Back to Index