Manual

MAN eIDAS 20210628 Preservation Evidence Policy EN

Entaksi Solutions SpA

Table of contents

Document information

Project	Integrated Management System
Type	Manual
Document ID	MAN eIDAS 20210628 Preservation Evidence 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 Evidence 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
18/06/2024	1.2.0	Alessia Soccio	IMSM	Specifies use of versioning on eIDAS document OIDs.	Public
02/12/2025	1.3.0	Alessia Soccio	IMSM	Update to EU Regulation No. 1183/2024 – eIDAS 2, minor corrections.	Public

Document approval

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 1 di 16

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

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS

Pag. 2 di 16

1. Introduction

This document is the **Preservation Evidence 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").

1.1. Document identification

This document is identified by the following OID:

Table 1. Document name and identification.

OID	Description	Permanent Link
1.3.6.1.4.1.57823.1.3	MAN eIDAS 20210628 Preservation Evidence Policy EN	https://r.entaksi.eu/oids/ 1.3.6.1.4.1.57823.1.3

The OID is intended to identify the general content and scope of the document, and always refers to the latest available version.

Variations may occur between subsequent versions of the same document, and each of them is recorded on the document itself as a new version. To identify a specific version of a document it is possible to point to the OID plus the version (e.g. 1.3.6.1.4.1.57823.1.3.1.0.0 will refer to version 1.0.0 of this document, 1.3.6.1.4.1.57823.1.3.1.1.0` to 1.1.0 and so on).

For technical reasons the OID 1.3.6.1.4.1.57823.1.3 will always refer to version 1.0.0.

The OIDs identifying the specific preservation evidence policies are identified within the document.

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 3 di 16

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 4 di 16

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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 7 di 16

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 8 di 16

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"".

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 9 di 16

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 10 di 16

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 11 di 16

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).

Other roles are defined in "MAN eIDAS 20210628 Preservation Service Policy EN" and "MAN eIDAS 20210628 Preservation Service Practice Statement EN".

5. eCON Preservation Evidence Policies

This document is the evidence preservation policy for the eCON preservation service in a human-readable form.

Preservation evidence policies are identified through an OID structured according to the following numbering hierarchy:

Table 4. OID hierarchy.

Number	Meaning
1.3.6.1.4.1.57823	Entaksi Solutions SpA
2	Long-Term Preservation
2	Preservation Evidence Policies
n	Specific Policy.

The policies used by Entaksi are as follows:

Table 5. eCON Preservation Evidence Policies.

OID	Description
Validity	1.3.6.1.4.1.57823.2.2.1
eCON Preservation Evidence Policy 2022-01	2022-01 - *current*

5.1. eCON Preservation Evidence Policy 2022-01

5.1.1. Preservation evidence creation

The eCON Preservation Service implements the long-term preservation of the validity of electronic signature performing a validation of the electronic signature as specified in "MAN eIDAS 20210628 Signature Validation Policy EN".

Such procedure produces a validation report that is compliant with ETSI EN 319 102-1 as an XML document defined by ETSI TS 119 102-2.

The validation report contains the following elements about the validated electronic signature:

- **Signature Validation Report Element**, containing the overall signature validation status for the signature as well as additional information on the signature validation performed. This element is described in ETSI TS 119 102-2 clause 4.3.
- **Signature Validation Objects Element**, that contains the materials collected during the validation procedure, such as CRLs, trust anchors, OCSP responses, etc. and the Proof of Existence at the earliest time of the existence of the object. This element is described in ETSI TS 119 102-2 clause 4.4.
- **Validator Information Element**, that identifies the entity validating the signature. This element is described in ETSI TS 119 102-2 clause 4.5.
- **Validation Report Signature**, that contains the validation report signature. This element is described in ETSI TS 119 102-2 clause 4.6.

The signature validation process creates a validation report for each electronic signature during the Submission Information Package (SIP) validation.

Such report is stored in a dedicated archival registry, and it is correlated to the original signature by mean of the SHA-256 hash value of the file that contains the signature.

For instance, if the validating digital signature is a signed PDF file, then the validation report correlation code will be the SHA-256 hash of the PDF file content.

This correlation strategy allows the system to associate the validation report with the digital signature without adding a correlation code to the signed document metadata set. At the same time the archived validation report is free from any link

with the original document for the purposes of an eventual long-term preservation without storage implementation.

5.1.2. Preservation evidence storage

Each file in the eCON Preservation System is stored in an Archival Information Package that carries in an index in the form of a UNI 11386:2020 standard compliant XML file.

The AIP index contains the hashes computed on each file.

While signed documents are stored in an AIP that depends on the documents and their metadata, validation reports are stored in an AIP of a special archival registry dedicated for such purpose.

The AIP index is digitally signed with the XAdES B–LTA profile so that integrity and proof of existence is extended to every preserved object contained in the AIP.

The resulting data structure is a hash-tree that has the digitally signed PDA index as the root hash, and, as leaf nodes, the hash value of the contained preserved objects. These are the preserved objects, for AIPs containing preserved objects, and the signature validation reports for AIPs containing validation reports.

Hence, for AIP containing preserved objects, the digitally signed index of the AIP is effectively a preservation evidence for preserved objects included in the AIP, digitally signed or not, by mean of the hash values of the corresponding files that are part of a hash-tree that has the AIP index hash as the root node.

Furthermore, for the same reason, the digitally signed index of the AIP containing validation reports is effectively a preservation evidence of the digital signatures by mean of the proof of existence of related validation report at the time of digital signature ingestion.

With the information contained in the validation report it is possibile to verify the validity of electronic signature over time as long as the preservation system guarantees the authenticity of the validation report and the proof of existence at the time of ingestion.

5.1.3. Preservation evidence augmentation

Preservation evidence augmentation is performed on the digital signature of the AIP index in the following two cases:

- when the time-stamp is about to expire or at risk of loosing its validity because the TSA signing certificate is expiring or compromised or at risk of being compromised;
- when a cryptographic attacks become feasible on the signature algorithm or the hash algorithm used in the AIP index signature.

In the former case a periodic renewal of the time-stamp is performed when the TSA renew its signing certificate.

In the latter case a hash-tree renewal is performed in the whole data structure by rebuilding a new AIP index with an upgraded signature or hash algorithm.

5.1.4. Preservation evidence policy explicit information

The digitally signed AIP indexes, that are the preservation evidences, contains explicit information about the preservation service, the preservation evidence policy and the preservation profile.

This information is specified attaching a signature policy to the digital signature of the AIP index.

The attached policy is the present Preservation Evidence Policy, it is identified by the OID defined in Document identification and it also contains four XAdES documentation references, also part of the signed attribute set:

- A reference to the Preservation Evidence Policy.
- A reference to the Preservation Profile used when building the AIP.
- A reference to the Preservation Service
- A reference to the Signature Validation Policy

5.1.5. Use of other trust services

eCON Preservation Service uses services of other trust service providers in the following preservation process phases:

- when applying a timestamp the service invoke the RFC 3161 service provided by a Qualified Time Stamp Trust Service;
- when building the certificate validity chain, the service collects the issuer CA Certificates using the issuer CA Certificate

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 14 di 16

URI in the Authority Information Access (AIA) extension in the certificates;

- when validating an electronic signatures, the service obtains OCSP responses from the OCSP service indicated with an URI in the Authority Information Access (AIA) extension of the certificate in order to verify the revocation status of the certificate.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 15 di 16

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 6. 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.