Preservation System Manual

Ver. 4.0

Version of the document

Action	Date	Name	Department
Draft	01.09.2023	Simone Fiore Patrizia Sormani Simone Diodati Beatrice Tafini Stefano Scagni	
Check	30.10.2023	Simone Fiore Patrizia Sormani Simone Diodati Beatrice Tafini Stefano Scagni	
Approval	03.11.2023	Riccardo Genghini Paolo Sironi	RSC CEO, Chairman

Version Register

Ver. No./Rev/Draft	Issue date	Changes	Observations
1.0	28.03.2015		
1.1	04.06.2015	Additions to paragraphs 7.1, 7.2, 7.3, 7.4, 7.6, 7.7, 2, 7.9	
2.0	30.05.2016	Formal adjustments as required by "*Preservation manual layout v.2*"	Added link "Back to Table of Contents"; added illustration captions; updated bullets.
2.1	26.10.2016	Updated department managers, following the corporate changes	

2.2	12.02.2019	Added privacy roles (items 2 and 4) Updated privacy regulations (items 1.2 and 8.4) and electronic invoicing (item 3) Added role log (4.3) Clarifications on PdD management (item 4 par. 5.2). Specification of support of web services for PdV acquisition as well (section 6.2), with the conversion of the IPdV from PDF/A to XML. Updated IPdV format. Updated electronic invoice file format in the PdA (section 6.3); updated metadata specifications for the PdA. Added items 7.1.2, 7.2 .1, 7.10, 8.5 and 9.2 Amended management of PdV rejection notices: PEC prescribed (section 7.4) Reference to 2015 version of ISO 9001 (section 8.4)	In general, several typing and formatting errors were corrected, although not detailed as they do not represent material amendments. In general, any references throughout the document to the FTP acquisition channel alone have been revised by adding the web service channel as well.
2.3	22.06.2020	elimination notification mode type. Par. 7.6 - better enunciation encryption of PdD on removable media. Inserted service levels for the creation of PDs. Par. 8.3 changed Data Center location specifications	
		Update following the entry into force of the Guidelines on the formation, management and	

		preservation of electronic documents. Par. 1 – Better description of the document elimination procedure and inclusion of the link where the Manual is made public. Par. 1.1-6-6.1-7.9- – Regulatory alignment. Par. 1.2.-2-4.1-5.1-5.3-7-7.3-7.6– Alignment to LLGGs. Par. 3.1 - Verification and updating of current regulations. Par. 3.2 - Verification and updating of current reference standards. Par. 4 - Update of Roles. Par. 4.2 - Added new figure within the Privacy Team. Par. 5.2 - Formal adjustment. Par. 6.2 - Formal adjustment. Par. 6.3 - Descriptive aligned with current activities and LLGGs and correction and addition of More Info PdA. Par. 6.4-7.0 - Added specification regarding the signing of PDDs. Par. 7.1 - Improvement of the described on the acquisition of deposit packets for their taking charge and updating of Fig. 2 and elimination notification mode type. Par. 7.6 - better enunciation encryption of PdD on removable media.	

		Inserted service levels for the creation of PDs. Par. 8.3 changed Data Center location specifications	
3.0	22.12.2022	Update following the entry into force of the Guidelines on the formation, management and preservation of electronic documents. Par. 1 – Better description of the document elimination procedure and inclusion of the link where the Manual is made public. Par. 1.1-6-6.1-7.9- – Regulatory alignment. Par. 1.2.-2-4.1-5.1-5.3-7-7.3-7.6– Alignment to LLGGs. Par. 3.1 - Verification and updating of current regulations. Par. 3.2 - Verification and updating of current reference standards. Par. 4 - Update of Roles. Par. 4.2 - Added new figure within the Privacy Team. Par. 5.2 - Formal adjustment. Par. 6.2 - Formal adjustment. Par. 6.3 - Descriptive aligned with current activities and LLGGs and correction and addition of More Info PdA. Par. 6.4-7.0 - Added specification regarding the signing of PDDs.	

		Par. 7.1 - Improvement of the described on the acquisition of deposit packets for their taking charge and updating of Fig. 2 and relative description. Deletion of previous par. 7.1.1. Par. 7.1.2. - Removal of detached mode on time stamp. Par. 7.2 - Better enunciation of the paragraph regarding the checks made on the deposit packets and the objects contained therein. Par. 7.2.1. - Better descriptive statement on virus management. Par. 7.4 - Better enunciation of the elimination of deposit packets and on how to report faults. Par. 7.5 - Improved descriptive on the preparation and management of the storage packets. Par. 7.7.2 - Simplified and aligned with current regulations. Par. 7.6 - Added specification regarding the signing of PDDs. Par. 7.8 - Improvement through the example of three case scenarios in which elimination of storage packets can occur.	

		Par. 9.7 - Added reference to the Interoperability Models between preservation systems, issued by AgID. Par. 7.10 - Improvement of the descriptive on the procedure of destruction of PdVs. Par. 8.1 - Improved descriptive on the logical components of the preservation system. Par. 8.3 - Addition of initial description of Cloud infrastructure to further support the physical system and editing related image. Par. 9.2 - Improving the descriptive. Par. 9.3 - Deleting the example.	
3.1	24.03.2023	Update following the acquisition of the eWitness s.r.l. business unit by Intesi Group S.p.A. The whole document - Intesi Group replaces eWitness Par. 4 - Updated roles. Par. 4.2 - Updated the Privacy reference. Par. 4.3 - Updated the role log.	
4	03.11.2023	Changes: Par. 1. Best explanatory detail Par. 2. Revision Par. 3 Revision and updating	

		Par. 4 LLGG alignment and simplification. Par. 5 LLGG alignment and simplification - process alignment Par.6-7-8-9 process alignment	

Sommario

1. Purpose and Scope of the document

This Manual describes, from an organizational, technical and operational point of view, the *preservation system* of electronic documents that Intesi Group S.p.A (hereinafter also only" Intesi Group") has created, manages and controls in order to implement a regulation-compliant Preservation service in favor of its customers.

This Manual, in particular:

- identifies the organizational model defined by Intesi Group for the *preservation system*;
- defines the competencies, roles and responsibilities of the actors involved in the document preservation process;
- lists the types of objects subject to preservation, including an indication of the formats managed, the metadata to be associated with the different types of documents, and any exceptions;
- illustrates the procedures to ensure the preservation of electronic documents produced and received by individual clients, as well as computer files, guaranteeing their characteristics of authenticity, integrity, reliability, readability and availability;
- describes the processing of the entire management cycle of the preserved object within the preservation process;
- describes how to access the preserved documents and files, for the period prescribed by the standard, regardless of the evolving technological environment, and how to carry out the process of exhibition and export from the *preservation system* with the production of the distribution packet;
- defines the procedures for monitoring the functionality of the preservation system and the integrity checks of the archives with evidence of the solutions adopted in case of faults;
- specifies procedures for the production of *duplicates* or *copies* pursuant to Legislative Decree No. 82/2005, as amended (Digital Administration Code - hereafter also just CAD);
- indicates the timeframes within which, different types of documents are to be eliminated where the Customer, as Holder has not given appropriate directions to Intesi Group regarding discarding and/or the there is no longer a contract in place.

This Manual fully incorporates the provisions contained in the CAD and the Guidelines on the Formation, Management and Preservation of Electronic Documents, as well as additional regulations

and directions set forth in the legal or practical measures, including administrative ones, referred to in the chapter "*reference regulations and standards*".

This Manual is made public in PDF format digitally signed by the legal representative of Intesi Group on the Intesi Group S.p.A. website.

The Customer, as the Holder as well as the Storage Manager (see §4.1):

- is required to consult this Manual prepared by Intesi Group with the utmost diligence and care;
- approves by adopting the contents of this Manual.

1.1 Reference context

The outsourced Preservation service is supported by Article 44 of the CAD under which preservation can be entrusted, in whole or in part, to other entities, public or private, offering suitable organizational and technological safeguards.

Customers in need entrust Intesi Group with the preservation of their documents according to the organizational model agreed upon between the parties and set forth in the Guidelines on the Formation, Management and Preservation of Electronic Documents.

1.2 The Preservation Manager's Preservation service trust process

Under the provisions of article 44 of CAD and the Guidelines on the Formation, Management and Preservation of Electronic Documents, preservation will be entrusted to Intesi Group through a special contract providing the obligation to comply with the preservation manual prepared by its manager. Following that trust, Intesi Group assumes the role of external data processor as required by Article 28 of Regulation (EU) 679/2016 (GDPR).

2 Terminology (Glossary, Acronymism)

The Glossary of Terms and Acronyms, Annex 1 to the document "Guidelines on the Formation, Management and Preservation of Electronic Documents" and its subsequent amendments and/or additions, is fully referred to with reference to the terminology used in this Manual.

In any case, the following definitions, useful in the consultation and comprehension of this Manual, are provided.

Access: Operation that allows computer documents to be viewed.

Deposit agreement: Agreement between customer and registrar in which describes how documents will be transmitted into the preservation system. Resumes a provision of the OAIS - ISO 14721 standard and indicates the formal document that establishes the category of documents and their metadata subject to preservation, the formats to be managed, the operational methods of transfer, the controls for taking charge of packets, and the specific responsibilities in charge of all those involved in the preservation process. The document constitutes together with the Customer Preservation Manual an integral part of the Contract.

Reliability: A characteristic that, with reference to a document management or preservation system, expresses the level of trust the user places in the system itself, while with reference to the electronic document it expresses the credibility and accuracy of the representation of acts and facts contained therein.

Electronic document aggregation: Set of electronic documents or set of electronic files brought together by homogeneous characteristics, in relation to the nature and form of the documents or in relation to the subject and matter or in relation to the functions of the entity

Archive: Set of documents produced or acquired by a public or private entity in the course of its activities.

Computer Archive: Archives consisting of electronic documents, organized into electronic document aggregations.

Attestation of conformity of computer image copies of an analog document: Statement issued by a notary public or other public official authorized to do so attached or sworn to the computer document.

Authenticity: Characteristic by virtue of which an object must be regarded as corresponding to what it was at the original moment of its production. Therefore, an object is authentic if at the same time it is

intact and complete, having not undergone any unauthorized modifications in the course of time or space. Authenticity is assessed on the basis of precise evidence.

Certification: Third-party attestation regarding conformity to specified requirements of products, processes, people and systems.

Classification: Activity of organizing all documents according to a scheme consisting of a set of hierarchically articulated items that identify, in the abstract, the functions, competencies, activities, and/or subjects of the producing entity.

Customer: The holder, sole and legitimate Holder of the objects, data, documents sent to the preservation system; s/he is also the person legally entitled to the subscription and acceptance of the Contract for the outsourcing of the digital Preservation service of electronic documents.

Code or CAD: Legislative Decree no. 82 of 7 March 2005, as amended;

Registrar: Public or private entity that performs electronic document preservation activities.

Preservation: Set of activities aimed at defining and implementing the overall preservation system policies and at governing the management in relation to the adopted organizational model, guaranteeing the characteristics of authenticity, integrity, legibility, and availability of documents over time.

Contract: the electronic document digital preservation service trust document, signed by Intesi Group and the Customer. The Contract governs the general digital Preservation aspects for electronic documents owned by the Customer.

File naming conventions: Set of syntactic rules that define the name of files within a filesystem or packet.

Analogue document digital copy: the electronic document with content identical to that of the analogue document from which it was taken.

Electronic document digital copy: the electronic document with content identical to that of the document from which it was taken on electronic support with different sequence of binary values.

Personal Data: This is the information that identifies or makes identifiable, directly or indirectly, a natural person and may provide information about his or her characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc.

Recipient: Subject or system to which the electronic document is addressed.

Digest: See Cryptographic Footprint.

Computer administrative document: Any representation, graphic, photocinematic, electromagnetic or of any other kind, of the contents of acts, including internal ones, formed by public administrations, or, in any case, used by them for the purposes of administrative activity.

Computer document: Any content stored in electronic form, especially text or sound, visual or audiovisual recording.

Electronic document: Electronic representation of legally significant deeds, facts or data.

Digital duplicate: See Article 1, paragraph 1, letter i) quinquies of the CAD.

eSeal: See electronic seal.

Exhibit: an operation to display a stored document.

eSignature: See electronic signature.

Extract of electronic document: Part of the document taken from the original document.

Extract for summary of electronic document: Document in which facts, states or qualities inferred from electronic documents are attested in a summary manner.

Static data extraction: Extraction of useful information from large amounts of data (e.g., databases, data warehouses, etc.), through automated or semi-automated methods.

IT evidence: Finite sequence of bits that can be processed by a computer procedure.

Electronic file: Structured and uniquely identified computerized document aggregation containing computerized acts, documents or data produced and functional for the performance of an activity or the conduct of a specific procedure.

File: Set of logically related information, data, or commands collected under one name and recorded, by means of a processing or writing program, in the memory of a computer.

Filesystem: File management system, structured by one or more tree hierarchies, that determines how files are named, stored, and organized within a storage facility.

Digital signature: a particular type of advanced electronic signature based on a qualified certificate and an encoded key system, one public and one private, related to each other, which allows the holder using the private key and the recipient using the public key, respectively, to manifest and verify the origin and integrity of an electronic document or a set of electronic documents.

Electronic signature: See Article 3 of the eIDAS Regulation.

Advanced electronic signature: See Articles 3 and 26 of the eIDAS Regulation.

Qualified electronic signature: See Article 3 of the eIDAS Regulation.

Flow (binary): Sequence of bits produced in a finite, continuous time interval that has a definite origin but whose instant of termination may not be predetermined.

Container format: File format designed to allow the inclusion ("enveloping" or wrapping), in the same file, of one or more pieces of digital evidence subject to different types of encoding and with which specific metadata may be associated.

File format: Mode of representing the sequence of bits that constitute the electronic document; commonly identified through the file extension.

Cryptographic hash function: Mathematical function that generates, from digital evidence, a cryptographic fingerprint or digest (see) in such a way that it is computationally difficult (in fact impossible), from it, to reconstruct the original digital evidence and to generate equal fingerprints from different digital evidence.

Document Management: Process aimed at the efficient and systematic control of the production, receipt, holding, use, selection and storage of documents.

Hash: English term used, improperly, as a usage synonym for "cryptographic fingerprint" or "digest" (see). Unique identifier Sequence of numbers or alphanumeric characters uniquely and persistently associated with an entity within a specific scope.

IdPdV: Deposit Packet Index;

Footprint The sequence of binary symbols of predefined length generated by the application of a suitable hash function.

Integrity: Characteristic of an electronic document or document aggregation by virtue of which it appears that they have not undergone any unauthorized alteration in time and space. The characteristic of integrity, together with that of completeness, concurs to determine the characteristic of authenticity.

Interoperability: Ability of a computer system whose interfaces are public and open to automatically interact with other similar computer systems for information exchange and service delivery.

Legibility: Ability of a computer document that ensures the quality of being able to be decoded and interpreted by a computer application.

Log: Chronological record of transactions performed on a computer system for purposes of access control and verification, or for logging and tracking changes that transactions introduce into a database.

Preservation manual: Electronic document prepared by the Holder that describes the preservation system and details the organization, the individuals involved and the roles played by them, the operating model, process description, and description of architectures and infrastructure.

Preservation System Manual: An electronic document prepared by the Preservation provider that describes all the activities carried out to implement, manage and monitor the preservation system by governing its operation in relation to the organizational model adopted.

Timestamp: digital evidence that allows you to make a time reference enforceable before third parties; the timestamp proves the existence of a particular piece of information at a certain time, in the form of data structure signed by a Time Stamping Authority.

Metadata: Set of data associated with an electronic document, or an electronic file, or electronic document sets, to identify and describe its context, content and structure, as well as to allow its management over time in accordance with ISO 15489-1:2016 standard and more specifically by ISO 23081-1:2017 standard.

OAIS: Open Archival Information System is the ISO 14721:2012 standard that defines concepts, models and functionality inherent in digital archives and aspects of digital preservation.

Preservation object: Digital object deposited into a preservation system.

Digital object: Digital information object, which can take various forms, including those of electronic document, electronic file, electronic document aggregation or computer archive.

Storage packet: Electronic packet consisting of the transformation of one or more deposit packets according to the methods indicated in the preservation manual.

Distribution packet: Electronic packet sent from the preservation system to the user's request for access to preservation objects.

File package: Finite set of multiple files (possibly organized in a subtree structure within a filesystem) that constitute, collectively as well as individually, unitary, self-consistent information content.

Deposit packet: Electronic packet sent from the author to the preservation system according to the format described in the preservation manual.

Pathname: Ordered concatenation of a file path and its name. Path Information about the virtual location of the file within the filesystem expressed as an ordered concatenation of the name of the path nodes.

Preservation system security plan: A document that, in the context of the overall security plan, describes and plans activities aimed at protecting the electronic document preservation system from possible risks.

Taking charge: Acceptance by the preservation system of a deposit packet as it complies with the procedures set forth in the preservation manual and, in the case of outsourcing the service, in the agreements entered into between the holder of the object of preservation and the preservation service manager.

Process: Set of related or interacting activities that transform input elements into output elements.

Preservation process: Set of activities aimed at the preservation of electronic documents.

PdV producer: Natural person, usually different from the person who formed the document, who produces the deposit package and is responsible for transferring its contents to the preservation system. In public administrations, this figure is identified with the head of document management.

qSeal: Qualified electronic seal, as per Article 35 of the eIDAS Regulation.

qSignature: Qualified electronic signature, as per Article 25 of the eIDAS Regulation.

Deposit log: Electronic document certifying that the preservation system has taken charge of the deposit packets sent by the producer.

eIDAS regulation: electronic IDentification Authentication and Signature, Regulation (EU) 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Preservation computer system manager: Person who coordinates the information systems within the registrar, possessing the professional requirements identified by AGID.

Preservation service manager person who coordinates the preservation process within the registrar (preservation provider), possessing the professional requirements identified by AgID.

Preservation Manager: Person who defines and implements the overall policies of the preservation system and governs its management with full responsibility and autonomy.

Archival preservation function manager: Person who coordinates the preservation process from an archival perspective within the registrar, possessing the professional requirements identified by AgID.

Data Protection Officer: Person with specialized knowledge of data protection legislation and practices, capable of fulfilling the tasks set forth in Article 39 of Regulation (EU) 2016/679.

Preservation system security manager: Person who ensures compliance with security requirements within the registrar, possessing the professional requirements identified by AgID.

Preservation system development and maintenance manager: Person who ensures the development and maintenance of the system within the preservation system, possessing the professional requirements identified by AgID.

Data Processor: Natural or legal person, public authority or any other entity that processes personal data on behalf of the Data Controller.

Time reference: Data set representing a date and time with reference to Coordinated Universal Time (UTC).

Transfer: A procedure by which one or more electronic documents are converted from one file format (i.e., envelope format, or file packet format) to another, leaving the content unchanged as far as possible by the technical characteristics of the target file format(s) and encodings.

Elimination: Operation by which documents deemed no longer relevant for legal-administrative and historical-cultural purposes are permanently disposed of, in accordance with current regulations.

SDI: The Interchange System, managed by the Internal Revenue Authority, is a computer system capable of:

- receive invoices in the form of files with PA Invoice characteristics,

- carry out checks on received files,
- forward the invoices to the recipient Administrations.

The Interchange System has no administrative role and does not perform tasks related to invoice storage and archiving.

Series: Grouping of documents with homogeneous characteristics (see also electronic document aggregation).

Electronic seal: Data in electronic form appended or connected by logical association to other data in electronic form, to ensure the origin and integrity of the latter.

Preservation system: Set of rules, procedures and technologies that ensure the preservation of electronic documents in implementation of the provisions of Article 44(1) of the CAD

Time Stamping Authority: Entity enabled and accredited by AgID to issue the Time Stamp.

Holder (of the preservation object): Producer subject of conservation objects.

Data Controller: Natural or legal person, public administration or any other entity responsible for decisions regarding the purposes and processing methods of personal data and the relevant means, including the security profile.

Transfer: Transfer of custody of documents from one person or entity to another person or entity.

User enabled: A person, entity, or system that interacts with the services of an electronic document management system and/or an electronic document preservation system in order to use the information of interest.

Deposit: Transfer of custody, ownership and/or responsibility of documents. In the case of a state judicial and administrative body operation by which the preservation manager also transfers the records to the State Archives or Central Archives.

For any other definitions, please refer to the Glossary of Terms and Acronyms, Annex 1 to the document "Guidelines on the Formation, Management and Preservation of Electronic Documents."

The following table shows the acronyms for the business functions defined in this document:

Role	Acronym
Preservation Service Manager	RSC
Security Manager for Preservation Systems	RSSI
Preservation Archival Department Manager	RFA
Data Protection Officer	DPO
Preservation Computer System Manager	RSI
Preservation System Development and Maintenance Manager	RSM

3 Reference Regulations and Standards

3.1 Reference regulations

The main reference regulations for preservation service are detailed below

At the date of this Manual, the list of the main pertinent Italian legal regulations, ordered according to the criterion of source hierarchy, consists of:

- Decree of the President of the Republic no.633 of 26 October 1972 , *Establishment and regulation of value-added tax;*
- Legislative Decree no. 357 of 10 June 1994, *Urgent tax provisions to accelerate the recovery of the economy and employment, as well as to reduce taxpayer requirements;*
- Circular 98/E 2000, Circular of the Ministry of Finance dated 17/05/2000 - Provides clarifications and answers to questions regarding direct taxes, IRAP, VAT and various tax penalties;
- Guidelines *on the accessibility of IT tools* drafted in accordance with what is reported and contained in Article 11 of Law No. 4 of 9 January 2004;
- Legislative Decree no. 52 of 20/02/04, Implementation of Directive 2001/115/EC simplifying and harmonizing the conditions laid down for invoicing in respect of value added tax;
- Legislative Decree no. 82 of 7 March 2005 *Digital Administration Code (CAD)*;
- Law no. 244 of 24 December 2007, *Provisions for the formation of the annual and multi-year budget of the State;*
- Revenue Agency Circular No. 36/E of 6 December 2006 *Methods of fulfilling tax obligations*

related to computer documents and their reproduction in different types of media;

- Ministerial Decree of 7 March 2008, (Ministry of Economy and Finance), Identification of the operator of the electronic invoicing interchange system as well as its attributions and competencies (Official Gazette, 3 May 2008, No. 103);
- M.D. 23 January 2004, M.D. 24 October 2000, no. 370. Substitute storage process of mechanographic billing slips. Books and records formed on computer media, may be kept similarly to those kept mechanographically;
- Community Directive No. 45 of 13 July 2010, on the common system of value added tax with regard to electronic invoicing rules;
- Prime Minister Decree of 22 February 2013, *Technical rules concerning the generation, affixing and verification of advanced qualified and electronic digital signatures;*
- Ministerial Decree No. 55 of 3 April 2013, *Regulations on the issuance, transmission and receipt of electronic invoices to be applied to public administrations*;
- Provision of 30 April 2018, *Technical rules for the issuance and receipt of electronic invoices for the supply of goods and provision of services made between persons residing, established or identified in the territory of the State and for changes thereto, using the Interchange System, as well as for the telematic transmission of data of cross-border supply of goods and provision of services and for the implementation of the additional provisions of Article 1, paragraphs 6, 6a and 6b, of Legislative Decree No. 127 of 5 August 2015;*
- Provision of 13 June 2018, *Proxy arrangements for the use of electronic invoicing services*;
- Legislative Decree No. 101 of 10 August 2018, *Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*;
- Art. 2215-bis cc, Computer records, Books, directories, records and documentation the keeping of which is compulsory by provision of law or regulation or which are required by the nature or size of the enterprise may be formed and kept by computer;
- Art. 2421, 2478 and 2519 cc, Corporate books, Maintenance is mandatory for corporations and cooperatives;
- Art. 2375 cc, Book of Meetings and Resolutions of Meetings, Resolutions must be recorded in the minutes signed by the chairman and the secretary or notary (in the case of an extraordinary meeting). The minutes must be prepared in accordance with the principle of "without delay," i.e., within the time required for the timely performance of filing or publication obligations, which, according to the deadline for filing with the Business Registry, corresponds to "within 30 days" of the resolution (Articles 2435 and 2436 cc) - (a deadline that is not exhaustive, as a minute could also be prepared late as long as it is before the next meeting (paragraph 25, Article 2379-bis cc);

- Law No. 120 of 11 September 2020 - Conversion into law, with amendments, of Decree-Law No. 76 of 16 July 2020, on «*Urgent measures for simplification and digital innovation*» (Simplification Decree);
- Guidelines *on the formation, management and preservation of electronic documents dated 10 September 2020.*

3.2 Reference standard

In the preparation of its preservation system, Intesi Group adapted its infrastructure, processes and procedures to the standards listed in the Guidelines on the formation, management and preservation of electronic documents, indicating the versions updated as detailed below:

- ISO 14721:2012 OAIS Open Archival Information System;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, ISMS requirements (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management. Requirements for the implementation and management of secure and reliable systems for electronic information preservation.
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Evaluation guidelines for secure and reliable electronic information preservation.
- UNI 11386:2010 SInCRO Standard - Supporting Interoperability in Preservation and Retrieval of digital Objects.
- ISO 15836-1:2022 Information and documentation - l Dublin Core metadata element set - Part 1
- ISO 15836-2:2022 Information and documentation - l Dublin Core metadata element set - Part 2.

4. Roles and Responsabilities

Below are the tasks performed and the names of the people who hold the leading roles – as specified in the Guidelines on the formation, management and preservation of electronic documents - in the

organization assigned to managing the preservation system developed by Intesi Group specifying that all profiles already present within the infrastructure are still provided for.

Role: Preservation Service Manager (RSC)	
Name	Notary Riccardo Genghini
Duty	Person who coordinates the preservation process within the registrar, possessing the professional requirements identified by AGID
Period in the role	From 2006 to date
Any proxies	None
Relationship with Intesi Group	Creator of the Preservation System
Role: Security Manager for Preservation Systems (RSSI)	
Name	Christian Gallina
Duty	Person who ensures compliance with security requirements within the registrar, possessing the professional requirements identified by AGID
Period in the role	From March 2023 to date
Any proxies	None
Relationship with Intesi Group	Permanent employee
Role: Preservation Archival Department Manager (RFA)	
Name	Notary Riccardo Genghini
Duty	Person who coordinates the preservation process from the archival point of view within the preservation system, possessing the professional requirements identified by AGID
Period in the role	From 2006 to date
Any proxies	None
Relationship with Intesi Group	Creator of the Preservation System

Role: Data Protection Officer (DPO)	
Name	Jolanda Giacomello
Duty	Person with specialized knowledge of data protection legislation and practices, capable of fulfilling the tasks set forth in Article 39 of Regulation (EU) 2016/679.
Period in the role	From March 2023 to date
Any proxies	None
Relationship with Intesi Group	External advisor
Role: Preservation Computer System Manager (RSI)	
Name	Simone Diodati
Duty	Person who coordinates the information systems within the preservation system, possessing the professional requirements identified by AGID.
Period in the role	From August 2016 to date.
Any proxies	None
Relationship with Intesi Group	Permanent employee
Role: Preservation System Development and Maintenance Manager (RSM)	
Name	Simone Fiore
Duty	Person who ensures the development and maintenance of the system within the preservation system, possessing the professional requirements identified by AGID
Period in the role	From March 2020 to date
Any proxies	None
Relationship with Intesi Group	Permanent employee

4.1 Preservation Manager

The Preservation Manager is the natural person officially appointed within the Company that owns the documents subject to preservation

As Holder of the electronic documents subject to preservation, the Customer, through its RdC, defines and implements the overall preservation system policies thus governing their management with full responsibility and autonomy in relation to the organizational model explained in the Preservation Manual.

The RdC works closely with the external Data Processor, with the Security Manager and the Computer System Manager as well as with the Preservation Archival Department Manager. The roles of Preservation Service Manager, Author and External Data Controller are filled by Intesi Group staff and/or collaborators.

4.2 Privacy Team

Following the introduction of the GDPR, the management of personal data (privacy) and in general the management of data protection now requires a multi-disciplinary approach. In this regard, a Privacy Team is established within Intesi Group, acting in cooperation with the Data Protection Officer pro tempore.

4.3 Role Log

The register of current and historical roles is maintained by the Intesi Group Registrar in separate document periodically reviewed and updated as necessary.

5. Organizational structure for the Preservation Service

5.1 Organizational chart

The Customer outsources the Preservation service to Intesi Group, which assumes the role of Registrar. The Registrar will perform all the activities necessary for the proper preservation of electronic documents entrusted to it as described by this Preservation Manual in accordance with the Guidelines on the Formation, Management and Preservation of the electronic document and the technical standards referred to therein. Within the Preservation Service, the Preservation Service Manager is currently an Official Notary Public.

Everyone involved in the Preservation service has been appointed to process data for preservation activities.

The following is the organizational chart of the roles involved in the Preservation service:

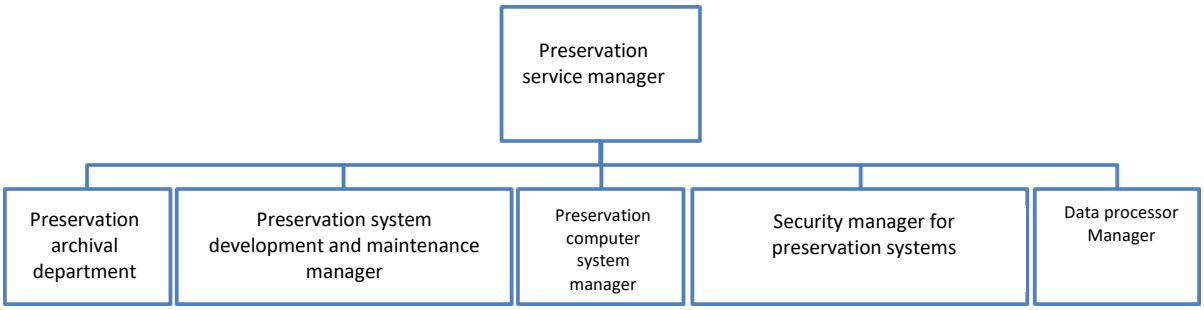


Figure 1 - Organizational chart of the roles involved in Intesi Group's Preservation service.

5.2 Organizational structures

This paragraph schematically describes the preservation process phases, computer system management activities with their relevant managers.

Activities specific to each person involved in the Preservation service			
Status	**Activities**	**Description**	**Manager**

1	Preservation service activation (following the signing of the contract).	The Customer requires the Registrar to activate the service by contracting the outsourced service.	• RSC • RTD • RFA • RSM
2	Acquisition, verification and management of Deposit Packets and generation of the Deposit Report.	Checks are made on the PdV for the certain identification of the subject, the digital signature, formats and metadata. If checks are successful, the RdV is generated.	• RFA • RSC
3	Storage Packet preparation and management.	The deposited objects are transformed into PdA, which will have to contain, in addition to the objects to be preserved, the IdPA format according to SInCRO standard rules. The IdPA is signed with a digital signature by RdC and time stamped.	• RFA • RTD • RSC
4	Distribution Packet preparation and management for the exhibition and production of digital duplicates and copies upon request.	The PdD are created according to Customer's requirements. The PdD can be exhibited via web service (non-standard case, for automated procedures and for small PdA), saved on non-rewritable optical drives or saved on rewritable mobile drives.	• RFA • RTD • RSC
5	Preservation system operation and maintenance.	Maintenance activities are carried out on both processes and hardware and software infrastructure. Activities are checked daily and any extraordinary procedures are planned in the event of faults.	• RSM • RSSI
6	Preservation system monitoring.	Log system monitoring for logging access and events. The archive integrity checks and fault management activities are also monitored.	• RdC • RFA • RSSI • RSC
7	Change management.	The policies, priorities and adjusting schedules to technological developments are defined to ensure that the preservation system guarantees the integrity, availability and security of the system over time.	• RFA 1 RSI
8	Periodic verification of compliance with reference regulations and standards.	Compliance to regulatory evolutions and standards in the field of long-term preservation is constantly monitored and updated if necessary, thanks to the supervision work by RdC.	• RdC • RSSI • RSC

5.3 Preservation service activation

The following activities were defined for Preservation service activation:

- identification of document classes to be sent to preservation;
- identification of the data or specific attributes to be correlated to each document class
- shared definition also with the client and in accordance with the law of the format of the documents and monitoring of their possible obsolescence
- identification of preservation times
- definition of the document registry i.e., the Homogeneous Organizational Area (HOA) and/or the office that owns the documents to be sent for preservation;
- definition of the time interval between packet receipt and closure of the preservation process after which documents can be exhibited;
- operational definition for document consolidation (time stamp).

6. Objects subject to preservation

The preservation system created by Intesi Group will be able to preserve both computerized documents (also files) and computerized administrative documents (also document aggregations) together with the metadata associated with them referred to in Annex 5 to the document "Guidelines on the Formation, Management and Preservation of Electronic Documents."

The preserved objects are processed by the preservation system in **electronic packets** according to the Open Archival Information System (OAIS) ISO 14721:2012 standard and interoperability is ensured according to UNI SinCRO 11386:2020.

6.1 Preserved objects

This paragraph only lists those types of electronic documents with tax relevance and subject to the Preservation service. This list, to be considered as an unbinding example, does not take into account the more specific types agreed and under contract with the Customer, including the acquisition of original analogue documents, also unique ones.

Preserved document type: Invoices issued	
Description	Sales invoices: Tax relevant documentation issued by VAT entities

Preservation delivery frequency	Documents must be sent to preservation within three months of the tax return deadline
Preservation duration	Ten years
Foreseen file formats	All foreseen formats
Preserved document type: Invoices received	
Description	Purchase invoices - Tax relevant documentation received by taxable persons
Preservation delivery frequency	Documents must be sent to preservation within three months of the tax return deadline
Preservation duration	Ten years
Foreseen file formats	All foreseen formats
Preserved document type: SdI receipts and notifications	
Description	Messages and notifications that the Interchange System (SdI), managed by the Inland Revenue Service (AE), sends to the invoice sender
Preservation delivery frequency	Documents are sent to preservation simultaneously with the preservation of the invoice to which they refer
Preservation duration	Ten years
File format	XML Format
Preserved document type: Accounting books and ledgers	

Description	• Tax relevant documentation required by the standard code and nature and size of the company for proper bookkeeping • Entry Ledger • Inventory Ledger • General Ledger • Chronology log • Asset book • Income tax book • Purchase Invoice Daybook • Travel Agents Purchase Daybook • Sales Invoice Daybook • Bills Pending Daybook • Daily takings book • Cash register • VAT Summary Ledger • Intra EU VAT Purchase Sectional Ledger • Intra EU Non Comm Purchase Ledger • Intra EU Transfers Ledger • Issued Declaration of Intents book • Received Declaration of Intents book • Donation Daybook • COD Prod Memory Book • COD Prod Processing Book • COD Prod Load Book • IT Download Book • Deposit Receipts Book • Publishers Book	• Travel Agents Daybook • VAT Emergency Ledger • DdT receipt book • Daybook • Single VAT Ledger • Other Ledgers • COD Prod Unload book • Warehouse Assets Book • Subcontracted Assets Book • Lease Assets Book • Test Assets Book • Internal VAT Sectional Ledger • Tax Printout Load Ledger • Parent Subsidiary Ledger • Analytical Method Margin Regime Load Unload Ledger • Global Method Margin Regime Purchase Ledger • Global Method Margin Regime Sales Ledger • IT Upload Book
Preservation delivery frequency	Documents must be sent to preservation within three months of the tax return deadline	
Preservation duration	Ten years	
Foreseen file formats	All foreseen formats	

Preserved document type: Statutory books	
Description	● Documentation required for standard code certifying the firm's business life ● Shareholders' ledger ● Stock Ledger ● Assembly Meeting Minutes Book ● Board of Directors Meeting Minutes Book ● Board of Auditors Meeting Minutes Book ● Executive Committee Meeting Minutes Book ● Shareholders Assembly Meeting Minutes Book ● Other statutory books
Preservation delivery frequency	At the customer's option and in any case within the terms of the law
Preservation duration	Ten years
Foreseen file formats	All foreseen formats

Preserved document type: Tax returns	
Description	● Relations Registry ● Tax relations registry ● Shareholder's Assets ● Lease contracts ● Single Certification ● Tax code and health card (Form AA4/8, form AA5/6) ● Share sales ● Application for registration in the single non-profit registry ● Annual VAT data communications ● Tax registry communications ● IRAP option communication ● Health facilities communications ● Communication by associations (EAS form) ● Communication for 730-4 form receipt ● Communication - Transactions with blacklisted countries ● Multi-purpose communications (income and expenses) ● VAT Declarations ● Virtually paid stamp duty declaration ● INPS proxies, FORM 730, other proxies for tax purposes ● INTRASTAT ● Five per thousand list registration (Application for the benefit) ● IPEC application ● Personal - corporate tax refund application ● Carry over tax refund application ● DSU-ISEE form ● 730 form ● 770 form ● Single form PF ● Single form SP ● Single form SC ● Single form non-commercial organizations ● IRAP form (PF, SP and SC) ● Intrastat form ● National and World Consolidated Form ● F24 Form ● RED Form ● Legally disabled forms (ICRIC, ICLAV or ACCAS/PS) ● VAT number (AA9/11 form, AA7/10 form, ANR/3 form) ● Industry studies questionnaires ● Application for the voluntary collaboration procedure ● Refunds (Credit, quarterly VAT reimbursement, EU ● Refunds, residents and non-resident objects, Irap refund, etc.)
Preservation delivery frequency	At the customer's option and in any case within the terms of the law

Preservation duration	Ten years
Permitted file formats	All foreseen formats

Preserved document type: Certified Electronic Mail Messages and receipts (PEC)	
Description	Documentation certifying the correct delivery and receipt of certified email messages
Preservation delivery frequency	At the customer's option and in any case within the terms of the law
Preservation duration	Ten
Permitted file formats	EML Format

The indicated preservation periods may, upon the request of the Client's Preservation Manager, be extended.

The preservation system accepts all types of formats and guarantees readability in accordance with Annex 2 of the "Guidelines on the formation, management and preservation of electronic documents" also in accordance with the guidance document prepared by the International Comparison of Recommended File Formats group (ICRF) for the comparison of internationally recommended file formats, as well as accepting and guaranteeing the following best-known standard formats:

- PDF and PDF/A (.pdf) MIME type: application/pdf Viewer: Adobe Reader
- Holder/Manufacturer Adobe Systems Standard: ISO32000-1, ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
- TIFF (.tif or .tiff) MIME type: image/tiff
- Viewer: Imagemagick or other image viewers
- XML (.xml) MIME type: application/xml or text/xml Holder/Manufacturer: W3C
- Viewer: Text editor
- TXT format (various extensions) MIME type: application/text Viewer: Text editor
- CAdES digital signature format (p7m) MIME type: application/pkcs7-mime Viewer: Digital Signature Software
- Standard: ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES)
- EML format (.eml) MIME type: message/rfc822 Standard: RFC2822

- Viewer: E-mail management software (i.e. Mozilla Thunderbird).

6.2 Deposit packet (PdV)

Documents massively acquired from the preservation system, regardless of their type, make up a daily deposit packet divided by Author. The acquisition takes place via web service on secure channel with authentication using Client certificates.

During the data acquisition phase, computer information is recognized and/or calculated, including the document hash, the acquisition time reference, the name and size of the file received. This computer information will form the Index of Spill Packages (IPdV) related to an individual Author and the previous business day. The IPdV is an XML file.

The deposit packet index (IPdV) is uniquely identified according to the following default naming convention yyyy-MM-dd#DAILY-LOG-WS-NOTARY-CUSTOMER.xml

Please note that: conventionally, NOTARY is the name of the notary to whom the Daily Log refers, while CUSTOMER is the customer code -Author of the Deposit Packet.

Below are the structure and the definition of the IPdV:

- a heading is present, stating the IPdV version, the access channel to which the IPdV refers and the name of the notary public in charge of the preservation service;

this is followed by the actual deposit packet information:

- Daily transaction count: unique ID of the transition (absolute progressive unique) – Long int type
- Timestamp: time reference corresponding to the time when the file was stored (in the format yyyy-MM-dd HH:mm:ss.fff)
- Label that identifies the relevant action (Start Upload, ... up to Preserved – relevant action for preservation purposes)
- Customer ID: unique key identifying the customer in the corresponding table – INT type
- Customer name: Descriptive customer string

- Username auth: Account/Username used for FTP or web service transfer
- Customer IP: unique IP address and customer identification from which the FTP or web service transfer originates
- File name: filename (with extension)
- File size: size in bytes
- File hash (SHA-256): Footprint calculated with SHA-256 algorithm of the archived file

6.3 Storage packet (PdA)

For the purposes of this Manual, the storage packet (PdA) is made up of the document (or document file) subject to the preservation process, and of an XML file structured according to the SinCRO UNI 11386 standard updated at the time of the creation date of the packet (as of the date of this UNI SinCRO 11386:2020 version) (IdPA) digitally signed and stamped (XADES-T) by the Preservation Service Manager. The PdA may be the result of a combination of multiple deposit packets, possibly transformed in line with the contract terms, according to the document type contained.

The storage packet index (IPdA) contains computer footprints of electronic documents divided by homogeneous type, enriched by the metadata of the type represented and required by the relevant regulations in force.

The IPdA may contain additional metadata according to Contract specifications.

Below is a description of the structure of the PdA index complete with the elements contained in "MoreInfo" provided by the SinCRO standard (PIndex).

SelfDescription: General description of the packet.

- ID: Unique Id of the PdA generated by the Preservation System (PdA Id generated by the database).
- CreatingApplication:
    - Name: PDA Service
    - Version: 1.0
    - Producer: INTESI GROUP S.p.A.
- PVolume :
    - ID: Unique Id of the PdA generated by the Preservation System

    - Label: Label of the document type.
    - Description: Description of document type
    - MoreInfo:
        - ExternalMetadata:
            - ID: Unique id of the metadata file generated by the Preservation System
            - Path: Path relative to metadata file
            - Hash: Hash SHA-256 relative to metadata file
- FileGroup*:
    - ID: Unique id corresponding to the Volume ID.
    - Label: (MASTER_FILE | METADATA_FILE | ATTACHED_FILE | EVIDENZE_DI_VERSAMENTO)
    - Description: Description of the file group in relation to the Label
    - File:
        - ID: Unique Id of the file generated by the Preservation System
        - Path: Relative path to file
        - Hash: Hash SHA-256 relative to file
- Process:
    - Submitter:
        - AgentName:
            - FormalName: Business name of the PDV payer
        - RelevantDocument: Intesi Group Preservation Service Manual
    - Holder:
        - AgentName:
            - FormalName: Business name of the document holder
        - RelevantDocument: Intesi Group Preservation Service Manual
    - AuthorizedSigner:
        - AgentID: Subject identifier based on one of the identification types predefined by the ETSI standard
        - AgentName:
            - NameAndSurname:
                - FirstName: Subject name
                - LastName: Subject's last name
        - RelevantDocument: Intesi Group Preservation Service Manual
    - TimeReference:
        - TimeInfo: Date of production of the index file.

*The File Group tag has multiple occurrences, one for each type described in Label:

- MASTER_FILE: Group of files main object of preservation of the documentary unit

- METADATA_FILE: Group of metadata files associated with the documentary unit.
- ATTACHED_FILE: If provided, group of files attached to the documentary unit
- EVIDENZE_DI_VERSAMENTO: Group of files generated by the preservation system

6.4 Distribution packet (PdD)

The distribution packet (PdD) may coincide with a PdA, be an extract thereof. As for the technical specifications of the PdD, they are the same as those described in Section 6.3 above, in accordance with what is described in the "Guidelines on the Formation, Management and Preservation of Electronic Documents."

PdDs for the purpose of the performance requested by the Client are digitally signed, with a digital signature or qualified or advanced electronic signature of the Preservation Service Manager.

7. The preservation process

e Intesi Group preservation process, in accordance with Article 44, paragraph 1 of the CAD, ensures long-term electronic preservation according to the law, by adopting rules, procedures and technologies capable of ensuring – with regard to the preserved documents – the characteristics of authenticity, integrity, reliability, legibility and availability.

The system is able to ensure the processing of the entire cycle of the object stored in the Preservation service, guaranteeing access – for the period provided by the standards according to the different document types – to the same object up to its elimination.

As established in par. 4.2 of the Guidelines on the Formation, Management and Preservation of Electronic Documents, preservation objects are processed within the Preservation Service in electronic packets.

Electronic packets are distinguished as follows:

- deposit packets (PdV): relate to data and documents subject to preservation and owned by the Customer, sent to the Intesi Group preservation system;
- storage packets (PdA): consist of the IPdA and the set of documents subject to preservation relating to the same IPdA;
- distribution packets (PdD): may consist of documents preserved according to the law,

available for research, consultation and exhibition, via web portal or stand-alone support or other media agreed with the Customer and described in this document.

In accordance with the provisions of par. 4.7 of the Guidelines on the Formation, Management and Preservation of Electronic Documents, Intesi Group's regulation-compliant reservation process includes:

- acquisition by the preservation system of the deposit packet;
- verification of the deposit packet and its objects. In particular, compliance with the provisions of this Manual, any specifications agreed with the Client, and the provisions of the Guidelines on the Formation, Management and Preservation of Electronic Documents;
- automatic generation of the deposit report relative to one or more of deposit packets, uniquely identified by the preservation system and containing a time reference, specified with reference to the coordinated universal time (UTC), and all the footprints calculated on the PdV content, as described in this Manual;
- preparation, Preservation Service Manager's digital signature and management of the storage packet on the basis of the data structure specifications contained in standard UNI 11386 and in the manners specified in this Manual;
- preparation of the distribution packet for the exhibition purposes required by the Customer;

the production of distribution packets coinciding with storage packets for the purposes of interoperability between storage systems.

Below is the diagram of the preservation process:

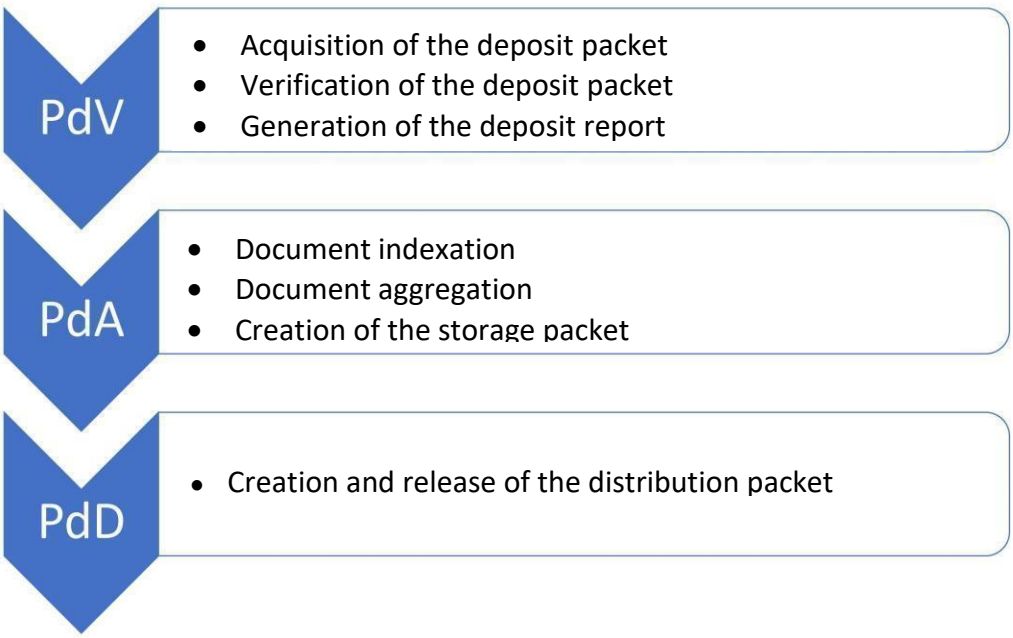
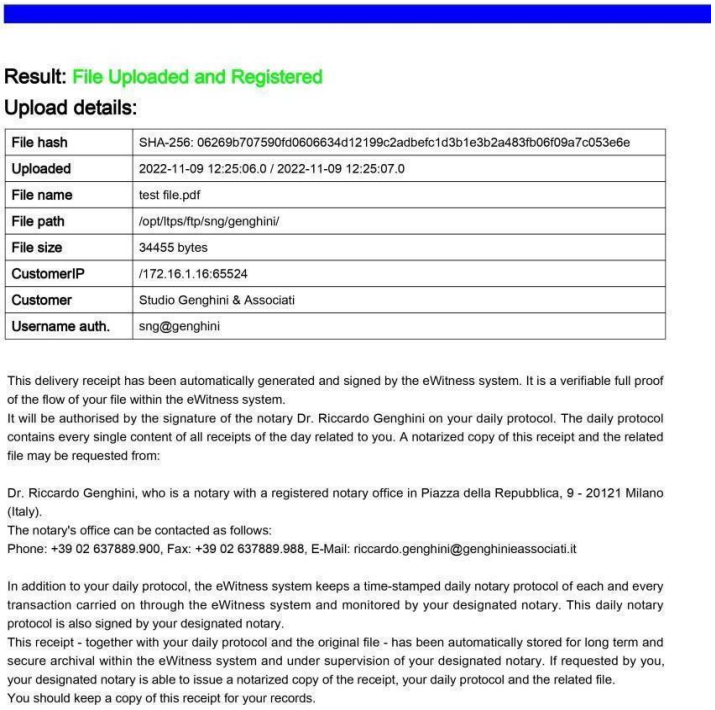


Figure 2 - Intesi Group S.p.A. preservation process diagram

7.1 Deposit packet acquisition mode

8. The PdV are sent to the preservation system via Web API, through the certified channel described under § 7.2.
9. Relative to the Web API transfer channel, the Client uses the HTTPS protocol. This communication channel allows a secure connection to be established within an encrypted connection using asymmetric encryption (SSL/TLS).
10. Authentication over the HTTPS communication channel is handled through a certificate provided by Intesi Group.
11. In the case of native computer-generated documents on Intesi Group management systems, the latter will send the documents to the preservation system through the above channels.
12. For each file transferred to the Intesi Group preservation system, a file acquisition receipt bearing electronic signature is generated and transferred to the Customer, certifying the results of the transmission and bearing the hash of the file transmitted.
13. The Customer has the ultimate responsibility for making sure that the transmission is successful, even by checking the hash of the file contained in the Intesi Group acquisition receipt, in order to inform Intesi Group without undue delay if any anomalies are found.



Result: File Uploaded and Registered

Upload details:

File hash	SHA-256: 06269b707590fd0606634d12199c2adbefc1d3b1e3b2a483fb06f09a7c053e6e
Uploaded	2022-11-09 12:25:06.0 / 2022-11-09 12:25:07.0
File name	test file.pdf
File path	/opt/ltps/ftp/sng/genghini/
File size	34455 bytes
CustomerIP	/172.16.1.16:65524
Customer	Studio Genghini & Associati
Username auth.	sng@genghini

This delivery receipt has been automatically generated and signed by the eWitness system. It is a verifiable full proof of the flow of your file within the eWitness system.
It will be authorised by the signature of the notary Dr. Riccardo Genghini on your daily protocol. The daily protocol contains every single content of all receipts of the day related to you. A notarized copy of this receipt and the related file may be requested from:

Dr. Riccardo Genghini, who is a notary with a registered notary office in Piazza della Repubblica, 9 - 20121 Milano (Italy).
The notary's office can be contacted as follows:
Phone: +39 02 637889.900, Fax: +39 02 637889.988, E-Mail: riccardo.genghini@genghinieassociati.it

In addition to your daily protocol, the eWitness system keeps a time-stamped daily notary protocol of each and every transaction carried on through the eWitness system and monitored by your designated notary. This daily notary protocol is also signed by your designated notary.
This receipt - together with your daily protocol and the original file - has been automatically stored for long term and secure archival within the eWitness system and under supervision of your designated notary. If requested by you, your designated notary is able to issue a notarized copy of the receipt, your daily protocol and the related file.
You should keep a copy of this receipt for your records.

Figure 3 - Intesi Group system receipt

The receipt (shown in Figure 3) issued by Intesi Group system reports, for each document received, the following information:

- Timestamp: time reference corresponding to the time when the file was stored (in the format yyyy-MM-dd HH:mm:ss.fff)
- Object ID
- Object name: String uniquely identifying the document (format yyyy-MM-dd#12345)
- Customer ID: unique customer identification key
- Customer name: Descriptive customer string
- Username auth.: Account/Username used for transfer ( )
- File name
- File full path: complete path of the folder where the file is uploaded
- File size: size in bytes
- File hash (SHA-256): Footprint calculated with SHA-256 algorithm of the archived file

7.1.1 Optional addition of a time stamp to the receipt

If contractually provided for, it is possible to produce for each receipt from the Intesi Group system an additional digital evidence of successful preservation consisting of a qualified time stamp, thus enabling an electronic time validation enforceable against third parties (see Art. 20, paragraph 3 Digital Administration Code Legislative Decree 82/2005).

7.2 Verifications performed on the deposit packets and the objects contained therein

Below is a description of the controls carried out by the preservation system on PdV

- **Check on the person who created the document:** the authorship of the individual who sends the document to the preservation system is inherently guaranteed by the fact that there is authentication by the payer over secure transmission channel.

The following checks are also run during the PdV generation process.

Document type check: The preservation system checks the received document types. On the basis of contract specifications set with the Customer, adequate check procedures are implemented to ensure that the documents received are in fact consistent with the types expected.

These checks may be different in nature and based on:

- check of the naming convention of the files received;
- extraction and comparison of text from the electronic document, also in order to provide the metadata required for storage;
- verification of the completeness of the metadata expected by document type
- Integrity check of received files

7.2.1 Virus management

A monthly storage file scan is defined in the Intesi Group System. The tool is activated by initiating a full scan of the month prior to file storage, generating a report highlighting the resulting outcomes results

7.3 Discarding of deposit packets and how to report anomalies

The following is a list of anomalies that may lead to the discarding of some documents deposited into the preservation system:

- technical problems with saving the file being taken over;
- problems concerning compliance with contract provisions or the commercial validity of the contract itself.

The discarding of documents deposited in the preservation system is agreed with the Customer in accordance with the procedures provided by Intesi Group.

7.4 Storage packet preparation and management

The process steps leading to the creation of the storage packet (PdA) are described below:

- processing of the documents contained in the PdV in order to obtain the identification of the document type and the retrieval of the mandatory metadata identifying each type;
- possible elaboration of the documents contained in the PdV to comply with any contractual specifics;
- aggregation of documents for the creation of the PdA with specific rules and logic. A PdA consists of documents from one or more PdVs. Documents related to a PdV will not necessarily all be contained in the same PdA;
- IPdA creation as per SInCRO standard – Supporting Interoperability in Preservation and Retrieval of digital Objects (UNI 11386:2010) – concerning the data set structure supporting the preservation process.

The IPdA contains the following data:

- unique internal identifier;
- evidences (hash, file name, etc.) already contained within the PdV;
- the hash and unique index of the PdV to which they refer;
- the required metadata linked to related document type;

digital signature and time stamp affixed on the IPdA by the RSC;

7.5 Distribution packet preparation and management for exhibition purposes

The management of PdDs is the responsibility of the Preservation Service Manager, the Archival Function Manager and the External Data Processing Manager.

The production of Distribution Packets takes place following a request from the Customer, as indicated in par. 4.7(h) of the Guidelines on the Formation, Management and Preservation of Electronic Documents.

The generation request of one or more distribution packets from the preservation system is only permitted by authorized individuals. The Customer, represented by the legal representative or the Preservation Manager, or another person delegated by him in writing is considered authorized.

Following a PdD generation request, the preservation system carries out consistency and correctness checks on the generated PdD in addition to the documents contained.

In this regard, the preservation system checks that the footprints of the documents returned in the PdD match those found in its IPdA to ensure that these documents have not been altered or modified in content.

When PdD need to be distributed on removable physical media, they will not bear any immediately recognizable reference to the author or their content on the exterior; the content will be protected with suitable encryption systems and the corresponding decryption key will be delivered to the recipient through different channels than those used to deliver the physical media.

These supports will be exclusively delivered by selected staff, specifically in charge of their transportation, in accordance with the contractual agreements between the parties. The size of the PdD could influence the level of service in preparing it. Based on the current infrastructure, we have the following directions for the client:

- PdD up to 20 GB: online datacenter-to-site transfer;
- PdD between 20 and 40 GB: if there is no critical service level, you may decide to do everything online, possibly with overnight transfer;
- PdD over 40 GB: necessary transfer to mobile media at the data center, with inevitable increase in time.

PdDs for the purpose of the performance requested by the Client are digitally signed, with a digital signature or qualified or advanced electronic signature of the Preservation Service Manager.

7.6 Production of digital duplicates and copies

The support of the possible intervention of the public official in the stipulated cases can also be provided upon specific agreement.

7.6.1 Digital duplicates

In addition to the standard preservation modes described in this manual, duplicates or copies can be generated on optical media upon the Customer's request. These copies are sent by the Preservation Service Manager to the Customer. Since the copies and/or duplicates are only generated upon the Customer's request, the latter must submit a request to the contact persons agreed in the terms of the Contract.

7.6.2 Digital copies

The creation of digital copies of the preserved document is carried out in accordance with the provisions of Article 23-bis of the Digital Administration Code and in accordance with the manner of requests agreed with the Customer. For the case of requesting digital copies or analog copies of the original electronic document (also certified by the Preservation Service Manager, Delegate of the Preservation Manager), a specific agreement must be signed in which roles, methods, timing and fees must be agreed upon.

7.7 Storage packet elimination

The preservation system allows for the elimination of electronic documents preserved according to the law and contained in one or more PdA

The possibility of executing elimination from the preservation system cannot disregard the assessment regarding the legal nature of the holder of the documents subject to preservation, or his delegate.

The following are distinguished to this end:

- private entities: with the exception of archives "declared to be of great historical interest", whose preservation scope is subject to special laws, for routine documentation and, particularly, for tax relevant documentation, the regulatory deadlines are provided by the code standard (see Article 2220 Civil Code) as well as the primary tax law;
- public entities: with regard to documents of public nature or value, without prejudice to the binding principles of code standards, some provisions of special character become applicable, including those concerning cultural and environmental heritage pursuant to Legislative Decree no. 42 of 10 January 2004 (Code of Cultural and Environmental Heritage).

Regarding documents of historical and artistic interest, the PdA can only be eliminated upon authorization by the Ministry of Cultural Heritage and Activities, upon the Customer's request, as per the current legislation.

Normally, the elimination of documents is related to three instances that can occur:

- commencement of terms for the preservation period
- termination or cancellation of the contract
- express request by the Holder

In the event of **expiration of the preservation period**, unless the Holder requests to extend the preservation period for a further and subsequent period, the elimination and deletion of the documents and related storage packets from the preservation system is perfected, giving notice to the "Holder".

In event of **termination of the contract that provides for the delivery to the "Customer" of the PDDs** a physical support or transfer is prepared in the agreed manner of the entire documental heritage previously preserved, the elimination and deletion of the documents and related storage packets of the preservation system is perfected, after the period necessary for all the necessary checks and verifications to be carried out by the "Customer" itself as provided for in the current general conditions of service, in order to define the congruity of what has been prepared in the PDDs and according to the operation always provided for below.

In the event of **an express request by the "Holder" to proceed to the elimination and** deletion of the documents and related storage packets, the elimination and deletion of the documents and related storage packets from the preservation system is perfected. The purpose of elimination is, on the one hand, the selection and preservation of documentation with legally and historically relevant value and, on the other hand, the destruction of part of the documentation that has exhausted its legal and/or administrative validity and can be eliminated.

The entire process inherent to the management of elimination shall be carried out as described in the appropriate procedure "Elimination and discard data and storage packets from the Intesi Group System provided according to ISO 27001:2017 standard.

Any assistance activities to be provided by the Registrar toward the "customer" to perfect the list of documents subject to elimination and deletion will be the subject of appropriate and possible economic quotation.

The purpose of elimination is, on the one hand, the selection and preservation of documentation with legally and historically relevant value and, on the other hand, the destruction of part of the documentation that has exhausted its legal and/or administrative validity and can be eliminated.

In the case of public or private archives, which are of historical interest, the elimination of the archival packet is done with the prior authorization of the Archival Superintendence and in accordance with the provisions of the relevant legislation in force (Legislative Decree No. 42 of January 22, 2004, *Code of Cultural Heritage and Landscape pursuant to Article 10 of Law No. 137 of July 6, 2002.*

7.8 Measures guaranteeing interoperability and portability to other registrars

The Intesi Group preservation system is designed to handle the most appropriate formats to ensure the principles of interoperability between preservation systems, according to current regulations concerning the specific document types.

To this end, Intesi Group preservation system, in accordance with the provisions of Annex 2 to the document Guidelines on the formation, management and preservation of electronic documents, adopts the main standards of formats and data path management as follows:

- for preserved object acceptance purposes, adherence to the formats provided by this Manual and Annex 2 of the Guidelines on the formation, management and preservation of electronic documents;
- for IPdA generation purposes, adherence to SInCRO standard UNI 11386:2020;
- for PdD generation purposes, as specified in paragraph lett. h) of the Guidelines on the formation, management and preservation of electronic documents, the unique match between acquired PdV, generated PdA and PdD, as specified in the document Interoperability Models between preservation systems, issued by AgID.

The information, in any case, will be provided in a standard format compatible with other preservation systems, as required by the current regulations according to the above-mentioned Guidelines on the formation, management and preservation of electronic documents, among others ISO 14721:2012 OAIS, ISO/IEC 27001:2013, ETSI TS 101 533-1 V1.3.1 (2012-04), ETSI TR 101 533-2 V1.3.1 (2012-04), UNI 11386:2020 Standard SInCRO, ISO 15836:2009. This list is intended to be non-exhaustive and not compulsory.

The Registrar will deliver to the "customer" and for it to the person who represents the client (legal representative, preservation manager or person expressly delegated by them) the documents and digital copies with enclosed list of the documents contained in the digital media sorted by type and reference period.

Upon delivery, the "customer" will issue specific attestation confirming receipt of the documents in accordance with the agreed transfer arrangements. Within 60 (sixty) working days after the delivery of the material, the "customer" shall proceed to verify the readability of the transferred files. This procedure will end with the "customer" signing the "Final Verification Minutes," which must be delivered to the Registrar. If such verification report is not delivered within the above deadline, the transfer shall be deemed to be completed by silent consent.

All disputes directly related to the integrity of the contents in the optical media that the "customer" optionally requests, which have not been formally made within 60 (sixty) days from the delivery, may no longer be made by the "customer" itself. In any case, after the above time limit has elapsed without the "customer" having carried out any activity, all material delivered and referred to in the transmitted list shall be deemed to have been accepted by him without reservation. The "customer" hereby waives - and the "Provider - Preservation Service Manager" agrees - to exercise such claims.

It is understood that the Registrar for the entire period up to the expiration of the deadline for the verifications and the signing of the "final verification report", will keep at its premises a copy of everything delivered/ made available by the "customer". Only after the "final verification report" has been signed and delivered can the elimination procedure as provided above begin.

The Registrar guarantees that it will implement the databases by adopting formats, standards, and technical and operational solutions suitable for interoperability so as to enable the "customer," in the event of termination of the Contract, to migrate the data to databases managed by other parties. Should additional operations and/or activities be necessary or be requested by the "customer," these will be subject to economic evaluation by the Registrar according to the rates in force.

7.9 PdV elimination procedure

The procedure for the removal of documents from the preservation system follows the steps below:

- The Customer provides a list of hashes to be deleted. The list must be sent in a secure manner, i.e. it must bear a digital signature (the standard mode is to receive a text file with a list of hashes, one for each row).
- Different format conventions may be agreed upon with the customer.
- Both the sender and the digital signature holder must be vested with suitable powers or have been appointed by the Preservation Manager or by the legal representative of the customer. This request will be digitally preserved by the Preservation Service Manager.
- The list of hashes will be acquired by the Intesi Group system which prepares the system to delete certain file lots.
- The summary of the preparation activity is submitted by e-mail to the Preservation Service Manager for approval (depending on the document type, the Preservation Service Manager may ask a customer's representative to attend in person or by videoconference);
- After receiving the authorization, the Intesi Group system launches the deletion procedure in accordance with the provisions of the procedure "Deletion of data from the Intesi Group system" included among the management and operational procedure set forth in ISO Certification 27001/2017.
- For large amounts of data, the processing may be divided into lots, although seamlessly. Every single deletion operation is traced, including deletion date and time;
- At the end of the deletion activity, a summary report containing the list of deleted hashes is generated. The report is signed by the Preservation Manager and stored by the Preservation Service Manager.
- A copy of the report is delivered to the customer.

Deletion implies the removal of a timely identified digital object from the list described in the previous point from all Intesi Group primary, secondary, backup copies, other copies under Intesi Group control.

Intesi Group may support the customer in defining the list of hashes to be deleted; however, the Customer is the only one responsible for approving the list of objects to be deleted. Full deletion may require a few days.

8. The preservation system

This paragraph describes the preservation system, by analyzing its logical, technological and physical components.

8.1 Logic components

The layout and description of the functional components relating to the preservation system and its operation are provided below.

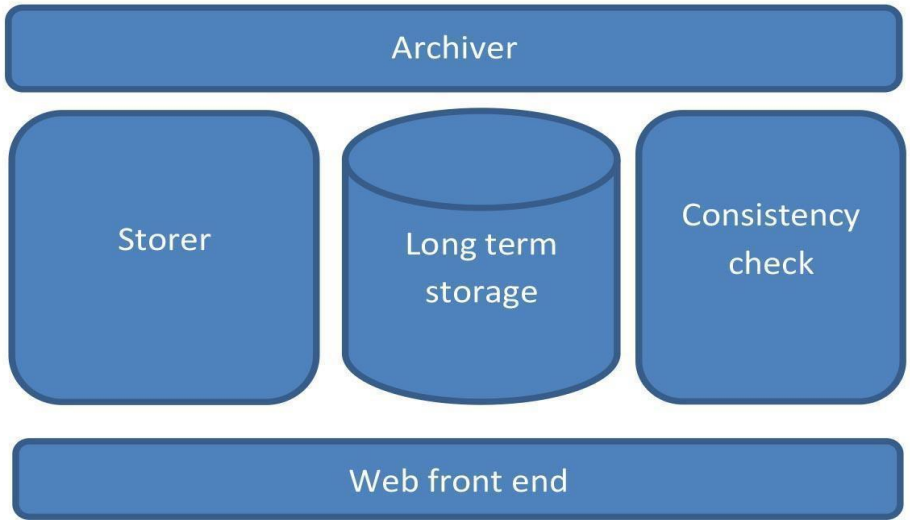


Figure 4 - Functional components of the eWitness preservation system®

Archiver: receives documents from the Customer. Documents are received according to the protocols described in Section 7.1 - Deposit packet acquisition mode. It also creates the PdV by acquiring basic additional information of each document subject to preservation.

Storer: generates the PdA, affixes the RSC's digital signature and correctly stores supports and documents in the *Long term storage*.

Web front end: represents the set of application procedures intended for interaction with the various stakeholders Holder, Author of the Deposit Packet, Enabled User, Preservation Service Manager).

Consistency check: agent that checks the consistency and coherence of the three copies of the PdA residing in the main and backup data centers.

8.2 Technological components

The following are the technological components that implement the preservation system as outlined in paragraph 8.1 above:

- Archiver: implemented by an API web service with components created with Java technology on MySQL database;
- Storer: created with Java technology on MySQL database
- Web Front-end: front-end application developed with Angular and Java
- WebServices on MySQL database and Microsoft SQL Server;
- Consistency check: subsystem in charge of verifying the consistency of the documents in storage, achieved using the following technologies: Python for massive hash calculation; MySQL as a database for comparison with the preservation database; Java for the implementation of effective control and delivery of reports; finally, bash as a wrapper to simplify the implementation and integration of all control and data extraction functions.

8.3 Physical components

The diagram and description of preservation sites and connections between different sites and between different preservation system components are provided below:

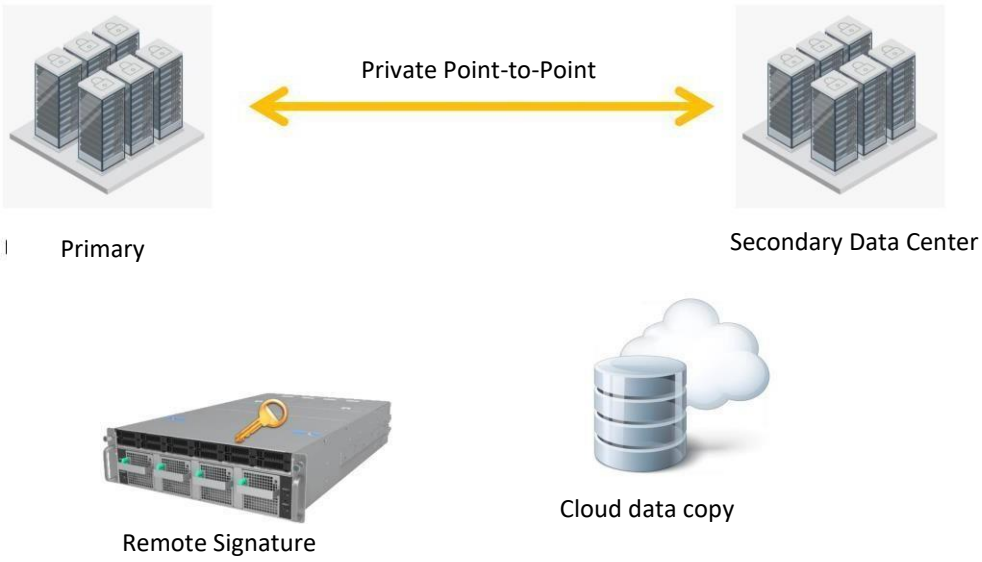


Figure 5 – Preservation sites and connections between various components of the preservation system

The storage system is located in -Rack dedicated at British Telecom's datacenter.

Application components run on virtual servers hosted on VMWare clusters in active-passive configuration

Persistence of stored documents is realized speculatively on two dedicated and physically separate storage devices.

The affixing of qualified signatures of the Rd, on the PdAs is done through the use of appropriate qualified remote signature service.

Applications and data (PdA) are replicated on dedicated infrastructure at backup datacenters. Replication procedures, based on rsync technology, are performed through point-to-point tunnels between the two DCs (primary site and backup) both British Telecom.

An additional backup copy of files in preservation was made on AWS Cloud infrastructure located in one of the EU Regions, for all files in preservation prior to the end of the year 2022.

8.4 Management procedures

The preservation system respects and reflects the management and evolution procedures foreseen in the awarded ISO/IEC 27001:2017 and ISO 9001:2015 certifications with respect to:

- operation and maintenance of the preservation system: maintenance activities are on processes, hardware and software facilities, through daily audits on infrastructures. Extraordinary procedures are planned in parallel with these activities in the event of faults;
- log management and storage: all security-related events on critical or sensitive systems are logged; audit logs are protected and stored; The administrator and operator login logs are also part of the security-related event logs that are stored for all machines. All system logs are stored and kept for a minimum period consistent with Regulation (EU) 679/2016 (GDPR);
- preservation system monitoring: adequate and effective preservation system monitoring procedures are designed and detailed in § 9 below;
- periodic verification of compliance with reference regulations and standards: the periodic verification of compliance with reference regulations and standards is implemented by the management also by involving qualified outsourced personnel.

The management of all these processes is carried out by the department managers that hold the role from time to time, as stated in the Role Log.

8.5 Evolution and change management procedures

The acceptance criteria for new systems, upgrades and new versions are previously established and appropriately tested during development and prior to approval.

The operating process is certified by ISO 27001 operating procedure and outlined in a flow chart for the "Design and development of solutions and services for electronic management of documents and System Integration". This procedure details the operating modes and responsibilities applicable to services as possibly requested by the Customer, including Intesi Group itself, i.e. the so-called internal Customer.

The services to be rendered according to the Customer's requests will be performed with different methods and levels of detail depending on the type of request received.

As far as the tracing of information, steps, logs, significant notices, test evidences, etc. is concerned, everything has been consolidated into the Agile Board-type collaborative operating tool.

As far as process automation is concerned, the following tools are in use:

- a version management system;
- a continuous integration automated management system;
- a deployment automation system between the various environments.

All internal developments are also tested on test systems. The acceptance of the new software is considered after making sure that such software meets acceptance criteria.

The Preservation System Development and Maintenance Manager and his staff are in charge of these checks.

9. Monitoring and controls

Given the complicated nature of the preservation system and process adopted and described in this Manual, Intesi Group has defined a set of system functional analyses and verifications designed to measure the overall performance of the preservation system, monitor the security levels to be maintained and proactively manage any detected system faults.

The functional monitoring and control system of the preservation system is organized on three levels:

- control and monitoring activities relating to virtual hosts;
- control and monitoring on services;

To ensure a high level of operational, technological and infrastructure efficiency of the preservation system, the monitoring system implemented by Intesi Group also provides for the regular execution of controls on physical hosts, regardless of the storage system.

9.1 Monitoring procedures

The entire preservation system structure is constantly monitored in its main logical and physical components. Monitoring is conducted by Intesi Group every ten minutes.

The adopted control systems are organized on two different levels of detail:

- First-level checks: basic checks carried out on virtual servers. They include checks on the server accessibility and, secondly, checks on the use of all resources in use: CPU, Memory, Swap, Disk And Network;
- Second-level checks: as a second level of control, the accessibility to all the services necessary to the preservation system infrastructure is constantly monitored through specific queries on each of them. By way of example, web service, SQL and HTTP queries are run to check main systems.

In case of excessive resource consumption or unavailable services, the monitoring system will immediately launch an exception, which is notified to all Preservation System Maintenance Managers by sending an e-mail.

The log of all control and query results is saved to a specific database, from which data is periodically extracted in order to determine trends and improve sizing, via space occupancy reports.

A further level of monitoring is included in the modular preservation system itself, in which an internal process checks the logs written by the various modules. Where the system detects errors or even simple warnings, those responsible for the system maintenance are automatically notified by e-mail.

9.2 Verifying archive integrity

The archive integrity verification allows the preservation system to check preserved document compliance compared to their delivery to preservation. In order to ensure the continued integrity and legibility of data stored, the monitoring system applied to the preservation system periodically and automatically runs a structured procedure to check integrity, described below.

This procedure is performed directly at the file level. The preservation system is set to automatically inhibit any data overwrite or deletion operations, thus limiting the number of actions that can be performed that jeopardize the integrity of the data stored. However, to further increase the level of certainty of the actual integrity of all data stored, the system continuously runs a *Consistency Check*, a custom check that calculates the hash SHA256 of each file in all preservation archives on the physical level (thus the two main hosts and backup host) and compares it with the logical level of data in the preservation database.

9.3 Solutions adopted in the event of faults

If the preservation system checks described above find faults, the system automatically notifies the previously designated system managers via e-mail. Whenever a problem is reported, the system managers analyze it and assess its cause to identify the most efficient normalization strategy. Managers thus apply the corrections deemed necessary to resolve the discrepancy. After repairing any fault, maintenance operators assess and implement, if necessary, the corrections on the system to prevent the emergence of additional errors of the same type or, at least, to a low faster detection.

9.4 Termination Procedure

The Preservation Service Manager guarantees that he/she will implement all necessary actions in the event that he/she ceases to provide preservation service.

These activities are described in the Termination Plan that the Preservation Service Manager has duly prepared in accordance with the law and which may be shared with the Holder or Author where necessary.

These actions will ensure that the various stakeholders monitor the migration of the preservation service in accordance with the stipulated provisions and the specially prepared termination plan. This

means guaranteeing, through a transitional phase of interoperability, the availability and complete integrity of the preserved information assets, until the moment of termination, making them available to any new Registrars that may take over the service.

The termination procedure will take place according to the timetable agreed with the successor Registrar, in compliance with the procedures foreseen by the different types of migration that can be implemented in accordance with the OAIS standard (ISO 14721:2012), providing for the generation of Distribution Packets, derived from the preservation packets stored in the system, to be delivered by means of the agreed methods and in accordance with the procedures described in the Intesi Group Preservation Manual.

Termination of the preservation service delivery activity could occur due to any of the following circumstances:

- Bankruptcy and Other Insolvency Proceedings
  Estimated time for the migration procedure: 4 months
- Business Branch Sale/Disposal
  Estimated time for the migration procedure: 4 months
- Failure of the Customer to comply with contractual obligations
  Estimated time for the migration procedure: 90 days

The indication of times for each event is to be considered as a guideline, to be adjusted in addition to the estimates of each service provided, for each Customer.
This regulation guarantees the customer the possibility of having a new Registrar take over, who can then ensure continuity in the delivery of the preservation service.

The Preservation Service Manager undertakes where necessary to inform, by PEC, the Digital Italy Agency (AgID), as the supervisory entity, about the implementation of the termination procedure.