ENTAKSISOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
SERVIZIO DI CONSERVAZIONE CERTIFICATO
ETSI 319-401 | ETSI 119-511
PER LA CONSERVAZIONE A LUNGO TERMINE

Manuale

MAN eCON 20210628 Preservation Evidence Policy EN

Entaksi Solutions SpA

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manual
Nome documento	MAN eCON 20210628 Preservation Evidence Policy EN
Versione	1.0.0
Data creazione	28/06/2021
Ultima revisione	01/12/2021
Autore	Alessia Soccio
Stato	Released
Classificazione	Internal

Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
28/06/2021	0.0.1	Alessia Soccio	Archival Function Manager	Draft creation.	Internal
01/12/2021	1.0.0	Alessia Soccio	Archival Function Manager	Review and release.	Pubblic

Approvazione del documento

Data	Addetto	Mansione	Firma
01/12/2021	Alessandro Geri	Preservation Service Manager	*Firmato digitalmente*

1. Introduction

This document represents the Preservation Evidence Policy regarding the eCON Preservation Service provided by Entaksi Solutions SpA, via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT) (website: http://www.entaksi.eu).

The eCON Preservation Service is a trust service providing long-term preservation of digital signatures and general data using digital signature techniques, as defined by eIDAS Regulation (EU) No 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.

1.1. Document identification

This document is identified by the following OID:

OID	Description
1.3.6.1.4.1.57823.1.3	MAN eCON 20210628 Preservation Evidence Policy EN 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 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 takes 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.

Entaksi makes available to all the preservation services customers and to the 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.

Any change that might affect the acceptance of the service by the subject, subscriber or relying parties, will be communicated by Entaksi 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.

delta preservation object container

special preservation object container describing the difference to an already existing preservation object container.

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 Regulation (EU) 910/2014.

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

CA

Certification Authority

IP

Internet Protocol

IT

Information Technology

TSP

Trust Service Provider

UTC

Coordinated Universal Time

AUG

Augmentation goal

CSA

Certificate Status Authority

EUMS

European Union Member State

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

QES

Qualified Electronic Signature or Qualified Electronic Seal

SigS

digital Signature creation Service

SubDO

Submission Data Object

TS

Trust Service

TSA

Time-Stamping Authority

TSP

Trust Service Provider

ValS

Validation Service

WOS

Without Storage

WST

With Storage

WTS

With Temporary Storage

3. References

In order to ensure the compliance of the eCON Conservation 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 regulation and the Italian digital preservation regulation.

3.1. Normative references

3.1.1. Long-Term Preservation

ETSI TS 119 512 V1.1.2 (2020-10)

Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services.

ETSI TS 101 533-1 V1.3.1 (2012-04)

Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management.

ETSI TR 101 533-2 V1.3.1 (2012-04)

Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors.

ETSI EN 319 102-1 V1.1.1 (2016-5)

Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

3.1.2. Italian Digital Preservation Regulation

CAD

Legislative Decree No 82/2005 Code for Digital Administration, "Codice dell'Amministrazione Digitale".

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

Official 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 "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

3.1.3. Certifications

Entaksi obtained the following certifications:

UNI ISO 9001:2015

Quality management systems - Requirements.

ISO/IEC 20000-1:2018

Information technology - Service management - Part 1: Service management system requirements.

ISO/IEC 27001:2013

Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018:2019

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO/IEC 27035:2016

Information technology — Security techniques — Information security incident management.

ISO/IEC 22301:2019

Security and resilience — Business continuity management systems — Requirements.

Sistema di conservazione dei documenti digitali

Digital Preservation Service - art. 24 EU Regulation n° 910/2014 (eIDAS).

ETSI EN 319 401 V2.3.1 (2021-05)

Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, policy e requisiti per i fornitori di servizi fiduciari.

ETSI TS 119 511 v1.1.1 (2019-06)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques, policy e requisiti di sicurezza per servizi fiduciari di conservazione di firme digitali e la conservazione di dati mediante tecniche basate sulla firma digitale.

3.1.4. Data Protection

GDPR

Regulation (EU) No 679/2016OF 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).

3.1.5. Other provisions

ISO/IEC 14721:2012

Space data and information transfer systems — Open archival information system (OAIS) — Reference model.

ETSI TS 119 312 V1.4.1 (2021-08)

Electronic Signatures and Infrastructures (ESI) - Cryptographic Suites.

3.2. Informative references

Entaksi Qualified Long-Term Preservation Service is supported by the following policies:

Tabella 1. eCON Preservation Service Policies

Document name	Document version	Valid from
MAN SIG 20210708 Preservation Service Policy	1.0.0	01/12/2021
MAN eCON 20200628 Signature Validation Policy	1.0.0	01/12/2021
MAN eCON 20200628 Preservation Evidence Policy	1.0.0	01/12/2021
MAN SIG 20200511 Politica per la sicurezza delle informazioni	1.1.0	01/12/2021

Additionally eCON Preservation Service is described in the following practice statements and manuals:

Tabella 2. eCON Preservation Service Documents

Document name	Document version	Valid from
MAN SIG 20210708 Preservation Service Practice Statement	1.0.0	01/12/2021
MAN eCON 20151222 Conservazione	1.7.0	01/12/2021

All the previous enlisted documents are classified as "public" and disclosed to the relying parties on the company website.

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

Tabella 3. eCON Preservation Service Confidential Documents

Document name	Document version	Valid from
MAN eCON 20190918 Piano di cessazione	1.3.0	01/12/2021
MAN eCON 20151222 Piano della sicurezza	1.4.0	01/12/2021

Entaksi, due 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 14721:2012, 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**.
- **Archival Function Manager**.
- **Data Protection Manager**.
- **Preservation System Security Manager**.
- **Preservation Information System Manager**.
- **Preservation System Development and Maintenance Manager**.

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.

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

Entaksi Solution SpA is responsible for the provision of the service, and the Preservation Service Manager 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 SIG 20210708 Preservation Service Policy" and "MAN SIG 20210708 Preservation Service Practice Statement".

5. eCON Preservation Evidence Policy

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

The eCON Preservation Evidence policy is identified by OID 1.3.6.1.4.1.57823.2.2.1 according to the following number hierarchy:

Number	Meaning
1.3.6.1.4.1.57823	Entaksi Solutions SpA
2	Long-Term Preservation
2	Preservation Evidence Policies
1	eCON Preservation Evidence Policy 2022-01

5.1. 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 eCON 20200628 Signature Validation Policy.

Such procedure produces a validation report that is compliant with ETSI EN 319 102-1 V1.1.1 (2016-5) as an XML document defined by ETSI TS 119 102-2 V1.1.1 (2016-5).

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 V1.1.1 (2016-5) 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 V1.1.1 (2016-5) clause 4.4.
- **Validator Information Element**, that identifies the entity validating the signature. This element is described in ETSI TS 119 102-2 V1.1.1 (2016-5) clause 4.5.
- **Validation Report Signature**, that contains the validation report signature. This element is described in ETSI TS 119 102-2 V1.1.1 (2016-5) 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.

5.2. 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 (SinCRO) 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_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.

5.3. 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.

5.4. 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

5.5. 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 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.

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 by 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.

Other provisions are defined in "MAN SIG 20210708 Preservation Service Policy" and "MAN SIG 20210708 Preservation Service Practice Statement".