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 Service Policy EN

Entaksi Solutions SpA

Indice

Document information

Project	Sistema Integrato di Gestione
Type	Manual
Document ID	MAN eCON 20210628 Preservation Service Policy 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 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.

Within the document the following topics are set out:

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

1.1. Document identification

This document is identified by the following OID:

OID	Description
1.3.6.1.4.1.57823.1.1	MAN eCON 20210628 Preservation Service Policy EN 1.0.0

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

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

1.2. Document maintenance

Entaksi has defined a review process for all the internal documents, including policies 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 and standards

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 Service. However, other third parts may be involved in the process, such as legal control bodies, authorities, and auditors.
Entaksi always requires non-disclosure agreements to any non-contractual access to the system, such as for audits, and applies anonymization and minimization of personal data wherever possible.

4.3. Suppliers

Entaksi Solutions has decided to:

- Use a housing / hosting server infrastructure. Servers that host and provide the various components of the eCON Preservation Service and other company's activities are located in datacenters managed by specialized suppliers. Contracts between Entaksi and those suppliers are periodically reviewed, in order to obtain the best performances according to the market value. The same consideration takes place for the use of general network services (such as domain names and the related DNS), which are entrusted to external services too.

- Use for all employees and collaborators a contract based on remote working.

The result of these statements is that the company operates entirely on the network, not using physical headquarters. Therefore, Entaksi does not regulate directly the control of physical access to the infrastuctures, but checks the suppliers during the qualification phase, monitors the SLA defined by the contract and, if necessary, conducts audits.

Hence Entaksi guarantees the compliance with the requirements about the management of the physical security of the central infrastructure through an accurate qualification process and by monitoring the suppliers, who are selected on the basis of market convenience and on the quality standard guaranteed in terms of security, such as, for example, the certification ISO/IEC 27001:2013. Entaksi also requires, according the limits of the contract, the possibility for the supplier to be subjected to audits and inspections, in order to identify any elements not sufficiently covered by the contractual conditions or by the certifications themselves.

Regarding other suppliers not related to the physical infrastructure, Entaksi uses external time-stamps, provided only by qualified Time-Stamping Authorities (TSAs). The qualification process requires the same security level and the auditing opportunity defined for the server hosting.

5. Policies

5.1. Organization reliability

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

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

5.2. Human resources

Entaksi commits to employ qualified staff who possess the necessary expertise, reliability, experience, and qualifications to work on the eCON Preservation Service. Also provides constant training regarding security and personal data protection rules as appropriate for the offered services and the job function.
Personnel have access to the trusted functions only after the management completes the necessary checks.

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

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

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

Entaksi foresees in its documentation, formally accepted by the employee, that adequate disciplinary sanctions can be put in place to personnel who violate the security policies or procedures. Personnel shall exercise administrative and management procedures and processes that are in line with Entaksi's management procedures.
The acceptance procedure involves a reviewing from the management and the signature of the employee on the appointment document.

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

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

5.3. Financial resources

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

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

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

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

5.4. Assets

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

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

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

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

5.5. Risk assessment

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

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

5.6. Incident Management

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

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

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

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

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

Regarding the "Plan and prepare" phase:

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

Concerning the "Detection and reporting" phase:

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

Concerning the "Assessment and decision" phase:

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

About the "Response" phase:

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

About the "Subsequent activities" phase:

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

Regarding the "Lessons learned" phase:

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

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

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

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

5.7. Monitoring and logging

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

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

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

5.8. Controls

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

5.8.1. Operational controls

Entaksi uses trustworthy systems and products that are protected against modification, and guarantees the technical security and reliability of the processes supported by them.
All these organisational procedures are established and implemented for all trusted and administrative roles that impact on the provision of the eCON Preservation Service.

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

Change control procedures are applied for software releases, modifications and emergency fixes of any operational software or configuration change that are affected by Entaksi's safety policy. The procedures include documentation and record of changes. Any change that could impact the established security level must be approved by Entaksi's management.

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

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

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

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

5.9. Physical Security

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

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

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

5.10. Network Security

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

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

Entaksi states that:

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

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

5.11. Vulnerability Assessment and Penetration Test

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

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

the infrastructure or application.

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

5.12. Access Security

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

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

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

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

Entaksi provides a description of its access management policy and access security control practices in its user manuals and public documentation, which are available for consultation on the Entaksi website.

5.13. Private Key protection and cryptographic module controls

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

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

5.14. Accessibility

Entaksi works constantly to make its software accessible and to remove any possible discrimination related to access and usability.

The eCON Preservation Service is designed and constantly revised to implement the "Accessibility requirements for ICT products and services" as required by the ETSI standard "EN 301 549".

Entaksi is careful to listen to all requests from customers with disabilities in order to improve the service and its accessibility.

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.

6.2. 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.

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

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali" and also on the Entaksi website.

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