



## ANNEX C – TECHNICAL ANNEX Safe LTA

### Sommario

|                                              |    |
|----------------------------------------------|----|
| 1. EXTERNAL REFERENCES .....                 | 1  |
| 2. Description of the service .....          | 1  |
| 3. Technical-regulatory specifications ..... | 2  |
| 4. TECHNICAL SPECIFICATIONS .....            | 7  |
| 5. SLAs and KPIs:.....                       | 11 |
| Responsibility delegation .....              | 13 |

\*\*\*

## 1. EXTERNAL REFERENCES

| Documentation                                                 | Detail links                                                                                                                                                                                                              |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operating Manual: Tinexta Infocert Preservation Manual</b> | <a href="https://www.infocert.it/pdf/conservazione/manuale-conservazione-infocert.pdf">https://www.infocert.it/pdf/conservazione/manuale-conservazione-infocert.pdf</a>                                                   |
| <b>User Manual</b>                                            | <a href="https://knowledgecenter.infocert.digital/home/guida/manuale-utente-safe-lta">https://knowledgecenter.infocert.digital/home/guida/manuale-utente-safe-lta</a>                                                     |
| <b>API documentation</b>                                      | <a href="https://developers.infocert.digital/safe-lta/">https://developers.infocert.digital/safe-lta/</a>                                                                                                                 |
| <b>Submission agreement</b>                                   | <a href="https://www.infocert.it/documentazione#menuid5">https://www.infocert.it/documentazione#menuid5</a>                                                                                                               |
| <b>Support links (FAQs, Videos, Guides)</b>                   | <a href="https://knowledgecenter.infocert.digital/cerca?searchText=Conservazione%20Digitale&amp;idProdotto=176">https://knowledgecenter.infocert.digital/cerca?searchText=Conservazione%20Digitale&amp;idProdotto=176</a> |

## 2. Description of the service

SAFE LTA (Long-Term-Archiving) is a service for the storage of data and electronic documents in accordance with the law (hereinafter the "Service").

In particular, the Service includes:

1. the license to use the software that makes up the Services provided by Tinexta Infocert, in non-exclusive and non-transferable use;
2. the provision of the space necessary to store the data and documents sent at the Data Center;
3. the adaptation, maintenance and updating of the Services;
4. support activities;
5. appointment to handle preservation procedure

In addition, the preservation system ensures, from taking charge to any rejection, the preservation of the digital objects stored in it, through the adoption of rules, procedures and technologies that guarantee the



characteristics of authenticity, integrity, reliability, legibility, availability, pursuant to the AgID Guidelines on the formation, management and storage of electronic documents of May 2021 and subsequent amendments and additions and the D.M.E.F 17.06.2014. The preservation system guarantees access to the stored object for the period provided for by the conservation plan of the owner of the storage object and by the regulations in force, or for a longer time that may be agreed between the parties, regardless of the evolution of the technological context. The system also guarantees the possibility of showing a document already stored (distribution package), of possible cancellation and discarding.

Since 2014, Tinexta Infocert has been among the first Italian companies accredited by the Agency for Digital Italy (AgID) as a provider, when it was a regulatory requirement necessary to provide compliant Digital Preservation services for the Italian Public Administration according to the Prime Ministerial Decree then in force. Since 2022, Tinexta Infocert has been among the first Italian companies registered in the AgID Preservation Services Marketplace, according to the most recent Guidelines fully applicable from January 1 of that same year. The presence of Tinexta Infocert in the List of registered registrars frees the Administration that entrusts it with the preservation service from the obligation to transmit the relevant contracts to AgID within thirty days of signing so that the Agency can carry out the activities of verifying the general requirements as well as the quality, security and organization requirements referred to in Annex A of the Regulation on the criteria for the provision of preservation services for electronic documents.

In addition, the Safe LTA storage service has been registered since October 2023 in the Catalog of Qualified Cloud Services for PA (Cloud Marketplace) managed by the National Cybersecurity Agency (ACN).

Safe LTA adopts the European e-ARK specifications on information packages and the international standard OAIS - *Open Archival Information System* (ISO 14721:2012) provided for long-term storage and, where necessary, adopts the specific legislation of the individual country. Details of the main references for legislation and standards on the subject are reported in the corresponding paragraph of the Tinexta Infocert Preservation Manual.

#### **Limitation of the Service in mere consultation**

The Customer may request that the Service be used in a reduced mode, i.e. with the mere consultation of documents already archived, but without the possibility of transmitting new ones for storage.

The request for limitation can be made to Tinexta Infocert on the occasion of the expiry of the service or one of the subsequent renewals, by certified email or registered mail with return receipt, at least 30 days before the expiry date.

In the event of a timely request, Tinexta Infocert will formulate a specific economic offer for the mere consultation service. If the Parties do not reach an agreement on the fee for the new Service, the Agreement is deemed terminated at the deadline in which the Client has made the request for limitation.

### **3. Technical-regulatory specifications**

The Customer is understood as the one who accepts the terms of the Framework Agreement and can identify himself as the legal representative of the Data Controller, i.e. the person authorized to purchase this product or may have purchased it on his own, paying the fee for the Service to Tinexta Infocert. The owner of the objects to be stored (the "Owner") or producer is the person who has created or who is in any case the owner of the document that will be stored (he may coincide with the Customer and/or with the Preservation Manager - *a subject attributable both to the organization of the Owner, and external to this organization, who defines and implements the overall policies of the preservation system of the latter and governs its management with full responsibility and autonomy and who signs the Appointment to Preservation, on behalf of the Owner, towards the Tinexta Infocert Provider*- and/or may coincide with the Producer of the payment packages (hereinafter "Payment Packages" or "PdV") - the producer of the payment packages of the objects to be stored



(it may coincide with the Owner and/or the Customer) - when it also forms the payment package of the storage objects. The Data Controller's data and documents are considered definitively acquired when they are highlighted to the user by making the payment report available.

#### **Assignment of the preservation service**

For the purposes of carrying out the activities referred to in point 2 by Tinexta Infocert, the Data Controller, for the entire duration of the Framework Agreement, entrusts Tinexta Infocert with the Data Controller's data and document preservation service, subject to the signing of the Appointment by the Data Processor (whether internal or external to the Data Controller's organization). Tinexta Infocert therefore assumes the role of "Provider" pursuant to point 4.4, par. 1, letter e) of the Guidelines.

#### **Appointment of the Data Processor (or sub-Processor) of the processing of personal data, pursuant to EU Regulation no. 679/2016.**

Pursuant to point 4.10 of the Guidelines, Tinexta Infocert, as an external party to whom the Preservation Officer, in the name and on behalf of the Data Controller, entrusts the storage service, assumes the role of data processor of which the Preservation Manager is the "data controller" pursuant to art. 4, no. 7) of the Regulation, or assumes the role of sub-processor, in the event that the Data Processor is in turn "Data Processor" pursuant to art. 4, no. 8, of the Regulation. In particular, the Preservation Manager entrusts Tinexta Infocert with the execution of the following processing operations, to be carried out with the aid of electronic tools and within the specific limits provided for by the Guidelines and the Framework Agreement: collection, recording, organization, storage, consultation, processing, selection, extraction, interconnection, communication, cancellation and (possible) destruction of data. The Data Processor, therefore, guarantees to base the processing of the aforementioned personal data (and the related delegation in favor of Tinexta Infocert) on a suitable legal basis, pursuant to art. 6 of the Regulation, presenting itself as an independent data controller or as a data processor in turn legitimately appointed. The Data Processor, therefore, appoints Tinexta Infocert as data processor or sub-processor (the "Data Processor" - it should be noted that, for simplicity, this term is used both in the event that Tinexta Infocert is the Data Processor and in the event that it is a sub-processor), assuming all related obligations and responsibilities and indemnifying Tinexta Infocert from any claim that may come from third parties in reference to the processing operations implemented by Tinexta Infocert by virtue of the mandate conferred on it by this deed. The very nature of the Service implies that the only instructions that the Data Processor will receive will be those provided for by the Framework Agreement, its Annexes and the legislation on the storage of electronic documents.

In light of the above, Tinexta Infocert undertakes to:

- adopt the security measures provided for by the applicable legislation, including those referred to in Article 32 of Regulation (EU) 679/2016;
- comply with the obligations imposed on the Data Processor (or sub-Processor) by Article 28 of Regulation (EU) 679/2016;
- assist the Data Processor (or, where necessary or requested, the Data Controller) in fulfilling the obligations arising from Regulation (EU) 679/2016, within the limits of the commitments undertaken pursuant to the Agreement, in order to ensure compliance with the obligations referred to in Articles 32 to 36 of Regulation (EU) 2016/679, taking into account the nature of the processing and the information available to the Data Processor;
- with particular reference to the obligations regarding the notification of personal data pursuant to Articles 33 and 34 of the Regulation, inform the Data Protection Officer (or, where necessary or requested, the Data Controller) of any personal data breach without undue delay, after becoming aware of the breach itself;
- delegate individual processing operations to any third-party companies, duly designated in writing as sub-processors and instructed to assume the same obligations assumed by Tinexta Infocert by virtue of this appointment with respect to the protection of personal data;



- instruct in writing the persons who will process personal data on behalf of the Data Processor, authorizing them to carry out only the processing operations strictly necessary for the correct provision of the Service, with a commitment to confidentiality and indication of any instructions necessary for the execution of a processing in compliance with Legislative Decree 196/2003 and Regulation (EU) 679/2016;
- to follow up on requests or measures of the Guarantor for the protection of personal data or other competent authority in relation to the processing of data for which Tinexta Infocert is responsible;
- carry out data deletion operations, when requested by the Data Processor or directly by the Data Controller during the effectiveness of the Agreement and within the terms established therein;
- delete and/or return - at the choice of the Data Controller, or directly of the Data Controller - the data subject to processing at the end of the Service, without prejudice to any obligations to retain personal data deriving from European Union or the relatives States Member law;
- not communicate the personal data subject to processing to third parties.

In the event that the Preservation Manager (or directly the Data Controller) expresses in writing needs such as to require processing other than that referred to in the Framework Agreement, after assessing the regulatory compliance of the storage Manager/Data Controller's request, Tinexta Infocert will inform the Preservation Manager/Owner/Customer in writing about the feasibility of the requested solution and the related costs, by means of a specific offer, possibly also re-evaluating the classification to be given to the relationship, also pursuant to Regulation (EU) 2016/679. The Data Processor, in its capacity as data controller or data processor, acknowledges and accepts that Tinexta Infocert is authorized to use Amazon Web Services, Inc. and Wiit S.p.A. as Sub-Data Processor for the performance of cloud data storage services. The Data Processor informs the Data Processor that cloud data storage at Amazon Web Services, Inc. and Wiit S.p.A. takes place on servers located in Italy.

### **Data retention**

The Data Controller's data and documents are considered definitively acquired when they are evidenced to the Producer of the submission agreement and/or to the User through the provision of the payment report. Prior to this operation, Tinexta Infocert assumes no responsibility, except in cases of willful misconduct or gross negligence, for any theft, loss, destruction or loss of the Data Controller's data and documents, who, for the purposes of their preservation, must send them again.

### **Obligations of Tinexta Infocert**

Tinexta Infocert undertakes to store the documents sent by the Customer/Owner and/or the Producer of the submission agreement, subject to the positive outcome of the verification of compliance of the documents sent with the characteristics provided for in the Submission Agreement attached below and to the verification of the format and other specifications agreed upon in the design phase of the preservation system, according to the provisions of the Preservation Appointment and on the basis of the specific procedures for each service as best as possible. highlighted in the Offer, the Submission Agreement and the Preservation Manual. In particular, the Customer/Producer/Data Controller acknowledges that, by virtue of the provisions of point 4.7, par. 2, letter b) of the Guidelines, this verification of conformity is carried out with regard exclusively to what is established in the Tinexta Infocert Preservation Manual and to what is indicated, on the subject of file formats, in Annex. 2 to the Guidelines, as well as, as regards metadata checks, to what is reported in the Guidelines.

The retention of documents is limited to a period of 10 years from the date of time stamping affixed to the archiving packages, unless otherwise specifically agreed in the Order or in the Framework Agreement signed.

### **Tinexta Infocert's responsibilities**

Tinexta Infocert undertakes to provide the Services requested by the Customer in compliance with the provisions of the Framework Agreement, the Annexes relating to it, the AgID Guidelines, the Ministerial Decree



on Economics and Finance of 17.06.2014 and any subsequent amendments or additions thereto, not assuming any responsibility other than what is expressly established therein.

For the purposes of the previous point, the scope of this Framework Agreement does not include the interpretation of the above-mentioned rules and, more generally, of the tax legislation, in relation to individual concrete cases, since these are competences more properly attributable to members of the respective regulated professional categories. Tinexta Infocert, except in the case of wilful misconduct or gross negligence, will not incur liability for direct or indirect damages of any nature and entity that may occur to the Producer of the submission agreements, the Customer, the Owner, the User and/or third parties as a result of use that does not comply with the provisions of the Annexes and the regulations referred to in the paragraph "Obligations of Tinexta Infocert", and any subsequent modifications, and/or non-use of the Services, even in the event of delays or interruptions or due to errors and/or malfunctions of the same, if they fall within the scope of the parameters of unavailability.

The Customer and/or Owner alone, in the event of exceeding the unavailability parameters established in the service levels, except in the case of intervention for ordinary and/or extraordinary maintenance, will be entitled to obtain, by way of compensation for all damages suffered, a refund of the price paid for the service related to the period of non-use of the same.

Except in cases of willful misconduct and gross negligence, Tinexta Infocert will be required to indemnify the Customer and/or the Data Controller and/or the User, in the event of failure to comply with the timing and procedural methods for the storage of the documents transmitted established by the legislation and the Annexes, only in the event of assessment and imposition by the tax administration of administrative sanctions against them and within the limit of the sanction applied. Reimbursement cannot be requested if the non-use is attributable to the connectivity operator or derives from fortuitous circumstances, force majeure or causes not attributable to Tinexta Infocert, such as, by way of example, strikes, riots, earthquakes, acts of terrorism, popular riots, organized sabotage, chemical and/or bacteriological events, war, floods, measures of the competent authorities on the subject or inadequacy of the structures, of the hardware and/or software machinery used by the Customer and/or Owner and/or by the User.

Furthermore, Tinexta Infocert, except in the case of willful misconduct or gross negligence, shall not be encumbered by charges or liability for direct or indirect damages of any nature and entity that may occur to the Customer and/or Producer and/or the User caused by tampering or interventions on the service or equipment carried out by the Customer and/or the Producer and/or the User and/or by third parties not authorized by Tinexta Infocert.

### **Obligations of the Customer, the User and the Owner**

The Customer declares, under his/her sole responsibility, to be endowed with the powers necessary for the signing of this deed or to have received formal assignment from the Data Controller, pursuant to art. 1387 et seq., of the Italian Civil Code, and, if applicable, 1704 of the Italian Civil Code, for the signing of the Framework Agreement. The Client undertakes to inform the User of the provisions of this Agreement and, in particular, of the obligations and charges specifically required for the purpose of using the Services. The Client, the Data Controller, the Preservation Manager and the User undertake to provide all the information necessary for the activation of the Services and to equip themselves with all the necessary requirements for access to the same as better specified in the relevant Attachments. The Preservation Manager, the Producer, the Customer, the Data Controller and the User also undertake to send all the documents that must be stored in electronic form in the manner and in the formats provided for in the Preservation Manual and in the Submission Agreement and in compliance with the methods and terms established by the relevant legislation. The Client and/or the Data Controller and/or the Preservation Manager have autonomy in the configuration of the storage environments based on certain companies, document classes, certain metadata and formats. The Data Controller and/or the User are required to send all communications to the Tax Administration and to carry out, on their own, all the obligations prescribed by tax legislation on the storage of documents. In any case, each



subject will have, in addition to what is provided for in the Agreement, the obligations and responsibilities deriving from their role, as defined by the Guidelines.

### **Responsibilities of the Customer, the User and the Owner**

The responsibility for the Data Controller's Data, including those for which the Data Controller carries out processing, even if not in its capacity as Data Controller, pursuant to EU Regulation 679/2016, is exclusively borne by the Data Controller and/or the User and/or the Preservation Manager. Access to the Services is allowed only in the manner indicated in the Submission Agreement and the Client, the Owner, the User and the Data Processor undertake not to use or to use different applications and/or manual processes or automatic applications to access, view, copy or use the Services.

You may not use the Services to store, store, send, publish, transmit and/or share data, applications or electronic documents that:

1. infringes or infringes the intellectual property rights, trade secrets, trademarks, patents or other proprietary rights of any third party;
2. has defamatory, libelous or threatening content;
3. contain pornographic, obscene or otherwise contrary to public morals; contains viruses, worms, Trojan horses or other contaminating or destructive characteristics;
4. in any case are in contrast with the applicable laws and/or regulations.

The Data Controller/Processor acknowledges that Tinexta Infocert, also pursuant to the provisions of art. 14, 15, 16 of Legislative Decree 9.4.2003, n. 70, has no obligation to monitor the content of the documents and the data that are stored, viewed or shared through the Services and, therefore, will have no obligation to monitor or examine them.

Tinexta Infocert, pursuant to the provisions of art. 17 of the aforementioned legislative decree, is subject to the information obligations provided for therein and also reserves the right to suspend the Services, or to prevent access to the documents and/or data contained therein, if it becomes aware of a violation of the above provisions and/or an express request is made to that effect by a judicial or administrative body competent in the matter according to the regulations in force.

In the cases referred to in the previous paragraph, Tinexta Infocert will communicate by certified e-mail to the Data Controller/Preservation Manager the reasons for the adoption of the measures established therein, with the right of the same to terminate the relationship pursuant to the Framework Agreement.

### **Obligations and responsibilities regarding the generation and association of metadata**

The Client, the Data Controller, the Producer and the Preservation Manager, each within their own sphere of competence, acknowledge that, pursuant to point 2.1.1 of the Guidelines, "At the time of the creation of the unmodifiable electronic document, the relevant metadata must be generated and permanently associated with it", as defined in Annex. 5 to the Guidelines themselves (the "Metadata").

The obligation of the correct and complete association of the Metadata with the electronic document being stored is exclusively the responsibility of the Data Controller, who therefore assumes, also towards Tinexta Infocert, all responsibility in this regard. The Producer, however, as the person who prepares the Payment Package, is jointly and severally liable with the Owner of the Metadata association activity.

Tinexta Infocert, as Provider, has no burden of verification regarding the content of the Metadata.

Furthermore, within the scope of this Agreement, Tinexta Infocert does not carry out any consultancy activity aimed at regularizing electronic documents with respect to the provisions of the applicable legislation and the Guidelines. In the event that the electronic document transmitted for storage does not comply with the provisions of the Submission Agreement, Tinexta Infocert will send the Data Controller and/or the Preservation Manager a communication of error and rejection with the report of the problem. After, again for the reasons indicated in the previous paragraph, the refusal has been repeated three times, it is the responsibility of the



Data Controller and/or the Preservation Manager to contact the Tinexta Infocert technical assistance service to try to solve the problem.

### Restitution

In any case of termination of the Framework Agreement and/or the preservation service, Tinexta Infocert returns the Distribution Packages (submission agreement) to the Customer/Owner, allowing the Customer, free of charge, to *download the* Data Controller's data and documents. The *download* must be made within 30 (thirty) days from the termination of the effectiveness of the Framework Agreement and/or Service.

As an alternative to the provisions of the first paragraph, at the request of the Data Controller, the Data will be provided by Tinexta Infocert, against the payment of specific fees to be defined, on physical media prepared for this purpose by Tinexta Infocert itself.

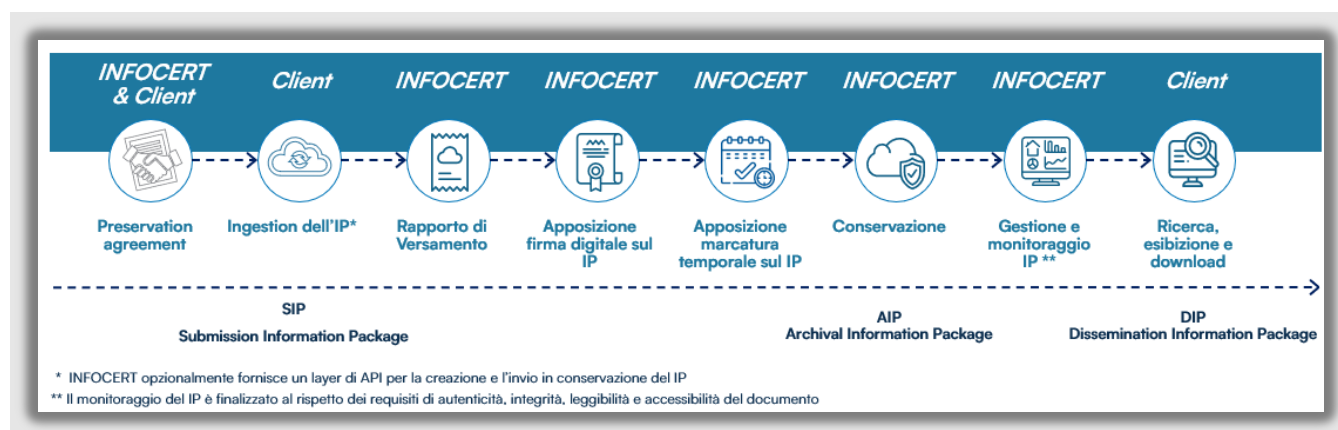
After 30 (thirty) days from the date of termination of the Framework Agreement and/or Service, Tinexta Infocert will no longer have any responsibility for the storage of the Data Controller's or the User's Data and, consequently, will cease its role as Data Processor.

### Activation

Tinexta Infocert, having verified the access requirements, assigns the Owner/User an enabling profile for access to the requested Services within 10 days of activation of the Service.

## 4. TECHNICAL SPECIFICATIONS

### The preservation process



The proposed preservation process, according to the ISO 14721 OAIS standard, manages the preservation of documents through the creation of "Information Packages" (IPs). These packages contain the document and all the related information (metadata), which allow it to be enriched and made available to the Customer over time.

To perform long-term retention of the document, two macro-phases take place:

#### A. Synchronous phase – Submission of the SIP (Submission Information Package):

1. Receipt of the SIP package, produced by the Customer itself (in which case the CORE APIs will be used for integration with the Customer's applications) or by the system (through the storage frontend or integration with the BUSINESS APIs);
2. Validation and preparation of the retention flow management job;
3. System response with acceptance (payment report) or rejection of the preservation request.

#### Tinexta Infocert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM) , Italy  
T +39 06 836691  
info@infocert.it  
infocert.it infocert.digital

Company subject to the management and coordination of Tinexta SpA  
P.IVA 07945211006 REA n. 1064345  
Share Capital subscribed and paid-up € 21,099,232.00

## B. Asynchronous Phase – Preservation:

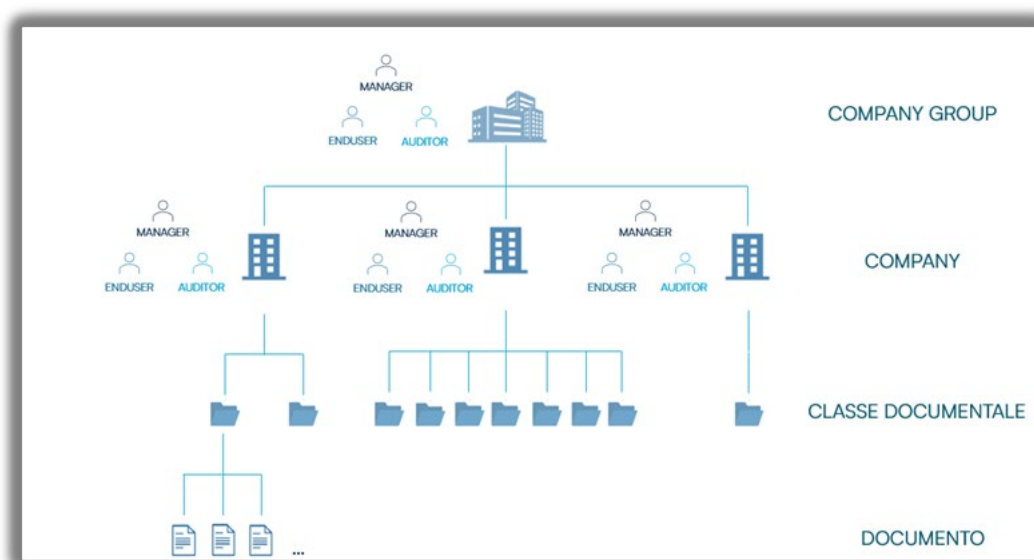
1. Transformation of the SIP package into AIP (Archiving Information Package), if the SIP verification and validation have been successful;
2. Enrichment of the AIP with additional audit trail data;
3. AIP package retention and indexing.

The description file of the AIP packages (pindex.xml, for AIPs compliant with the AgID Guidelines) is sealed and marked by Tinexta Infocert as the Preservation Service Manager.

Tinexta Infocert is therefore responsible for monitoring the AIP, in order to ensure its integrity, authenticity, reliability, readability, availability and availability throughout the storage period.

The Client/User will be able to search for and retrieve the document or the PdD (distribution package), i.e. the document itself together with the complete set of the description file of its IP), either via web interface or via REST API call.

## Retention environment: hierarchical structure and user roles



Safe LTA has the following hierarchical entities:

- **Company Group:** identifies a logical box on which one or more Companies, i.e. storage areas, can depend. Each Company Group is intended for the exclusive use of a single customer and can be configured exclusively by Tinexta Infocert.
- **Company:** a document storage area that can be used to store, for example, the documents of a single company/company in a group (Company Group), naming each Company (Producer) with the name of the individual company/company that is part of the Group. Companies can only exist within a Company Group and are uniquely identified by their name within their Company Group.

During the definition phase, a Company is uniquely associated with a *Country*: this field identifies the regulatory standards adopted by the preservation system within that Company. Currently, the following standards are envisaged:

- *Italy*: for Italy, it will contain only the Document Classes (see below) accompanied by the relevant set of metadata compliant with Annex 5 of the AgID Guidelines.

One Company Italy will support the national technical standard UNI SInCRO (UNI 11386:2020 -

### Tinexta Infocert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM) , Italy

T +39 06 836691

info@infocert.it

infocert.it infocert.digital

Company subject to the management and coordination of Tinexta SpA

P.IVA 07945211006 REA n. 1064345

Share Capital subscribed and paid-up € 21,099,232.00



*"Support for interoperability in the preservation and retrieval of digital objects") for the creation of the so-called closure file (pIndex) of storage packages (otherwise called Preservation Index or Index of the archiving package).*

- **Other:** for all other countries except Italy, ensuring the possibility of configuring the supported data structures according to any local regulations other than those of Italy. A Company Other will support the internationally widely used METS (Metadata Encoding and Transmission Standard) metadata format for the creation of the Preservation Index.
- **Document Class :** identifies a type of document to which the relevant metadata is associated. For example: active invoices, expense reports, contracts, books and accounting records, etc. Document Classes can only exist within a Company (storage area) and are uniquely identified by their name within their Company.
- **Documents:** Leaves in the preservation environment, which represent a single inserted document with its accompanying metadata. Documents can only exist within a Document Class and are uniquely identified in Safe LTA by randomly generated version 4 UUIDs.

The above objects define the permissions in terms of visibility and operation of the configured users.

A user can only be created within a Company Group, Company, or Document Class node. The scope of operation of a given user depends on the level of the retention environment in which that user has been defined:

- if a user is defined at the Company Group level, he will be able to operate on the entire tree of the preservation environment rooted in that Company Group, including all the Companies and associated Document Classes (and related Documents) under that Company Group. The other Company Groups (and the related Companies, Document Classes and Documents) will be invisible to the user;
- if a user is defined at the Company level, he will be able to operate only on the subtree of the preservation environment rooted in that Company, including all Document Classes and Documents associated with that Company. The other Company Groups (and the related Companies, Document Classes and Documents) will be invisible to the user, but also the other Companies (and the related Document Classes and Documents) defined in the Company Group to which the defining Company belongs will be invisible to the user;
- if a user is defined at the level of the Document Class, he will be able to operate only on that specific Document Class and the Documents contained therein. All other nodes in the preservation environment and their Documents will be invisible to you.

Users have the following roles associated with them:

- **Manager:** is the user authorized to **perform configurations** within his Company Group. This user has visibility by default on all Companies and all Document Classes. The Manager has the right to independently configure new Auditor or EndUser users. Alternatively, the Customer can request Tinexta Infocert to fully configure its preservation environment;
- **End-user:** is the user authorised to deposit in storage, research and extraction/exhibition of documents;
- **Auditor:** is the user authorized only to **search** and **extract/exhibit** documents.

### Key features

- Provisioning Retention Environments (Company)
- Document class configuration
- Manage users, groups, and permissions
- Sending for storage of payment packets and transformation into preservation packets composed according to E-ARK specifications
- Advanced search tasks
- Document and metadata retrieval



- Downloading preservation packages as ZIP files

### How to provide the SAFE LTA service

The service can be provided in the following ways:

- ❖ In SaaS mode
- ❖ On-premise

The Customer will be able to access the service and its functions via a dedicated web interface, or via API.

The service provided may cover the entire preservation and consultation process or consultation only, as described in 3. TECHNICAL-REGULATORY SPECIFICATIONS.

### Minimum technical requirements

The minimum requirements are for a worker node with the following specifications: 4 CPU cores, 4 GB of RAM, 40 GB of disk space.

### Supported formats

For each Document Class, indicated in the appropriate section of the Submission Agreement, it is possible to provide for the payment for storage of one or more file formats (mime-type), as required by the Italian AgID legislation on formats, i.e. Annex 2 - File formats and transfer" of the AgID Guidelines. The Customer/Owner/Producer/User undertakes to maintain the tools necessary for viewing the same documents and any documents attached to them.

For MSG and EML formats, the Producer undertakes to keep the software necessary to read the attached files.

In the case of sending encrypted files for preservation, the Producer undertakes to keep the software necessary for their decryption, relieving Tinexta Infocert of responsibility for their display.

In the event that it is necessary to store a "compressed archive" file (to be indicated in the appropriate section of the Submission Agreement), such as .zip or .rar, the Producer/User undertakes to maintain the tools necessary for viewing the documents contained within the 'compressed archive' files (and any attachments attached to them). In such cases, the Producer/User must in fact ensure the provisions of the aforementioned AgID Guidelines, in particular Annex 2 and subsequent amendments, relating to the programs for viewing the documents themselves and the obligation to show them.

### High-level architecture

SafeLTA is designed to be delivered both on-premise and in the cloud. The product architecture provides for two modes:

- ❖ Standalone mode, with which the assets can all be dispensed on the Kubernetes platform
- ❖ AWS cloud mode, with which the integration of AWS services can be leveraged:
- ❖ Object Storage S3
  - OpenSearch
  - DocumentDB

Safe LTA is designed to be cloud-native in the Amazon Web Services (AWS) environment, using Amazon Simple Storage Service (S3) for storing captured documents and Amazon OpenSearch Service for indexing their metadata.

#### Tinexta Infocert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM) , Italy  
T +39 06 836691  
info@infocert.it  
infocert.it infocert.digital

Company subject to the management and coordination of Tinexta SpA  
P.IVA 07945211006 REA n. 1064345  
Share Capital subscribed and paid-up € 21,099,232.00



In its standard SaaS delivery, it is delivered through the Italian AWS Region and interacts with the following Tinexta Infocert services delivered through the Tinexta Infocert Data Center:

- Tinexta Infocert Identity Provider, for the management of digital identities;
- Tinexta Infocert SignAPI, for eSealing and Time Stamping functionality.

SafeLTA has an architecture approach to MicroServices and the latter provide precise functional and business perimeters. The business perimeters that together make up the SafeLTA product are as follows:

- Provisioning perimeter provided by the "SafeLTA Provisioning Manager" MicroService
- Perimeter of management of templates, document classes and metadata provided by the MicroService "SafeLTA DocumentClass Manager"
- Perimeter of storage provided by the MicroService "SafeLTA Preservation Manager"
- Indexing and document search perimeter provided by the "SafeLTA DataKeeper Manager" MicroService

The perimeters and components listed are part of the "SafeLTA Core Services".

Each business perimeter provides the functions of its competence and all together they make up the catalog of REST APIs provided by the product.

The provision of the API catalog is delegated to the "Tinexta Infocert API Gateway" component, which also acts as a reverse proxy to the micro-services that are in turn secured.

The REST API catalog can be used over the HTTPS protocol and only by trusted software agents governed by authentication flows according to the OpenIDConnect/OAuth2 standard.

In addition, the latter can be used both by Web interface applications, already provided by the SafeLTA product and part of the "SafeLTA UI Services" module, and by external systems that need to integrate the SafeLTA functions within their application context and mentioned as "External Customer Systems".

#### **Identification and access to the system**

The Owner and/or Customer and/or the User may use the Services after verifying the requirements for access to the system, using the identification tools provided in the appropriate Attachments.

The Data Controller and/or Customer and/or the User are informed of the fact that the knowledge of the identification tools by third parties would allow the latter to access the Services and Data of the Data Controller. The Data Controller and/or Customer and/or the User is therefore required to keep and have its staff who use the Services keep these identification tools with the utmost confidentiality and with the utmost diligence, undertaking not to transfer them or allow their use to third parties. Tinexta Infocert may not in any case be held liable for any direct and/or indirect damage resulting from the failure of the Data Controller and/or Customer and/or the User to comply with the above.

## **5. SLAs and KPIs:**

### **Service SLA**

In terms of delivery, the following monthly service availability values are expected:



| KPIs Availability | Service         | Schedule | Availability |
|-------------------|-----------------|----------|--------------|
| <b>D01</b>        | <b>Safe LTA</b> | 24x7     | 99,00%       |

The following describes how availability KPIs are calculated:

| KPI                  | Scope                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>D01, D02, ...</b> | Availability of Services | <p>The calculation method for availability indicators is based on the following values:</p> <p><b>observed period</b> = duration in seconds of the observation period, net of scheduled maintenance</p> <p><b>Unavailability time</b> = sum of the durations in seconds of the service unavailability times, in the observation period</p> <p>The availability value is calculated, for each service, using the following formula:</p> $D = \frac{\text{observed period} - \text{Unavailability time}}{\text{Observed period}} * 100$ <p>The observation period is monthly.</p> <p>The violation is identified when <b>D &lt; agreed availability</b></p> |

Tinexta Infocert limits its responsibility to the provision of its services, and is therefore not responsible for any performance anomalies due to unavailability or slowness in the network that connects the Customer to the IDC.

Tinexta Infocert is also not responsible for anomalies deriving from:

- incorrect configuration or sizing of the Customer's infrastructure;
- incorrect installation or configuration of software using Tinexta Infocert services on the Customer's infrastructure.

### Performance KPIs

The following performance KPIs have been identified for Safe LTA:

1. Average SIP packet takeover time: 900ms – 1.6s
2. Average time to sign and time stamp on the package: 480ms
3. Average Full Retention Time: 3.8s



## Responsibility delegation

The undersigned **Preservation Manager** (the "**Preservation Manager**"), for this purpose and in this role appointed by the following person, in the name and on behalf of whom he acts:

[COMPANY NAME] \_\_\_\_\_ - Tax Code \_\_\_\_\_;  
(the "**Owner of the objects of preservation**")

Surname and Name \_\_\_\_\_

Date of Birth \_\_\_\_/\_\_\_\_/\_\_\_\_ Tax Code \_\_\_\_\_ Citizenship \_\_\_\_\_

PEC address for communications \_\_\_\_\_@\_\_\_\_\_

as part of its role as **Preservation Officer**, as provided for by par. 4.5 of the "AgID Guidelines on the formation, management and storage of electronic documents" adopted by AgID in September 2020 and by art. 34 paragraph 1-bis of the Digital Administration Code (Legislative Decree no. 82 of 7 March 2005 and subsequent amendments), and in any case declaring, for all legal purposes, to be entitled to sign this document, in the name and on behalf of the Owner(s) of the objects of preservation,

### ENTRUSTS

to Tinexta Infocert S.p.a., with registered office in Rome, Piazzale Flaminio 1/B, VAT number 07945211006, the preservation service of the electronic documents of the Data Controller(s) of the objects of preservation, in accordance with the provisions of the Technical Annex.

Data \_\_\_\_\_

Signature of the preservation Manager \_\_\_\_\_

Especially:

- 1) The activities of transferring stored documents from one storage medium to another, which constitute a service in its own right, carried out upon any express and separate request, are excluded from the assignment of the activities that precede the sending of the documents (e.g., the digitization of analogue documents, compliance with the times prescribed for sending them for storage, the suitability of the software adopted by the Data Controller) and the correctness and consistency of the contents of the same.
- 2) For the purposes of the preservation of the original analogue documents, the Owner of the object of storage or another person duly delegated by him must independently affix the digital signature to the documents and, where applicable, for particular types of unique original analogue documents, to have a public official intervene, who certifies the conformity between the document stored and the original, pursuant to art. 22, c. 4 and 5 of Legislative Decree 7.03.2005, no. 82 CAD and art. 4 of the D.M.E.F 17.06.2014 for documents relevant for tax and tax purposes.
- 3) On the basis of this appointment, Tinexta Infocert S.p.a. will act as Preservation Service Manager of the electronic documents of the Owner(s) of the object of storage, providing for the execution of the tasks defined



by the AgID Guidelines, in accordance with the provisions of the Framework Agreement and the Technical Annex defined therein.

In particular, within its organization, Tinexta Infocert S.p.A. has appointed a Preservation Officer, who:

- a) defines the storage policies and functional requirements of the storage system, in accordance with current legislation and taking into account international standards, due to the specificities of the digital objects to be stored (electronic documents, computer aggregations, computer archive), the nature of the activities that the Owner of the storage object carries out and the characteristics of the IT document management system adopted;
- b) manages the preservation process and ensures compliance with current legislation over time;
- c) generates and signs the payment report, according to the procedures provided for in the preservation manual;
- d) generates and signs the distribution package with digital signature, in the cases provided for in the preservation manual;
- e) monitors the correct functionality of the preservation system;
- f) carries out periodic verification, every five years, of the integrity and legibility of electronic documents and documentary aggregations of archives;
- g) in order to ensure the preservation of and access to electronic documents, it shall take measures to promptly detect any deterioration of storage systems and recordings and, where necessary, to restore proper functionality; it adopts similar measures with regard to the obsolescence of formats;
- h) provides for the duplication or copying of electronic documents in relation to the evolution of the technological context, in accordance with the provisions of the preservation manual;
- i) prepares the necessary measures for the physical and logical security of the storage system;
- j) ensures the presence of a public official, in cases where his intervention is requested, guaranteeing him the assistance and resources necessary for the performance of the activities attributed to him;
- k) provides the competent bodies provided for by the regulations in force with the assistance and resources necessary for the performance of verification and supervision activities.

---

(Signature of the Preservation Officer)

---