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 Service Practice Statement EN

Entaksi Solutions SpA

Indice

Document information

Project	Sistema Integrato di Gestione
Type	Manual
Document ID	MAN eCON 20210628 Preservation Service Practice Statement EN
Version	1.0.0
Creation Date	28/06/2021
Last Revision	01/12/2021
Author	Alessia Soccio
Status	Released
Classification	Internal

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

Revisions and releases

Date	Version	Name	Mansion	Action	Release
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

Document approval

Date	Employee	Role	Signature
01/12/2021	Alessandro Geri	Preservation Service Manager	*Digitally signed*

1. Introduction

This document represents the Preservation Service Practice Statement for 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.

Within the document the following topics are set out:

- a list of all policies and documents related to the eCON Preservation Service;
- practices and procedures used to address all the requirements identified for the applicable Preservation Service Policy
- the description of the obligations of all external organizations supporting the eCON Preservation Service, including the applicable policies and practices;
- roles and responsibilities assigned for the eCON Preservation Service management;
- how all the enlisted practices have been implemented by Entaksi;
- the procedure for termination of service.

1.1. Document identification

This document is identified by the following OID:

OID	Description
`1.3.6.1.4.1.57823.1.2`	MAN eCON 20210628 Preservation Service Practice Statement EN 1.0.0

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

3.1. Normative references and standardas

3.1.1. Certifications

Entaksi has 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.

3.1.2. Long-Term Preservation

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 and repealing Directive 1999/93/EC.

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

3.1.3. 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".

3.1.4. 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).

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 Sevice. 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 delivers services from its own infrastructure: all software systems are entirely under control of the company. Hardware and network connectivity are managed by the datacenters suppliers.

The physical components of the eCON Preservation Service are distributed among servers located in various datacenters, geographically distributed in order to guarantee high availability of the service.

The preservation system is located in the following three datacenters:

- *Aruba S.p.A.*

Via Sergio Ramelli 8
52100 Arezzo (AR)

- *Aruba S.p.A.*
  Via Piero Gobetti 96
  52100 Arezzo (AR)
- *Aruba S.p.A.*
  Via San Clemente 53
  24036 Ponte San Pietro (BG)

The replication of the system strengthens operational continuity and allows the service to be available in case of fault in any of the three poles.

Some components of the system such as processing, verification, indexing and presentation procedures, may determine the temporary transit of data in the following two datacenters located within the European Union:

- *Hetzner Online AG*
  Am Datacenterpark 1
  08223 Falkenstein
  Germany
- *Hetzner Finland Oy*
  Huurrekuja 10
  04360 Tuusul
  Finland

Entaksi uses GNU/Linux operating systems on its servers. Configuration and access to these systems are entirely under the exclusive control of Entaksi Solutions. Software systems operate on virtual machines configured within an encrypted data area.

The datacenters provide the highest levels of performance in terms of reliability, security and connectivity, using both IPv4 and IPv6 protocols and are ISO/IEC 27001:2013 certified.

The qualified Time-Stamping Authorities (TSAs) that supplies time-stamps for the eCON Preservation Service are:

- *Aruba PEC S.p.A. - P.IVA IT01879020517 - REA N. BG445886.*
- *Namirial S.p.A. - P.IVA IT02046570426 - REA N. AN157295.*

5. eCON Preservation Service statement

5.1. Preservation profiles

eCON Preservation Service supports the following preservation profiles:

Legacy preservation system profile	
OID	1.3.6.1.4.1.57823.2.1.1
Valid from	n/a
Valid to	31/12/2021
Description	This profile represents the eCON Preservation System before eIDAS compliance and ETSI TS 119 511 v1.1.1 (2019-06) implementation. It is compliant with the Italian digital preservation system guidelines for legally binding electronic document preservation for private and government bodies.
Long-term preservation profile for general data and digital signatures with storage and augmentation 2022-01	
Valid from	01/01/2022
Valid to	undefined
Description	This profile aims to preserve signed and unsigned digital documents with storage, performing digital signature validation, preservation and augmentation of associated proof of evidences. It is compliant with both the Italian digital preservation system guidelines, and eIDAS regulations, ETSI EN 319 401 V2.3.1 (2021-05) and ETSI TS 119 511 v1.1.1 (2019-06) requirements.

Preservation profiles identifiers use and OID in order to reserve a unique code for each profile. The OID is allocated under the following number hierarchy:

Number	Meaning
`1.3.6.1.4.1.57823`	Entaksi Solutions SpA
2	Long-Term Preservation
1	Preservation Profiles

Hence, the supported profiles OIDs are:

Dot notation	URI	Description
1.3.6.1.4.1.57823.2.1.1	`https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.2.1.1`	Legacy preservation system profile
1.3.6.1.4.1.57823.2.1.2	`https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.2.1.2`	Long-term preservation for general data and digital signatures with storage and augmentation 2022-01

The chapter Informative references contains the list of policies supported by eCON Preservation Service.

For the purposes of the current Preservation Service Practice Statement the following chapters describe the "Long-term preservation for general data and digital signatures with storage and augmentation 2022-01" preservation profile.

5.2. Preservation scheme

The preservation profile supports a preservation scheme composed by the WST (With Storage) preservation storage model, the PGD (Preservation of General Data), the PDS (Preservation of Digital Signature) and the AUG (Augmentation) preservation goals.

The following URI identifies the preservation scheme: `http://uri.etsi.org/19512/scheme/pds+pgd+wst+aug`

5.3. Preservation storage model

The preservation profile supports the preservation storage model "Preservation with storage (WST)" according to clause 4.3.1 of ETSI TS 119 512 V1.1.2 (2020-10).

5.4. Preservation goals

The preservation profile supports the following preservation goals:

- **Preservation of General Data (PGD)** that provides a proof of existence over long periods of time of the submission data object (SubDO) submitted to the preservation service.
  `http://uri.etsi.org/19512/goal/pgd`
- **Preservation of Digital Signatures (PDS)** that extends over long periods of time the ability to validate a digital signature, to maintain its validity status and to get a proof of existence of the associated signed data.
  `http://uri.etsi.org/19512/goal/pds`
- **Augmentation of submitted evidences (AUG)** that supports the augmentation of submitted preservation evidences.
  `http://uri.etsi.org/19512/goal/aug`

5.5. Supported input formats

The preservation profile accepts the following file formats:

Tabella 4. Supported file formats.

Type	Filename	Developed by	Viewers	Standard	mime type
PDF	`.pdf`	Adobe System Inc.	Adobe Reader, Evince, others	ISO 32000-2	`application/pdf`
PDF/A	`.pdf`	Adobe System Inc.	Adobe Reader, Evince, others	ISO 19005	`application/pdf`
TIFF	`.tiff`, `.tif`	Aldus Corporation, now Adobe System Inc.	Various image software	ISO 12639	`image/tiff`
JPEG	`.jpg`, `.jpeg`, `.jpe`, `.jif`, `.jfif`, `.jfi`	Joint Photographic Experts Group	Various image software	ISO/IEC 10918 ITU-T T.81 ITU-T T.83 ITU-T T.84 ITU-T T.86	`image/jpeg`
PNG	`.png`	World Wide Web Consortium	Various image software	ISO/IEC 15948 RFC 2083	`image/png`

Type	Filename	Developed by	Viewers	Standard	mime type
OOXML	.docx .docm .xlsx .xlsm .pptx .pptm	Microsoft	Microsoft Office, LibreOffice, OpenOffice and others	ISO/IEC 29500 ECMA-376	application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.spreadsheetml.sheet application/vnd.openxmlformats-officedocument.presentationml.presentation
ODF	.odt, .fodt, .odp, .fodp, .ods, .fods, .odg, .fodg	OASIS	Microsoft Office, LibreOffice, OpenOffice and others	ISO/IEC 26300	application/vnd.oasis.opendocument.text application/vnd.oasis.opendocument.presentation application/vnd.oasis.opendocument.spreadsheet application/vnd.oasis.opendocument.graphics
XML	.xml .xsd	World Wide Web Consortium	Browser, various text viewers	W3C XML	application/xml text/xml
TXT	.txt	n/d	Various text viewers	ASCII ISO/IEC 8859 UTF-8	application/txt text/plain
EML	.eml	OASIS	Outlook, Mail, Thunderbird, various clients	RFC 822 RFC 5322	message/rfc822

The preservation profile accepts the following evidence input formats:

URI	Format	Note
http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3	CAdES Archive Time Stamp V3	The ASN.1-based Archive Time Stamp V3 attribute according to ETSI EN 319 122 V1.1.1 (clause 5.5.3).
http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp	XAdES Archive Time Stamp	The XML-based Archive Time Stamp property according to ETSI EN 319 132 V1.1.1 (clause 5.5.2).
http://uri.etsi.org/ades/PAdES/document-time-stamp	PAdES Document Time-Stamp	The Document Time-Stamp according to ETSI EN 319 142-1 (clause 5.4).

eCON Preservation Service accepts documents, digital signatures and general data.

The preservation profile uses the following preservation evidence policy described in "MAN eCON 20200628 Preservation Evidence Policy":

- eCON Preservation Evidence Policy 2022-01 (OID `1.3.6.1.4.1.57823.2.2.1`)

The preservation profile uses the following signature validation policy described in "MAN eCON 20200628 Signature Validation Policy":

- Signature Validation Policy 2022-01 (OID `1.3.6.1.4.1.57823.2.3.1`)

5.6. Preservation protocol

eCON Preservation Service provides a protocol for the communication between the service and the preservation service client.

This communication is based on a set of APIs that exchange JSON and XML messages over HTTPS connection.

eCON Preservation Service doesn't implement the full set of API specified in ETSI TS 119 512 V1.1.2 (2020-10). Instead, it defines its own set of REST API for most of the preservation protocol functionalities.
Thought, some the these functionalities are available with ETSI TS 119 512 V1.1.2 (2020-10) API.

A full implementation of the ETSI TS 119 512 V1.1.2 (2020-10) set of API could be done in future evolution of the eCON Preservation Service.

5.6.1. Preservation process description

Access to the digital preservation system

For the management of login credentials, the eCON Preservation Service uses an identity management system compatible with OAuth2 standards (RFC-6749, RFC-6750, RFC-6819, RFC-7662, RFC-7009, RFC-7519), SAMLv2 and with the OpenID Connect protocol.

The system allows the users to use a Single Sign On authentication system with which they can access to the various components of the service. System administrators regulate the authorization level. The authentication and authorization system leverages the OpenID Connect protocol in order to secure communications with the APIs of the service.

Access to service functionalities starts with a user account provided to the user identified by his or her email address. The first user account has a "service manager" role that has privileges over all the functions of the service. Among these, the "service manager" can manage other user accounts and their specific access role.

The eCON Preservation Service has the following roles available:

- service manager;
- service user;
- user enabled to manage and upload documents;
- read-only user.

Users with the "service manager" role can add or remove other users identified by their email address. Each action will be notified by email.
The removal of a user does not delete user data but only removes the privileges on the user, recording the date of revocation of the privilege and maintaining the data related to the use of the service until the termination of the service.

Preservation Object Ingestion

Data objects are submitted to the eCON Preservation Service by mean of a Submission Information Package (SIP) that contains a set of submitted data objects and related metadata.

Uploaded SIPs are validated asynchronously and, at the end of the validation process, a submission validation report is issued for each SIP to the email address of the submitter.

The submission validation report informs the user weather the SIP has been accepted or rejected and, in the latter case, it contains various information about the violations that occurred causing the rejection of the SIP.

Available preservation profiles

Although the eCON Preservation Service doesn't fully implement the ETSI TS 119 512 V1.1.2 (2020-10) specification, the `RetrieveInfo` API defined in ETSI TS 119 512 V1.1.2 (2020-10) clause 5.3.2 is implemented for retrieving information about the preservation profiles supported by the preservation service.

Access to preserved objects

The eCON Preservation Service has a search function that allows the user to query the archive using the metadata associated with the data objects as search criteria.

Data objects that match criteria defined for the query are shown to the user that can issue a Dissemination Information Package (DIP) request to the system.

The resulting DIP contains data objects and related proof of existence at the time of submission. The DIP is then available for download only by the authorized requesting user.

Preserved objects validation

The eCON Preservation Service implements the API defined in ETSI TS 119 512 V1.1.2 (2020-10) clause 5.3.8 (`ValidateEvidence`) in order to allow the user to submit a preservation evidence and a sequence of preservation objects to which the evidence corresponds. The service replies with the result of a validation of the submitted preservation evidence that is with a preservation evidence validation report.

Deletion of preserved objects

the eCON Preservation Service deletes the preserved objects and all the related preservation evidences within its archive in the following cases:

- upon request of the subscriber;
- at the end of the validity period set on the service agreement.

Both the occurrences shall be approved by Archival Function Manager.

Some circumstances such as conducting a tax or criminal investigations can prevent the deletion of documents according to the local State regulation. In such case the deletion request will be rejected with a formal motivation.

Deletion requests can be submitted during the validity period of the service agreement only. After the end of the contract the user has a period of 6 months to retrive his preserved objects before the permanent deletion. On-request deletion will be suspended in this period.

All deletion requests and responses are logged, and the logs are kept as described in Audit logging paragraph.

The eCON Preservation Service implements the API defined in ETSI TS 119 512 V1.1.2 (2020-10) clause 5.3.5 (`DeletePO`) that allows the user to delete a preserved object. Thought, when dealing with preserved objects coming from Italian entities that are subject to the Italian digital preservation system guidelines this method always return `http://uri.etsi.org/19512/error/noPermission` error code as these guidelines forbid preserved object deletion.

Export-import package

The service client uses functions described in Access to preserved objects to request and retrieve Dissemination Information Packages (DIPs) that contains parts or all the preservation objects stored by the service and their related preservation evidences.

Dissemination Information Package format complies with the UNI 11386:2020 standard.

Update of preservation object

The eCON Preservation Service doesn't implement the optional protocol operation for updating a preserved object.

Audit trail access

The eCON Preservation Service implements its own REST API for retrieving audit trail element for various entities involved in the preservation process: SIP, AIP, DIP.

5.7. Notification protocol

The eCON Preservation Service notifies service subscriber using their email address.

As described in the paragraph Access to the digital preservation system the eCON Preservation Service can be accessed after a registration procedure available in the service user interface, using the email address provided within the service agreement

("Condizioni generali del servizio").

After the stipulation of the contract, the email address recorded in the terms and condition is considered the only secure channel through which the eCON Preservation Service will send messages concerning the management of the service, such as: system changes, scheduled outages, technical or regulatory updates, obsolescence of data and technologies.

Any change or security concern that may affect the preservation profile, the policies of the service, including the preservation evidence policy and the signature validation policy, or this statement will be notified by email to affected subscribers.

The eCON Preservation Service provides a tool to configure email notifications sent automatically by the system for certain functions, such as the report for the SIP upload process or the availability of a DIP.

At the first access all the notifications are disabled, and each user can configure his or her own settings by him/herself through the service user interface.

6. Technical Security Controls

6.1. Risk assessment

Entaksi carries out a risk analysis on a regular basis, aimed at protecting the entire management system. The risk assessment identifies, analyses and evaluates threats, impacts and probabilities on every configuration item with particular attention to the trust service risks, taking into account business and technical issues.

The analysis produces a document that describes all the risk treatment measures to ensure that the level of security is commensurate to the degree of risk.

The methodology and practice used to implement and conduct the risk management system are compliant to the standard described in the chapter References.

The risk analysis carried out by Entaksi in order to protect the eCON Preservation Service is divided into the following phases:

- **Identification of the Designated Community**, the relying party involved in the risk analysis.
- **Identification of assets/CI**, the identification of all those assets in the Entaksi CMDB that are considered critical for the provision of the service.
- **Identification of threats** defined as potentially harmful events to which assets can be exposed during the service delivery.
- **Definition of risk tolerance**, the calculation of the "acceptable risk threshold", arbitrarily identified by the organization as a tolerability limit, after a careful evaluation of costs/benefits resulting by the adoption of any mitigation countermeasures.
- **Estimate of threats occurrence probability** calculated on the likelihood that the event will occur within a certain period of time, conventionally established in three years.
- **Estimate of impacts**, the damage deriving from adverse events that could be produced on critical assets in the face of identified threats, calculated on the economic damage that would result to the company.
- **Calculation of vulnerability**, that is the 'propensity' of an asset to be damaged by a particular threat.
- **Risk analysis** entry of the probability, impact and vulnerability values of each threat on critical assets, calculated on the values of the previous analysis and on measurements carried out on the systems.
- **Countermeasures adopted** application, execution of activities or adoption of behaviors that can lead to the containment, reduction, transfer or elimination of risk.
- **Management of the residual risk** the recalculation of the risk after the application of the countermeasures, and its management.
- **Drafting of the Risk Assessment Report and the Risk Treatment Plan**.

The risk assessment is reviewed and revised at least yearly, unless regulatory or structural major changes.

The results of the assessment are reviewed by Entaksi management, that checks for each identified threat the correct countermeasure has been applied, approve the risk assessment and accept the residual risk identified.

6.2. Cryptographic controls

eCON Preservation Service follows the requirements from ETSI TS 119 312 V1.4.1 (2021-08) for cryptographic algorithms. Hashing and time-stamp use exclusively the SHA-256 set of hash functions. Time-stamps come from Trust Service Providers that follow state-of-the-art practices for policy and security requirements, in accordance to ETSI EN 319 421 V1.1.1 (2016-03). In addition, signing certificates used in the service are issued only by trust service providers that implements ETSI EN 319 411-1 V1.3.1 (2021-05) or ETSI EN 319 411-2 V2.3.1 (2021-05).

eCON Preservation Service takes care of verifying these requirements during the supplier qualifications phase.

eCON Preservation Service uses time-stamps and signature certificates that are verifiable using CRLs or OCSP responses which include a 'reason code' in case of the revocation of a public key certificate.

eCON Preservation Service states that the digital signatures affixed by the system use an EAL4 ISO/IEC 15408 device (i.e. a smart card or a certified HSM) with a certificate issued by an eIDAS CA, and does not employ FIPS PUB 140-2 devices.

Devices chosen by Entaksi for use in the eCON Preservation Service do not allow the backup of the private key.

6.3. Network security

Users can access the eCON Preservation Service only through the functions provided by the user interface or through the REST APIs made available on request.

Service features are accessible via secure HTTPS connection from the public network, using the OAuth2 OpenID Connect authentication mechanism (see RFC-6749 and http://openid.net/).

eCON Preservation Service uses the TLS protocol (Transport Layer Security) version 1.2 or higher for encrypted communications with the services exposed by the infrastructure on the public network.

Previous versions of TLS and SSL (Secure Socket Layer) protocols are disabled.

The areas of application of this protocol are:

1. Protection of connections to services conveyed through the HTTP protocol.
2. Securing connections to e-mail services or other services based on TCP connections.
3. Protection of VPN connections.
4. Protection of other interconnection channels between TLS-based internal services.

6.4. Audit logging

eCON Preservation Service uses event log collection and review as a necessary component of its information security management system. This paragraph provides a description about types of log collected and reviewed, frequency of auditing and preservation procedures.

Logs record:

- failed and successful logins;
- modification of security settings;
- privileged use or escalation of privileges;
- system events;
- modification of system-level objects;
- all operations related to a specific preservation object identifier;
- session activity
- account management activities including password changes (success and failure);

Each log reports the following information:

- date and time of activity;
- peer IP address (for connection logs);
- user ID;
- description of attempted or completed activity;
- client requests and server responses;
- abnormal usage, e.g. number of transactions, usage spikes, etc.;
- abnormal application behavior, including repeated application restart;
- data modification where required for regulatory compliance.

eCON Preservation Service ensures an appropriate log monitoring, and review logs in response to suspected or reported security problems.

Log retention is set to 6 months. The retention period may be shortened or lengthened according to contract terms, law and regulations.

The preservation is performed within the eCON Preservation Service. Logs are sent for digital preservation daily.

Logs are accessed, secured and protected according to the nature of the information they may contain. Except for Entaksi any activity of logging review, such as auditing or inspection, is recorded.

For any questions or assistance with logs and to repoert suspicious activities the user can contact Entaksi's helpdesk.

7. TSP termination and termination plans

The decision of terminate the eCON Preservation Service can be taken only by the Entaksi Solution SpA management.

The CEO, hearing the opinion of shareholders, will formalize the termination of eCON Preservation Service and the activation the termination plan.

A specific document describes the termination plan and the procedure to apply for each termination step. The plan is constantly kept up-to-date by Entaksi management and complies both with Italian and international legislation on long-term preservation services.

The termination plan describes all the activities summarized in the following list:

1. **Decision to terminate the service**: the management of Entaksi Solutions SpA, having heard the opinion of the shareholders, can declare the termination of the eCON Preservation Service. Contextually the management drafts a special report in which the reason for the termination is detailed, the termination is scheduled, and the termination program is started.
   At the same time, the acquisition of new customers is ceased.
2. **Communication to interested parties**: during the termination procedure the interested parties, listed in the chapter Roles and responsibilities, are notified of the ceasing of the service. Communication takes place at least 60 days before the actual termination of the service. All parts must be notified without delay.
   Responsibility for communication is entrusted to Preservation Service Manager, which approves the content of the e-mail. The database of third-party e-mails is kept updated on the system.
   In addition to sending e-mail communications, a notice of the termination of the service is published on the company's website "www.entaksi.eu".
3. **Termination of subcontractors**: Entaksi does not currently use subcontractors for the eCON Preservation Service, but it has a specific internal procedure that regulates relations with suppliers and other subcontractors.
4. **Identification of preservation system for the service documentation**: within 30 days from the start of the termination procedure, Entaksi will choose another preservation service to deposit the documentation proving the functioning of the conservation system (technical documentation, service manuals, system logs, service contracts).
   The identification of the service follows the supplier qualification procedure as indicated in the internal procedure that regulates relations with suppliers. The identified TSP is also offered to customers as a new preservation service to which the archives can be transferred.
5. **Transfer of storage data to a new preservation system**: the documentation proving the management of the storage system (technical documentation, service manuals, system, SLA template) is selected by the Archival Function Manager. The consistency list is approved by the Preservation Service Manager and the Data Protection Manager, and the Dissemination Information Package (DIP) are prepared by the Preservation System Development and Maintenance Manager, which is also responsible for completing the transfer procedure.
   The upload is made within the same time frame foreseen for customers to the termination date.
   The communication of the new designated preservation system is sent to AgID by the Preservation Service Manager according to the communication procedure with the authority.
6. **Notification of termination by the Preservation Service Manager**: once the new preservation supplier has been identified, a second communication is prepared for customers, which makes the technical specifications available for subscribers to prepare their own DIPs to be exported or for letting Entaksi to transfer hosted documents directly to the new supplier on their behalf automatically.
   The access to the preservation service is guaranteed until the contractually established end of service date (6 months from the notification) in order to allow the autonomous export of the preservation objects by mean of DIP.
   If the preservation activity is terminated without the indication of a TSP replacement and it is not possible to guarantee the conservation and availability of the documentation and archives, the preservation object and the related documents are deposited within 60 days into the AgID archive, which guarantees preservation and availability, according to art. 37 comma 4-bis of the CAD.
7. **Termination**: once the 6-month period for the transfer of documentation has ended, the Preservation System Development and Maintenance Manager, assisted by indication of the Archival Function Manager and with the approval of Preservation Service Manager, proceeds to permanently delete the preservation objects no longer subject to the storage.

The deletion is extended to all backup copies and it is done using the most up-to-date secure cancellation technology available.

The termination plan is referenced as "MAN eCON 20190918 Piano di cessazione" and is classified as "Confidential".

8. Other provisions

8.1. 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.

8.2. Terms and Conditions

Entaksi provides a service agreement ("Condizioni generali del servizio") to interested subscribers to be informed about terms and conditions of the eCON Preservation Service, before entering into a contractual relationship.

The service agreement contains:

- general terms and conditions of eCON Preservation Service;
- limitation on the use of the service;
- subscriber's obligations;
- information for parties relying on the trust service;
- the period of time during which Entaksi's event logs are retained;
- limitations of liability;
- limitations on the use of the services provided including the limitation for damages arising from the use of services exceeding such limitations;
- procedures for complaints and dispute settlement;
- whether the Entaksi trust service has been assessed to be compliant with the trust service policy, and through which conformity assessment scheme;
- Entaksi contact information;
- any undertaking regarding availability and Service Level Agreements.

Regarding specifically the preservation system:

- the reference to this document and other relevant policies, and the preservation profile supported;
- a reference to the user manual, that explains the role of the submitter in the preservation process, the specifics of validation data, how to import Submission Information Packages (SIP) and to request Dissemination Information Packages (DIP);
- the maximum number of errors allowed for a single SIP to be validated, and how the system notifies errors.

Entaksi makes the terms and conditions regarding eCON Preservation Services available to all subscribers and relying parties, and can transmit the document in paper form or electronically.

Entaksi does not employ subcontractors or outsourcing for the provision of critical service functions. Any third party involved is named in the contract.

Entaksi automatically preserves the signed digital document of the service agreement both on its and the customer preservation system. If the contract is signed in paper form proceeds to digitize it and archives both the copies.

Terms and conditions are available in two languages, Italian and English.

8.3. Documents format and language

The eCON Preservation Service documents as stated in the chapter Informative references are available in human readable form.

Signature validation policies are available in machine readable format.

The documents are available in two language versions: English and Italian.

Due to language interpretation there may be small differences between the two versions, which however do not impact on the content. In case of ambiguity the English version takes precedence.

8.4. 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 Processor, by virtue of by specific legal delegation conferred by the Customer.

The complete set of provisions relating to the processing of personal data performed by the eCON preservation service is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

The complete set of provisions relating to the processing of personal data performed by Entaksi is reported in the Entaksi website.

8.4.1. Data Breach

According to the General Data Protection Regulation (EU) 2016/679 (GDPR), articles 33-34, "(...) in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent (...)".

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay".

Therefore, as soon as Entaksi becomes aware of a data breach of the personal data processed, as data Processor, it will notify the violation both to the subscriber(s) than to the supervisory authority and relying parties, without undue delay, **within 72 hours** from the time it became known.

The obligation does not exist in the event that it is possible to demonstrate that the violation is unlikely to represent a risk to the rights and freedoms of individuals such as: loss of control of personal data or limitation of their rights, discrimination, theft or usurpation of identity, financial losses, unauthorized deciphering of pseudonymisation, prejudice to reputation, loss of confidentiality of personal data protected by professional secrecy, or any significant economic or social damage to the data owner.

After 72 hours from the violation the notification must be accompanied by the reasons for the delay, and must be given in any case the maximum willingness to collaborate with the competent authorities.