ENTAKSISOLUTIONS

CERTIFIED MANAGEMENT SYSTEM
ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
QUALIFIED TRUST SERVICES
ETSI 319 401 | ETSI 319 411-1 and 2 | ETSI 319 421 | ETSI 119 511
ELECTRONIC SIGNATURES AND SEALS - TIME STAMPS
LONG-TERM PRESERVATION

Manual

MAN eIDAS 20210628 Preservation Service Policy EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20210628 Preservation Service Policy EN
Version	1.3.0
Creation Date	28/06/2021
Last Revision	02/12/2025
Author	Alessia Soccio
Status	Released
Classification	Public
Translation	This document is the original version. Italian translation: "MAN eIDAS 20210628 Preservation Service Policy".

Paper reproductions of this document are to be considered working copies not registered by the SIG.

Revisions and releases

Date	Version	Name	Role	Action	Release
28/06/2021	0.0.1	Alessia Soccio	IMSM	Draft creation.	Internal
01/12/2021	1.0.0	Alessia Soccio	IMSM	Review and release.	Public
15/12/2023	1.1.0	Alessia Soccio	IMSM	Periodic update, review of company presentation, formal review of definitions and regulatory references, minor corrections.	Public
05/12/2024	1.2.0	Alessia Soccio	IMSM	Periodic update, certifications and references review, minor corrections.	Public
02/12/2025	1.3.0	Alessia Soccio	IMSM	Update to EU Regulation No. 1183/2024 – eIDAS 2, minor corrections.	Public

Document approval

Date	Employee	Role	Signature
02/12/2025	Alessandro Geri	Sole Manager	*Digitally signed*

1. Introduction

This document is the **Preservation Service Policy regarding the eCON Preservation Service provided by Entaksi Solutions SpA - Irish Branch** (hereinafter "Entaksi"), a branch of the Italian company with VAT-ID IT01621900479 Entaksi Solutions SpA, operating in Ireland with National Trade Register number 909882.

Entaksi is a **Trust Service Provider** for:

- **The issuance of qualified certificates for electronic signatures**.
- **The issuance of qualified certificates for electronic seals**.
- **The qualified preservation service for qualified electronic signatures**.
- **The qualified preservation service for qualified electronic seals**.
- **The creation of qualified electronic timestamps**.

Entaksi is registered as a Trust Service Provider by the competent national supervisory body in Ireland (currently the Department of the Environment, Climate and Communications – DECC) and is included in the national trusted list in accordance with the eIDAS Regulation.

The eCON Preservation Service is a qualified trust service providing long-term preservation of digital signatures, seals and general data using digital signature techniques, as defined by EU Regulation 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended by EU Regulation No. 1183/2024 – eIDAS 2 (hereinafter "eIDAS")

Within the document, the following topics are set out:

- the description of all the policies regarding the eCON Preservation Service;
- the set of rules applicable to the qualified eCON Preservation Service, addressed to the determined preservation community;
- the security requirements applied.

1.1. Document identification

This document is identified by the following OID:

Table 1. Document name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.1	MAN eIDAS 20210628 Preservation Service Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1

The OIDs identifying the specific eCON Preservation Service policies are identified within the document.

The following URI is the service digital identifier for eCON Preservation Service:
`https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.3.1`

1.2. Document maintenance

Entaksi has defined a review process for all the internal documents, including policies, statements and practices.

The documents are periodically reviewed under the responsibility of Entaksi management, in order to assess their compliance with national and international requirements, standards, mandatory legislation, regulations in force, particular needs imposed by the technical and technological evolution, evolution of the business context.

The review and any update take place at least once a year, or whenever one of the following circumstances occurs:

- internal organizational changes that impact on the system;
- major changes to the hardware or software architecture;
- regulatory updates;
- changes in procedures, methodologies or business context.

1.3. Approval and publication

This document and all the internal policies and practices mentioned in it have been approved by Entaksi's management, published and communicated to employees and, as regards those classified as "public", published on the company website at the following link: https://www.entaksi.eu/en/documentation.html.
The website is available on 24x7 basis.

Entaksi makes available to all customers of trust services and relying parties any update of this document and other relevant documentation as soon as the update is approved and revised on the basis of what is described in the revision procedure.

Entaksi, will communicate any change that might affect the acceptance of the service by the subject, subscriber or relying parties through the communication channel established in the terms and conditions of the service.

2. Definitions and abbreviations

2.1. Definitions

Certificate Status Authority

authority providing certificate status information.

Container

Data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships.

Data Object

Actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type.

EU qualified preservation service

Preservation service that meets the requirements for qualified preservation service for qualified electronic signatures and/or for qualified electronic seals as laid down in EU Regulation No. 910/2014 - eIDAS.

Evidence record

Unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time.

Expected Evidence Duration

For a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal long-term: time period during which technological changes may be a concern.

Metadata

Data about other data.

Notification interface

Interface provided by the preservation client supporting the notification protocol.

Notification Protocol

Protocol used by a preservation service to notify the preservation client.

Preservation Client

Component or a piece of software which interacts with a preservation service via the preservation protocol.

Preservation Evidence

Evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object.

Preservation Evidence Policy

Set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.

Preservation Evidence Retention Period

For a preservation service With Temporary Storage (WTS) the time period during which the evidences that are produced asynchronously can be retrieved from the preservation service.

Preservation Goal

One of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmentation of externally provided preservation evidences.

Preservation Interface

Component implementing the preservation protocol on the side of the preservation service preservation manifest: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container.

Preservation Mechanism

Mechanism used to preserve preservation objects and to maintain the validity of preservation evidences.

Preservation Object

Typed data object, which is submitted to, processed by or retrieved from a preservation service.

Preservation Object Container

Container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships.

Preservation Object Identifier

Unique identifier of a (set of) preservation object(s) submitted to a preservation service.

Preservation Planning

Monitoring changes and risks e.g. concerning innovations in storage, access and preservation technologies, new design strategies, etc.

Preservation Period

For a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences.

Preservation Profile

Uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.

Preservation Protocol

Protocol to communicate between the preservation service and a preservation client.

Preservation Scheme

Generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated.

Preservation Service

Service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time.

Preservation Storage Model

One of the following ways of implementing a preservation service: with storage, with temporary storage, without storage.

Preservation Submitter

Legal or natural person using the preservation client to submit the submission data object.

Preservation Subscriber

Legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations.

Proof of Existence

Evidence that proves that an object existed at a specific date/time.

Proof of Integrity

Evidence that data has not been altered since it was protected.

Signer

Entity being the creator of a digital signature.

Submission Data Object

Original data object provided by the client.

Time Stamp

data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time Stamping Authority

Trust service provider which issues time stamps using one or more time stamping units.

Time Stamping Service

Trust service for issuing time stamps.

Time Stamping Unit

Set of hardware and software which is managed as a unit and has a single time stamp signing key active at a time.

Trusted List

List that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

Validation Data

Data that is used to validate a digital signature.

2.2. Abbreviations

AUG

Augmentation Goal.

PDS

Preservation of Digital Signatures.

PGD

Preservation of General Data.

PO

Preservation Object.

POC

Preservation Object Container.

PRP

Preservation Service Protocol.

PSP

Preservation Service Provider.

SigS

Digital Signature creation Service.

SubDO

Submission Data Object.

ValS

Validation Service.

WOS

Without Storage.

WST

With Storage.

WTS

With Temporary Storage.

3. References

In order to ensure the compliance of the eCON Preservation Service to rules and regulation, Entaksi defines the criteria and the processes of the Service according to the relevant Italian and European legislation, and, as well, implements international standards that define the theoretical, operational and functional management of the system. Below are enlisted the normative and informative references the company is subject to.

This policy complies with the normative references enlisted below, as required by eIDAS and the Italian digital preservation regulation.

3.1. Normative references

3.1.1. eIDAS Regulation

Entaksi's Integrated Management System, which also oversees the processes described within this document, is certified against the following international standards:

- **ISO 9001:2015**: Quality management systems - Requirements.
- **ISO/IEC 20000-1:2018**: Information technology - Service management - Part 1: Service management system requirements.
- **ISO/IEC 27001:2022**: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- **ISO/IEC 27017:2015**: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27018:2019**: Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- **ISO/IEC 27035:2016**: Information technology — Security techniques — Information security incident management.
- **ISO/IEC 22301:2019**: Security and resilience — Business continuity management systems — Requirements.
- **UNI ISO 37001:2016**: Anti-bribery management systems - Requirements with guidance for use.
- **eIDAS Regulation for Qualified Trust Service Providers**:
  - **ETSI EN 319 401 V3.1.1 (2024-06)**: Electronic Signatures and Infrastructures (ESI) - General Policy Requirements for Trust Service Providers.
  - **ETSI EN 319 411-1 V1.5.1 (2025-04)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements.
  - **ETSI EN 319 411-2 V2.6.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates.
  - **ETSI EN 319 412-1 V1.6.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures.
  - **ETSI EN 319 412-2 V2.4.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons.
  - **ETSI EN 319 412-3 V1.3.1 (2023-09)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 3: Certificate profile for certificates issued to legal persons.
  - **ETSI EN 319 412-5 V2.5.1 (2025-06)**: Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 5: QCStatements.
  - **ETSI EN 319 421 V1.3.1 (2025-07)**: Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
  - **ETSI EN 319 422 V1.1.1 (2016-03)**: Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles.
  - **ETSI TS 119 511 V1.2.1 (2025-10)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
- **CSA STAR**: Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) Level 2.

All the certifications are publicly available at the following link: https://www.entaksi.eu/en/certifications.html.

The Trust Services Management System, a subcomponent of Entaksi's Integrated Management System, complies with the relevant requirements laid down in eIDAS 2 and meets the additional conformity requirements of the following standards:

- ETSI Standards:
  - **ETSI EN 319 102-1 V1.3.1 (2021-11)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation;
  - **ETSI TS 119 102-2 V1.4.1 (2023-06)**: Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 2: Signature Validation Report;
  - **ETSI TS 119 172-4 V1.1.1 (2021-05)**: Electronic Signatures and Infrastructures (ESI) Signature Policies - Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists;
  - **ETSI TS 119 431-1 V1.3.1 (2024-12)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy and security requirements for trust service providers - Part 1: TSP services operating a remote QSCD / SCDev;
  - **ETSI TS 119 441 V1.3.1 (2025-10)**: Electronic Signatures and Trust Infrastructures (ESI) - Policy requirements for TSP providing signature validation services;
  - **ETSI TS 119 442 V1.1.1 (2019-02)**: Electronic Signatures and Infrastructures (ESI) - Protocol profiles for trust service providers providing AdES digital signature validation services;
  - **ETSI TS 119 461 V2.1.1 (2025-02)**: Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects;
  - **ETSI TS 119 495 V1.7.1 (2024-07)**: Electronic Signatures and Trust Infrastructures (ESI) - Sector Specific Requirements - Certificate Profiles and TSP Policy Requirements for Open Banking;
  - **ETSI TS 119 512 V1.2.1 (2023-05)**: Electronic Signatures and Infrastructures (ESI) - Protocols for trust service providers providing long-term data preservation services;
  - **ETSI EN 301 549 V2.1.2 (2018-08)**: Accessibility requirements for ICT products and services;
- ISO Standards:
  - **ISO 14641:2018**: Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
  - **ISO/IEC 14721:2025**: Space data and information transfer systems - Open archival information system (OAIS) - Reference model;
  - **CEN/TS 18170:2025**: Functional requirements for the electronic archiving services.

3.1.2. Long-Term Preservation

The applicable standards for the qualified preservation service for qualified electronic signatures and the qualified preservation service for qualified electronic seals, pursuant to the "Commission Implementing Regulation (EU) n° 2025/2162 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the accreditation of conformity assessment bodies performing the assessment of qualified trust service providers and the qualified trust services they provide, the conformity assessment report and the conformity assessment scheme", are:

- ETSI EN 319 401 V3.1.1 (2024-06).
- ETSI TS 119 172-4 V1.1.1 (2021-05).
- ETSI TS 119 511 V1.2.1 (2025-10).
- ETSI TS 119 512 V1.2.1 (2023-05).
- ETSI EN 301 549 V2.1.2 (2018-08).

3.1.3. Italian Digital Preservation Regulation

Codice dell'Amministrazione Digitale (CAD)

Codice dell'Amministrazione Digitale (Decreto Legislativo del 7 marzo 2005, n. 82, e successive modifiche).

"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"

"Guidelines on the creation, management and preservation of IT documents", issued on 09 September 2020 by the Agenzia dell'Italia Digitale (AgID).

AgID Preservation Service Providers Regulation

"Determinazione" No 455/2021 of the Agenzia dell'Italia Digitale (AgID) of 25 June 2021 on the adoption of ""Regulation on the criteria for the provision of IT document preservation services"".

3.1.4. Data Protection

General Data Protection Regulation (EU) 2016/679

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

3.1.5. Other provisions

The eCON digital preservation system also conforms to the following standards:

UNI 11386:2020

Supporting interoperability in preservation and retrieval of digital objects.

ISO 15489-1:2016

Information and documentation - Records management - Part 1: Concepts and principles.

ISO 15836-1:2017

Information and documentation - The Dublin Core metadata element set - Part 1: Core elements.

ISO 16363:2025

Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

ISAD(G)

General International Standard Archival Description, description standard for archives intended for the registration of documents produced by organizations, individuals and families.

3.2. Informative references

Entaksi's Qualified Long-Term Preservation Service is supported by the following policies, practice statements and manuals:

Table 2. LTP documents name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.1	MAN eIDAS 20210628 Preservation Service Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1
1.3.6.1.4.1.57823.1.4	MAN eIDAS 20210628 Signature Validation Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4
1.3.6.1.4.1.57823.1.3	MAN eIDAS 20210628 Preservation Evidence Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3
1.3.6.1.4.1.57823.1.2	MAN eIDAS 20210628 Preservation Service Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2

The italian conformity document is "MAN eCON 20151222 Digital Preservation Manual".

All the previous enlisted documents are classified as "public" and disclosed to the relying parties on the company website: https://www.entaksi.eu/en/

Furthermore, the subsequent documents illustrate some confidential topics about the eCON Preservation Service, mostly related to system security procedures and technical questions.

Table 3. eCON Preservation Service Confidential Documents

Document name	Document version	Valid from
MAN eCON 20190918 Termination Plan	1.4.0	01/12/2021
MAN eCON 20151222 Security Plan	1.5.0	01/12/2021

Entaksi, due to their confidential content, doesn't disclose these documents and any of its other internal manuals, procedures and security documents. However, according to the company's availability and commitment, it is available to undergo audits by its subscribers or other interested parties, upon signing an un-disclosure agreement.

4. Roles and responsibilities

The **designated community of eCON Digital Preservation Service**, as required by the Open Archival Information System (OAIS) Standard ISO/IEC 14721:2025, is described in the eCON User Manuals, and also are enlisted the roles and activities for each Entaksi's staff member.

Entaksi is appointed as Trust Service Provider for the eCON Long-Term Preservation Service.

The eCON Preservation Service is administrated by various "**Managers**", each of whom covers a very specific role in the company and in the service in particular, in order to better ensure the reliability of the system without overlapping activities and with compartmentalization of roles:

- **Preservation Service Manager (PSM)**.
- **Deputy Preservation Service Manager (DPSM)**.
- **Archival Function Manager (AFM)**.
- **Data Protection Manager (DPM)**.
- **Preservation System Security Manager (PSSM)**.
- **Preservation Information System Manager (PISM)**.
- **Preservation System Development and Maintenance Manager (PSDMM)**.

All the data relating to the persons and specific roles covered by the various managers of the Preservation Service eCON are available in the eCON preservation manual, published both on the Agenzia per l'Italia Digitale website and on the Entaksi Website: https://www.entaksi.eu/en/

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification, or misuse of the Entaksi's assets.

Entaksi Solutions SpA is responsible for the provision of the service, and the Preservation Service Manager (PSM) is the role appointed for service delivery tasks.

In accordance with art. 38 of the "Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013" (Prime Minister's Decree), the following individuals are appointed in addition to those listed above:

- Security Manager.
- Qualified Service Manager;
- Responsible for the technical management of the systems.
- Responsible for technical and logistical services.
- Responsible for audits and inspections (auditing).

4.1. Subscribers

A subscriber is the legal or natural person bound by agreement with a service provider.

Customers can sign the service agreement ("Condizioni generali del servizio") with the preservation trust service provider Entaksi, in order to access the eCON Preservation Service.

4.2. Relying party

Entaksi doesn't involve any external party to perform critical tasks on the eCON Preservation Service. However, other third parts may be involved in the process, such as legal control bodies, authorities, and auditors.
Entaksi always requires non-disclosure agreements to any non-contractual access to the system, such as for audits, and applies anonymization and minimization of personal data wherever possible.

4.3. Suppliers

Entaksi Solutions SpA stated:

- **To place in housing / hosting most of its server infrastructure**.
  Servers that host and provide the various services that the Company needs to carry out its task activities, as well as those that are disbursed to its customers, are placed in data centers managed by specialized suppliers for this purpose. The choice of data centers is reviewed periodically according to the dynamics of the market, choosing each time the structures which offer the most convenient performance/price ratio. The same criterion comes adopted for the use of general

network services (such as, for example, name resolution a domain and related DNS), also entrusted to external services.

- **To hold physical ownership of hardware involved in the provision of trust services for which the legislation requires the Qualified Trust Service Provider's direct control**.
  Such hardware resources are owned by the company and are located in a physical perimeter in which other organizations do not have access, implemented through a dedicated cabinets subject to access control. These cabinets are made available by specialized and qualified suppliers in compliance with sector regulations.
- **Use for all employees and collaborators a contract based on remote working.**.

The result of adopting of these statements is that the company operates entirely on the network, not using physical operational headquarters.

So in Entaksi's organization access controls are managed in three ways:

- through the use of quality checks that are performed during the suppliers' qualification phase and the monitoring of the external services used;
- through the use a controlled environment of accesses;
- through the application of controls relating to information security, in especially way to the assets entrusted to individual employees.

From the point of view of physical security of central infrastructure it is necessary to point that Entaksi's choice, that was an avant-garde choice, today it is a widely established trend that consider the cloud migration as the safest way to manage services.

Entaksi guarantees compliance with minimum requirements in the management of the physical security of the central infrastructure through the qualification process and the monitoring process of suppliers who are selected both on the basis of market convenience and on quality guarantees security offers, such as the ISO/IEC 27001:2022 certification and, if it is necessary, the willingness to be subjected to audits and inspections in order to find any elements not sufficiently covered by the contractual conditions or by the certifications themselves.

Regarding other suppliers not related to the physical infrastructure, Entaksi uses time-stamps provided by its own qualified Time-Stamping Authority.

5. Policies

5.1. Organization reliability

Entaksi's Management is constantly committed to guarantee the reliability of the entire organization and in particular of the eCON Preservation Service provided to the customers.

Entaksi undertakes to be non-discriminatory and to guarantee access to the eCON Preservation Service to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the terms and conditions.

5.2. Human resources

Entaksi commits to employ qualified staff who possess the necessary expertise, reliability, experience, and qualifications to work on the eCON Preservation Service. Also provides constant training regarding cybersecurity and personal data protection rules as appropriate for the offered services and the job function.

TSP's personnel is formally appointed to trusted roles by senior management responsible for security.

Personnel have access to the trusted functions only after the management completes the necessary checks.

Trusted roles defined for the eCON Preservation Service are enlisted in the chapter Roles and responsibilities.

The reviewing process of the training scopes and of the experience gained by the staff takes place periodically, on an annual basis at least. Accrued skills are recorded in the Entaksi databases.

Entaksi's personnel (both temporary and permanent) have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege. The positions are based on the duties and access levels, background screening and employee training and awareness.

Entaksi foresees in its documentation, formally accepted by the employee, that adequate disciplinary sanctions can be put in place to personnel who violate the security policies or procedures.
Personnel shall exercise administrative and management procedures and processes that are in line with Entaksi's management procedures.

The acceptance procedure involves a reviewing from the management and the signature of the employee on the appointment document.

Security roles and responsibilities are clearly identified in job descriptions and in the internal documents, persistently available to all concerned personnel. The roles are differentiate between general functions and eCON Preservation Service specific functions.
Entaksi defines the minimum requirements to fill the roles: all the personnel shall possess experience or training with respect to the service provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

All eCON Preservation Service's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of Entaksi's operations.

5.3. Financial resources

Entaksi arranges its financial resources in order to commensurate them with the safe provision of the eCON Preservation Service, and aim to ensure the financial stability and the necessary resources required to operate in conformity with this policy.

The maintenance of a constant appropriate level of resources to guarantee the correct functioning of technical and structural operations on the eCON Preservation Service is achieved thanks to a constant review of the values deriving from monitoring data.

In addition to these monitoring and adaptation measures, the service is covered by an insurance policy, in line with the requirements of Italian law.

Entaksi has policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the eCON Preservation Service or any other related matters.

5.4. Assets

Entaksi ensure an appropriate level of protection of its assets, including information assets, and it is responsible for the commitment of all the personnel to handle all the media securely, in accordance with its policies and procedures.

Entaksi uses its own software to manage all the resources, a Configuration Management Data Base (CMDB) that constitutes an inventory of all information assets, and declares for each object a classification consistent with the risk assessment.

In order to avoid that sensitive data stored in the assets could be exposed to threats relating to confidentiality, integrity and availability, Entaksi sets specific internal procedures, that describe:

- how to set up the assets to ensure the highest level of protection;
- how to manage backups and copies;
- how to act when is necessary to move the device or dispose it for another use;
- specific requirements to ensure the secure deletion of all the information contained if necessary.

5.5. Risk assessment

Entaksi applies all security controls and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the Information Security Policy and the Preservation Service Practice Statement.

Entaksi carries out regularly a risk assessment to identify, analyse and evaluate risks related to the eCON Preservation Service.

5.6. Incident Management

Entaksi defines a "security incident" as any event that compromises or threatens the correct functioning of the organization's systems and/or networks or the integrity and/or confidentiality of the information stored in the systems or in transit, or that violates the defined security policies or laws in force, with particular reference to General Data Protection Regulation (EU) 2016/679.

The Incident Response Team (IRT) is a group of suitably qualified and trusted members of the organization that manages incidents throughout their lifecycle.

Incident management procedures are based on adherence to ISO/IEC 27035:2016 standard.

The incident management process defined by Entaksi is divided into the following phases:

- **Plan and prepare** - establish an information security incident management policy, form an Incident Response Team, prepare the organization to respond to any malicious event.
- **Detection and reporting** - one or more security events need to be recognized as an incident and each incident is assigned a severity level.
- **Assessment and decision** - the IRT makes an assessment that determinates whether it is in fact an incident and qualifies it.
- **Response** - implementation of countermeasures in order to minimize the damage caused by the accident, and, if necessary, adjustment of the resources and restoration if needed.
- **Subsequent activities** - the update of the risk analysis and the adequacy of the accident management procedures.
- **Lessons learned**: Entaksi's management reviews the incident and identifies possible points for improvement.

Regarding the "Plan and prepare" phase:

- the management appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with Entaksi's procedures;
- system activities concerning access to IT systems, use of IT systems, and service requests are constantly monitored;
- the monitoring activities take into account the sensitivity of any information collected or analysed;
- the Incident Response Team Manager evaluates which parameters to monitor, such as logging functions, service availability, network, memory, etc;
- Entaksi defines and maintains a continuity plan to enact in case of a disaster.

Concerning the "Detection and reporting" phase:

- abnormal system activities that indicate a potential security violation, including intrusion into Entaksi's network are detected and reported as alarms;
- Entaksi must address any critical vulnerability or event detected rapidly, no later than 48 hours after its discovery.

Concerning the "Assessment and decision" phase:

- are available the Incident Response Team procedures for the evaluation of the incident, and the personnel is adequately trained and have appropriate tools always available to evaluate the events.

About the "Response" phase:

- Entaksi's personnel is trained to act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security;
- incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

About the "Subsequent activities" phase:

- Entaksi has established procedures to notify the subscribers and relying party about any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained there in within 24 hours of the breach being identified, in line with the applicable regulatory rules;
- where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, Entaksi is required also to notify the natural or legal person of the breach of security or loss of integrity without undue delay, as described in Data protection.

Regarding the "Lessons learned" phase:

- Entaksi's Management and personnel review the data and perform the risk analysis for any occurred incident, in order to improve the system.

Even not in the presence of an event, a vulnerability can be discovered. The process of treating vulnerabilities is the same as for incidents, so, given the potential impact, Entaksi will:

- create and implement a plan to mitigate the vulnerability, as for the incident; or
- document the factual basis for a determination that the vulnerability does not require remediation.

In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the eCON Preservation Service, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

5.7. Monitoring and logging

Entaksi's systems are constantly monitored: this activity includes regularly monitoring or reviewing audit logs to identify evidence of malicious activity, implementing automated mechanisms to process audit logs and alerting staff of possible security-critical events.

Entaksi records and stores in its eCON Preservation Service the event logs produced by its systems for at least 6 months. These logs are fully archived as confidential, and may provide evidence in legal proceedings and in order to guarantee continuity of service. The log preservation policy is the same as for documents, digital signatures and seals, in order to maintain the confidentiality and integrity of records relating to the operation of the service.

Each log contains the exact time of the event, a reference to the user and a description of the operation. Logs are recorded in chronological order, and the time used to record events as required in the audit log is synchronised with UTC time at least once a day.

5.8. Controls

Entaksi implements several types of controls to prevent loss, damage or compromise of assets and interruption of business activities.

5.8.1. Operational controls

Entaksi uses trustworthy systems and products that are protected against modification, and guarantees the technical security and reliability of the processes supported by them.

All these organizational procedures are established and implemented for all trusted and administrative roles that impact on the provision of the eCON Preservation Service.

A security requirements analysis is carried out in the design and requirements specification phase for each system development project undertaken by the ICT management to ensure that security is implemented within the IT systems.

Change control procedures are applied for software releases, modifications and emergency fixes of any operational software

or configuration change that are affected by Entaksi's safety policy.
The procedures include documentation and record of changes. Any change that could impact the established security level must be approved by Entaksi's management.

The integrity of eCON Preservation Service and of the organization's information is strongly protected against viruses, malicious and unauthorized software, as detailed in the paragraphs Physical Security, Network Security and Access Security.

Precise procedures are defined by Entaksi to ensure that the media used within the organization's systems are managed securely to protect them from damage, theft, unauthorized access, and obsolescence, as specified in Assets.
Specifically, the asset management procedures describe how to protect media from obsolescence and deterioration for the period of time that the data is to be retained in the eCON Preservation Service.

Regarding the service management operational controls, specific procedures ensure that:

- security patches are applied within a reasonable time after they come available;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
- the reasons for not applying any security patches are documented.

5.9. Physical Security

As stated in the chapter Suppliers, Entaksi does not directly regulate the control of physical access to infrastructures, but applies controls on the qualification phase of the suppliers.

As for servers, a similar consideration applies to workstations, mostly portable devices assigned to employees and collaborators. In this case, Entaksi requires staff to adopt correct behaviour in the management of the device and imposes countermeasures aimed at preserving at all costs the logical protection of the devices, such as access protection, storage encryption, and others.

All these policies ensure adequate protection on all physical infrastructures and, should these be breached in any case, the company assumes the risk of losing the device as long as the loss does not result in any data breach, as the data will have been made inaccessible to third parties.

5.10. Network Security

Entaksi applies appropriate network security controls to protect its network and systems from any attack.

ICT management has identified critical networks aimed to supply the service, based on risk assessment and considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
Security controls are executed on all networks.

Entaksi states that:

- production environment shall be separated from development and test environments;
- although separation of environments is enforced, the highest levels of security checks on connections are still applied in any configuration;
- the communication between clients and the eCON Preservation Service shall take place only through trusted channels;
- any not needed connections or service shall be explicitly forbidden or deactivated;
- shall not use systems used for administration of the security policy implementation for other purposes;
- communication between distinct trustworthy systems is established only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- the external network connection shall be redundant to ensure availability of the services in case of a single failure.

The policy and the network technical features are review at least yearly, or after any significant change.

5.11. Vulnerability Assessment and Penetration Test

Entaksi regularly undergoes a Vulnerability Assessment and Penetration Test. The vulnerability scan is done on public and private IP addresses identified by the Preservation System Security Manager, and is performed by an external body with the necessary skills, tools, proficiency, code of ethics, and independence to provide a reliable report.

Vulnerability and penetration tests on Entaksi's systems are set up at least yearly or after significant upgrades or changes to

the infrastructure or application.

Entaksi archives in its systems the records, evaluations and minutes of all tests performed.

5.12. Access Security

All users accessing the eCON storage service are assigned to a specific group in order to protect the segregation of roles and information.
Access is restricted to authorised individuals.

All access controls are defined to protect Entaksi's internal network from unauthorized intrusion.
Access security controls include the separation of trusted roles, logs, the separation of security administration and operation functions, controlled use of system utility programs.
Firewalls are configured to prevent all protocols and accesses not required for the operation on the eCON Preservation Service.

Entaksi's personnel must be identified and authenticated before using critical service-related applications. Entaksi's users are accountable for their activities, and event logs are digitally stored in the eCON Preservation Service daily.

The Preservation Service Manager administers user access of all operators of the eCON Preservation Service, that includes subscribers and third parties, administrators and system auditors. All subscribers are connected to a user account management system, that includes information about logs, user privileges, access validation. The removal procedure is connected to terms and condition contract.

Entaksi provides a description of its access management policy and access security control practices in its user manuals and public documentation, which are available for consultation at Entaksi's website at the following link: https://www.entaksi.eu/en/.

5.13. Private Key protection and secure cryptographic device controls

Entaksi ensures that appropriate security controls are in place for the management of cryptographic devices and private keys.

The ICT management is committed to constantly checking that the algorithm used for data encryption does not lose effectiveness.

6. Other provisions

6.1. Compliance and audit

The applicable legal system is declared in References.

The configuration of the eCON Preservation Service is regularly checked by the management to avoid any change which violate Entaksi's security policies.

Entaksi's eCON Preservation Service is supervised by the Agenzia dell'Italia Digitale (AgID), which has the responsibility of regularly checking and revising the compliance of the system at the requirements defined in accordance with the Italian regulations on digital preservation.

Moreover, the system is checked at least yearly by an accredited certification body, recognized by Accredia, the Italian Accreditation Body.

Audit working papers and inspection documents are classified as confidentials.
The conformity certificates and their updates are published on the Entaksi website] in accordance with the assessment results: https://www.entaksi.eu/en/certifications.html

Entaksi's qualified service for the long-term preservation of signatures, seals and general data is outlined by the following documents:

Table 4. LTP documents name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.1	MAN eIDAS 20210628 Preservation Service Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1
1.3.6.1.4.1.57823.1.2	MAN eIDAS 20210628 Preservation Service Practice Statement EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2
1.3.6.1.4.1.57823.1.3	MAN eIDAS 20210628 Preservation Evidence Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3
1.3.6.1.4.1.57823.1.4	MAN eIDAS 20210628 Signature Validation Policy EN	https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4

All Entaksi's qualified trust services documents are available at the following link:
https://www.entaksi.eu/en/documentation.html.

6.2. Accessibility

Entaksi provides its documentation, contract forms, and web-based interfaces for Trust Services management through channels designed to be accessible to persons with disabilities and users with accessibility needs, in accordance with the requirements of ETSI EN 301 549 and applicable national legislation.

Where a subscriber or relying party cannot reasonably use the standard online channels due to an accessibility need or disability, Entaksi will provide alternative accessible means (like assisted support via email or telephone) to guarantee access to identical information and services without discrimination.

Entaksi takes into account feedbacks that involve accessibility issues from users and is committed to continually improving the accessibility of its services.

6.2.1. User interface accessibility

Entaksi delivers its Qualified Trust Services through a web-based interface (Entaksi's Console).
Entaksi develops the user interface using Angular, an open-source, TypeScript-based framework and platform developed by Google. While accessibility is not automatic, Angular provides a structured, component-based architecture that supports the correct implementation of accessibility features; in particular, it facilitates the use of semantic HTML, consistent form-handling

patterns, keyboard event management, and reusable interface components, providing a stable technical basis for meeting the ETSI EN 301 549 clause 9 (*WCAG 2.1 Level AA*) requirements.
The user interface currently supports:

- text alternatives for non-text elements;
- structured and semantic HTML with programmatic headings and landmarks;
- keyboard operability for core functions;
- programmatically associated labels for buttons and input fields;
- compatibility with assistive technologies such as screen readers;
- responsive layouts supporting zoom, viewport resizing, and text scaling.

Periodic accessibility reviews are carried out as part of Entaksi's quality and maintenance processes. These reviews include both automated evaluations—using recognized accessibility testing tools—and manual checks such as keyboard navigation testing, screen-reader verification, and visual inspection of contrast and layout behaviour. The objective of these activities is to identify potential accessibility barriers and ensure continuing alignment with the requirements of ETSI EN 301 549.

Entaksi monitors and evaluates all accessibility-related requests, feedback, and defect reports received from users, customers, or internal teams. Once the issue has been verified, it is addressed in the maintenance improvement cycle to further enhance the accessibility features.

6.2.2. Documentation accessibility

All service documentation is provided in accessible electronic PDF format. These PDFs are produced with accessibility considerations in accordance with the requirements of ETSI EN 301 549 clause 10 for non-web documents. In particular, documentation includes:

- alternative text for images and non-text elements;
- a tagged and logical reading order;
- semantic and properly structured headings and lists;
- accessible tables with correctly defined headers;
- visual elements with adequate colour contrast.

All these measures support the readability and usability of the documentation for persons with disabilities and users with accessibility needs.

Upon request documentation can be provided in the HTML alternative accessible format, where reasonably practicable.

6.2.3. Support for accessibility

Entaksi's Help Desk, accessible at helpdesk@entaksi.eu, provides information on the accessibility and compatibility features of the service portal and its documentation, and ensures effective communication with persons with disabilities and users with accessibility needs.

Support services can be accessed through the channels described in the service's Terms and Conditions, including:

- accessible email communication channels;
- telephone support;
- alternative communication methods upon request.

Any documentation or information supplied through the support service is provided in accessible formats consistent with Entaksi's documentation accessibility practices.

6.3. Data protection

As part of the processing of personal data related to the performance of the activities provided for eCON Preservation Service, Entaksi acts as a Data Protection Manager or Processor, by virtue of by specific legal delegation conferred by the Customer.

Entaksi operates in the European Union, and follows the Regulation (EU) 2016/679 that repeals the Directive 95/46/EC.

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali" and also on Entaksi's website at the following link: https://www.entaksi.eu/en/privacy.html.

Entaksi's management operates to guarantee that appropriate technical and organizational measures will be constantly taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.