# Conservation Manual

*INTESA SPA*

MDC_V15112021

**Issued**

| Action | Date | Name | Role |
|---|---|---|---|
| Drafted by | 15/11/2021 | Francesco De Cesare | SCS consultant |
| Verified by | 15/11/2021 | Luigi Traverso | Conservation Service Manager |
| Approved by | 15/11/2021 | Luigi Traverso | Conservation Service Manager |

**Revisions log**

| Ver. /Rev./Draft no. | Issued on | Changes made | Notes |
|---|---|---|---|
| MDC_V22102014 | 23/10/2014 | Additions and clarifications requested by AgID | AgID requests |
| MDC_V24112014 | 24/11/2014 | Clarifications regarding roles and responsibilities | AgID requests |
| MDC_V29012016 | 29/01/2016 | Adaptations to reflect template version 2_1 published by AgID | AgID requests |
| MDC_V14062021 | 14/06/2021 | Various adaptations | Introduction of AGID Guidelines |
| MDC_V24092021 | 24/09/2021 | Professional roles update | Change of personal data processor |
| MDC_V15112021 | 15/11/2021 | Company logo update | Change to corporate structure |

Intesa

# Contents

# 1 Purpose and scope of document

This manual describes the conservation system provided by In.Te.S.A. S.p.A. (hereinafter Intesa) named Trusted Doc. It sets out the qualifications, roles and responsibilities of those involved in the document conservation process and the operating model. It contains a description of the process, architectures and infrastructures used, the security measures adopted and all other information useful to managing and overseeing the operation of the conservation system.

In particular, it describes the operating procedures adopted by Intesa for electronic conservation provided via a dedicated Service to the Client.

Intesa also provides qualified trust services (as QTSP – Qualified Trust Service Provider) in accordance with Reg. (EU) 910/2014 (eIDAS) for electronic signatures, electronic seals and timestamps.

The document describes the procedures adopted by Intesa in accordance with the provisions of the contract entered into between the parties and the relevant Technical Annex, in compliance with the relevant regulatory requirements and practices.

The manual summarises the tasks described in the Italian Digital Administration Code, hereinafter also "CAD" (Italian Legislative Decree no. 82 of 7 March 2005, and subsequent amendments/supplements).

## 1.1 Scope of reference

The conservation Service provided on a fully outsourced basis is underpinned by Article 44 of the CAD, according to which conservation can be carried out by assigning the task, on a full or partial basis, to other public or private entities that offer adequate organisational and technological guarantees and ensure the protection of personal data.

The Client, i.e. the owner of the stored material, entrusts the conservation process to Intesa and its internal managers serving the various roles provided for by the regulations, described in the relevant section of this Conservation Manual, titled "Roles and Responsibilities".

Annex A of the Technical Specifications outlines the specific details of the Service for the Client.

## 1.2 Conservation Manual Structure

This Manual is produced in digital form by Intesa (in collaboration with the Client as regards the Technical Specifications) and stored in a dedicated repository of the Service, used internally by Intesa and made available to the Client.

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

In the event of any updates and changes made by either party to the Technical Specifications, a copy shall be sent to the Head of Conservation and/or Client's Project Manager.

This document partially describes existing architectural aspects and processes. For more technical/operational details, see the following documents:

- conservation Service Contract;
- Technical Specifications (Annex A of the Conservation Manual) – previously referred to as the Specific Details of the Contract;
- Any Functional Analysis document concerning aspects relating to the technical implementation of the conservation Service, not annexed to this Conservation Manual but prepared based on the specific context of the Client's project.

# 2 Terminology (glossary and acronyms)

## 2.1 Acronyms

The main acronyms used in the document and relevant definitions are listed here below:

| Acronym | DEFINITION |
|---|---|
| **AgID** | Digital Italy Agency [Agenzia per l'Italia Digitale] |
| **CAD** | Italian Digital Administration Code [Codice dell'amministrazione digitale], Italian Legislative Decree no. 82 of 7 March 2005, and subsequent amendments and supplements |
| **IPdA** | Archival Information Package Index – electronic evidence associated with each archival information package containing a set of information expressed according to the SInCRO standard |
| **IPdV** | Submission Information Package Index |
| **LLGG** | Guidelines on the creation, management and conservation of computerised documents |
| **CM** | Conservation Manual |
| **AIP** | Archival Information Package |

| | |
|---|---|
| **DIP** | Dissemination Information Package |
| **SIP** | Submission Information Package |
| **HC** | Head of Conservation |
| **CSM** | Conservation Service Manager |
| **SSSM** | Conservation Systems Security Manager |
| **ASM** | Archival Conservation Manager |
| **PDP** | Personal Data Processor |
| **SISM** | Conservation Information Systems Manager |
| **DMM** | Conservation System Development and Maintenance Manager |
| **SR** | Submission Report |
| **SInCRO** | Support for interoperability in the conservation and retrieval of digital objects [Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali - UNI11386] - Italian standard, in xml language, concerning the structure of the set of data supporting the conservation process |
| **SLA** | Monitoring of the fulfilment of service levels |

## 2.2 Glossary of terms

A glossary of the terms used in the text and relevant definitions are provided here below:

| Acronym | DEFINITION |
|---|---|
| **Reliability** | A characteristic that, when used to refer to a document management or conservation system, expresses the degree of trust that the user places in that system. When used to refer to the electronic document, meanwhile, the term expresses the credibility and accuracy of the representation of acts and facts |

| | |
|---|---|
| | contained therein. |
| **Annex A** | The technical specifications section of this manual; it contains a description of the detailed elements of the conservation process. |
| **Authenticity** | Characteristic on the basis of which an object can be considered to correspond to what it was at the original moment of its production. As such, an object is authentic if it meets the criteria of both integrity and completeness, having not undergone any unauthorised changes over time or space. Authenticity is assessed on the basis of specific evidence. |
| **Conservation Provider** | A public or private entity that performs electronic document conservation activities. |
| **Conservation** | Set of activities aimed at defining and implementing the overall policies of the conservation system and governing their management in relation to the organisational model adopted, guaranteeing the characteristics of authenticity, integrity, legibility and retrievability of the documents over time. |
| **Electronic document** | Electronic document containing the representation of acts, facts or legally relevant 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 group of documents on the basis of which it is found not to have undergone any unauthorised changes over time or space. The characteristic of integrity, together with completeness, contribute to determining the characteristic of authenticity. |
| **Interoperability** | The characteristic of an information system, with public and open interfaces, which is capable of interacting automatically with other information systems to exchange information and provide services. |
| **Guidelines** | Guidelines on the creation, management and conservation of computerised documents published in the Italian Official Gazette no. 259 of 19 October 2020. |
| **Conservation Manual** | Electronic document that describes the conservation system and outlines in detail the organisation, the persons involved, the roles performed by those persons, and the operating model, as well as providing a description of the process, architectures and infrastructures. |
| **Conservation system security plan** | Document that, in the context of the general security plan, describes and plans the activities aimed at protecting the electronic document conservation system against potential risks. |
| **Qualified service** | Entities that issue qualified certificates in accordance with Regulation (EU) no. |

| | |
|---|---|
| **provider** | 910/2014 of the European Parliament and Council of 23 July 2014 (eIDAS) |
| **Trusted Doc** | The Intesa conservation service, provided on an outsourced basis |
| **Trusted Hub** | Technological platform of the conservation service provided on an outsourced basis by Intesa |

# 3 Applicable regulations and standards

## 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
- 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.
- REGULATION (EU) NO. 910/2014 OF THE EUROPEAN PARLIAMENT AND COUNCIL of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND 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)
- 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 Applicable standards

The standards that apply to Intesa are:

- ISO 14721:2012 OAIS (Open Archival Information System);
- ISO/IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems – Requirements;
- 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;
- UNI 11386:2020 SInCRO Standard - Support for Interoperability in the conservation and Retrieval of Digital Objects;
- ISO 15836:2009 Information and Documentation - The Dublin Core Metadata Element Set.

# 4 Roles and responsibilities

The roles involved in the conservation system are the following (potentially among others):

- Owner of the stored material;
- SIP producer;
- Authorised user;
- Head of Conservation;
- Conservation Provider.

The owner of the stored material is the entity that produces the stored digital objects.

The SIP producer is a natural person, usually different from the entity that prepared the document, who produces the submission information package and is responsible for transferring its content to the conservation system. It is usually the person tasked with producing and/or managing the documents and/or relevant metadata to be sent to the conservation system, and is responsible for the content of the document.

If the conservation service is entrusted to third parties, the SIP producer generates the submission information packages and sends them to the conservation system according to the procedures and formats agreed upon with the Conservation Provider and described in the conservation system Conservation manual. They also verify the successful completion of the transfer to the conservation system, by checking the submission report generated by the conservation system.

The authorised user is the person, entity or system that interacts with the services provided by an electronic document management system and/or an electronic document conservation system, in order to use the information in question; they submit a request to the conservation system to access the documents, to obtain the information in question within the limits provided for by law. As such, the authorised user corresponds to the Client or persons authorised to access the documents.

The Head of Conservation defines and implements the overall policies of the conservation system and has full and independent responsibility for governing its management.

Under their own responsibility, the Head of Conservation can delegate their tasks to one or more persons with specific qualifications and experience within the organisational structure. Such delegation, to be specified in the Conservation Manual, must include identification of the specific duties and competences delegated.
If the conservation service is entrusted to a conservation Provider, all or some of the aforementioned tasks, with the exception of preparing and updating the Conservation Manual, may be entrusted to the service manager, with it however being understood that general legal liability regarding the conservation processes cannot be delegated and, therefore, remains with the Head of Conservation, who is also required to perform the necessary supervision and oversight activities pursuant to regulations governing the services outsourced by the public administration bodies.

As such, the Client appoints its Head of Conservation who, in turn, having the capacity and authorisation to do so, entrusts the electronic conservation process to Intesa.

The Head of Conservation remains responsible for overseeing the proper performance of the storage process. The conservation Provider is contractually liable to the Client.

The identification details of the Head of Conservation are included in the Technical Specifications and, following the award, the conservation process is entrusted to the conservation Provider.

The conservation Provider is the public or private entity that performs electronic document conservation activities.

## 4.1 Details of roles and related tasks

In order to guarantee that the services offered meet an adequate and satisfactory quality standard, Intesa adopts a process-based organisational structure. As such, the applicable general framework of procedures and relevant competences and responsibilities is defined at a company level.

Each operator, individually or as part of a team and according to their competences, adheres to the content of the procedures and the company instructions developed.

Activities are assigned based on defined company roles.

The conservation process is also implemented according to this organisational framework, as regards both the provision and monitoring aspects.

The responsibilities of Intesa, in its capacity as conservation Provider to which the conservation service has been entrusted, are set out in the Technical Specifications provided to the Client in accordance with regulatory provisions.

Also as required by the regulations, Intesa performs its role with the utmost care and oversight, via a specialist group of employees in the form of a permanent team, internal to the company, dedicated to providing, managing, supporting and overseeing the Service. This guarantees the presence of qualified staff, diversified based on the specific requirements, with appropriate professional experience and technical knowledge, available to engage with the Client's Head of Conservation throughout the various stages of the Service.

The roles defined within the Intesa organisation and performed in the context of the conservation process are described here below. Specific details are included in the Technical Specifications.

### 4.1.1 Head of Conservation

The Head of Conservation is the Client – represented by the natural person formally appointed from within the company that owns the stored documents – and is responsible for the set of activities aimed at ensuring the conservation of the electronic documents covered by the outsourcing contract awarded to Intesa.

In managing the overall conservation process, the HC guarantees – both to the entity for which they work and to the tax authorities – the proper management of the process in accordance with established and documented security principles, adopting traceability procedures to guarantee proper management of the information packages, and the conservation, accessibility and display of individual documents.

The Head of Conservation works within their organisation in collaboration with the Personal Data Processor, the Security Manager, and the Information Systems Manager.

The activities of the Head of Conservation, in collaboration with the conservation Provider, are critical at various stages of the conservation process:

- at the stage of applying the seal to the archival information package index and the dissemination information package; Intesa has chosen to work on individual documents or individual pieces of electronic evidence;
- the Head of Conservation, in collaboration with the conservation Provider, sets out details, in the Technical Specifications, of the situations that require the presence of a public official/notary, if required for the type of document handled or the specific process defined in agreement with the conservation Provider;
- the Head of Conservation prepares the Conservation Manual, in collaboration with the conservation Provider, including a description of the specific details of the project.

### 4.1.2 Conservation Service Manager

The tasks of the Conservation Service Manager are as follows:

- defining and implementing the overall policies of the conservation system, as well as oversight of conservation system management;
- defining the characteristics and requirements of the conservation system in accordance with applicable regulations;
- proper provision of the conservation service to the producer;
- managing conventions, defining the technical and operational aspects and validating the Technical Specifications that set out the detailed aspects and operating procedures involved in providing the conservation services.

### 4.1.3 Archival Conservation Manager

The Archival Conservation Manager handles the task of configuring the conservation process, in collaboration with the Development and Maintenance Manager.
This is the figure that performs the following tasks, via the dedicated company team:

- defining and managing the conservation process, including the procedures governing transfer by the producer and the acquisition, verification of integrity, and archival description of the documents and groups of documents transferred, as well as the display, access and use of the stored document and information assets;
- defining the set of conservation metadata for the electronic documents and files;
- monitoring the conservation and archival analysis process to develop new conservation system functionalities;
- collaborating with the producer as regards transfer to conservation, selection, and managing dealings with the Ministry of Cultural Heritage and Activities for matters within its remit.

### 4.1.4 conservation Information Systems Manager

The tasks of the Conservation Information Systems Manager are as follows:

- managing operation of the hardware and software components of the conservation system
- monitoring fulfilment of service level agreements (SLAs) entered into with the producer
- reporting any non-compliance with the SLAs to the Conservation Service Manager and identifying and planning the required corrective measures
- planning development of the technological infrastructures of the conservation system
- monitoring and overseeing the levels of service provided by third parties and reporting any non-compliance to the Conservation Service Manager.

### 4.1.5 Conservation System Development and Maintenance Manager

The tasks of the Conservation System Development and Maintenance Manager are as follows:

- coordinating the development and maintenance of the hardware and software components of the conservation system;
- planning and monitoring conservation system development projects;
- monitoring SLAs relating to conservation system maintenance;
- interfacing with the producer concerning procedures for transferring the electronic documents and files as regards the electronic formats to be used, the technological evolution of hardware and software, and migration to new technological platforms where applicable;
- managing the development of websites and portals connected to the conservation service.

### 4.1.6 Conservation System Security Manager

The tasks of the Conservation System Security Manager are as follows:

- complying with and monitoring the conservation system security requirements set out in the standards, regulations, and internal security policies and procedures;
- reporting any non-compliance to the Conservation Service Manager and identifying and planning the required corrective measures.

### 4.1.7 Personal Data Processor

The tasks of the Personal Data Processor are as follows:

- ensuring compliance with applicable provisions on personal data processing;
- ensuring that the data provided by the Clients are processed in accordance with the instructions given by the Data Controller, subject to a guarantee of security and confidentiality.

# 5 Organisational structure for the conservation service

Intesa's organisational structure is based on a vision of management that aims to focus on certain key figures in the specific roles required for the conservation process.

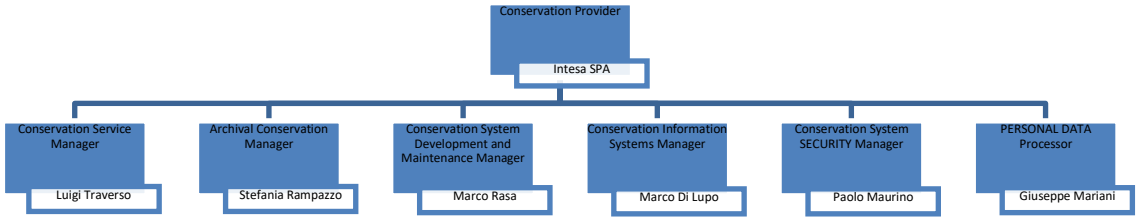
Intesa has identified and appointed the professional figures that make up the document conservation work team.

The team consists of employees from across various company departments, to ensure proper performance of the service with regard to all technical/organisational issues specific to the service in question.

As such, appropriate internal organisational procedures have been defined to ensure streamlined coordination of the employees in the team, so that their work is performed in a manner fully consistent with the content of the service and the quality objectives of the company.

## 5.1 Organisational chart

Intesa's internal organisational chart is provided here below. It indicates the company departments and roles involved in the conservation system:



## 5.2 Organisational structures

Intesa's internal organisational chart is provided here below. It indicates the company departments and roles involved in the conservation system:

| Legend | |
|---|---|
| **HC** | Head of Conservation |
| **CSM** | Conservation Service Manager |
| **CSSM** | Conservation System Security Manager |
| **ACM** | Archival Conservation Manager |
| **PDP** | Personal Data Processor |
| **CISM** | Conservation Information Systems Manager |
| **DMM** | Conservation System Development and Maintenance Manager |

| **Activities covered by the role of conservation service managers** | | | | | | |
|---|---|---|---|---|---|---|
| | **Responsibility** | | | | | |
| | **CSM** | **CSSM** | **ACM** | **PDP** | **CISM** | **DMM** |
| Setting up the conservation service (after a contract has been signed) | X | X | X | X | X | X |
| Acquiring, verifying and managing the submission information packages accepted, and generating the submission report | X | X | X | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| Preparing and managing the archival information package | X | X | X | | | X |
| Preparing and managing the dissemination information package for the purposes of display, and making duplicates and electronic copies as requested | X | X | X | X | | X |
| Disposing of the archival information packages | X | X | X | | X | X |

| | **Information systems management activities** | | | | | |
|---|---|---|---|---|---|---|
| | **Responsibility** | | | | | |
| | **SSM** | **SSSM** | **ASM** | **PDP** | **SISM** | **DMM** |
| Operating and maintaining the conservation system | | X | | | | X |
| Monitoring the conservation system | | X | | | X | X |
| Change management | X | X | | | X | X |
| Periodically verifying compliance with applicable regulations and standards | X | | X | X | | |

# 6 Objects submitted for conservation

## 6.1 Stored objects

The Intesa conservation system has functionality to ensure the conservation – from the time of acceptance from the producer to disposal, where applicable – according to technological procedures, of the following objects: electronic documents and their metadata (conservation information).

The digital objects stored are handled by the conservation system in information packages that can be subdivided as follows:

a) Submission information packages;
b) Archival information packages;
c) Dissemination information packages.

The conceptual model governing long-term conservation is the OAIS model, based on the creation, archiving and conservation of information packages, which are entities made up of four elements:

- the electronic content, i.e. the digital object (to be stored) and the set of information that enables it to be represented and understood at a user level;
- the conservation information, including information on identification, context, origin and integrity;
- the information on "packaging", i.e. data that indicate the logical location of the archival information package in the Intesa conservation system;
- the stored objects including a description of the types, conservation information, representation information, intervals of sending for conservation, conservation duration period, accepted file formats provided, regulatory references and submission procedures (described in the technical specifications).

Interoperability among the conservation systems of entities that perform this activity is guaranteed by the application of the technical specifications for archival information packages set out in the UNI 11386 regulation – SInCRO Standard – Support for Interoperability in the conservation and Retrieval of Digital Objects.

A general table of the stored objects is provided here below. The related Client-specific details, agreed upon with the producer, are set out in the Technical Specifications.

| file format | viewer | producer | MIME type | standard | extension |
|---|---|---|---|---|---|
| PDF | Adobe Reader | Adobe | application/ pdf | ISO32000 | .pdf |
| PDF/A | Adobe Reader | Adobe | application/ pdf | ISO19005 | .pdf |

| | | | | | |
|---|---|---|---|---|---|
| XML | Internet Browser | W3C | application/xml text/xml | | .xml |
| TIFF | Image reader | Adobe | image/tiff | ISO 12234 | .tif, .tiff |
| JPEG | Image reader | Joint Photographic Experts Group | image/jpeg image/jpg | | .jpg, .jpeg |
| EML | E-mail client | | application/email | RFC-5322 RFC2822 | .eml |

Any alternative file format must be agreed upon in advance and incorporated into the Technical Specifications.

## 6.2 Submission Information Package

At the data acquisition stage, the document must be sent in one of the formats provided for in Annex 2 of the Guidelines. As indicated in the regulations, the conservation system must guarantee the usability of the stored documents.

The electronic document conservation process therefore involves identification of the document types and management of the index fields associated with the documents, to enable their proper identification.

The indexes to be associated with the documents are selected, in collaboration with the Client, based on the type of documents to be stored and the search requirements, in accordance with the specific needs and context.

A description of the types of objects stored, including specification of the formats managed and the metadata to be associated with the various types, is provided in the Technical Specifications.

As such, the Client sends the documents to be stored to the Intesa platform, together with the index structures to be associated with them.

Document indexing may potentially be performed by the Intesa processing procedures, based on specific agreements with the Client.

The conservation system is configured to handle the formats best able to guarantee the principles of interoperability among the conservation systems and based on applicable regulations concerning specific document types.

As such, in agreement with the Client and in accordance with the provisions of Annex 2 of the Guidelines, the formats that enable the legibility and interoperability of the electronic document in the conservation system are selected.

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

The submission information package consists of the following objects:

- the submission information package index;
- the submitted object;
- the file containing the metadata provided for in the AGID Guidelines;
- any XSD schema.

## 6.3 Archival Information Package

The Archival Information Package (hereinafter AIP) is a container file (uncompressed ZIP format) that contains the original document submitted, the Archival Information Package Index file (hereinafter IPdA), signed (and sealed) and timestamped, the submission report file (hereinafter SR), signed and timestamped and, in the event of a migration, the IPdA file from the previous conservation provider, the XSD schema files and a ReadMe.txt file.

The AIP, with naming convention PDA.INTESA.IDHUB.ID.zip, will consist of:

- ReadMe.txt (text file that describes the composition, type and significance of the files it contains);
- PIndex.INTESA.IDHUB.ID.xml.p7m (IPdA file for the object submitted);
- pdv\ (Folder containing the SIP)
  - <DOC.INTESA.IDHUB.ID.ext> (Submitted Object)
  - <MT.INTESA.IDHUB.ID.xml> (Metadata file Annex 5 LLGG);
- rdv\ (Folder containing the submission report)
  - RDV.INTESA.IDHUB.ID.xml.p7m (Submission report file);
- ipda_previous\ (Folder containing the IPdA of the previous conservation provider if applicable)
  - <previous_ipda.ext> (IPdA of the previous conservation provider, if applicable);
- xsd\ (Folder of the templates used in the information package)

The IPdA file conforms to the Italian SInCRO standard – Support for Interoperability in the conservation and Retrieval of Digital Objects (UNI 11386) – concerning the structure of the set of data supporting the conservation process, which involves specific expression using formal XML language.

The SInCRO xml structure also provides for:

- an additional "MoreInfo" section where subjective metadata can be specified (specific "custom" indexes, related to the particular document category to which the index refers) defined by Intesa in agreement with the Client based on the type of document handled
- the minimum metadata required by the regulation, specified in Annex 5 of the AGID Guidelines.

Such additional "MoreInfo" structures refer to specific schema files, included in the archival information package and referred to in the SInCRO xml.

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

## 6.4 Dissemination Information Package

The conservation system provides authorised users with direct access, including remotely, to the stored document, which can be viewed and displayed both online (databases) via the Intesa web portal, and via standalone media.

The dissemination information package consists of a signed zip file with an INTESA seal containing the same structures as the Archival Information Package. For a description of the individual data structures, see the previous paragraph.

By way of logical correlations, directed by the conservation platform database, each dissemination information package contains documented data structures, enabling an overall link between the dissemination information package and the following elements:

- SInCRO xml data structure (in xml.p7m format), including the MoreInfo sections for custom metadata and minimum metadata;
- .xsd schema of the custom metadata (metadata saved according to a database structure and included in the MoreInfo section of the SInCRO xml);
- .xsd schema of the minimum metadata (metadata saved according to a database structure and included in the MoreInfo section of the SInCRO xml);

The document search function operates via search keys that correspond to the specific metadata for each type of document flow.

Dedicated functionalities make it possible to view, verify the integrity of, or export the dissemination information packages and those containing copies of the stored objects.

Any specific and additional display procedures that enable connection to, and integration with, the Client's systems may be subject to joint consideration by the Client and Intesa and included in the Technical Specifications (e.g. via Web Services, physical storage devices).

As such, the Service uses tools suitable for enabling the display of the stored documents in the event of access, inspections and checks by persons within the Client's organisation and/or competent authorities (e.g. in the event of audits by the Tax Authorities or the competent bodies tasked with supervision and oversight activities under the applicable regulations).

# 7 The conservation process

The conservation process involves preparation of a submission information package, containing the digital objects to be stored, accompanied by metadata, defined according to specific rules (storage index), that must be sent to the conservation system using the methods agreed upon by Intesa and the owner of the stored material. The conservation index completes the submission information package. The conservation provider that manages the conservation repository is responsible for the tasks of receiving the SIP, validating the SIP, transforming the SIP into an AIP, and sending the DIP to the owner of the stored material when requested.

The functional components of the Trusted Doc conservation system ensure that the entire stored object management cycle is handled as part of the conservation process.

The system assigns a unique identifier specific to the platform, which enables its direct and lasting identification.

The system guarantees access to the stored object, for the period required by regulations, regardless of how the technological context evolves.

As specified in paragraph 4.2 of the AGID LLGG, stored objects are handled by the conservation system in the form of information packages that can be subdivided as follows:

a) Submission information packages: these are structures containing data to be stored and received by the Intesa platform, which also include the relevant metadata, in accordance with the agreements reached with the Client;
b) Archival Information Packages (AIP): structures containing data that follow submission, which also include the IPdA in SInCRO standard;
c) Dissemination Information Packages: structures containing data required at the time of display.

The Intesa conservation service is configured to enable it to handle data from different companies, creating strictly separate environments for each entity. These can be appropriately identified thanks to specific system codification, and may be available in the indexes when the documents are acquired by the platform in the case of multi-company groups.

The system is design to enable the consistent management – while guaranteeing the complete separation – of:

- configurations;
- processes applied by the workflows, including signature processes;
- information packages (submission, archival, dissemination);
- monitoring;
- input and output data flows.

While ensuring separate management for the various companies, the system offers the Conservation Service Manager and its operators a global overview of the various management processes, and in particular the monitoring, oversight and alert functions.

The documents transferred to the submission system and subject to appropriate checks during uploading are not exposed to risks of alteration or modification during the logical transfer to the conservation process, which, in any case, involves verification of document integrity – using automatic procedures – at each stage of the process.

Verification and anomaly identification are therefore performed upstream of the process, as part of the submission system, during which any grounds for rejection are identified. The subsequent stages are subject to monitoring by the management system, which oversees the proper performance of the conservation process and produces the relevant reports relating both to any anomalies identified and to the successfully stored material.

Each document is sent to the conservation system by way of a submission information package containing the object to be stored.

With reference to civil law regulations concerning electronic document conservation, and in full compliance with such, Intesa has chosen to perform the process for each individual document.

Indeed, the archival information package for each individual document enables it to be displayed with the primary requirements, necessary for its full verification by the inspection authorities, already included. The individual document may also be produced during legal proceedings and authenticated by judges or public officials in civil law or tax cases.

Traceability of the individual document in the context of the conservation process is guaranteed and potentially made available by way of web publication as regards the various document statuses (received and stored).

Such considerations have therefore led to the solution that regards each individual document as a submission, archival and, potentially, dissemination information package, to which the various steps required by the CAD and relevant guidelines should be applied.

## 7.1 Procedures for acquiring submission information packages for the purposes of their acceptance

The Trusted Doc conservation service enables transfer of the data and relevant indexes securely using the https protocol or other methods agreed upon with the Client, always with a view to protecting the security of the data sent.

Intesa provides the services at its Server Farm.

The conservation objects received by the Intesa platform generate service requests (SR) to which unique identifiers (SRID) are assigned, enabling the traceability of the activities performed during the operation, from acceptance through to the creation of archival information packages. Each processing step is

appropriately indexed in specific tables of the database dedicated to consultable tracking/logging (logs). The submission information packages received are saved, at various stages of the processing operations, to the primary database, the single consistency point of the platform, with redundancy in a secondary instance, via "data guard" functions.

Historicization of the data during processing enables a restart/recovery in the event of a procedural failure.

The intervals at which documents are sent to the conservation system are determined by the functioning of the procedures on the Client's systems and agreed upon with Intesa (daily, monthly, etc.), in accordance with regulatory requirements concerning conservation /retention periods.

During service setup, the specific details of the submission information package and the relevant metadata structure are established in relation to each document type.

The metadata to be associated with documents to be sent for conservation are produced, and supplement those already defined during production. In particular, the metadata are supplemented to include specification of the conservation System to which the document should be sent.

Each document is sent to the conservation System, identified using appropriate rules defined based on the document type and the information contained in the document metadata.

The Intesa activities for each document type are performed in accordance with the timeframes for sending the documents to the conservation system and within the maximum retention period established by the regulations.

Based on agreements reached with the Client and requirements associated with the document type, Intesa configures the processing workflows and all parameterization required for proper processing of the documents.

## 7.2 Checks performed on submission information packages and the objects contained therein

The submission system requires performance of a series of conformity, reconciliation and accuracy checks on the documents to be stored. In particular:

- Conformity checks:
  - verification of sender details (Client/Owner of the stored material);
  - verification of file format. The conservation system verifies the format of each file submitted, according to the specifications set out in Annex 2 of the Guidelines;
  - presence of all information defined for the specific mandatory document categories.
- Accuracy checks:

  During the analysis stage, specific rules are agreed upon regarding the performance of any checks concerning uniqueness, duplication, consistency and completeness of the documents prior to

conservation. Any documents that do not comply with the rules agreed upon with the Client will be reported.

The checks referred to above give rise to blocking or non-blocking errors, if applicable, and therefore may result in rejection of the submission information packages.

## 7.3 Acceptance of the submission information packages and generation of the submission acceptance report

Following performance of the checks on the submission information packages and digital objects in accordance with the foregoing, they are accepted by the system and an acceptance message (ACK1) is generated.

At the end of the submission information package processing stage, and the checks, a submission report is also generated.

The submission report is an XML-type digital object that confirms the successful acceptance by the conservation system of multiple submission information packages sent by the producer, which have therefore successfully passed the various checks required.

The submission report includes the INTESA platform ID file, fingerprint, and date of submission of each stored object.

Within the Intesa conservation system, each submission report is assigned a unique file name and, subsequently, signed in cades .p7m format by the Conservation Service Manager.

The Service involves the creation of a submission report for each flow sent by the Client, containing references to submission information packages relating to that Client and document type.

The submission report is signed using a qualified electronic signature by the Intesa Conservation Service Manager, and stored with automatic correlation to the submission information packages reported therein; by searching the submission information package, the relevant submission report can be viewed.

## 7.4 Rejection of submission information packages and methods for reporting anomalies

The conservation process is designed to minimise rejection of SIPs. The service workflow includes a pre-ingestion step, required for successful acceptance of the packages.

If the submission information packages fail to pass the blocking checks, anomaly events are generated and reported to the Client.

All such events are collected and described for subsequent reporting to the Client's contact person, with whom an agreement will be reached concerning actions to complete the process.

As such, the checking process is characterised by:

- performance of the verification workflow;
- identification and tracking of the anomaly (database table and historicization of the attachment in the records);
- generation of a certain error report and document rejection;
- sending of the report and related reason (anomaly report) by e-mail to the contact person at the Client's company;
- management involving direct engagement with the contact person with regard to the different error situations, which may require different approaches and solutions.

The proper checking procedure is shared and agreed upon with the Client at the analysis stage.

An anomaly notification contains:

- the unique identifier of the rejected packaged;
- the related unique indexes agreed upon with the Client (i.e. document number and date);
- description of the error identified.

List of anomalies managed:

- incorrect submission information package format;
- metadata layout and content errors (data type error, length error);
- total or partial absence of metadata, with reference to the mandatory requirements established for the specific document categories;
- error identified while verifying the integrity of the Submission Information Package;
- duplication error with regard to the uniqueness rules established;
- error checking the sequence of the documents, with regard to the agreed rules ("gap check" procedure).

As such, anomaly reports represent an operational tool involving verification and communication with the Client.

Such notifications are recorded in the company e-mail application, in dedicated databases, used exclusively for the conservation Service and only by appropriately profiled and appointed persons.

## 7.5 Preparation and management of the archival information package

Following acquisition and verification of the submission information package, Intesa transforms the SIPs into archival information packages.

The Intesa conservation system provides for management of the archival information package based on the data structure specifications set out in the Guidelines.

The archival information package consists of:

- the digital object;
- metadata;

- the archival information package index;
- the submission report.

The .p7m file format used for the IPdA enables it to be displayed with the primary requirements necessary for it to be fully verified by the inspection authorities already included. The individual document may also be produced during legal proceedings and be authenticated by judges or public officials in civil law or tax cases.

Traceability of the individual document in the context of the conservation process is guaranteed and potentially made available by way of web publication as regards the various document statuses (received and stored).

Based on the document type, the retention periods for the documents are established during setup, correctly assigned by the system at the time the Submission Information Package is received.

The conservation System is configured to manage the retention period for each document based on the document category, current regulations and the service contract.

Applications of the seal and timestamp to the IPdA are carried out in accordance with the specific regulations on signatures and timestamping.

That process makes it possible to fulfil the requirements of authenticity, non-modifiability, integrity and static form.

These operations complete the electronic conservation process, with the document status being updated within the tracking process and successfully stored, and generation of the dedicated archiving report (ACK2) made available to the Client with the relevant information.

The seal certificate of the Conservation Service Manager is issued by Intesa CA and saved on HSM devices, capable of guaranteeing high levels of security, reliability and performance in terms of signing operation speed.

## 7.6 Preparation and management of the dissemination information package for display purposes

The structure of dissemination information packages is the same as archival information packages.

As dissemination information packages result from the process of applying the electronic seal and timestamp, the file extension is .p7m, and the files are made available to the producer and Intesa, in its capacity as conservation provider.

The display of stored objects is agreed upon with the client and may take place according to the Intesa platform standard or other specific methods set out in the Technical Specifications of the contract:

- Intesa web portal;
- standalone conservation devices;
- web services;

- single sign-on;
- other agreed methods.

### 7.6.1 Web portal method

Documents can be consulted via the web by accessing the Intesa portal using the https protocol, availing of the online native functions of the platform.

The consultation functions make it possible to search the documents stored in a database using a customised search engine for each index associated with the document, and view, verify the integrity of, or download the document, for the duration of the service contract.

The service also makes it possible to handle dissemination information packages with multiple signature levels, relating to the document generation/issuance/electronic conservation processes performed by the Client prior to the submission and archiving process.

Users with access to the consultation system must be duly registered and profiled.

Profiling is defined on the basis of specifications provided by the Client, enabling user profiles, relationships among them, and access control to be defined.

### 7.6.2 Standalone conservation device method

Dissemination information packages can also be consulted using standalone conservation devices if requested by the Client in the contract specifications.

In that case, the dissemination information packages are extracted, in order for the stored documents, arranged in logical archives, to be displayed.

The concept of 'logical conservation archives' refers to the logical organisation of the documents involved in the electronic conservation process, defined by type, retention period, or other parameter agreed upon with the Client to enable standalone devices to be created and given to the Client, if required.

This activity involves establishing the number of archives and the names to be assigned to them for the various document types, with the relevant search keys and conservation device characteristics, as described in Annex A.

The consultation search indexes (metadata) are agreed upon and defined at the service analysis stage.

In order to track all details relating to the creation and conservation of dissemination information packages on external devices, specific service application functions generate an acknowledgement report (ACK3), which makes it possible to track the activity performed both at a system level and as part of the database tasked with tracking the archives and devices generated.

The device generation stage activates the procedure of verifying and checking the number of packages actually contained in the archive and the number of indexes included in a dedicated check file. An error log is generated in the event of a discrepancy, making it possible to carry out the necessary verification activities.

If the result of these procedures is positive, the archive creation activity is completed and the reconciliation, writing and unique identification of the removable physical device (USB or other) is performed, as well as the shipping or delivery according to the methods agreed upon with the Client.

Dissemination information packages can be consulted on a device using the viewer software produced by Intesa and included on the device itself, which features search, verification, view and download functionality.

The viewer is written in Java language to make it compatible with the operating systems on the market and guarantee maximum longevity. It does not require recognition of licences for software components contained therein, and therefore does not involve additional distribution costs.

The functionality of the viewer is summarised here below:

- Document search

Using defined metadata that (via XML files) describe the structure of the archive, a search window appears, containing the selection fields and relevant operators. The documents that satisfy the search criteria are listed, as well as any page numbers. A specific column can be selected to display results in increasing or decreasing order;

- Functions relating to individual documents

The following functions are available:

- view document
- view PKCS#7 objects (fingerprint, signature, timestamp)
- extract PKCS#7 objects (signature, timestamp, full PKCS#7, original file in cleartext)
- verify integrity of the PKCS#7 and check validity of signature certificate and timestamp on external file of the CRL and "trusted" Certification Authority.

## 7.7 Creation of duplicates and electronic copies and description of any intervention by a public official in the situations provided for

By viewing the dissemination information packages, the Client can download electronic duplicates if required.

They can submit a dedicated request to Intesa to request the creation of true copies of the documents.

By logging on to the portal with a username and password, a public official can access the following functionality:

- view and select individual or bulk electronic documents;
- associated activities aimed at verifying that the electronic document is a true copy of the original document already available to the public official;
- perform a local download of the documents, for the purposes of verifying the authenticity and integrity of those documents using a pre-selected verifier available on the market, thus ensuring the full independence of the oversight process and the utmost guarantee as regards verification.

## 7.8 Disposal of the archival information packages

As the end of the established electronic conservation period approaches, the Intesa conservation Service notifies the Client of the documents reaching the end of their life cycle, providing appropriate advance notice.

The parameters for the procedure are set by filling out an application database table that lists all of the types of documents stored, broken down by Client, document type, and retention period (e.g. 5 years for the Single Employment Ledger, 10 for other documents or other timeframes agreed upon contractually with the Client and specified in the Technical Specifications).

The system generates a dedicated report with a list of archival information packages containing the documents designated for disposal, and a warning regarding imminent deletion, i.e. disposal of the archival information packages and logical archives from the Intesa systems.

A certified e-mail will be sent if such an address is available, or a standard e-mail. Return receipts will be stored by the Manager of the devices at the primary site. The data will be physically deleted following an appropriate notice period.

Deletion of the data will affect both the documents in the database and those transferred to the archives on NAS.

If the Client wishes to continue to store the documents, they have 1 month from receipt of the e-mail to give notice of the same. In this case, the contractual conditions governing this aspect will be amended.

### 7.8.1 Termination of the conservation Service

At the request of the Client, and subject to specific agreement between the parties, at the end of the conservation period, Intesa will hand over the originals of the stored data, arranged in homogeneous archives based on parameters agreed upon with the Client, via a connector or on suitable standalone storage devices.

If the contract ends or in the event of withdrawal by the Client or Intesa, Intesa remains obligated to store the material for the period required by the regulations based on the type of document stored or as

otherwise agreed upon with the Client. The Client may, in any case, request that the data be returned and thus release Intesa from its obligations under par. 4.5 of the Guidelines.

In the event that the Contract is terminated, or the service is discontinued, Intesa shall hand over the data in its possession to the Client, having been released from its conservation obligation and the obligations arising from par. 4.5 of the Guidelines.

In all cases involving return of the data, they will be extracted to logical archives containing the packages with standard data structures, arranged as agreed upon with the Client.

Once the data have been returned to the Client, they will be securely removed from the Intesa systems.

## 7.9 Provision of measures to guarantee interoperability and transferability to other conservation providers

Thanks to the structure implemented for holding the stored data, Intesa provides for natural interoperability and integration with other conservation solutions and/or document management platforms.

Furthermore, as format conversion and transformation has always been an essential feature of Intesa's core business, it is capable of adapting promptly, including to any evolution of the regulatory and technological context, which is certainly to be expected over time.

In that sense, the Intesa operations already incorporate the following technological characteristics:

- use of the standard formats required by the relevant regulations for document conservation;
- adoption of standard signature formats recognised by the Certification Bodies in accordance with PAdES-T and CAdES-T specifications, with application of timestamps;
- The decision by Intesa to process individual documents rather than batches completely eliminates the need to develop and manage complex and detailed proprietary algorithms, required to process the document both at the time of placing it in conservation and at the delicate stage of displaying it to the competent authorities, and in all instances of a legal dispute;
- The individual document therefore has all of the technical and regulatory attributes required to facilitate any operation involving portability or interoperability with external structures and relies on the relevant XML format indexes for compatibility purposes, thanks to application of the SInCRO standard widely recognised for its interoperability features.

As part of its processes, Intesa adopts formats that comply fully with the recognised standards and, as a further protection and guarantee measure for clients, it does not use proprietary formats, often found on the market but that present challenges in terms of portability.

As such, when the producer (the Intesa Client) requests the transfer of the archival information packages to another conservation provider, the functions activated by Intesa and guaranteed by the conservation system requirements listed above enable quick transfer to a new conservation system. These functions provide for the controlled export of the archival information packages, related archival information package indexes (IPdA) and search metadata.

# 8 The conservation system

From acceptance through to disposal, where applicable, the conservation system guarantees conservation of the digital objects stored through the adoption of rules, procedures and technologies, guaranteeing the characteristics of authenticity, integrity, reliability, legibility and retrievability as specified in par. 4.1 of the Guidelines.

Trusted Doc, the electronic conservation service provided by Intesa, is based on the Intesa proprietary platform, Trusted Hub, as described below.

Given its importance, the Service has been developed entirely by Intesa, enabling prompt alignment of the solution with regulations and market best practice guidelines, and its customisation over time, in order to enhance the services provided.

The Trusted Hub Service infrastructure, used to provide the Trusted Doc conservation service to clients on an outsourcing basis, is the product of over 25 years' experience gained by Intesa is electronic document management, and over 10 years' experience as a Certification Authority registered with AgID for Digital Signatures. As such, its native features combine the functionality of a hub designed to handle the processing and exchange of large volumes of electronic documents with the functionality and guarantees that Intesa can provide as a Certification Authority and conservation Provider.

There is therefore native integration between the Trusted Hub platform and the signature functionality offered by Intesa in its capacity as Certification Authority. Bulk signing of documents is performed using HSMs that offer powerful encryption acceleration, key management at a hardware level, and provide for management of multiple configuration profiles. They are recommended in particular for processes such as generating electronic documents at source and their electronic conservation, in which security and performance are priorities.

Featuring the latest technology, the Trusted Hub infrastructure is robust yet flexible. Indeed, it is based on standard commercially available middleware, combined with proprietary components to enable the streamlined and independent management of aspects such as tracking, administration, workflows, digital signing, etc.

The service provided by Intesa and the relevant infrastructures are hosted at the INTESA server farms located at sites connected in campus mode across a high-speed geographical network. The infrastructure consists of virtual partitions and physical servers, with full redundancy at the primary site and duplication at the Disaster Recovery site.

The modularity provided by its infrastructure/configuration means the Service is scalable and, as such, capable of managing potential increases in volume.

Equipped with adequate conservation capabilities, the infrastructure is specifically designed for data-intensive applications involving significant levels of high-reliability performance.

## 8.1 Logical components

The platform, the logical architecture of which is outlined in the drawing below, can be divided into a series of "Basic Modules" required for:

- defining communities, relationships, users and their profiles;
- the system administrator's tasks;
- the conservation system's tasks;
- managing the web portal;
- managing the processing workflows;
- store & forward functionality for non-synchronous documents (mailbox);
- monitoring and tracking flows and the documents involved in the same.

The above basic components are combined with "specialised modules", called to perform specific processing operations on the flows and/or data based on workflow rules:

- Timestamping Module, to timestamp documents for evidentiary purposes;
- Bulk Digital Signing Module, which enables centralised signing of the documents using dedicated high-security equipment.

The logical components of the Intesa Trusted Hub platform on which the conservation system is located are set out here below:

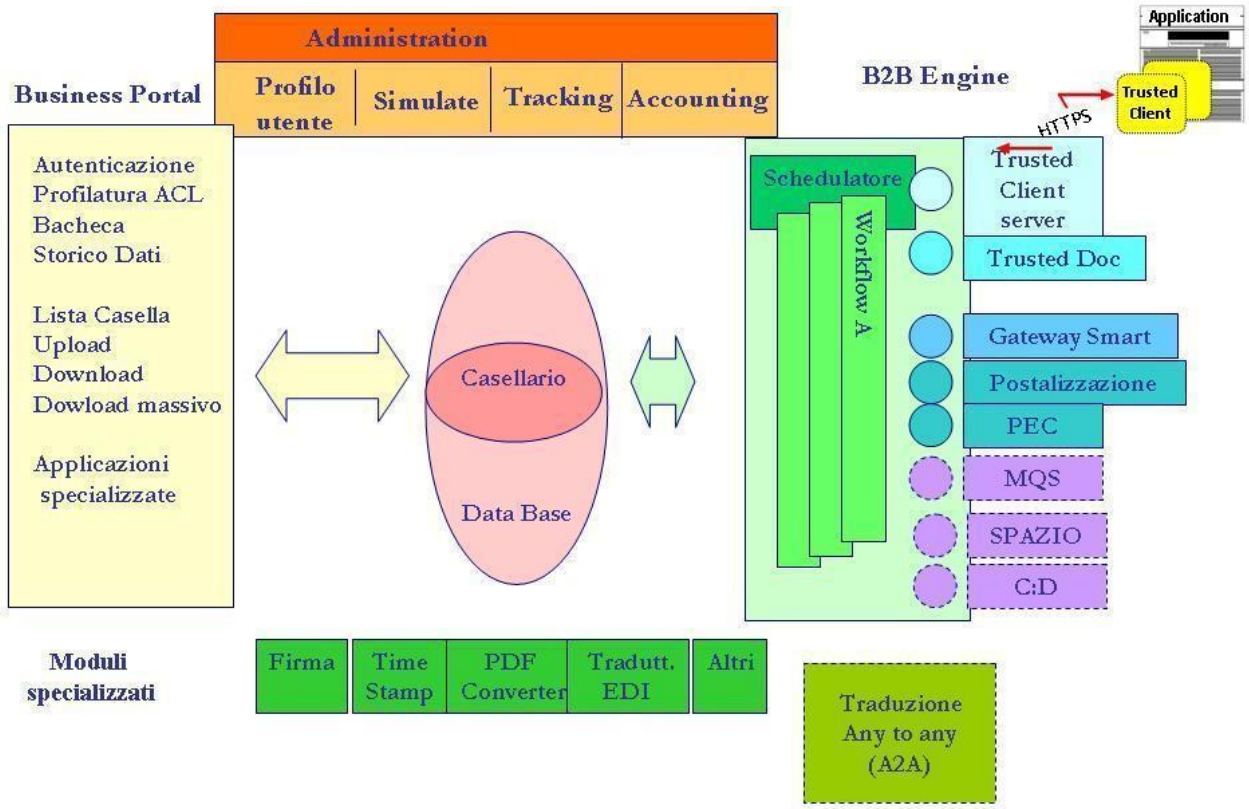



*Figure 1: Outline of the logical components*

## 8.2 Technological Components

The technological components of the conservation system described above are outlined here below.

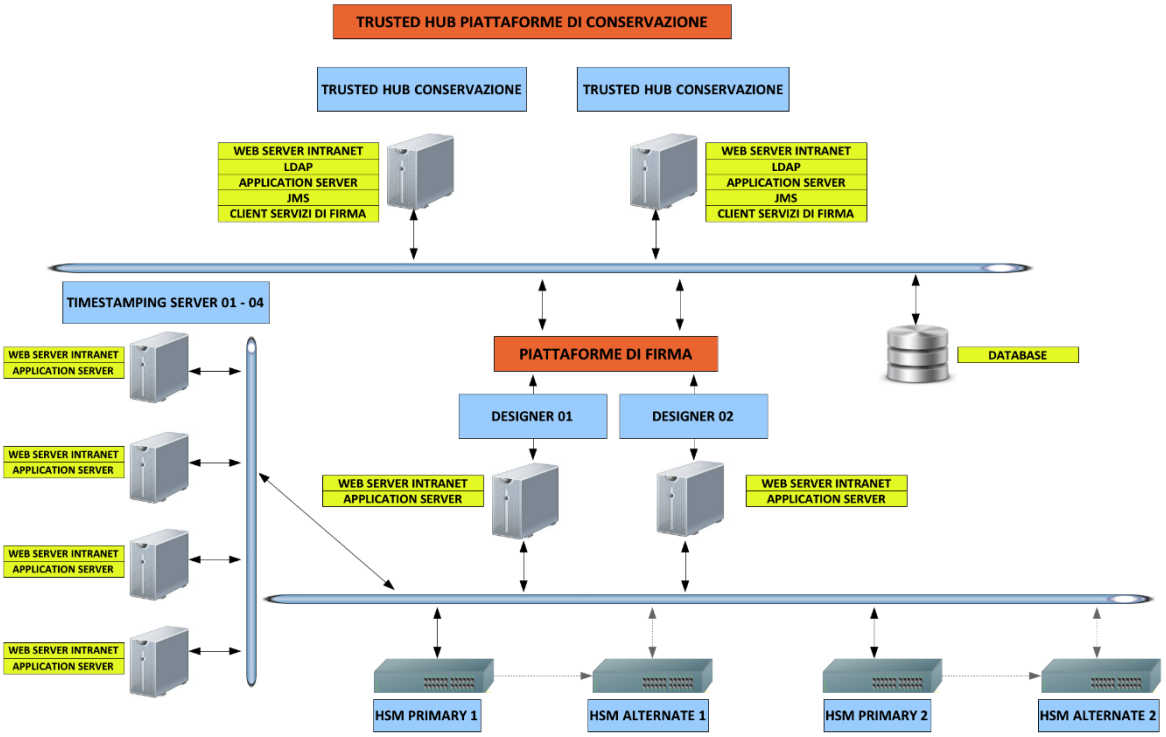



*Figure 2: Technological components*

## 8.3 Physical components

The most advanced ESXi version of Virtual Machine VMware technology has been adopted to provide the conservation service.

The technological components of the conservation sites are described here below:

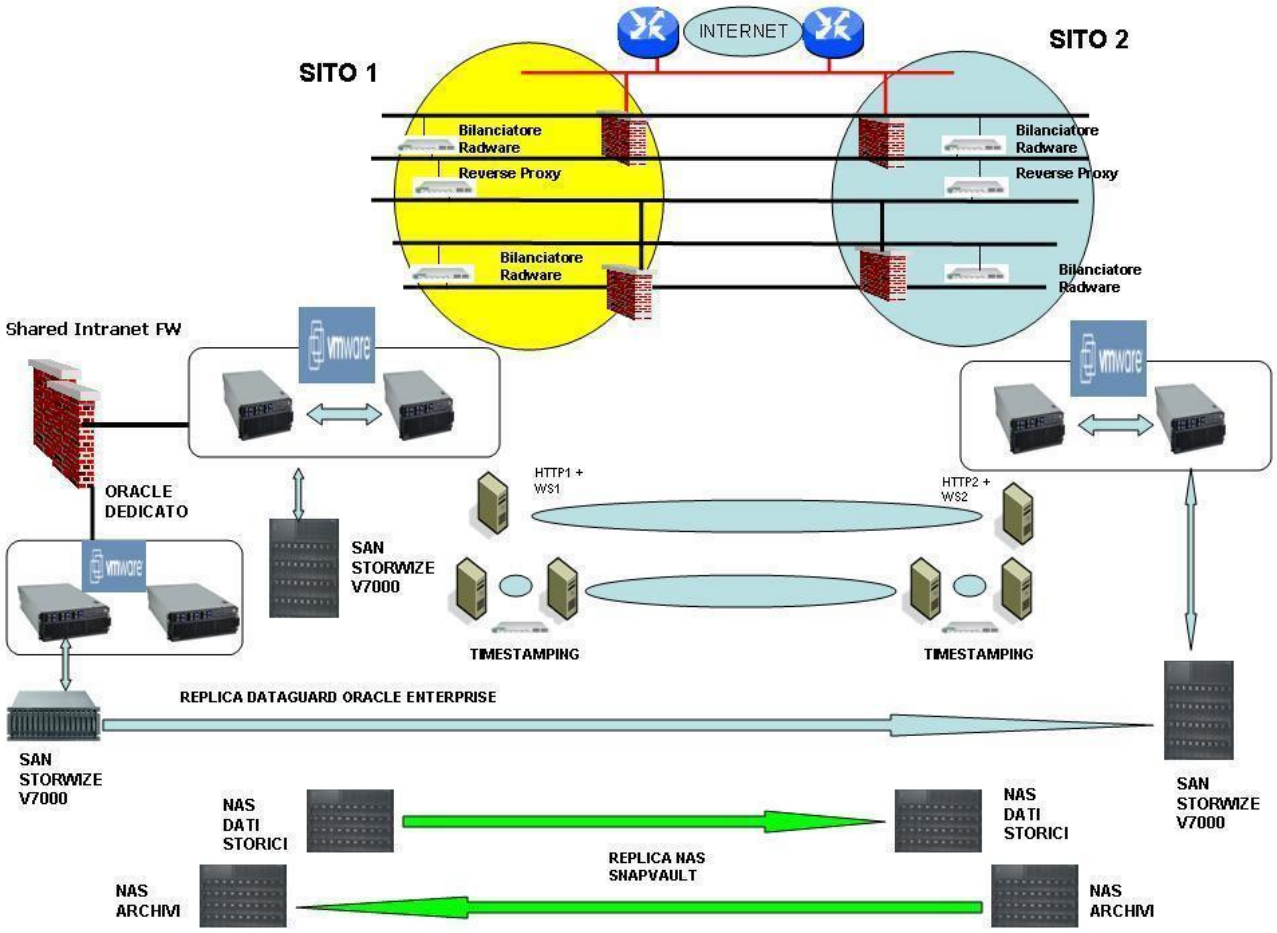



*Figure 3: Physical components of the* conservation *sites*

The VMWare environment is made up of latest generation IBM xSeries servers that, via fibre optic dual switches for crossed and redundant connections, share multiple Storwize V7000 Storage Area Networks (SANs) with TIER SSD to guarantee high performance.

The VMWare platform draws on concepts that have already been widely tested and consolidated in Enterprise Mainframe environments, where partitions that are completely isolated and dynamically manageable at both a resource and storage level are created on extremely reliable and scalable hosts.

The virtual machines (VMs) use high-level HW storage on a shared or direct basis, guaranteeing Vmotion operations (hot migration of the VM from host to host without interruption of activities). The VMs can be defined with extreme flexibility, responding to horizontal and vertical scalability requirements.

Via the Virtual Centre, the resources (CPU, RAM, I/O, network) can be dynamically modified to optimise the performances of each individual VM.

## 8.4 Management and evolution procedures

### 8.4.1 Managing and maintaining the conservation system

The Intesa Conservation System has been structured with a view to managing and maintaining the documents and the platforms that support them, as well as maintaining oversight and ensuring evolution of the platforms.
The conservation system is managed by the appointed staff, based on the type of activities to be performed and the actions to be taken.
The Intesa various operating departments perform the tasks within their respective remits based on coordination aimed at ensuring a shared vision of the system.
The tasks are divided into:

- System tasks: maintenance of the infrastructure components and their evolution, monitoring the proper functioning of the structure;
- Application and software management tasks: managing evolution and corrective and evolutionary measures, application releases, workflow and procedure development;
- Application monitoring tasks specific to the Client: daily monitoring of the platform processes and workflows;
- Client support tasks: support in dealing with anomalies reported to the helpdesk team;
- Hardware maintenance tasks: management and maintenance of the hardware infrastructure to guarantee proper functioning of the same. Planning any intervention measures.

The Intesa organisation responds with increasing efficiency to Clients' requests for intervention, drawing on its ongoing experience with the specific product or service.

With regard to software products developed by Intesa, the Maintenance Managers are responsible for suggesting action to be taken in terms of evolutionary maintenance; with regard to third-party products, on the other hand, the Maintenance Managers have the role of reporting issues and submitting requests and enhancement recommendations to the producer or distributor, as well as proposing specialist interventions to the Client.

The corrective maintenance process is implemented if anomalous behaviour by the service/product (i.e. not compliant with the relevant specifications) is detected.

Corrective/evolutionary maintenance involves a procedure-based series of steps, intended to ensure that the corrective/implementation action taken is complete and effective:

- detection of anomalies (in the case of corrective maintenance) and/or intervention requirements (in the case of evolutionary maintenance);
- diagnosis, approval and assignment;
- correction;
- testing,

- release;
- propagation.

### 8.4.2 Monitoring and security

The conservation system provides for adequate technological and infrastructural oversights, aimed at ensuring high reliability and disaster recovery measures consistent with regulatory provisions on the matter and market practices.

Based on the provisions of par. 4.10 of the Guidelines on training, management and conservation of electronic documents, private entities belonging to organisations that already adopt specific sector rules on information system security configure their conservation system in accordance with those rules.

In providing the Intesa Trusted Doc conservation service, the security aspects comply with the standards expressed:

- in the Intesa company policies;
- in ISO 27001 certification for specific purposes: generation/issuance of electronic documents, electronic conservation and legal archiving, and production of electronic signature, advanced electronic signature, qualified electronic signature, and certified e-mail solutions;
- the Personal Data Protection Code, referred to in Italian Legislative Decree no. 196 of 30 June 2003.

Information security combines physical, logical and administrative elements, the management of which is implemented in various ways:

- infrastructure-based physical and logical security;
- application-based logical security;
- continuity.

In light of the need to protect data and information, a specific system has been developed that meets the following criteria:

- to protect the transmission of information against data losses, disclosure or unauthorised modifications;
- to grant access to the provision systems only to those that require it (in terms of specific responsibilities) and arrange for the relevant authorisations;
- to perform appropriate checks to guarantee that the oversight mechanisms operate effectively.

With regard to logical security from a structural perspective, the procedures provided for involve:

- security administration;
- protecting the provision environments;
- identifying and authenticating users;

- authorising access to the information at various levels.

and take various directions:

- guaranteeing the confidentiality and privacy of the information transmitted by the Client using appropriate network architecture;
- guaranteeing the integrity of the data transmitted by using appropriate and advanced communication protocols;
- guaranteeing the stored data by way of controlled authorisations supplied by dedicated IT applications (e.g. ACL).

As regards confidentiality and privacy, the underlying software products used and management procedures adopted have been designed to assure the Client that:

- their information is logically identified, with access to it granted only to authorised persons;
- access authorisations are currently valid and subject to oversight;
- reporting procedures are in place in the event of any breaches, and procedures are implemented to review such attempts.

### 8.4.3 Log management and conservation

The conservation system records the operating system and platform application access logs. These logs are stored.

Furthermore, Intesa maintains within its infrastructure – and makes available to the Client for inspection purposes – logs relating to the receipt of flows sent by the Client, and the application logs relating to processing operations performed on the Intesa systems, for 90 (ninety) days from the date of receipt and processing respectively.

During the service provision period, Intesa makes its management structure available for the purposes of monitoring proper data flow trends and taking appropriate action in the event of malfunctions, errors or critical situations in general.

It is hereby noted that the Intesa process operates on an individual-document basis, thus enabling simple, effective and complete monitoring.

Upon first analysis, the monitoring activity refers to:

- ACK1: implementation of the internal workflow relating to the processing of documents and related web publication (acceptance of submission information packages);
- the submission report;
- ACK2: (archiving report) implementation of the internal workflow relating to electronic conservation; a flow is generated containing a list of all documents belonging to the conservation package and related outcome of the operation and, in the event of an error, specification of the type of error detected. The return flow indicates a unique code relating to the conservation package assigned.

For each flow, Intesa sends the Client the various outcome reports (ACK) using CSV standard record layouts, or formats agreed upon with the Client, enabling reconciliation of the status on their systems if required.

Based on the agreements reached with the Client, these reports can also be sent by e-mail to the company contact person.

### 8.4.4 Change management

This procedure is performed by Intesa with the aim of tracking all of the evolutions and changes made to the developed objects used for application implementations via the dedicated versioning tool.

The developers obtain the objects via check-in operations, make the necessary changes and/or corrections and consolidate these activities respectively in the development, testing and, finally, production, environments via the respective check-out operations, using versioning that enables saving at a platform file system level for all of the environments referred to above.

The party tasked with configuration authorises the transfer between the various environments (enhancement), and non-regression, compare and merge testing is carried out, as well as testing relating to contention object management by developers.

Once the activities have been completed, definitive deployment is performed in the production environment.

### 8.4.5 Periodic compliance checks and relevant standards

The Conservation Service Manager checks the various logical, technological and physical components of the system, in accordance with the requirements set out in the Guidelines, with reference to the obligations of the Head of Conservation and the stages of the conservation process.

Such checks are performed in accordance with the internal audit procedures, documented in company operating instructions and reported in relevant reports concerning their performance and outcome.

# 9 Monitoring and oversight

The Intesa conservation system requires the adoption of specific measures and tools to promptly detect any issues with the conservation systems and records and, where required, restore proper operation.

The available tools enable checks and monitoring of the proper functioning of the conservation system, in terms of the system- and application-based management of its various components.

A dedicated Help Desk service is provided for any issues relating to access or specific anomalies concerning the transmission of documents.

The Intesa system- and application-based monitoring system detects specific anomalies with the conservation system and reports them by sending dedicated alerts to management teams arranged according to area of competence.

These teams take charge of the issue, communicating as required with area specialists (e.g.: platform, physical infrastructure, connectivity, database, specific application services, etc.) and oversee it until it is resolved. The actions taken are documented in specific system logs, entered in the internal repository established in accordance with the company quality system.

To ensure proper management of the conservation system, Intesa keeps a chronological log of the software for the programmes used, including the various versions used over time, and the chronological log of conservation system management events, including the solutions adopted to resolve any anomalies.

## 9.1 Monitoring procedures

For the purposes of monitoring the conservation system, Intesa adopts tools and procedures aimed at analysing the various components of the system, detecting any anomalies to enable intervention and involvement of staff tasked with resolving critical issues.

The oversight and management of the conservation system are based on continuous monitoring of the environment and its individual components, using the instruments and tools specified below to ensure that the fundamental parameters of the service comply with contractual and quality requirements.

Centralised and controlled management of service provision operations is governed by specific procedures and tools that guarantee:

- constant oversight of service levels, by monitoring the environment and critical elements, including effective performance of management activities such as, for example, checking available space, ensuring that limits are not exceeded, and simulating log-on to check service availability;
- service performance monitoring, arrangement or verification of testing and periodic data or library saving operations, and any preparation of input data and verification of the results;
- management of changes to service parameters (e.g. user authorisation, passwords, etc.), in order to promptly bring the service into line with the updated needs of the Client;
- management of security and access to the service, to prevent intrusion and unauthorised access. Security is arranged across multiple levels (network, system, and application service), supported by appropriate and advanced technological solutions and managed by dedicated staff within the company, who continuously monitor and perform periodic checks concerning the completeness and effectiveness of the solutions adopted (e.g. penetration testing);
- the controlled performance of any changes to the operating environments (HW, SW, etc.). Each "change" request must be documented, justified, analysed and authorised. A thorough impact analysis carried out in advance by the most qualified staff, concentrated implementation in appropriate time "windows" during periods of low use, and exhaustive testing aimed in particular at verifying backward compatibility, tend to minimise the risks of interruption to the service;

- continuous maintenance and updating of the HW and SW configurations relating to each environment managed. Such oversight makes it possible to identify the technological components involved in providing each service (including on an historical basis), to better plan any change and restoration activities;
- optimal management of service interruptions, whether scheduled or unexpected. Specific design activities are performed to contain and limit the impact of potential malfunctions and automatically or promptly implement alternative solutions (e.g. routing, switch, etc.);
- resumption of activities in the event of problems. Appropriate and automated saving of environments, libraries, applications and data enable controlled recovery (full, sector-based or partial) of the resources, to promptly restore the interrupted services;
- maintenance of a high level of availability and reliability of the individual technological components, via specific scheduled maintenance contracts. Interventions aimed at preventing potential HW problems are performed periodically by expert personnel;
- maintenance of a work environment appropriate to the activities to be performed.

### 9.1.1 NAGIOS system- and application-based monitoring system

The monitoring system has been developed based on the NAGIOS Open Source module, on a LINUX RED HAT operating system. The system is configured to guarantee high availability of the service.

Multiple plug-ins have been developed in addition to those native to the product. This has made it possible to achieve various functionality that would not otherwise be available, to enhance the system.

As well as the specific check to be performed, each monitoring plug-in recognises the relevant parameters and limits or rules to identify priority levels.

Each plug-in is scheduled independently, thus enabling more or less frequent checks based on the needs of the specific object/function to be monitored.

The system enables monitoring across three levels:

- system-based monitoring;
- application-based monitoring, specifically configured on the conservation system;
- business monitoring, supplied as a configurable service.

The system allows for the profiling of operator users in order to provide each with one or more consultation Users, in relation to the specific checking activities assigned.

As such, each operator can be assigned visibility over specific plug-ins (ACL), while a user can be assigned to one or more service teams.

In terms of system-based checks, the status of the various application layers is verified, via standardised or custom probes based on specific needs and SLOs - SLAs agreed upon with the Client:

- physical discs;
- Websphere/Application Server;
- https access;

- database.

## 9.2 Archive integrity checks

The archival information packages are stored by Intesa on separate storage devices in high-reliability mass storage systems (NAS), with automatic redundancy at geographically separate sites.

The electronically stored documents are subject to dedicated checks/tests to ensure their integrity over time, for the entire time period legally required for the document type and area in question (e.g. 10 years for tax documents) and as agreed upon with the Client.

Intesa verifies the conservation status of the archival information packages, arranging, where necessary, for their copying in accordance with par. 3.7 of the Guidelines.

The testing process involves checking the integrity of all documents, arranged in logical archives and stored at the various sites, and a consistency check on a significant number of documents.

The integrity checks concern the non-alteration of the data over time, while the consistency checks relate to:

- display (sample legibility, verifiability);
- checking the seal and timestamp;
- accuracy and consistency with the metadata.

The results of the procedures and checks are reported in a dedicated section of the company repository.

## 9.3 Solutions adopted in the event of anomalies

A conservation system anomaly may be highlighted by members of the Intesa management and monitoring team, in which case they will record it directly in the problem management system, thus notifying the team tasked with taking corrective action. It may also be highlighted by a Client user, by notifying the Help Desk (corrective maintenance).

The need for new service functionality, on the other hand, may be highlighted by the Client, by submitting a new request/order, by the Service Manager in an internal proposal, or by support personnel, by proposing a potential improvement action (evolutionary maintenance).

The anomaly resolution or corrective/evolutionary action process involves the following operating stages:

- detection of an anomaly and/or the need for evolutionary action;
- diagnosis and assignment: this stage involves diagnosing the cause of the malfunction (in the case of corrective maintenance) or the potential to integrate new functionality into the product/service (in the case of evolutionary maintenance) and arranging for it to be assigned to the most appropriate staff;
- correction/evolution: the software components responsible for the malfunction, or new functionality, are identified, and the necessary measures taken. In the event of a blocking

problem, a bypass can be implemented at this stage, to prepare an immediate solution that allows for continued use, potentially to a reduced extent;

- testing: makes it possible to verify that the change made to the product/service resolves the reported fault or meets the new functional requirements and perform non-regression testing in relation to the corrective action taken. The tests are carried out with a particular focus on ensuring that the changes made do not cause regression issues for other components of the application. A careful examination is then performed in order to apply the changes to the other current versions of the product/service. All activities and the results of the product/service maintenance are recorded in a dedicated software entitled "SW maintenance sheets", an important database that can be used to review the quality of products and the anomaly reports submitted by each client;
- release: the modified product/service or application is made available to the Client/Principal, to enable it to be used;
- propagation: the change is propagated, if required, to other target platforms of the product/service or application;
- post-sales support: post-sales support is provided via Intesa Customer Care (Helpdesk).

If the monitoring activities referred to above, supported by dedicated automated mechanisms, detect any problems or the risk that such may occur, corrective action is promptly taken to prevent deterioration of the service. An appropriate record of such events, and their resolution, is kept using a tool to support the records, and a dedicated analysis is performed to update the security measures in force, if required.

Furthermore, the Client has access to a Customer Care "Help Desk" service provided by personnel trained in the conservation procedures and checking service availability and status.

The Client support service involves two levels:

1. **Level 1 help desk:**

Takes and records the call, provides support on matters relating to system functionality, identifies and, where possible, resolves the problem encountered by the user, or transfers them to the appropriate level two support team. Also notifies the user once the problems have been resolved at the end of the intervention cycle, using the established access/contact channels.

The main tasks of the Help Desk team are:

- to provide support to Clients to guarantee continuity of service provision;
- to provide information on the services;
- to receive and record problem reports;
- to analyse the problems, assign a severity level, and provide a resolution, which may be temporary or provisional (level one support);
- to engage the experts – i.e. specialists with specific skills in the area in question – to provide level two support in the event that the problem cannot be resolved directly;
- to remain in continuous contact with the Client to keep them updated on the resolution of critical problems affecting them;

- to close the problems together with the Client, notifying them of the effective resolution.

Each solution identified will be verified by the staff tasked with resolving the problem, to ensure its completeness and effectiveness, before being provided to the Client.

Throughout the problem management process, the Help Desk team constantly monitors the progress of the solutions and takes any follow-up action in relation to the experts tasked with establishing such, in order to guarantee their implementation within the target timeframes set.

A dedicated software (HDA) supports the implementation flow and recording of reports.

Dedicated measurement tools and an appropriate reporting system guarantee effective oversight of the functionality and effectiveness of the level one and level two support, and achievement of the established service levels.

2. **Level two support:**

This is provided by experts specialised in the services and products supplied. Such experts are contacted by the level one support team if the latter is unable to resolve a problem presented by the user.
As such, the level two team is not an organisational unit, but rather a virtual team, arranged horizontally according to the technical areas within their remit, and vertically across higher levels of specialisation. As such, the level two support team includes staff with system-based or application-based skills, tasked with resolving problems complex enough that they cannot be resolved by the level one helpdesk team. The level two team notifies the level one team when the intervention is complete.

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

This is a level two team, operating in the application environment, specifically set up for legal archiving projects.
It supports the Client with specific issues relating to the conservation process and notifications regarding the operational management of the Trusted Doc service. It works in close collaboration with the Project Lead and specialist Intesa personnel with technical and regulatory competences.