# In.Te.S.A. S.p.A.

## Qualified E-Archiving Service

**pursuant to the Regulation on the criteria for the provision of digital document storage services, issued by AgID with Decision no. 455/2021**

# E-Archiving Manual

*Document code: MdC_V28042025*

*OID: 1.3.76.21.20.1*

*Drafting: Francesco De Cesare*

*Verification: Maria Marchese*

*Approval: Luigi Traverso*
*(Head of Preservation Service)*

*Issue date: 28/04/2025*

*Version: 08*

## Issuance

| **Action:** | **Name** | **Revision date: 28/04/2025** |
|---|---|---|
| *Drafting* | Francesco De Cesare – Head of Preservation Archival Function | |
| *Verification* | Maria Marchese – Team Leader B2B Solutions | |
| *Approval* | Luigi Traverso – Head of Preservation Service | |

## Revision log

| **Version n°: 08** | | **Revision date: 28/04/2025** |
|---|---|---|
| *Change description:* | Update of professional roles, certifications, and reference regulations | |
| *Reasons:* | Update of regulations, inclusion of ISO certification, and change of IT systems manager | |
| **Version n°: 07** | | **Revision date: 31/01/2024** |
| *Change description:* | Review of the service structure | |
| *Reasons:* | Update on Company organization | |
| **Version n°: 06** | | **Revision date: 15/11/2021** |
| *Change description:* | Update Company logo | |
| *Reasons:* | Change of Company organization | |
| **Version n°: 05** | | **Revision date: 24/09/2021** |
| *Change description:* | Update of Professional Roles | |
| *Reasons::* | Change of Head of Personal Data Processing | |
| **Version n°: 04** | | **Revision date: 14/06/2021** |
| *Change description:* | Normative adjustments | |
| *Reasons:* | Adoption AgID Guidelines | |
| **Version n°: 03** | | **Revision date: 29/01/2016** |
| *Change description:* | Adjustment to schema version 2.1 published by AgID | |
| *Reasons:* | AgID Request | |

| | | |
|---|---|---|
| ***Version n°: 02*** | | ***Revision date: 24/11/2014*** |
| *Change description:* | Clarifications on Roles and Responsibilities | |
| *Reasons:* | AgID Request | |
| ***Version n°: 01*** | | ***Revision date: 23/10/2014*** |
| *Change description:* | Integrations and clarifications requested by AgID | |
| *Reasons:* | AgID Request | |

# Summary

# 1 Purpose of the document

This manual describes the preservation system of In.Te.S.A. S.p.A. (hereinafter Intesa) called Trusted Doc, defines the competences, roles, and responsibilities of the actors involved in the document preservation process, and the operating model. The document reports the description of the process, architectures and infrastructures used, the security measures adopted, and any other information useful for the management and verification of the functioning of the preservation system.

In particular, the operational procedures adopted by Intesa for the legally compliant electronic preservation process, implemented through a dedicated Service for the Client, are described.

Intesa, in addition to being a Qualified Trust Service Provider (QTSP) under Regulation (EU) 2024/1183 (eIDAS) for electronic signatures, electronic seals, and electronic time validations (timestamps), is registered in the AgID Marketplace for preservation services.

The document describes the procedures adopted by Intesa as defined in the contract stipulated between the parties and in the related Technical Annex, in compliance with the relevant regulations and practices.

The manual summarizes the tasks described by the Digital Administration Code, hereinafter also "CAD" (Legislative Decree 7 March 2005, No. 82 and subsequent amendments/integrations), and by the Guidelines on the formation, management, and preservation of electronic documents.

To comply with what is indicated in Chapter 4.6 of the AgID Guidelines, each Owner of the Object, client of the INTESA preservation service, and, consequently, each Preservation Manager, in carrying out the tasks assigned to them by the regulations, can freely refer to this document in their own Preservation Manual.

## 1.1 Scope of Reference

The preservation service provided in Full Outsourcing mode is supported by Article 44 of the CAD, according to which preservation can be carried out by entrusting it, totally or partially, to other subjects, public or private, that offer suitable organizational and technological guarantees and protection of personal data.

The Client, or the Owner of the preservation object, entrusts the preservation process to Intesa and its internal managers in the various functions provided by the regulations, described in the relevant chapter of this manual: "Roles and Responsibilities".

The Technical Specifications, attached to this Manual, outline the specificities of the Service for the Client.

## 1.2 Structure of the E-Archiving Manual

This Manual is produced in digital format by Intesa (in collaboration with the Client regarding the Technical Specifications), archived in a dedicated repository of the Service for Intesa's internal use and made available to the Client. The Manual is also published by Intesa on its official website.

In the event of any updates and adjustments to this document, the new version will be made available to the Client.

In the event of any updates and adjustments to the Technical Specifications, by either party, a copy is sent to the Preservation Manager and the Client's Project Manager.

In this document, architectural aspects and current processes are partially described; for more technical/functional details, please refer to the following documents:

- Preservation service contract;
- Letter of entrustment;
- Technical Specifications (Annex A to the Preserver's Manual) – previously defined as Contract Specificities;
- Technological components of the Preservation System (Annex B to the Preserver's Manual);
- Any Functional Analysis document, for aspects related to the technical implementations of the Preservation, not attached to this Preserver's Manual, prepared based on the specific project context of the Client;
- Cessation Plan of the Preservation System (a confidential document shared by Intesa with the Agency for Digital Italy (AgID)).

# 2 Terminology (acronyms and Glossary)

## 2.1 Acronyms

Below are the main acronyms used in the document and their respective definitions:

| Acronimo | Definizione |
|---|---|
| **AgID** | Agency for Digital Italy |
| **CAD** | Digital Admnistration Code, Legislative Decree 7 march 2005, n. 82 e smi |
| **IPdA** | Index of Archival Package – evidence associated with each Archival Package containing a set of information structured according to the SInCRO standard |

| | |
|---|---|
| **IPdV** | Index of Submission Package |
| **LLGG** | AgID Guidelines on the creation, management and preservation of electronic documents |
| **MdC** | E-Archiving Manual |
| **PdA** | Archive Package |
| **PdC** | Loading Package |
| **PdD** | Dissemination Package |
| **PdV** | Submission Package |
| **RdC** | Preservation Manager |
| **RSC** | Head of Preservation Service |
| **RSSC** | Head of Systems Security for Preservation |
| **RFA** | Head of Preservation Archival Function |
| **RTP** | Head of Personal Data Processing |
| **RSI** | Head of Information Systems for Preservation |
| **RSM** | Head of Development and Maintenance of the Preservation System |
| **RdV** | Submission Report |
| **SInCRO** | Support for Interoperability in the Preservation and Retrieval of Digital Objects (UNI 11386) - National standard in XML language, concerning the structure of the data set supporting the preservation process |
| **SLA** | Monitoring of service level agreement |

## 2.2 Glossary of terms

Below is a glossary of the terms used in the text and their respective definitions:

| Terminology | Definition |
|---|---|
| **Reliability** | Characteristic that, with reference to a document management or preservation system, expresses the level of trust that 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. |
| **Attachment A** | Technical specifications of this manual, containing the detailed description of the elements of the preservation process. |
| **Attachment B** | Document containing the technical-functional description of the logical and physical components of the preservation system. |
| **Authenticity** | Characteristic by virtue of which an object must be considered as corresponding to what it was at the original moment of its production. Therefore, an object is authentic if it is at the same time complete and intact, having not undergone any unauthorized modification over time or space. Authenticity is evaluated on the basis of precise evidence. |
| **Preserver** | Public or private entity that carries out the preservation of electronic documents. |
| **Preservation** | Set of activities aimed at defining and implementing the overall policies of the preservation system and governing its management in relation to the adopted organizational model, guaranteeing over time the characteristics of authenticity, integrity, legibility, and retrievability of documents. |
| **Electronic Document** | Electronic document containing the digital representation of legally relevant acts, facts, or data. |

| | |
|---|---|
| **HASH** | Digital fingerprint of a document obtained by applying a "hash function" and consisting of a sequence of binary symbols. |
| **Integrity** | Characteristic of an electronic document or a document aggregation by virtue of which it appears that it has not undergone any unauthorized alteration over time and space. The characteristic of integrity, together with that of completeness, contributes to determining the characteristic of authenticity. |
| **Interoperability** | Characteristic of an information system, whose interfaces are public and open, and capable of interacting automatically with other information systems for the exchange of information and the provision of services. |
| **Letter of Entrustment** | Formal document, verified and countersigned for approval by the Preservation Manager, attesting to the personal, contractual, and reference information to define the scope of implementation of the outsourced preservation service. |
| **Guidelines** | Guidelines on the creation, management, and preservation of electronic documents published in the Official Gazette no. 259 of October 19, 2020. |
| **Preserver's Manual** | Electronic document that describes the preservation system and illustrates in detail the organization, the parties involved and the roles played by them, the operating model, the process description, and the description of the architectures and infrastructures. |
| **Cessation Plan** | Confidential document, requested by AgID regarding registration in the Marketplace for preservation services, which summarizes the activities, roles, and procedures for managing the possible termination of the preservation system. |
| **Preservation System Security Plan** | Confidential document that, in the context of the general security plan, describes and plans the activities aimed at protecting the preservation system of electronic documents from possible risks. |

| | |
|---|---|
| **Qualified Trust Service Provider** | Entities that issue qualified certificates in accordance with Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024 (eIDAS). |
| **Trusted Doc** | Intesa's preservation service, provided in outsourcing mode. |
| **Trusted Hub** | Technological platform on which Intesa's outsourced preservation service is located. |

# 3 Regulations and standard

## 3.1 Applicable regulations

A list of the main applicable Italian regulations on the subject is provided here below:

- Italian Civil Code [Book 5 on labour, Title II on company labour law, Chapter III on commercial enterprises and other enterprises subject to registration, Section III on special provisions for commercial enterprises, Paragraph 2 on accounting records], Article 2215 bis - Electronic documentation;
- Italian Law no. 241 of 7 August 1990 and subsequent amendments and supplements – New regulations on administrative procedures and the right to access administrative documents;
- Italian Presidential Decree no. 445 of 28 December 2000 and subsequent amendments and supplements – Consolidated legislative and regulatory provisions on administrative documentation;
- Italian Presidential Decree no. 68 of 11 February 2005 – Regulation containing provisions on the use of certified e-mail;
- Italian Legislative Decree no. 196 of 30 June 2003 and subsequent amendments and supplements – Italian personal data protection code;
- Italian Legislative Decree no. 42 of 22 January 2004 and subsequent amendments and supplements – Italian Cultural Heritage and Landscape Code;
- Italian Legislative Decree no. 82 of 7 March 2005 and subsequent amendments and supplements – Italian Digital Administration Code (CAD);
- Italian Prime Ministerial Decree of 22 February 2013 – Technical standards on the generation, application and verification of advanced, qualified and digital electronic signatures in accordance with Articles 20, par. 3, 24 par. 4, 28 par. 3, 32 par. 3, point b), 35 par. 2, 36 par. 2, and 71
- Italian Prime Ministerial Decree of 3 December 2013 – Technical standards on conservation systems in accordance with Articles 20 pars. 3 and 5-bis, 23-ter, par. 4, 43, pars. 1 and 3, 44, 44-bis and 71, par. 1, of the Italian Digital Administration Code referred to in Italian Legislative Decree no. 82 of 2005 [*Entirely repealed by the AgID Guidelines in force since January 1, 2022*];

- Italian Prime Ministerial Decree of 13 November 2014 – Technical standards on the preparation, sending, copying, duplication, reproduction and timestamping of electronic documents as well as the preparation and conservation of public administration bodies' electronic documents in accordance with Articles 20, 22, 23-bis, 23-ter, 40, par. 1, 41, and 71, par. 1, of the Italian Digital Administration Code as referred to in Italian Legislative Decree no. 82 of 2005
- AGID Circular no. 65 of 10 April 2014 – Accreditation procedures and oversight of public and private entities that perform the electronic document conservation activities referred to in Article 44-bis par. 1 of Italian Legislative Decree no. 82 of 7 March 2005 [*Circular entirely repealed by the AgID Regulation in force since January 1, 2022*].
- Regulation (EU) No. 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No. 910/2014 as regards the establishment of the European framework for a digital identity;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Regulation (EU) 2016/679 of the European Parliament of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Decree of the Italian Ministry of Economy and Finance of 17.06.2014 – "Methods of complying with tax obligations concerning electronic documents and their reproduction across various types of media - Article 21 par. 5, of Italian Legislative Decree no. 82/2005"
- Decree of the Italian Ministry of Economy and Finance no. 55 of 3 April 2013 – "Regulation on the issuance, sending and receipt of electronic invoices applicable to public administration bodies in accordance with Art. 1, pars. 209 to 213, of Italian Law of 24 December 2007. Published in the Italian O.G. no. 118 of 22 May 2013"
- Guidelines on the creation, management and conservation of computerised documents published in the Italian Official Gazette no. 259 of 19 October 2020.

## 3.2 International Standard

The standards to which the Intesa system complies and, where applicable, is qualified are:

- ISO 14721:2025 OAIS (Open Archival Information System);
- ISO 9001:2015, Quality management systems — Requirements;
- ISO/IEC 27001:2022, Information technology - Security techniques - Information security management systems – Requirements;
- ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO 37001:2025, Anti-bribery management systems — Requirements with guidance for use;

- 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;
- 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;
- ETSI TS 119 511 V1.1.1 (2019-06) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- ETSI EN 319 401 V.3.1.0 (2024-06) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set;
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;
- ISO 16363:2012, Space data and information transfer systems — Audit and certification of trustworthy digital repositories.

# 4 Roles and responsibility

The preservation system identifies at least the following roles:

- Holder of the preservation object;
- PdV Producer;
- Authorized User;
- Preservation Manager;
- Preserver.

The holder of the preservation object is the producer of the digital preservation objects. In this document, and generally in the shared documentation, it is also understood as the Client.

The PdV producer is a natural person, usually different from the subject who created the document, who produces the submission package and is responsible for transferring its content to the preservation system. This is generally the subject in charge of producing and/or managing the documents and/or related metadata to be sent to the preservation system, responsible for the document's content.

In the case of entrusting the preservation service to third parties, the PdV producer provides for the generation and transmission of submission packages to the preservation system in the manner and formats agreed with the preserver and described in the preservation manual of the preservation system. It also

verifies the successful outcome of the transfer operation to the preservation system by viewing the submission report produced by the preservation system itself.

In the standard process prepared, and described in this manual, the creation of the PdV is entrusted to Intesa. The PdV is in fact constituted by Intesa systems at the end of the process, called pre-ingest, in which the documents sent by the Holder of the Object, in the information package defined as Loading Package, are processed, if a completion phase is foreseen through the functionalities offered by Intesa, and verified, through the execution of regulatory controls whose results are reported in the Submission Report.

The authorized user is the person, entity, or system that interacts with the services of a computerized document management system and/or a system for the preservation of electronic documents, in order to access information of interest; it requests the preservation system for access to documents to acquire information of interest within the limits established by law. This is therefore the client or subjects authorized by the Client itself to access the documents.

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

The Preservation Manager, under their own responsibility, may delegate the performance of their activities or part of them to one or more subjects who, within the organizational structure, have specific skills and experience. This delegation, reported in the Preservation Manual, must identify the specific delegated functions and competencies.

In the event that the Preservation service is entrusted to a Preserver, the aforementioned activities or some of them, with the exclusion of the preparation and updating of the Preservation Manual, may be entrusted to the Service Manager, it being understood in any case that the general legal responsibility for the preservation processes, not being delegable, remains with the Preservation Manager.

The latter is also required to carry out the necessary verification and control activities in compliance with the regulations in force regarding services entrusted in outsourcing by Public Administrations, where this is a Public Administration.

The Client therefore identifies its own Preservation Manager who, in turn, having the right and authorization, entrusts Intesa with the electronic preservation process in accordance with the law. The entrustment, governed by specific documentation called "Letter of Entrustment", allows to institutionalize the performance, by the Preserver, of the tasks listed and the activities required by the legislation.

The Preservation Manager remains responsible for overseeing the correct execution of the preservation process: the Preserver bears contractual responsibility towards the Client.

The identification data of the Preservation Manager are reported in the Technical Specifications and, following the entrustment, the preservation process is entrusted to the Preserver.

The Preserver, finally, is the public or private entity that carries out the preservation of electronic documents.

## 4.1 Details of roles and related task

To ensure an adequate and satisfactory level of quality in the services offered, Intesa has structured its company organization into processes. At the overall company level, a general framework of procedures is outlined, as well as the competences and responsibilities associated with them.

Each employee, individually or as part of a team, adheres to the indications of the defined company procedures and instructions based on their competence.
Activities are assigned based on the defined company roles.

The Preservation process is also implemented based on this organizational framework for both provision and monitoring aspects.
The responsibilities pertaining to Intesa, as the entrusted Preserver of the preservation service, are defined in the technical specifications provided to the Client in accordance with the provisions of the regulations.

Intesa, as required by current legislation, performs its function with the utmost care and supervision through a group of specialized resources dedicated to the provision, management, support, and oversight of the Service, based on a solid internal company organization. In this way, it guarantees the presence of qualified and diversified personnel according to specific needs, equipped with professional training and adequate technical knowledge, available for interaction with the Client's Preservation Manager in the various phases of the Service.

The roles defined within the Intesa organization and carried out within the preservation process are described below; specific references are provided in the technical specifications.

### 4.1.1 Preservation Manager (Customer)

The Preservation Manager is a figure defined by the Client - the physically designated person within the Company holding the documents subject to preservation - as responsible for all activities aimed at the lawful preservation of electronic documents within the scope of the outsourcing contract with Intesa.

In managing the entire preservation process, the PM acts as guarantor, not only towards the entity for which they work but also towards the tax authorities, for the correct management of the process according to established and documented security principles, adopting traceability procedures in such a way as to guarantee the correct management of information packages, preservation, accessibility to the individual document, and its exhibition.

The Preservation Manager within their own organization works in agreement with the data protection officer,

the security manager, and the IT systems manager.

The activities of the Preservation Manager in collaboration with the Preserver are crucial in various phases of the preservation process:

- Formal signing of the letter of entrustment, based on a template provided by Intesa, and participation in the launch of the preservation project;
- Review of the characteristics of the Service made available by Intesa: during the sealing phase of the archival package index and the distribution package; Intesa has chosen to operate on individual documents or individual electronic evidence;
- The Preservation Manager, in collaboration with the Preserver, includes in the Technical Specifications the details of cases requiring the presence of a public official/notary if foreseen within the type of documents processed or the specific process defined in agreement with the Preserver;
- The Preservation Manager prepares the Preservation Manual, referring, for the technical parts within their competence, to the available documentation (Technical Specifications and Preserver's Manual).

### 4.1.2 Head of Preservation Service

The activities of the Head of Preservation Service are the following:

- Definition and implementation of the overall policies of the preservation system, as well as the governance of the management of the preservation system;
- Definition of the characteristics and requirements of the preservation system in compliance with current legislation;
- Correct provision of the preservation service to the producing entity;
- Management of agreements, definition of technical and operational aspects, and validation of technical specifications that detail the specific aspects and operating procedures for the provision of preservation services.

### 4.1.3 Head of Preservation Archival Function

The Head of Preservation Archival Function is responsible for configuring the preservation process, in collaboration with the Head of Development and Maintenance.

This figure, through the relevant company structure, performs the following tasks:

- Definition and management of the preservation process, including the methods of transfer by the producing entity, acquisition, integrity verification and archival description of transferred documents and document aggregations, exhibition, access, and use of preserved documentary and information assets;
- Definition of the set of preservation metadata for documents and electronic records;

- Monitoring of the preservation process and archival analysis for the development of new functionalities of the preservation system;
- Collaboration with the producing entity for the purpose of transfer for preservation, selection, and management of relations with the Ministry of Culture for matters within its competence.

### 4.1.4 Head of Information Systems for Preservation

The activities of the Head of Information Systems for Preservation are as follows:

- Management of the operation of the hardware and software components of the preservation system;
- Monitoring the maintenance of service levels (SLAs) agreed with the producing entity;
- Reporting any SLA discrepancies to the Head of Preservation Service and identifying and planning necessary corrective actions;
- Planning the development of the technological infrastructures of the preservation system;
- Control and verification of service levels provided by third parties, with notification of any discrepancies to the Head of Preservation Service.

### 4.1.5 Head of Development and Maintenance of the Preservation System

The activities of the Head of Development and Maintenance of the Preservation System are as follows:

- Coordination of the development and maintenance of the hardware and software components of the preservation system;
- Planning and monitoring of development projects for the preservation system;
- Monitoring of SLAs related to the maintenance of the preservation system;
- Interface with the producing entity regarding the methods of transferring documents and electronic records concerning the electronic formats to be used, the technological evolution of hardware and software, and any migrations to new technological platforms;
- Management of the development of websites and portals connected to the preservation service.

### 4.1.6 Head of Systems Security for Preservation

The tasks of the System Security Manager for Preservation are as follows:

- Compliance with and monitoring of the security requirements of the preservation system established by standards, regulations, and internal security policies and procedures;
- Reporting any discrepancies to the Head of the Preservation Service and identifying and planning the necessary corrective actions.

### 4.1.7 Head of Personal Data Processing

The activities of the Head of Personal Data Processing are the following:

- Guarantee compliance with current regulations regarding the processing of personal data;
- Ensure that the processing of data entrusted by Clients will take place in compliance with the instructions given by the data controller, with a guarantee of security and confidentiality.

# 5 Organizational structure for the preservation service

Intesa's organizational structure is based on a management vision focused on key individuals in the specific roles required within the preservation process.

INTESA has identified and appointed the professionals who make up the document preservation work team.

The team consists of resources operating in various company areas to ensure the correct execution of the service in relation to all the technical/organizational issues peculiar to the service in question.

The appropriate internal organizational procedures have therefore been defined to guarantee the unambiguous coordination of the team's resources so that their work is carried out in full coherence with the service content and the company's quality objectives.

## 5.1 Internal Organization

Below is the internal organization chart of Intesa, highlighting the company areas and roles involved in the preservation system:

| | Role | Name |
|---|---|---|
| 1 | Head of Preservation Service | Luigi *TRAVERSO* |
| 2 | Head of Preservation Archival Function | Francesco *DE CESARE* |

| | | |
|---|---|---|
| **3** | Head of Personal Data Processing | Serena *DONEGANI* |
| **4** | Head of Systems Security for Preservation | Paolo *MAURINO* |
| **5** | Head of Information Systems for Preservation | Matteo *ROTA* |
| **6** | Head of Development and Maintenance of the Preservation System | Marco *RASA* |

## 5.2 Organization structure

Below is the internal organization chart of Intesa, highlighting the company areas and roles involved in the preservation system:

| **Activities covered by the roles of the managers involved in the preservation service** | | | | | | |
|---|---|---|---|---|---|---|
| | **Responsability** | | | | | |
| | **RSC** | **RSSC** | **RFA** | **RTP** | **RSI** | **RSM** |
| Activation of the preservation service (following the signing of a contract) | X | X | X | X | X | X |
| Acquisition, verification, and management of the submission packages taken in charge and generation of the submission report | X | X | X | | | X |
| Preparation and management of the Archival Package | X | X | X | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| Preparation and management of the Dissemination Package for the purpose of exhibition and the production of duplicates and electronic copies upon request | X | X | X | X | | X |
| Disposal of Archival Packages | X | X | X | | X | X |

| **Management activities of Information Systems** | | | | | | |
|---|---|---|---|---|---|---|
| | **Responsability** | | | | | |
| | **RSC** | **RSSC** | **RFA** | **RTP** | **RSI** | **RSM** |
| Management and maintenance of the preservation system | | X | | | | X |
| Monitoring of the preservation system | | X | | | X | X |
| Change management | X | X | | | X | X |
| Periodic verification of conformity to regulations and reference standards | X | | X | X | | |

# 6 Objects under preservation

## 6.1 Preserved objects

The Intesa archiving system is equipped with functionalities to guarantee the preservation, from the acquisition phase by the producer to the eventual disposal, of electronic documents accompanied by their

metadata, through the implementation of appropriate technological procedures.

The digital objects of the preservation are processed by the preservation system, as required by the OAIS standard, in information packages that are distinguished as:

1. Loading Packages (information structure that, in the standard process, describes the documentary object sent by the Owner of the Object in the pre-ingest phase);
2. Submission Packages;
3. Archival Packages;
4. Distribution Packages.

The conceptual reference model for long-term preservation is the OAIS model (ISO 14721 standard), which introduced the concepts related to the creation, archiving, and preservation of information packages into the current technical and regulatory landscape.

These packages are generically composed of four elements:

- The information content, i.e., the digital object and the set of information that allows its representation and understanding at the user level;
- The preservation information, which includes identification, context, provenance, and integrity information;
- The logical information, i.e., the data that points to the logical location of the information package archived in the Intesa preservation system;
- The Archival Package Index, defined based on the specifications contained in the UNI SINCRO standard, containing information relating to: description of the types, preservation information, representation information, information regarding sending for preservation, the file formats and extensions provided, regulatory references, and submission methods (which are then taken up and described analytically in the Technical Specifications).

Interoperability between the preservation systems of the subjects carrying out this activity is guaranteed by the application of the technical specifications of the Archival Package Index defined by the UNI 11386 standard - SInCRO Standard - Support for Interoperability in the Preservation and Retrieval of Digital Objects.

Below is the general, non-exhaustive table of the main file formats and extensions of the objects subject to preservation, the specific details of which for the Client, agreed upon with the producing subject, are reported in the Technical Specifications.

| File format | Viewer | Producer | MIME type | Standard | extension |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| PDF | Adobe Reader | Adobe | application/ pdf | ISO 32000 | .pdf |
| PDF/A | Adobe Reader | Adobe | application/ pdf | ISO 19005 | .pdf |
| XML | Internet Browser | W3C | application/xml<br>text/xml | | .xml |
| TIFF | Viewer of image | Adobe | image/tiff | ISO 12234 | .tif, .tiff |
| JPEG | Viewer of image | Joint Photographic Experts Group | image/jpeg<br>image/jpg | | .jpg, .jpeg |
| EML | Client of e-mail | | application/email | RFC-5322<br>RFC2822 | .eml |

Any other file format used to create electronic documents subject to the archiving process must be present in Annex 2 of the AgID Guidelines, agreed upon in advance and reported in the specific section of the Technical Specifications.

In particular, AgID has joined the international initiative promoted by the Open Preservation Foundation, with the aim of regularly publishing a complete and updated list of file formats recognized globally, including key information on interoperability and long-term preservation for each.

## 6.2 Submission Package

During data acquisition, the document is sent in one of the formats specified in Annex 2 of the Guidelines. A fundamental characteristic required by the regulations is that the preservation system must ensure the usability of the preserved documents over time.

Therefore, the electronic document preservation process involves identifying document types and managing index fields associated with the documents for their correct identification.

The choice of indexes to associate with the documents is made based on the type of documents to be preserved and the search requirements, in collaboration with the Client, in relation to specific needs and

context.

The description of the types of objects subject to preservation, including the indication of the managed formats and the metadata to be associated with the different types, is provided in the Technical Specifications.

The Client then sends the documents to be preserved, together with the index structures to be associated, to the Intesa platform according to the agreed timelines and operating procedures.

In the Intesa standard process, the information package sent by the Owner of the Object according to the agreed procedures is configured as a Loading Package, as the definitive technical structures and the operating components provided for by the Submission Package (PdV) are not present.

Intesa, through specific agreements, collaborates in defining the Submission Package which, consequently, is formed on Intesa's systems at the end of the defined pre-ingest phase.

The indexing of documents can eventually be carried out by Intesa's processing procedures based on what is specifically agreed with the Client.

The Preservation system is set up to manage file formats that can best guarantee the principles of interoperability between the systems themselves, in compliance with current legislation regarding specific document types.

Therefore, the formats that can allow the readability and interoperability of the electronic document in the preservation system are chosen and used in agreement with the Client and in compliance with the provisions of Annex 2 of the Guidelines.

Each PdV refers to a submitted object and is uniquely identified.

The Submission Package consists of the following objects:

- The Submission Package Index;
- The submitted object;
- The metadata file, according to the provisions of Annex 5 of the AgID Guidelines;
- Any XSD schemas.

## 6.3 Archival Package

The Archival Package (hereinafter PdA) is a container file (uncompressed zip format) that internally contains the original submitted document, the sealed and time-stamped Archival Package Index file (hereinafter IPdA), the signed and time-stamped Submission Report file (hereinafter RdV), in case of resubmission or internal

re-preservation the IPdA file of the previous process, the xsd schema files and a ReadMe.txt file.

The PdA, named PDA.INTESA.IDHUB.ID.zip, will be composed as follows:

- ReadMe.txt (text file describing the composition, type, and meaning of the files present);
- PIndex.INTESA.IDHUB.ID.xml.p7m (IPdA file of the submitted object);
- pdv\ (Folder containing the PdV)
    - <DOC.INTESA.IDHUB.ID.ext> (Submitted Object)
    - <MT.INTESA.IDHUB.ID.xml> (Metadata file Annex 5 of the Guidelines);
- rdv\ (Folder containing the Submission Report)
    - RDV.INTESA.IDHUB.ID.xml.p7m (Submission Report File);
- ipda_previous\ (Optional folder containing the IPDAs of the previous process)
    - <previous_ipda.ext> (Optional IPdA file of the previous process);
- xsd\ (Folder of the schemas used in the Information Package)

The IPdA file complies with the national SInCRO standard - Support for Interoperability in the Preservation and Retrieval of Digital Objects (UNI 11386), the standard concerning the structure of the data set supporting the preservation process which provides a specific articulation through the XML formal language.

The XML structure of SInCRO also includes:

- An additional "MoreInfo" section that allows specifying the subjective metadata (specific "custom" indexes, deriving from the particular document class to which the index refers) defined by Intesa in agreement with the Client in relation to the type of document processed;
- The metadata required by the legislation, indicated in Annex 5 of the AgID Guidelines.

These additional "MoreInfo" structures refer to specific schema files, present within the archival package and recalled within the SInCRO xml.

The IPdA and the RdV are digitally signed using the CAdES standard, thus generating a file with the xml.p7m extension.

## 6.4 Dissemination Package

The preservation system allows authorized subjects direct, remote access to the preserved document, which can be consulted and exhibited either online through the Intesa web portal, or through self-consistent extractions.

The Distribution Package consists of a zip file signed with the INTESA seal that contains the same structures as the Archival Package. The difference lies in the temporal affixing of the seal; in fact, the Distribution Package sealed at the time of consultation produces legal evidence attesting not only to the content of the package (hence the same structure as the PdA) but also to the guarantee of the correct maintenance of the preservation chain. For the description of the individual data structures, please refer to the previous paragraph.

Through logical correlations, conveyed by the preservation platform database, each Distribution Package is accompanied by documented data structures, allowing the overall link between the Distribution Package and the following elements:

- SInCRO xml data structure (in xml.p7m format), including MoreInfo sections for custom metadata and mandatory metadata;
- .xsd schema of custom metadata (metadata stored on the database structure and reported in the MoreInfo section of the SInCRO xml);
- .xsd schema of metadata (metadata stored on the database structure and reported in the MoreInfo section of the SInCRO xml).

Documents are searched using the search keys corresponding to the specific metadata for each type of document flow.

Specific functionalities allow the viewing, integrity verification, or export of Distribution Packages and the copying of preserved objects.

Any specific and further methods of exhibition that allow connection and integration with the Customer's systems can be jointly evaluated between the Customer and Intesa and reported in the technical specifications (e.g., via Web Services, physical storage media).

The Service is therefore equipped with suitable tools to present the preserved documents in case of accesses, inspections, and audits conducted by subjects within the Customer's organization and/or the competent authorities, such as in the case of audits by the Authority or the competent bodies prescribed by current regulations for the performance of control and supervision activities.

# 7 The Preservation Process

The preservation process, described as a linear instance, involves the preparation of a Submission Package containing the digital objects to be preserved, along with the metadata required by defined regulations (preservation index). This package is transmitted to the preservation system according to the methods agreed upon between Intesa and the Owner of the preservation object. The Submission Package Index

completes the Submission Package. The activities of the Preserver, the entrusted provider of the preservation process, are: receiving the Loading Package (PdC), completing the Submission Package (PdV), validating the PdV, transforming the PdV into an Archival Package (PdA), maintaining the PdA in preservation for the contractually established timeframes, and, based on business and verification needs, providing visibility of the Dissemination Package (PdD) to the Owner of the preservation object through agreed consultation methods, as required by the AgID Guidelines.

The functional components of the Trusted Doc preservation system ensure the processing of the entire lifecycle of the preserved object within the preservation process.

The system assigns a unique platform identifier that allows direct and persistent identification.

The system guarantees access to the preserved object for the period prescribed contractually based on regulations, regardless of the evolution of the technological context.

As indicated in paragraph 4.2 of the AgID Guidelines, the objects of preservation are processed by the preservation system in information packages that are distinguished as:

1. Submission Packages: these are the information structures containing the data to be preserved, consolidated by the Intesa platform, also accompanied by the relevant metadata, according to what has been agreed with the Client;
2. Archival Packages (PdA): data structures that follow the submission in the defined process, and among which is also the IPdA prepared according to the SInCRO standard;
3. Dissemination Packages: data structures provided for the purpose of exhibition.

The Intesa preservation service is configured to manage data from different companies, creating strictly separate environments for each entity, appropriately identifiable through a specific system coding and potentially available in the indexes at the time of document acquisition on the platform in the case of multi-company groups.

The system is set up to manage, uniformly but guaranteeing complete separation of:

- Configurations;
- Processes applied by workflows, including signing workflows;
- Information packages (submission, archiving, distribution);
- Monitoring;
- Input and output data flows.

While maintaining distinct management for different companies, the system allows the Head of the Preservation Service and their operators a unified view of the different management processes, particularly for monitoring, control, and alerting functions.

The documents entered into the submission system and subjected to appropriate checks during loading are not exposed to risks of alteration or modification during the logical transfer to the preservation procedures. However, these procedures support the integrity of the document through automatic checks at each stage of the process.

The checks and identification of anomalies are therefore carried out upstream of the process, within the submission system, where any discards are detected and reported using the agreed tools. Subsequent phases occur under the monitoring of the management system, which controls the correct execution of the preservation process and produces the relevant reports both in relation to any anomalies detected and in reference to what has been correctly preserved.

Each document is sent to the preservation system in the form of a Submission Package, which therefore contains the object to be preserved, and follows the Preservation process provided for by regulations and, in particular, by the OAIS standard.

In reference to the regulations on the preservation of electronic documents of a civil nature and in full compliance with them, Intesa has chosen, having evaluated the benefits and consistency with the service's approach, to apply the preservation process at the level of the single document.

In fact, the Archival Package created for each document allows its exhibition with all the primary requirements necessary for its complete verification by the inspection authorities. The document, preserved individually, can be easily exhibited during legal proceedings and with probative value recognized by judges or public officials in cases of a civil and tax nature.

The traceability of the single document within the preservation process is guaranteed and may be made available via web publication for the various statuses of the document (received and preserved).

These evaluations have therefore led to the definition of the currently used solution, which assumes the single document as the cornerstone of the process. Through the management of the submission, archiving, and distribution package, it implements the various steps required by the CAD and the related AgID Guidelines.

## 7.1 Methods of acquisitions of Loading Package for their acceptance

The Preservation Service (also known as Trusted Doc) allows the transfer of data and related indexes securely via Https protocol, or through other methods agreed with the Client, always with the aim of safeguarding the security of the data sent.

Intesa provides services in its own Server Farm; for further details on the technological components of the service, please refer to Annex B of this Manual.

The system, in the Intesa standard solution, includes the management of various operational steps, including those related to the completion of the Digital Object and the execution of the controls required by regulations. These activities are planned in a phase prior to the Submission process.

In particular, a management of the information package sent by the Owner of the Object, specifically called Loading Package, is outlined. This package constitutes the documentary core subject to verification and completion actions, where foreseen by the specific project, on which the Preservation system intervenes before finalizing the Submission Package.

The preservation objects received on the Intesa platform generate service requests (SRs) to which unique identifiers (IDSRs) are attributed, which allow tracking the activities carried out during processing, from acceptance to the creation of Archival Packages. Each phase of the process is accurately recorded and stored in specific database tables dedicated to tracking/logging (log records), making them easily consultable. The information packages received undergo progressive saving on the primary database, the single point of consistency of the platform, redundant on a secondary instance, through "data guard" functions, during the processing phases.

The historical record of the data during the processing allows its recovery in case of anomaly/procedural error.

The frequency of sending documents to the preservation system is determined by the operation of the procedures on the Client's systems and agreed with Intesa (daily, monthly, etc.) taking into account the regulatory deadlines for preservation.

During the service setup phase, the specifications of the Submission Package and the related metadata structure are defined for each document type.

The metadata to be associated with the documents to be sent for preservation are produced, integrating those already defined during production. The metadata are in particular integrated with the indication of the Preservation System to which the document should be sent.

Each document is sent to the Preservation System, identified through appropriate rules defined based on the document type and the information contained in the metadata of the document itself.

Intesa's activities related to each document type are carried out according to the document sending times to the preservation system and within the maximum preservation period established by regulations, with the exception of cases where the sending is carried out by the Client beyond the regulatory deadline (e.g., cases of past data recovery).

Based on what is agreed with the Client and according to the needs related to the document type, Intesa configures the processing workflows and all the necessary parameterizations for the correct handling of the documents.

## 7.2 Checks performed on Loading Package and the object contained within them

The submission system, during the pre-ingest phase, performs a series of compliance, reconciliation, and correctness checks on the documents to be preserved. Specifically, the following are carried out:

- Compliance checks:
  - Verification of the sender company's details (Client/Owner of the preservation object);
  - Verification of file format and extension. The preservation system checks the format of each submitted file according to the specifications in Annex 2 of the AgID Guidelines;
  - Presence of all mandatory information defined for the specific document categories.
- Correctness checks:
  - During the preliminary analysis phase, specific rules are agreed upon for performing any uniqueness, duplication, consistency, and completeness checks on the documents before preservation, with notification of any missing documents based on the rules defined in agreement with the client.

The aforementioned checks may potentially lead to blocking or non-blocking errors, and therefore the possible rejection of the Loading Packages.

In this regard, Intesa's standard process does not provide for the rejection of the Submission Package, nor the related negative Submission Report, but performs all the foreseen checks during the pre-ingest phase. Consequently, rejection and the related error reporting exclusively concern the Loading Package.

## 7.3 Acceptance of Submission Packages and generation of the Acknowledgment of Receipt

After the Loading Packages and digital objects have been checked as previously indicated, they are accepted by the system, resulting in the generation of an acceptance message (ACK1). The correct execution of the foreseen formal checks allows the Loading Package to be crystallized into a Submission Package.

At the end of the Submission Package processing and control phase, the Submission Report is also generated.

The Submission Report is a digital object of XML type that certifies the successful taking charge by the preservation system and that the various foreseen checks have been passed successfully.

The Submission Report includes the INTESA platform file ID, the hash, and the submission date of each preservation object.

In Intesa's preservation system, each submission report is assigned a unique file name and is subsequently signed in CAdES p7m format and time-stamped by the Head of the Preservation Service.

The Service provides for the creation of a Submission Report for each digital object sent by the Client.

The Submission Report is signed with a qualified electronic signature by the Head of Preservation Service of Intesa and is stored in correlation with the submission package it refers to; by searching for the submission package, it is possible to view the related Submission Report.

## 7.4 Rejection of Loading Package and methods for communicating anomalies

The preservation process is designed to minimize, if not eliminate, the rejection of Submission Packages (PdV). Within the service workflow, there is a pre-ingestion phase necessary for the correct acceptance of information packages, called Loading Packages (Pacchetti di Caricamento), which anticipates the verification and reporting of anomalies.

Failure to pass the blocking checks on the Loading Packages generates anomaly events that are notified to the Client through the agreed methods.

The Intesa standard process, which includes the implementation of adequate checks and controls during the pre-ingest phase, establishes the maximum number of rejections of the Submission Package as 0.

Any anomalies and/or blocking errors are reported and communicated to the Client in the preceding phases according to the established procedures.

All events are collected and described for subsequent notification to the Client's contact person, with whom the actions for completing the process will be agreed upon.

The control process is therefore characterized by:

- Execution of the verification workflow;
- Detection and tracking of the anomaly (database table and storage of the attachment in a repository);
- Generation of a certain error report with rejection of the document;
- Sending of the report with the relative reason (anomaly report) to the Client's company contact person in the established manner;
- Management through direct contact with the contact person for the various error cases that may have different treatments and solutions.

The correct control method is shared and agreed upon with the Client during the analysis phase.

The anomaly notification includes:

- The unique identifier of the rejected package;
- The related unique indexes agreed upon with the Client (e.g., document number and date);
- The description of the detected error.

List of managed anomalies:

- Incorrect format of the Loading Package;
- Errors in the layout and content of metadata (e.g., incorrect data type, incorrect lengths);
- Total or partial absence of metadata, with reference to the mandatory requirements defined for specific document categories;
- Error found during the integrity check of the Loading Package;
- Duplication error in relation to the established uniqueness rules;
- Error in the sequence check of documents, in relation to the agreed rules ("check buchi" procedure).

The anomaly reports therefore constitute an operational tool for verification and communication with the Client.

These communications are recorded in the agreed manner, such as within the company email application, on a specific database dedicated to the preservation service and used exclusively by appropriately profiled and authorized subjects.

## 7.5 Preparation and Management of Archival Package

Following the acquisition and verification of the Submission Package, Intesa proceeds with the transformation of the Submission Packages into Archival Packages.

The Intesa archiving system manages the Archival Package according to the data structure specifications outlined in the Guidelines.

The Archival Package is composed of:

- Digital object;
- Metadata;
- Index of the Archival Package;
- Submission Report.

The .p7m extension file of the Archival Package Index (IPdA) allows the preliminary exhibition of the PdA elements, already incorporating the primary and necessary requirements for its complete verification by the supervisory authorities. Furthermore, the single document can be presented for evaluation and authentication by judges or public officials in civil and tax contexts.
The traceability of the single document within the preservation process is guaranteed and can be made available via web publication for the various statuses of the document (e.g., received, preserved, etc.).

Based on the document type, the document retention times assigned by the system upon receipt and processing of the Submission Package are established during the setup phase.

The Preservation System is structured to manage the retention period of each document based on the document class, according to current legislation and the Service contract.

The operations of affixing a seal and time stamp to the IPdA are carried out in compliance with the specific regulations regarding signatures and time validation.

This process meets the requirements of authenticity, immutability, integrity, and fixity.

These operations complete the electronic preservation process, the status of the document within the tracking process is updated with the outcome of successful preservation, and a specific report, the archiving report (ACK2), is generated and made available to the Client with the relevant information.

The seal certificate of the Head of the Preservation Service is issued by CA Intesa and stored in HSM devices, which guarantee high levels of security, reliability, and performance in terms of the speed of execution of signing operations.

## 7.6 Preparation and management of Dissemination Package

The structure of Distribution Packages, according to INTESA's preservation logic, coincides with that of Archival Packages.

Distribution Packages, resulting from the application of the electronic seal and related timestamp, are represented by files with the .p7m extension and made available to the producing subject and Intesa, as the Preserver.

The exhibition of the preserved objects is agreed upon with the Client and can take place according to the Intesa platform standard in the specific ways indicated in the technical specifications of the contract, such as:

- Intesa web portal;
- Web services;
- Self-consistent storage media, if предусмотрено;
- Other agreed methods.

Through the Intesa web portal, it is specified that even when selecting multiple occurrences to consult as DPs, the system provides individual DPs that are self-consistent and usable for the intended purposes.

### 7.6.1 Web portal

Document consultation occurs via the web through access to the Intesa portal using the Https protocol, leveraging the platform's native online functions.

The consultation functionalities allow users to search for preserved documents in the database using a customized search engine for each index associated with the document and to view or download them for the duration established in the service contract.

The service also allows the processing of Distribution Packages characterized by multiple signature levels related to the processes of generation/issuance/electronic keeping of documents, by the Client and prior to the deposit and archiving phase.

Users who can access the consultation system are appropriately registered and profiled.

Profiling is defined based on the specifications provided by the Client, allowing the definition of user profiles and the relationships between them and the control of accesses.

### 7.6.2 Methods using storage media

Distribution Packages can be distributed, exceptionally and not recommended compared to the web portal method, for consultation also through the use of self-consistent storage media, if requested by the Client and expressly provided for within the contractual specificities.

In this case, the Distribution Packages are extracted for the exhibition of the preserved documents, organized in logical archives.

A logical preservation archive refers to the logical organization of the documents subject to the electronic preservation process, defined by type, period of competence, or any other parameter agreed with the Client to allow the production of self-consistent media to be delivered to the Client, if foreseen by the contractual agreements.

During this activity, the number of archives and the names to be attributed to them are defined for the different types of documents with the related search keys and the characteristics of the storage media, as described in the Technical Specifications.

The search indexes for consultation are agreed and defined during the Service analysis phase.

To track all details related to the production and storage of Distribution Packages on external media, specific application functions of the service generate an acknowledgment report (ACK3) that allows tracking the activity both at the system level and within the database dedicated to tracking the archives and media generated.

During the media generation phase, the procedure for verification and control between the number of actual packages present within the archive and the number of indexes reported in a specific control file is initiated. In case of discrepancy, an error log is generated, thus allowing the necessary verification activities.

If positive, the archive production activity is concluded, and the reconciliation and unique identification activities of the removable physical medium (hard disk or other specifically identified medium), shipping, and delivery are carried out according to the methods agreed with the Client.

The consultation of Distribution Packages on self-consistent media is based on the use of a viewing software (Viewer) created by Intesa and present on the medium itself, which includes the functions of search, verification, display, and download.

The Viewer is created in Java language to make it compatible with market operating systems and to ensure maximum longevity. It does not require the recognition of licenses for software components contained therein and therefore does not involve additional distribution costs.

The Viewer supports the functionalities summarized below:

- Document search:
  - Based on the defined metadata that describe (via XML file) the structure of the archive, a search form is presented showing the selection fields and related operators. The documents that meet the search criteria are listed with possible pagination. It is possible to select a specific column to perform ascending or descending sorts;
- The following functions are available on single documents:
  - Document display;
  - Display of the objects constituting the PKCS#7 (fingerprint, signature, timestamp);
  - Extraction of the objects constituting the PKCS#7 (signature, timestamp, complete PKCS#7, original clear file);
  - Verification of the integrity of the PKCS#7 with validity check of the signature and timestamp certificate on an external CRL file and of the "trusted" Certification Authorities.

## 7.7 Production of duplicates and digital copies, and description of any involvement of a public official in the cases provided for

The Client, by viewing the Distribution Packages and according to the agreed operating procedures, can proceed with the eventual download of digital duplicates.

In cases provided for by law, and following a formal request, the public official can request Intesa to produce certified copies of the documents themselves.

Intesa provides the public official with specific functionalities that include access to the consultation portal with username and password, allowing for:

- The viewing and precise or bulk selection of electronic documents;
- The related conformity verification activities of the electronic document compared to the original document already available to the public official;
- The local download of documents, to allow proceeding with the verification of authenticity, integrity, and validity of the affixed signatures through the use of a market verifier chosen by the public official, thus guaranteeing the total autonomy of the control process and the maximum guarantee of verification.

## 7.8 Disposal of Archival Package

Intesa's Preservation Service anticipates that, as the retention period approaches its expiry – contractually defined based on the regulatory requirements for the specific document type – the Client will be notified with sufficient notice about the documents nearing the end of their lifecycle.

The procedure is configured by compiling a table in the application database, which lists all stored document types, categorized by Client, document type, and retention period (e.g., 5 years for payroll registers, 10 years for other fiscally relevant documents, or other durations as contractually agreed with the Client and specified in the Technical Specifications).

The system generates a specific report containing the list of Archival Packages with documents slated for disposal and a warning about their imminent deletion. This is followed by the disposal of the Archival Packages and their logical archive references, excluding the references necessary for reporting information about the completed disposal, which will be maintained in Intesa's systems for tracking purposes.

A communication will be sent to the Owner of the Object and the Preservation Manager listed in the records, via certified email (PEC) to the registered address and via regular email to the associated standard address. The return receipts will be archived by Intesa and will constitute the first positive outcome of the disposal workflow. The physical deletion of data will occur starting 180 days after the formal communication, allowing the Client and the relevant Preservation Manager to submit, within 90 days of the communication, any requests for extension or return of the documents. These requests will be contractually consolidated and incorporated as updates to the system parameters or as operational activities for extraction and return.

If, following the formal communication, the Client wishes to extend the retention of the documents, they may notify Intesa within 90 days of receiving the communication. In this case, the contractual conditions governing this aspect will be adjusted.

The deletion, both logical and physical, will concern both the documents present in the platform's Database and those already transferred to archives on NAS.

### 7.8.1 Methods of return and management of the termination of the Preservation service

Upon Customer request and specific agreement between the parties, at the end of the retention period, Intesa delivers the preserved documents, organized in homogeneous archives via connector, or via another agreed technical method, based on the parameters agreed with the Customer in the related procedural activity.
In the event of termination of the contract or withdrawal by the Customer, or by Intesa, Intesa remains obligated to retain the documents for the period agreed with the Customer. Compliance with regulatory timeframes not specified in the contract remains the exclusive responsibility of the Customer, who, according to current regulations, can transfer the preserved documents to another preservation service provider

(defined as the succeeding provider). The Customer can then request the return of the data, through the agreed technical and operational methods, and the consequent release of Intesa from the obligations arising from paragraph 4.5 of the Guidelines.
In the event of termination of the Contract or Cessation of service, Intesa delivers the data in its possession to the Customer, being released from the obligation of preservation as well as from the obligations arising from paragraph 4.5 of the Guidelines.

In all cases of data return, the data is extracted into logical archives containing the packages accompanied by standard data structures, the organization of which is agreed with the Customer.

At the end of the return operations, the data is securely discarded from Intesa's systems.

Intesa, in compliance with the Regulation on the criteria for the provision of digital document storage services, has prepared its Cessation Plan in accordance with Annex B of the Regulation, subsequently sending a copy to AgID for verification and approval as part of the qualification for the Marketplace of preservation services. After obtaining a positive outcome on the submitted documentation, Intesa was correctly admitted to the Marketplace, which supersedes the previous institution of Accredited Preservers, starting from January 30, 2023.

## 7.9 Implementation of measures to ensure interoperability to other preservation providers

Thanks to its data storage structure, Intesa enables natural interoperability and integration with other archiving solutions and/or document management platforms.

In the event of termination or expiration of the contract, if this situation has been considered in the contractual agreements and includes the continuation of the archiving obligation by INTESA for the established period, this obligation is limited to application maintenance activities, system control, maintenance of the archival packages, and management of end-of-life disposal activities.

In this regard, Intesa operates through the following technological characteristics when providing the service:

- Use of file formats and extensions prescribed by regulations to ensure interoperability and counter technological obsolescence for document archiving;
- Adoption of standard signature formats recognized by Certification Authorities in compliance with PAdES-T and CAdES-T specifications, with the application of a time stamp;
- Intesa's choice to process single documents, rather than batches, completely eliminates the need to build and manage proprietary, complex, and articulated algorithms necessary to handle the document both during the archiving phase and in the delicate phase of exhibition to the competent

authorities and in all cases of judicial dispute;

- The single document is thus accompanied by all the technical-regulatory attributes that facilitate any portability or interoperability operation towards external structures and relies on XML formats, through the application of the SInCRO standard required for its specific interoperability characteristics, for association with the related indexes.

Intesa adopts formats that fully comply with recognized standards within its processes and, to further protect and guarantee Clients, does not use proprietary formats, often present on the market but of complex portability and whose interoperability value over time is doubtful.

Therefore, when the producing subject requests the transfer of Archival Packages to another Preserver, the functions activated by Intesa and guaranteed by the previous list of preservation system requirements allow a rapid transition to the new preservation provider. These are controlled export functions of the Archival Packages, the related Archival Package Indexes (IPdA), and the search metadata.

Regarding the TDOC 2.0 preservation system defined based on the requirements contained in the AgID Guidelines, Intesa corresponds to model no. 5 described in the document “Interoperability models between preservation systems” published by AgID in December 2022.

# 8 The Preservation System

The preservation system ensures, from the moment of acquisition until eventual disposal, the preservation of the digital objects stored within it, through the adoption of rules, procedures, and technologies, guaranteeing their authenticity, integrity, reliability, legibility, and retrievability as indicated in the Guidelines at paragraph 4.1.
Intesa's legally compliant electronic archiving service, called Trusted Doc, is based on Intesa's proprietary platform, Trusted Hub, as described below.
The Service has been entirely developed by Intesa, allowing for the prompt alignment of the solution with regulations, market best practices, and its customization over time to enhance the services provided.
The Trusted Hub Service infrastructure, used for providing the outsourced Trusted Doc archiving service to Clients, stems from over 25 years of Intesa's experience in electronic document management and over 10 years as a Certification Authority registered with AgID. It natively integrates the functionalities of a hub designed for processing and exchanging large volumes of electronic documents with the functionalities and guarantees that Intesa can offer as a Certification Authority and archiving provider.

The Trusted Hub platform is therefore natively integrated with the signature functionalities provided by ntesa itself as a Certification Authority; the mass signing of documents is carried out using HSMs that offer powerful cryptographic acceleration, hardware key management, and allow for the management of multiple

configuration profiles. They are particularly suitable for processes such as the generation of electronic documents at the source and legally compliant archiving, where security and performance are priorities.

Technologically up-to-date, the Trusted Hub infrastructure is robust and at the same time flexible. In fact, it is based on standard market middleware, alongside proprietary components to manage, in a streamlined and autonomous manner, specificities such as tracking, administration, workflow, digital signatures, and, in general, the various components of the service.

The services provided by Intesa and the related infrastructures are hosted at INTESA's Server Farms located in interconnected Campus sites on a high-speed geographical network. The infrastructure is composed of virtual partitions and physical servers and is fully redundant on the primary site and duplicated in the Disaster Recovery site.

By virtue of the modularity deriving from its infrastructure/configuration, the Service is scalable and therefore adequate to handle any increases in volumes.

Through the use of adequate storage, the infrastructure is specifically designed for data-intensive applications, achieving high performance with high reliability.

Below, information regarding the infrastructure of the Archiving Service will be provided; further details on the indicated elements are provided in Annex B to this manual: "Technological components of the Archiving system".

## 8.1 Logical components

The platform, whose logical architecture is shown in the following diagram, can be divided into a series of "Basic Modules" necessary for:

- Defining Communities, relationships, users, and their profiles;
- System administrator activities;
- Preservation system activities;
- Web portal management;
- Management of processing workflows;
- Store & forward of non-synchronous documents (mailbox);
- Monitoring and tracking of flows and documents within them.

These basic components are complemented by "Specialized Modules," invoked for specific processing of flows and/or data based on workflow rules:

- Time Stamping Module, for time-stamping documents for evidentiary purposes;
- Mass Digital Signature Module, which, using special high-security equipment, enables centralized document signing;
- PDF Module, which allows the transformation of received flows in various formats (spool, AFP, TXT, CSV, XML, etc.) into PDF;
- Trusted Invoice Module for the creation, transmission, reception, and publication of electronic invoices and related ACKs, and management of multi-channel forwarding (Postalization, e-mail, PEC, Web publication, SOGEI forwarding);
- Trusted Doc Module for legally compliant electronic archiving, for managing the process of electronic generation, preservation, publication of documents, and eventual production of storage media and maintenance of integrity, security, immutability, and readability over time;
- Trusted Exchange Module, which, through a Server component and a client component (Trusted Client), enables Https transmission of any type of flow according to a logic of service requests expressed in XML.

Furthermore, the platform has a series of "Connectors" that allow controlled interchange with other external platforms, which can be expanded over time based on specific Customer needs, such as:

- Trusted Exchange Connector;
- SAP Concur Connector (in partnership with ccelera);
- MQ Series Connector;
- SFTP Connector;
- Thema Spazio Connector;
- Connect Direct Connector;
- SOGEI Connector;
- PEC Connector (Trusted PEC).

Moreover, depending on specific customer needs, the software platform is designed for extension to other data interchange methods.

## 8.2 Technological components

Below is a diagram of the technological components of the preservation system previously described.

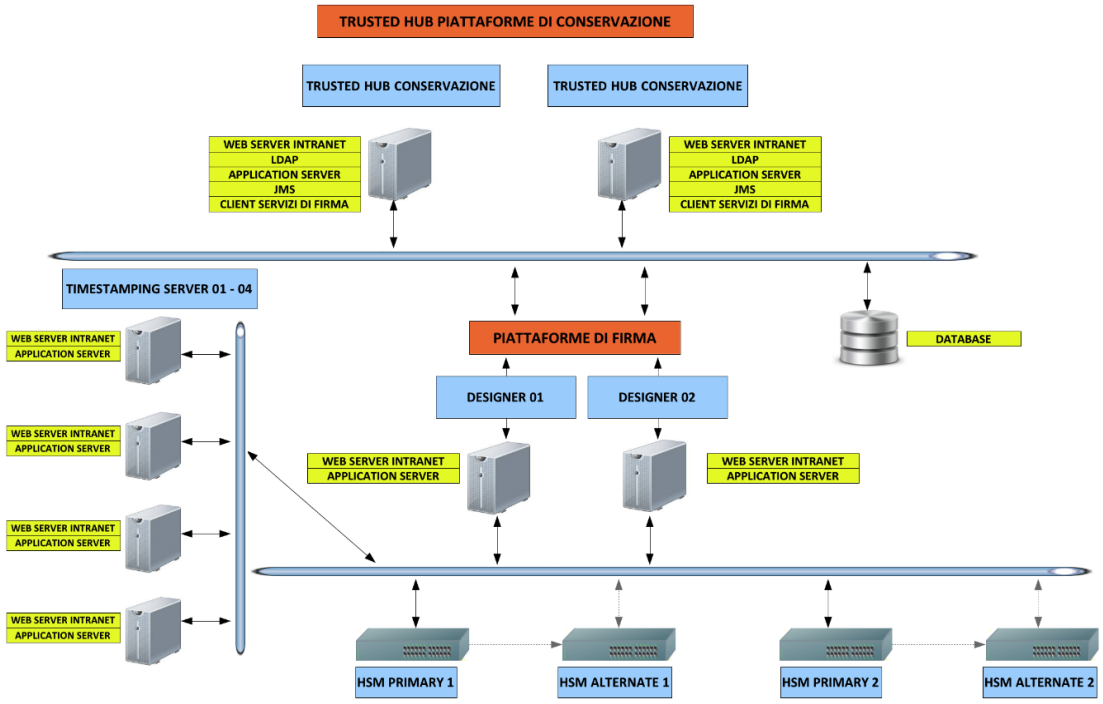


*Figura 1: Componenti tecnologiche*

## 8.3 Physical components

For the provision of the preservation service, the most advanced version of VMware Virtual Machine technology, ESXi, has been adopted.

The following is a description of the technological components of the preservation sites:

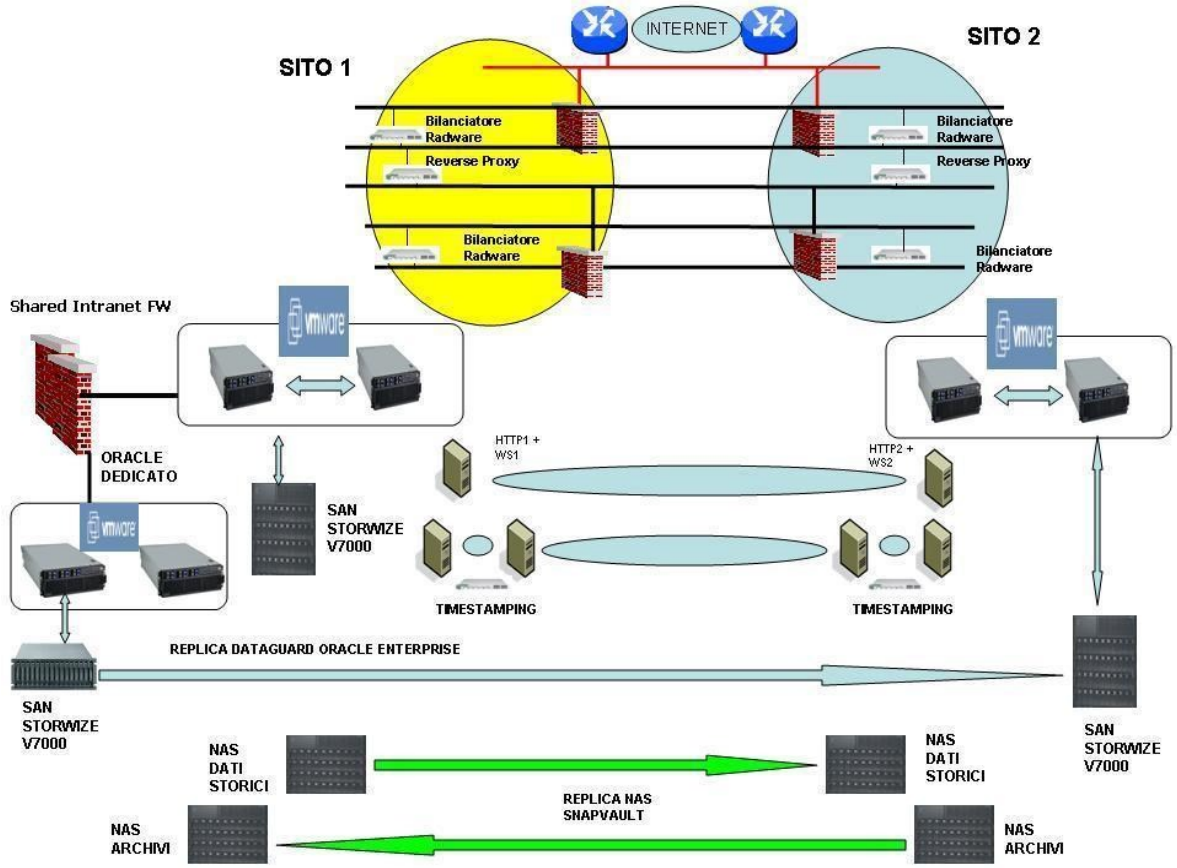


*Figura 2: Componenti fisiche dei siti di conservazione*

The VMware environment is built using the latest generation IBM xSeries servers that share, via dual fibre optic switches for cross and redundant connections, multiple Storwize V7000 Storage Area Networks (SAN) with SSD TIER to ensure high performance.

The VMware platform adopts concepts already widely tested and consolidated in Enterprise Mainframe environments, where completely isolated and dynamically manageable partitions are created on extremely reliable and scalable hosts, both in terms of resources and storage.

Virtual machines (VMs) utilize high-level HW storage in a shared or direct manner, which guarantees Vmotion operations (moving the VM from host to host without interrupting activities). VMs can be defined with extreme flexibility, meeting horizontal and vertical scalability requirements.

Through the Virtual Center, resources (CPU, RAM, I/O, network) can be dynamically modified to optimize the performance of each individual VM.

## 8.4 Management and evolution procedures

### 8.4.1 Operation and maintenance of the preservation system

The Intesa preservation system has been structured with the aim of pursuing the management and maintenance of documents and the platforms dedicated to them, as well as maintaining control and the evolution of the platforms.

The management of the preservation system is carried out by the designated figures based on the type of activity to be performed and actions to be taken.

The various operating departments of Intesa respectively carry out the activities within their competence based on a coordination aimed at a unified vision of the system.

The activities are classified into:

- System activities: maintenance of the infrastructure components and their evolution, monitoring of the correct functioning of the structure;
- Application and software management activities: management of evolution and corrective and evolutionary actions, application releases, workflow and procedure development;
- Specific application monitoring activities for the Client: daily monitoring of platform processes and workflows;
- Customer support activities: support in response to anomalies reported to the helpdesk structure;
- Hardware maintenance activities: management and maintenance of the hardware infrastructure in order to guarantee its proper functioning. Planning of any intervention actions.

Intesa's organization responds with increasing efficiency to Clients' requests for intervention, being able to leverage the continuous acquisition of experience on the specific service.
The Maintenance Managers themselves, regarding Intesa's in-house software products, suggest implementations in terms of evolutionary maintenance; for Third Party products, they represent the defined counterpart towards the Manufacturer or Distributor to report problems, requests, improvement proposals, and to propose specialized interventions at the Client's site.

When an anomalous behavior of the service/product is highlighted (not conforming to the relevant specifications), the corrective maintenance process is activated.

Corrective/evolutionary maintenance includes a procedural sequence of phases, aimed at ensuring the completeness and effectiveness of the corrections/implementations carried out:

- Anomaly detection (for Corrective Maintenance cases) and/or need for intervention (for Evolutionary Maintenance cases);

- Diagnosis, approval, and assignment;
- Correction;
- Testing;
- Release;
- Propagation.

### 8.4.2 Monitoring and Security

The preservation system includes adequate technological and infrastructural measures aimed at guaranteeing high reliability and disaster recovery in line with the requirements of the relevant legislation and with market best practices.

According to the provisions of the Guidelines on the formation, management and preservation of electronic documents par. 4.10, private entities belonging to organizations that already adopt specific sector regulations for the security of information systems adapt the preservation system to these regulations.

In the provision of Intesa's Trusted Doc e-archiving service, security aspects comply with the principles expressed by:

- Intesa's corporate policies;
- ISO 27001 certification, integrated with the ISO 27017 and 27018 certified guidelines, for the specific purposes of: generation/issuance of electronic documents, digital archiving and legally compliant electronic preservation, and production of electronic signature solutions, advanced electronic signature, qualified electronic signature, certified electronic mail;
- the Personal Data Protection Code, as per Legislative Decree no. 196 of 30 June 2003;
- The European Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

Information security involves physical, logical, and management elements, and its management is implemented under various aspects:

- Physical and logical infrastructural security;
- Application logical security;
- Continuity.

To address the needs for data and information protection, a specific system is defined that meets the following criteria:

- Protect the transmission of information against data loss, unauthorized disclosure, or modification;
- Allow access to service delivery systems only to those who need it (in relation to specific responsibilities) and provide the consequent authorizations;

- Conduct appropriate checks to ensure that control mechanisms are effectively functioning.

Regarding logical security from a structural point of view, the planned procedures relate to:

- Security administration;
- Protection of delivery environments;
- User identification and authentication;
- Authorization for access to information at different levels.

and are developed in the following directions:

- Guarantee of the confidentiality of the information transmitted by the Client through the use of an appropriate network architecture;
- Guarantee of the integrity of the transmitted data through the use of appropriate and advanced communication protocols;
- Guarantee of the archived data through controlled authorizations provided by specific computer applications (e.g. ACL).

Regarding confidentiality, the basic software products used and the management procedures adopted are designed to ensure the Client that:

- Their information is logically identified and access to it is allowed only to authorized personnel;
- Access authorizations are currently valid and under control;
- In the event of any violations, reporting procedures are available and review procedures for such attempts are active.

### 8.4.3 Logs management and Preservation

The preservation system catalogs access logs to the operating system and platform applications. These logs are subject to relative preservation.

Furthermore, Intesa maintains at its infrastructure, and makes available to the Client in case of audits, the reception logs of flows forwarded by the Client and the application logs of the processing carried out on Intesa's systems, for 90 (ninety) days respectively from the date of receipt and processing.

During the Service provision phase, Intesa provides its management structure in order to monitor the correct progress of data flows and take appropriate actions in case of malfunctions, errors, and critical situations in general.

It should be noted that Intesa's process is managed on a single document basis, thus allowing complete, simple, and effective monitoring.

In the first analysis, the monitoring activity refers to:

- ACK 1: execution of the internal workflow related to the processing of documents and their web publication (acceptance of submission packages);
- Submission Report;
- ACK2: (archiving report) execution of the internal workflow related to compliant preservation; a flow is generated containing the list of all documents belonging to the preservation package and the relative outcome of the operation, and in case of error, the indication of the type of error encountered. The return flow indicates the unique code relating to the assigned preservation package.

For each flow, Intesa sends the various outcomes (ACKs) to the Client using standard CSV format record layouts, or based on the formats agreed with the Client, allowing a possible reconciliation of the status on their own systems.
These reports can also be forwarded via e-mail to the company contact person, based on what has been agreed with the Client.

### 8.4.4 Change management

The initiation of this procedure, known as Change Management, is executed by Intesa with the aim of tracking all evolutions and modifications made to the development objects used for application implementations through a dedicated versioning tool.

A CHANGE is defined as any installation or modification of Hardware, Software, or Procedures that alter the production environment used for the provision of services to the Client.

The Change request can originate from various sources, such as: Client request, internal request made by the Project Manager; Application Management request; or anyone who needs to make a modification within, generally, the Delivery department.

Once a modification request (Change) is received, the IT function performs the necessary checks on the shared information, assesses the impacts and assets involved, and plans the Change date by evaluating the risk and feasibility, describing the intervention in detail. After preparing the documentation and completing the required checks, approval is requested from the manager, if necessary.

At the end of the Change activities, whose procedures and modifications are adequately monitored and tracked, the IT function conducts functional and non-regression tests to ensure the success of the Change. All activities carried out are recorded, and any negative results of the acceptance tests are reported to the competent teams.

### 8.4.5 Periodic compliance checks and reference standards

The Head of the Preservation Service verifies the preservation system in its various components, logical, technological, and physical, in accordance with the requirements of the Guidelines, with reference to the obligations entrusted by the Preservation Manager, through the signing of the letter of entrustment, and to the phases of the preservation process.

These verifications are carried out in compliance with internal audit procedures, documented by company operating instructions and reported through the relevant minutes of execution and outcome.

# 9 Monitoring and checks

The Intesa preservation system includes the adoption of specific measures and tools to promptly detect any degradation of storage systems and records and, where necessary, to restore correct functionality.

To counteract the progressive obsolescence of file formats and extensions, especially in relation to relatively long preservation periods, it is a fundamental part of the deposit agreements that the documents sent by the Holder are drafted in file formats recommended for preservation, as provided for by Annex 2 of the AgID Guidelines. The available tools allow the verification and monitoring of the correct functionality of the preservation system, at the level of system and application management of its various components.

A dedicated Help Desk service is available for any problems relating to access or any anomalies in the transmission of documents.

The Intesa system and application monitoring system identifies specific anomalies in the preservation system and notifies them through specific alerts to management groups organized by competence.

These groups take charge of the problem, interacting, if necessary, with area specialists (such as: platform, physical infrastructure, connectivity, DB, specific application services) and following the entire procedure until resolution. The actions taken are documented in specific system logs, entered in the internal repository defined by the company quality system.

To ensure correct management of the preservation system, Intesa prepares a chronological register of the software of the programs used, documenting the different versions that have followed over time. In addition, a chronological register of events relating to the management of the preservation system is drawn up, which includes the resolutions adopted to correct any anomalies.

## 9.1 Monitoring procedures

For the purpose of monitoring the preservation system, Intesa adopts tools and procedures aimed at analyzing the various components of the system, identifying any anomalies, and allowing the intervention and involvement of the competent figures for resolving critical issues.

The control and management of the Preservation system are based on the continuous monitoring of the environment and its individual components, through the tools indicated below, in order to ascertain the conformity of the fundamental parameters of the service to the contractual and quality requirements:

- The centralized and controlled management of service delivery operations is regulated by specific procedures and tools that guarantee:
- Constant monitoring of service levels through the monitoring of the environment and critical elements, including the execution of management activities such as checking available space, ensuring that threshold levels are not exceeded, and simulating log-ons to check service availability;
- Monitoring the performance of the Service, the preparation or verification of tests and periodic backups of data or libraries, and the possible preparation of input data and verification of results;
- Managing changes to Service parameters (e.g., user authorizations, passwords) to quickly adapt to the Client's changing needs;
- Managing security and access to services to prevent intrusions and unauthorized access, structured on different levels (Network, System, Application Service) and supported by advanced technological solutions, managed by dedicated company roles that carry out continuous monitoring activities and periodic checks on the completeness and validity of the solutions adopted (e.g., penetration tests);
- The controlled execution of any variation to the operating environments (HW, SW, etc.). Every "Change" request must be documented, justified, analyzed, and authorized. A severe and preventive impact analysis, carried out by the most qualified personnel, an execution concentrated in specific time "windows" located in periods of low usage, and an exhaustive test, particularly aimed at verifying backward compatibility, tend to minimize the risks of service interruptions;
- The continuous maintenance and updating of the HW and SW configurations related to each managed environment, allowing for the historical identification of the technological components involved in the delivery of each service to better plan any modification and recovery activities;
- The optimal management of service interruptions, planned or unforeseen, with particular design activities carried out to circumscribe and limit the impact of possible malfunctions and automatically or promptly activate alternative solutions (e.g., routing, switch, etc.);
- The resumption of activities in case of problems through appropriate and automated backup activities of environments, libraries, applications, and data, allowing a regulated recovery (total, sectorial, or partial) of resources for a prompt restart of interrupted Services;
- The maintenance of a high level of availability and reliability of individual technological components through specific scheduled maintenance contracts. Interventions aimed at preventing possible

hardware problems are carried out periodically by expert personnel;
- The maintenance of an appropriate work environment for the activities to be performed.

### 9.1.1 Monitoring systems

The INTESA monitoring system is currently present in parallel on two checking platforms:

- NAGIOS/NIMS+ module;
- CHECKMK module.

#### NAGIOS/NIMS module

The module is currently hosted on the LINUX RED HAT operating system and distributed across two servers, named FE and BE. The system configuration is designed to ensure high service availability. To this end, several additional plug-ins have been developed, integrated with the native ones of the Nagios open-source product. This implementation has allowed the addition of various functionalities to the system that would otherwise not have been available, thus contributing to its operational enrichment.

Each monitoring plug-in is designed to manage not only the specific check to be performed but also the reference parameters and the thresholds or rules to identify the attention levels. Each plug-in operates autonomously according to its own schedule, allowing more or less frequent monitoring based on the specific needs of the object or functionality to be monitored.

The system allows articulated monitoring on three different levels:

- Infrastructural monitoring (host alive, service up/down, TCP/IP ports);
- Application Monitoring specifically configured on the preservation system (web appl checks), and on explicit query probes of various application flows, through multiple SQL queries, directly on the various DATABASES (SQL QUERY functionality present on the NIMS+ software package);
- Business monitoring, provided as a configurable service, through programs that track the availability of checks and are therefore able to produce reports for SLA / KPI purposes.

#### CHECKMK Module:

The module in question is also installed on two balanced servers with a LINUX RED HAT operating system.

The system is configured to guarantee high service availability and remains open for the development of new controls upon request, which can be developed using programming languages. Several additional plug-ins have been created beyond the Nagios/NIMS+ platform. Specifically, the following types of controls are currently present:

- Verification of filesystem and disk sizes, both physical and virtual;
- Verification of NAS volume sizes;
- Controls on Websphere / applications;
- Access and reachability via HTTP(S) to web portals;
- Healthcheck statuses on various applications, in continuous migration (e.g., spring actuator, certificate expirations, etc.);
- Business monitoring has been implemented as a service within the CHECKMK product, which records the availability of controls and allows the generation of reports for SLA / KPI management.

Both modules allow profiling operator users to provide each of them with one or more consultation accounts, based on the specific control activities assigned. Each operator can be assigned visibility on specific plugins (ACL) and user access to one or more service groups. All controls performed are rationalized to verify the status of the various application layers through standardized and customized probes based on specific needs and agreements on SLOs, SLAs, and KPIs agreed with the Client, currently for both monitoring platforms.

## 9.2 Integrity check of the Archives

Archival packages are stored by Intesa on separate storage media in high-reliability mass storage (NAS) and automatically redundantly on geographically distinct sites.

The preserved electronic documents are subject to specific checks/tests to guarantee their integrity over time, for the entire duration coinciding with the legal obligations relating to the type of documentation and scope (e.g., 10 years for tax documentation), as well as based on what is agreed with the Client.

Intesa verifies the state of preservation of the archival packages, providing notification, if necessary, to the Client's Preservation Manager of any anomalies found and providing support to correctly define projects for data migration, based on the requirements of both paragraph 3.7 and Annex 2 of the Guidelines.

The testing process includes an integrity check of all documents, organized in logical archives and stored in different sites, and a consistency check on a specific sample of documents.

Integrity checks relate to the non-alteration of data over time, consistency checks are performed in relation to:

- Exhibition (readability on a sample basis, verifiability);
- Verification of the expiration date related to the time stamp;
- Correctness and consistency with the metadata.

The outcome of the completion of operations and verification is reported in a specific section on the company repository.

## 9.3 Solutions adopted in case of anomalies

Anomalies in the preservation system can be identified by Intesa personnel responsible for management and monitoring activities, who directly create a record in the problem management system involving staff assigned to corrective actions, or by a Client user who reports it to the Help Desk (corrective maintenance).

Conversely, the need for a new functionality can arise from a Client request/order, an internal proposal from the Head of Service, or a suggestion from a support member who identifies a possible improvement (evolutionary maintenance).

The process for resolving anomalies or performing corrective/evolutionary maintenance involves the following operational phases:

- Detection of anomaly and/or need for evolutionary intervention;
- Diagnosis and assignment: this phase involves diagnosing the cause of the malfunction (in cases of corrective maintenance) or the feasibility of integrating the new functionality into the product/service (in cases of evolutionary maintenance) and assigns it to the most suitable person;
- Correction/evolution: identification of the software objects responsible for the malfunction or the new functionality and making the necessary corrections. In the case of a blocking problem, a bypass may be activated during this phase to provide an immediate solution that allows continued use, possibly even to a reduced extent;
- Testing: verification that the modified product/service resolves the reported malfunction or meets the new functional requirements and testing the non-regression of the corrections made. Tests are carried out with particular attention to the non-regression aspects of the changes made to other components of the application. Subsequently, the changes are also applied to other current versions of the product/service. All activities and results of the product/service maintenance are recorded in a specific IT application, which constitutes an important database valid for a review of product quality and anomaly reports by each client;
- Release: the modified product/service or application is made available to the Client / Principal for use;
- Propagation: the modification is propagated, if foreseen, to other target platforms of the product/service or application;
- Post-sales support structure: the post-sales support structure is provided through Intesa's Customer Care (Helpdesk).

Monitoring activities, supported by specific automatic mechanisms, highlight any problems or the risk of them occurring. Appropriate corrective actions are taken promptly to avoid deterioration of the service. In addition to their resolution, events are recorded using tools to support logging and analyzed to update, if necessary, the security measures in place.

Furthermore, a Customer Care “Help Desk” service is available to Clients, composed of personnel trained in preservation procedures and in verifying the availability and status of services.

The customer support structure is organized on 2 levels:

1. **First-level help desk**

It takes charge and registers the call, provides assistance on system functionalities, identifies and resolves the problem encountered by the user if possible, or forwards it to the second level of competence. It also notifies the user of the resolution of the problems they reported at the end of the intervention cycle, using the предусмотренные access/contact channels.

The main tasks of the Help Desk structure are:

- Provide assistance to Customers to ensure continuity in the provision of services;
- Provide information on services;
- Receive and register problem reports;
- Analyze problems, assign a level of severity, and provide a resolution, which may be temporary or provisional (first-level support);
- Involve experts who provide second-level support, i.e., specialists with specific skills in the relevant area, if the problem cannot be resolved directly;
- Maintain continuous contact with the Customer to keep them informed about the resolution of critical problems affecting them;
- Close problems jointly with the Customer, communicating the resolution.

Each identified solution is verified for completeness and effectiveness by the resolver before being provided to the customer.

Throughout the problem management phase, the Help Desk structure continuously monitors the progress of solutions and takes any necessary follow-up actions with the experts responsible for defining them, to ensure that they are implemented within the set targets.

A specific IT application (HDA) supports the execution flow and registration of reports.

Specific indicators and adequate reporting ensure effective control of the functionality and effectiveness of first and second-level support and the achievement of the expected service levels.

2. **Second-level support:**

It consists of specialists in the services and products being supplied. They are called upon by first-level support whenever the latter is unable to resolve a problem raised by the user.

The second-level structure is therefore not an organizational unit, but a virtual structure that extends horizontally depending on the technical areas of expertise and vertically also to higher levels of specialization. The second-level structure therefore includes groups with system skills, with the task of resolving problems of such complexity that they cannot be resolved by the first-level help desk, to which they will communicate the end of the intervention, or application skills with the task of resolving problems of such complexity that they cannot be resolved by the first-level help desk, to which they will communicate the end of the intervention.

3. **Trusted Doc (Legal Archiving) specialist support**

This is a second-level structure, operating in the application area, created specifically for compliant archiving projects.

This structure supports the Customer on specific issues concerning the preservation process, in communications relating to the operational management of the Trusted Doc Service, carrying out its functions in close collaboration with the Project Manager and with Intesa's specialist figures with technical-regulatory skills.

## 9.4 Protection of personal data

The service is provided by Intesa as Data Processor for the protection of personal data, as better described in the relevant contractual documentation.

Furthermore, the service is subject to the management and control rules stipulated by the UNI ISO 27001, 27017, and 27018 certifications in use, which guarantee compliance with information security controls and data security and protection controls.

Therefore, the roles, responsibilities, processing methods, and security procedures are structured in compliance with the regulatory provisions and the qualification procedures of the aforementioned service.

*-----END OF THE DOCUMENT-----*