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 Practice Statement

Entaksi Solutions SpA

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN eCON 20210628 Preservation Service Practice Statement
Versione	1.0.0
Data creazione	28/06/2021
Ultima revisione	01/12/2021
Autore	Alessia Soccio
Stato	Rilasciato
Classificazione	Pubblico

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

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
28/06/2021	0.0.1	Alessia Soccio	RARC	Creazione bozza.	Pubblico
01/12/2021	1.0.0	Alessia Soccio	RARC	Revisione e rilascio.	Pubblico

Approvazione del documento

Data	Addetto	Mansione	Firma
01/12/2021	Alessandro Geri	Responsabile del Servizio di Conservazione	*Firmato digitalmente*

1. Introduzione

Questo documento rappresenta la dichiarazione di pratica (Preservation Service Practice Statement) del Servizio di Conservazione eCON fornito da Entaksi Solutions SpA, via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT) (sito web: http://www.entaksi.eu).

Il servizio di conservazione eCON è un servizio fiduciario che fornisce la conservazione a lungo termine di firme digitali e dati in generale utilizzando tecniche di firma digitale, come definito dal Regolamento (UE) eIDAS n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 relativo a servizi di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

All'interno del documento sono esposti i seguenti argomenti:

- un elenco di tutte le politiche e i documenti relativi al servizio di conservazione eCON;
- le pratiche e le procedure utilizzate per soddisfare tutti i requisiti identificati dalla Preservation Service Policy;
- la descrizione degli obblighi di tutte le organizzazioni esterne che supportano il Servizio di Conservazione eCON, comprese le politiche e le pratiche applicabili;
- i ruoli e le responsabilità assegnate per la gestione del Servizio di Conservazione eCON;
- come tutte le pratiche elencate sono state implementate da Entaksi;
- la procedura di cessazione del servizio.

1.1. Identificativo del documento

Questo documento è identificato dal seguente OID:

OID	Descrizione
1.3.6.1.4.1.57823.1.2	MAN eCON 20210628 Preservation Service Practice Statement 1.0.0

Gli OID che identificano specifiche entità relative al servizio di conservazione sono indicati all'interno del documento.

1.2. Aggiornamento del documento

Entaksi ha definito un processo di revisione di tutti i documenti interni, comprese le politiche e i documenti di pratica.

I documenti sono periodicamente rivisti sotto la responsabilità del management di Entaksi, al fine di valutarne la conformità ai requisiti nazionali e internazionali, agli standard, alla legislazione cogente, ai regolamenti vigenti, alle particolari esigenze imposte dall'evoluzione tecnica e tecnologica, all'evoluzione del contesto aziendale.

Il riesame e l'eventuale aggiornamento avvengono almeno una volta all'anno, oppure ogni qualvolta si verifichi una delle seguenti circostanze:

- cambiamenti organizzativi interni che impattano sul sistema;
- modifiche rilevanti dell'architettura hardware o software;
- aggiornamenti normativi;
- cambiamenti nelle procedure, nelle metodologie o nel contesto aziendale.

1.3. Approvazione e pubblicazione

Il presente documento e tutte le politiche e pratiche interne in esso menzionate sono state approvate dalla Direzione di Entaksi, pubblicate e comunicate ai dipendenti e, per quanto riguarda quelle classificate come "pubbliche", pubblicate sul sito web aziendale.

Entaksi mette a disposizione di tutti i clienti dei servizi di conservazione e delle parti interessate qualsiasi aggiornamento di questo documento e di altra documentazione pertinente non appena l'aggiornamento viene approvato e rivisto sulla base della procedura di revisione.

Qualsiasi modifica che possa influire sull'accettazione del servizio da parte del soggetto, dell'abbonato o degli affidatari, sarà comunicata da Entaksi attraverso il canale di comunicazione stabilito nei termini e nelle condizioni del servizio.

2. Definizioni e abbreviazioni

2.1. Definizioni

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. Abbreviazioni

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. Riferimenti

Per garantire la gestione a norma del Servizio di Conservazione eCON, Entaksi definisce i criteri e i processi del Servizio in base alla normativa italiana ed europea in materia, oltre ad implementare standard internazionali che definiscono la gestione teorica, operativa e funzionale del sistema. Vengono qui di seguito riportati le norme e gli standard di riferimento per l'azienda.

Il presente statement è conforme ai riferimenti normativi elencati di seguito, come richiesto dal regolamento eIDAS e dalla normativa italiana sulla conservazione digitale.

3.1. Riferimenti normativi e standard

3.1.1. Certificazioni

Entaksi ha ottenuto le seguenti certificazioni:

UNI ISO 9001:2015

Sistemi di Gestione per la Qualità – Requisiti.

ISO/IEC 20000-1:2018

Tecnologie informatiche – Erogazione di servizi informatici.

ISO/IEC 27001:2013

Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.

ISO/IEC 27017:2015

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO / IEC 27002 per i servizi cloud.

ISO/IEC 27018:2019

Tecnologia delle informazioni - Tecniche di sicurezza - Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che fungono da processori PII.

ISO/IEC 27035:2016

Tecnologia delle informazioni - Tecniche di sicurezza - Gestione degli incidenti di sicurezza delle informazioni.

ISO/IEC 22301:2019

Tecnologia delle informazioni - Sicurezza e resilienza - Sistemi di gestione della continuità operativa aziendale.

Sistema di conservazione dei documenti digitali

Tecnologia delle informazioni - Conservazione digitale - art. 24 Regolamento UE n° 910/2014 sull'identità digitale.

eIDAS

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

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

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

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, protocolli per fornitori di servizi fiduciari che forniscono servizi di conservazione dei dati a lungo termine.

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, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

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, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

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. Normativa italiana sulla conservazione digitale

CAD

Decreto legislativo N° 82/2005, "Codice dell'Amministrazione Digitale".

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Linee guida ufficiali sulla creazione, gestione e conservazione dei documenti informatici, pubblicate da AgID in data 11/09/2020 alle quali vengono aggiunte le modifiche con la relativa proroga contenute nella Determinazione 371/2021 del 17/05/2021.

Determinazione AgID 25 giugno 2021 n.455

Concernente l'adozione del "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici".

3.1.4. Protezione dei dati personali

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

Regolamento UE del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Decreto Legislativo 10 agosto 2018, n. 101

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

3.1.5. Altre disposizioni

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. Riferimenti informativi

Il servizio qualificato di conservazione a lungo termine di Entaksi è supportato dalle seguenti policy:

Tabella 1. Policy Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
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

Inoltre, il Servizio di conservazione eCON è descritto nelle seguenti dichiarazioni di pratica e manuali:

Tabella 2. Documenti Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
MAN SIG 20210708 Preservation Service Practice Statement	1.0.0	01/12/2021
MAN eCON 20151222 Conservazione	1.7.0	01/12/2021

Tutti i documenti elencati in precedenza sono classificati come "pubblici" e divulgati alle parti interessate tramite il sito web della società.

Oltre a questi, i documenti successivi illustrano alcuni argomenti confidenziali sul Servizio di Conservazione eCON, per lo più legati alle procedure di sicurezza del sistema e alle questioni tecniche.

Tabella 3. Documenti riservati Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
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, a causa del loro contenuto confidenziale, non divulga questi documenti e nessun altro dei suoi manuali interni, procedure e documenti di sicurezza. Tuttavia, secondo la disponibilità e l'impegno dell'azienda, è disponibile a sottoporsi a audit di verifica da parte dei suoi clienti o di altre parti interessate, previa firma di un accordo di non divulgazione.

4. Ruoli e responsabilità

La **comunità di riferimento del Servizio di Conservazione eCON**, così come richiesta in riferimento allo Standard ISO/IEC 14721:2012 OAIS (Open Archival Information System), è descritta nei manuali utente eCON, e per quanto riguarda il personale Entaksi vengono riportati anche i ruoli e le attività per ogni responsabile del servizio.

Entaksi è nominato Trust Service Provider per il servizio di conservazione a lungo termine eCON.

Il servizio di conservazione eCON è amministrato da vari "**Responsabili**", ognuno dei quali ricopre un ruolo specifico nell'azienda e in particolare nel servizio, al fine di garantire meglio l'affidabilità del sistema senza sovrapposizioni di attività e seguendo una compartimentazione dei ruoli:

- **Responsabile del Servizio di Conservazione**.
- **Vice Responsabile del Servizio di Conservazione**.
- **Responsabile della Funzione Archivistica**.
- **Responsabile del Trattamento dei Dati Personali**.
- **Responsabile della Sicurezza**.
- **Responsabile dei Sistemi Informativi**.
- *Responsabile dello Sviluppo e della Manutenzione.

Tutti i dati relativi alle persone e ai ruoli specifici ricoperti dai vari responsabili del Servizio di Conservazione eCON sono disponibili nel manuale di conservazione eCON, pubblicato sia sul sito dell'Agenzia per l'Italia Digitale che sul sito di Entaksi.

I compiti e le aree di responsabilità in conflitto sono segregati per ridurre le opportunità di modifiche non autorizzate o non intenzionali, o l'uso improprio degli asset di Entaksi.

Entaksi Solution SpA è responsabile della fornitura del servizio, e il Responsabile del Servizio di Conservazione è il ruolo incaricato per i compiti di fornitura del servizio.

In conformità con l'art. 38 del Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, all'interno dell'organizzazione sono nominate le seguenti persone in aggiunta ai ruoli sopra elencati:

- Responsabile della sicurezza.
- Responsabile del servizio qualificato.
- Responsabile della conduzione tecnica dei sistemi.
- Responsabile dei servizi tecnici e logistici.
- Responsabile delle verifiche e delle ispezioni (auditing).

4.1. Clienti

Un cliente è la persona fisica o giuridica vincolata da un accordo con un fornitore di servizi.

I clienti possono firmare l'accordo di servizio ("Condizioni generali del servizio") con il fornitore di servizi di conservazione Entaksi, al fine di accedere al Servizio di Conservazione eCON.

4.2. Parti coinvolte

Entaksi non coinvolge nessuna parte esterna per eseguire compiti critici sul servizio di conservazione eCON.
Tuttavia altre terze parti possono essere coinvolte nel processo, come gli organi di controllo legale, le autorità e i revisori.
Entaksi richiede sempre accordi di non divulgazione per qualsiasi accesso non contrattuale al sistema, come per gli audit, e

applica l'anonimizzazione e la minimizzazione dei dati personali ove possibile.

4.3. Fornitori

Entaksi eroga servizi dalla sua infrastruttura: tutto il sistema software è interamente sotto il controllo dell'azienda, mentre invece l'hardware e la connettività di rete sono gestiti direttamente dai fornitori dei datacenter.

I componenti fisici del servizio di conservazione eCON sono distribuiti in server situati in vari datacenter, distribuiti geograficamente allo scopo di garantire l'alta disponibilità del servizio.

Il sistema di conservazione è situato nei seguenti tre datacenter:

- *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)

La replica del sistema rafforza la continuità operativa e permette al sistema di rimanere disponibile in caso di guasto in uno qualsiasi dei tre poli.

Alcune componenti del sistema, come l'elaborazione, la verifica, l'indicizzazione e le procedure di presentazione dei dati, possono determinare il transito temporaneo dei dati nei seguenti due datacenter situati all'interno dell'Unione Europea:

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

Entaksi utilizza sistemi operativi GNU/Linux sui suoi server. La configurazione e l'accesso sono interamente sotto il controllo esclusivo di Entaksi Solutions. Il sistemi software operano su macchine virtuali configurate all'interno di un'area dati criptata.

I datacenter garantiscono i più alti livelli di performance in termini di affidabilità, sicurezza e connettività, utilizzano i protocolli IPv4 e IPv6 e sono certificati ISO/IEC 27001:2013.

Le Time-Stamping Authorities (TSA) qualificate che forniscono le marche temporali per il servizio di conservazione eCON sono:

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

5. Dichiarazione di pratica del servizio eCON

5.1. Profili di conservazione

Il servizio di conservazione eCON supporta i seguenti profili di conservazione:

Profilo di conservazione tradizionale	
OID	1.3.6.1.4.1.57823.2.1.1
Valido da	n/d
Fino a	31/12/2021
Descrizione	Questo profilo rappresenta il sistema di conservazione eCON prima della conformità eIDAS e dell'implementazione ETSI TS 119 511 v1.1.1 (2019-06). Il profilo è conforme alle linee guida italiane sulla conservazione dei documenti elettronici legalmente vincolanti per gli enti pubblici e privati.
Profilo di conservazione a lungo termine di dati e firme elettroniche con archiviazione ed estensione della validità 2022-01	
Valido da	01/01/2022
Fino a	Non definito
Descrizione	Questo profilo è rivolto alla conservazione di documenti elettronici firmati o meno, con archiviazione, validazione delle firme elettroniche, conservazione ed estensione della validità delle prove di esistenza associate. Il profilo è conforme sia con le linee guida italiane per la conservazione che con il regolamento eIDAS e i requisiti ETSI EN 319 401 V2.3.1 (2021-05) e ETSI TS 119 511 v1.1.1 (2019-06).

Gli identificativi dei profili di conservazione usano un OID allo scopo di riservare un codice univoco per ciascun profilo. L'OID è allocato sotto la seguente gerarchia di numeri:

Numero	**Descrizione**
1.3.6.1.4.1.57823	Entaksi Solutions SpA
2	Long-Term Preservation
1	Preservation Profiles

Quindi gli OID dei profili supportati sono:

Notazione puntata	**URI**	**Descrizione**
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	Profilo di conservazione tradizionale
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	Profilo di conservazione a lungo termine di dati e firme elettroniche con archiviazione ed estensione della validità 2022-01

Il capitolo Riferimenti informativi contiene una lista delle politiche supportate dal servizio di conservazione eCON.

Ai fini della presente "Dichiarazione di pratica del servizio eCON" i seguenti paragrafi descrivono il profilo di conservazione "Profilo di conservazione a lungo termine di dati e firme elettroniche con archiviazione ed estensione della validità 2022-01".

5.2. Schema di conservazione

Il profilo di conservazione supporta uno schema di conservazione composto dal modello di archiviazione WST (con archiviazione), e gli obiettivi di conservazione PGD (conservazione di dati in generale), PDS (conservazione di firme elettroniche) e AUG (estensione della validità).

Il seguente URI identifica lo schema di conservazione: `http://uri.etsi.org/19512/scheme/pds+pgd+wst+aug`

5.3. Modello di archiviazione

Il profilo di conservazione supporta la conservazione con archiviazione (WST) come definita nella clausola 4.3.1 di ETSI TS 119 512 V1.1.2 (2020-10).

5.4. Obiettivi di conservazione

Il profilo di conservazione supporta i seguenti obiettivi di conservazione:

- **Conservazione di dati in generale (PGD)** che, per il dato fornito al servizio di conservazione, fornisce una prova di esistenza per un lungo periodo di tempo.
  `http://uri.etsi.org/19512/goal/pgd`
- **Conservazione di firme elettroniche (PDS)** che estende per un lungo periodo di tempo la possibilità di validare una firma elettronica, di mantenere il suo stato di validità e di fornire una prova di esistenza dei dati firmati.
  `http://uri.etsi.org/19512/goal/pds`
- **Estensione della validità (AUG)** che supporta l'estensione della validità delle prove di esistenza fornite.
  `http://uri.etsi.org/19512/goal/aug`

5.5. Formati di input supportati

Il profilo di conservazione accetta i seguenti formati di file:

Tabella 4. Formati di file supportati.

Tipo	Nome del file	Sviluppato da	Visualizzatori	Standard	mime type
PDF	`.pdf`	Adobe System Inc.	Adobe Reader, Evince, altri	ISO 32000-2	`application/pdf`
PDF/A	`.pdf`	Adobe System Inc.	Adobe Reader, Evince, altri	ISO 19005	`application/pdf`
TIFF	`.tiff`,`.tif`	Aldus Corporation, ora Adobe System Inc.	Vari sofware che trattano immagini	ISO 12639	`image/tiff`
JPEG	`.jpg`, `.jpeg`, `.jpe`, `.jif`, `.jfif`, `.jfi`	Joint Photographic Experts Group	Vari software che trattano immagini	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	Vari software che trattano immagini	ISO/IEC 15948 RFC 2083	`image/png`

Tipo	Nome del file	Sviluppato da	Visualizzatori	Standard	mime type
OOXML	.docx .docm .xlsx .xlsm .pptx .pptm	Microsoft	Microsoft Office, LibreOffice, OpenOffice e altri	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 e altri	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	Navigatori web, vari visualizzatori di testo	W3C XML	application/xml text/xml
TXT	.txt	n/d	Vari visualizzatori di testo	ASCII ISO/IEC 8859 UTF-8	application/txt text/plain
EML	.eml	OASIS	Outlook, Mail, Thunderbird, varie applicazioni	RFC 822 RFC 5322	message/rfc822

Il profilo di conservazione accetta i seguenti formati di prova di esistenza:

URI	Formato	Note
http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3	CAdES Archive Time Stamp V3	L'attributo relativo alla versione 3 della marca temporale per archiviazione con sintassi ASN.1 secondo ETSI EN 319 122 V1.1.1 (clausola 5.5.3).
http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp	XAdES Archive Time Stamp	La proprietà relativa alla marca temporale per archiviazione nel formato XML secondo ETSI EN 319 132 V1.1.1 (clausola 5.5.2).
http://uri.etsi.org/ades/PAdES/document-time-stamp	PAdES Document Time-Stamp	La marca temporale sul documento secondo ETSI EN 319 142 V1.1.1 (clausola 5.4)

Il profilo di conservazione accetta documenti, firme elettroniche e dati in generale.

Il profilo di conservazione usa la seguente politica di gestione delle prove di conservazione descritta in "MAN eCON 20200628 Preservation Evidence Policy":

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

Il profilo di conservazione usa la seguente politica di validazione delle firme elettroniche descritta in "{documento_signature_validation_policy"}:

- Politica di validazione delle firme 2022-01 (OID 1.3.6.1.4.1.57823.2.3.1)

5.6. Protocollo di conservazione

Il servizio di conservazione eCON dispone di un protocollo per la comunicazione tra il servizio e il cliente del servizio di conservazione.

Questa comunicazione è basata su un insieme di API che scambiano messaggi JSON e XML su connessioni HTTPS.

Il servizio di conservazione eCON non implementa l'intero insieme di API specificato in ETSI TS 119 512 V1.1.2 (2020-10). Definisce invece un proprio insieme di API REST per la maggior parte delle funzionalità del protocollo di conservazione. Tuttavia alcune di queste funzionalità sono disponibili con le API ETSI TS 119 512 V1.1.2 (2020-10).

Una implementazione completa dell'insieme di API ETSI TS 119 512 V1.1.2 (2020-10) potrebbe essere sviluppata in una futura evoluzione del servizio di conservazione eCON.

5.6.1. Descrizione del processo di conservazione

Accesso al sistema di conservazione elettronica

Per la gestione delle credenziali di accesso, il servizio di conservazione eCON usa un sistema di gestione delle identità compatibile con gli standard OAuth2 (RFC-6749, RFC-6750, RFC-6819, RFC-7662, RFC-7009, RFC-7519), SAMLv2 e con il protocollo OpenID Connect.

Il sistema consente agli utenti di usare un sistema di autenticazione unico che consente di accedere alle varie componenti del servizio. Gli amministratori del servizio regolano il livello di autorizzazione. Il sistema di autenticazione e autorizzazione sfrutta il protocollo OpenID Connect per rendere sicure le comunicazioni con le API del servizio.

L'accesso alle funzionalità del servizio iniziano con un profilo utente fornito all'utente e identificato dal suo indirizzo email. Il primo profilo utente ha il ruolo di "gestore del servizio" che ha i privilegi su tutte le funzioni del servizio. Tra questi, il "gestore del servizio" può gestire altri profili utente e il loro specifico ruolo di accesso.

Il servizio di conservazione eCON ha i seguenti ruoli disponibili:

- gestore del servizio;
- utente del servizio;
- utente abilitato a gestire il caricamento dei documenti;
- utente in sola lettura.

Gli utenti con il ruolo "gestore del servizio" possono aggiungere o rimuovere altri utenti identificati dal loro indirizzo email. Tutte le operazioni vengono notificare via email.
La rimozione di un utente non elimina i dati dell'utente ma rimuove solo i privilegi di quell'utente, registrando la data di revoca dei privilegi e mantenendo i dati relativi all'uso del servizio fino alla terminazione dello stesso.

Versamento dei dati in conservazione

I dati vengono forniti al servizio di conservazione eCON attraverso un Pacchetto di Versamento (PDV) che contiene un insieme di dati e i relativi metadati.

I PDV caricati vengono validati in modo asincrono e, alla fine del processo di validazione, viene emesso un rapporto di versamento per ciascun PDV all'indirizzo email dell'utente che ha eseguito il caricamento.

Il rapporto di versamento informa l'utente se il PDV è stato accettato o rifiutato e, in quest'ultimo caso, contiene varie informazioni sulle violazioni che hanno causato il rifiuto del PDV.

Profili di conservazione disponibili

Anche se il servizio di conservazione eCON non implementa completamente le specifiche ETSI TS 119 512 V1.1.2 (2020-10), il metodo API `RetrieveInfo` definito in ETSI TS 119 512 V1.1.2 (2020-10) clausola 5.3.2 è implementata per recuperare le informazioni sui profili di conservazione supportati dal servizio di conservazione.

Accesso ai dati conservati

Il servizio di conservazione eCON ha una funzione di ricerca che consente all'utente di interrogare l'archivio usando i metadati associati agli oggetti conservati come criteri di ricerca.

I dati conservati che corrispondono ai criteri di ricerca per l'interrogazione vengono mostrati all'utente che può inoltrare al sistema una richiesta di Pacchetto di Distribuzione (PDD).

Il PDD risultante contiene i dati conservati e le relative prove di esistenza al momento del versamento. Il PDD è quindi disponibile per essere scaricato solo dall'utente autorizzato.

Validazione degli oggetti conservati

Il servizio di conservazione eCON implementa il metodo API definito in ETSI TS 119 512 V1.1.2 (2020-10) clausola 5.3.8 (`ValidateEvidence`) allo scopo di consentire all'utente di inviare una prova di conservazione e una sequenza di oggetti conservati a cui la prova di conservazione corrisponde. Il servizio risponde con il risultato di una validazione della prova di conservazione fornita cioè con un rapporto di validazione della prova di conservazione.

Cancellazione degli oggetti conservati

Il servizio di conservazione eCON cancella gli oggetti conservati e le relative prove di conservazione all'interno dei propri archivi nei seguenti casi:

- su richiesta del cliente;
- alla fine del periodo di validità impostato sugli accordi di servizio.

Entrambi i casi devono essere approvati dal Responsabile della Funzione Archivistica.

Alcune circostanze, come la conduzione di indagini fiscali o criminali può impedire la cancellazione di documenti in osservanza alle regole locali dello Stato. In questo caso la richiesta di cancellazione verrà rifiutata con una motivazione formale.

Le richieste di cancellazione possono essere inoltrate solo durante il periodo di validità degli accordi di servizio. Alla fine del contratto l'utente ha un periodo di 6 mesi per recuperare i suoi dati conservati prima che vengano cancellati permanentemente. In questo periodo le richieste di cancellazione saranno sospese.

Tutte le richieste di cancellazione e le risposte sono registrate e i registri vengono conservati come descritto nel paragrafo Registro di audit.

Il servizio di conservazione eCON implementa il metodo API definito in ETSI TS 119 512 V1.1.2 (2020-10) clausola 5.3.5 (`DeleteP0`) che consente all'utente di cancellare un oggetto conservato. Tuttavia, quando si ha a che fare con dati conservati provenienti da entità italiane che sono soggette alle linee guida sulla conservazione elettronica italiane, questo metodo restituisce sempre l'errore `http://uri.etsi.org/19512/error/noPermission` in quanto queste linee guida proibiscono la cancellazione degli oggetti conservati.

Pacchetti di Import-Export

Il cliente del servizio ussa le funzioni descritte in Accesso ai dati conservati per richiedere e recuperare i pacchetti di distribuzione (PDD) che contengono parti o tutti gli oggetti conservati dal servizio e le relative prove di conservazione.

Il formato dei pacchetti di distribuzione è conforme allo standard UNI 11386:2020.

Aggiornamento degli dati conservati

Il servizio di conservazione eCON non implementa l'operazione opzionale del protocollo per l'aggiornamento dei dati conservati.

Accesso all'audit trail

Il servizio di conservazione eCON implements un suo insieme di API REST per recuperare gli elementi dell'audit trail per le varie entità coinvolte nel processo di conservazione: PDV, PDA, PDD.

5.7. Protocollo di notifica

Il servizio di conservazione eCON notifica gli utenti del servizio utilizzando il loro indirizzo email.

Come descritto nel paragrafo Accesso al sistema di conservazione elettronica l'accesso al servizio di conservazione elettronica può avvenire dopo una procedura di registrazione disponibile nell'interfaccia utente del servizio, utilizzando l'indirizzo email fornito all'interno degli accordi di servizio ("Condizioni generali del servizio").

Dopo la stipula del contratto, l'indirizzo email registrato nelle condizioni di servizio viene considerato come l'unico canale sicuro attraverso il quale il servizio di conservazione eCON invia messaggi riguardanti la gestione del servizio, come: modifiche al sistema, interruzioni programmate, aggiornamenti tecnici o del regolamento, obsolescenza dei dati o delle tecnologie.

Qualsiasi modifica o problematica di sicurezza che possa interessare il profilo di conservazione, le politiche del servizio, incluse la politica per la gestione delle evidenze di conservazione e la politica di validazione delle firme elettroniche, o questa dichiarazione sarà notificata agli utenti interessati via email.

Il servizio di conservazione eCON fornisce uno strumento per configurare le notifiche email inviate automaticamente dal sistema per certe funzionalità, come il report di validazione per i PDV caricati o la disponibilità dei PDD richiesti.

Al primo accesso tutte le notifiche sono disabilitate e ciascun utente può configurare le sue impostazioni autonomamente mediante l'interfaccia utente del servizio.

6. Controlli tecnici di sicurezza

6.1. Valutazione dei rischi

Entaksi conduce regolarmente un'analisi dei rischi finalizzata a proteggere l'intero sistema di gestione. La valutazione dei rischi identifica, analizza e valuta le minacce, gli impatti e le probabilità di ciascun componente con particolare attenzione ai rischi del servizio fiduciario, considerando aspetti tecnici e gestionali.

L'analisi produce un documento che descrive tutte le misure per il trattamento del rischio per assicurare il livello di sicurezza commisurato al grado di rischio.

La metodologia e la pratica usate per implementare e condurre il sistema di gestione dei rischi sono conformi allo standard descritto nel capitolo Riferimenti.

L'analisi dei rischi condotta da Entaksi per proteggere il servizio di conservazione eCON è divisa nelle seguenti fasi:

- **Identificazione della Designated Community**, dove per la conduzione della DPIA si intende gli interessati al trattamento.
- **Identificazione degli asset / CI** ossia, per la DPIA, tutti quegli asset nel CMDB Entaksi che contengano dati personali.
- **Identificazione delle minacce** definite come eventi o fenomeni potenzialmente dannosi cui possono essere esposti gli asset durante l'operatività dell'azienda.
- **Definizione del rischio accettabile** ossia il calcolo della "soglia di rischio accettabile", individuata arbitrariamente dall'organizzazione come limite della tollerabilità, dopo una attenta valutazione dei costi/benefici indotti dalla adozione di eventuali contromisure di mitigazione.
- **Stima della probabilità di accadimento delle minacce** calcolata sulla verosimiglianza che il fenomeno si verifichi entro un determinato periodo di tempo, convenzionalmente stabilito in tre anni.
- **Stima degli impatti**, il danno derivante dagli eventi avversi che si potrebbero produrre sugli asset critici a fronte delle minacce identificate, calcolato sul danno economico che ne deriverebbe all'azienda (anche in relazione all'art. 83 GDPR).
- **Calcolo della vulnerabilità**, ossia la 'propensione' di un asset ad essere danneggiato da una particolare minaccia.
- **Analisi dei rischi** ingresso dei valori di probabilità, impatto e vulnerabilità di ciascuna minaccia su asset contenenti dati personali, calcolati sui valori dell'analisi precedente e su misure effettuate sui sistemi.
- **Contromisure adottate** applicazione esecuzione di attività o adozione di comportamenti che possono portare al contenimento, alla riduzione, al trasferimento o all'eliminazione del rischio.
- **Gestione del Rischio Residuo** il ricalcolo del rischio dopo l'applicazione delle contromisure, e la sua gestione.

- **Redazione del Rapporto di valutazione dei rischi e del Piano di trattamento dei rischi**.

La valutazione dei rischi viene rivista e revisionata almeno annualmente, a meno di modifiche strutturali o normative significative.

Il risultato della valutazione viene revisionato dalla direzione di Entaksi che controlla, per ciascuna minaccia identificata, che la corretta contromisura sia applicata, approva la valutazione di rischio e accetta i rischi residui identificati.

6.2. Controlli crittografici

Il servizio di conservazione eCON segue le raccomandazioni ETSI TS 119 312 V1.4.1 (2021-08) per gli algoritmi crittografici.

Per le impronte e le marche temporali viene utilizzato esclusivamente l'insieme di funzioni SHA-256. Le marche temporali provengono da un fornitore di servizi fiduciari che segue lo stato dell'arte nelle pratiche per definire le politiche e i requisiti di sicurezza, in accordo con ETSI EN 319 421 V1.1.1 (2016-03).

Inoltre, i certificati di firma utilizzati dal servizio sono emessi unicamente da fornitori di servizi fiduciari che implementano ETSI EN 319 411-1 V1.3.1 (2021-05) o ETSI EN 319 411-2 V2.3.1 (2021-05).
Entaksi verifica questi requisiti durante la fase di qualifica del fornitore.

Il servizio di conservazione eCON usa marche temporali e certificati di firma che sono verificabili usando liste di revoca (CRL) o risposte del servizio OCPS che includono il campo "reason code" in caso di revoca del certificato di una chiave pubblica.

Il servizio di conservazione eCON stabilisce che le firme elettroniche apposte dal sistema usino un dispositivo EAL4 ISO/IEC 15408 (cioè una smart card o un HSM certificato) con un certificato emesso da una autorità di certificazione eIDAS, e non utilizza dispositivi FIPS PUB 140-2.

I dispositivi scelti da Entaksi per il servizio di conservazione eCON non consentono il backup della chiave privata.

6.3. Sicurezza di rete

Gli utenti possono accedere al servizio di conservazione eCON tramite le funzioni fornite dall'interfaccia utente o tramite le API REST rese disponibili su richiesta.

Le caratteristiche del servizio sono accessibili mediante una connessione HTTPS dalla rete pubblica usando il meccanismo di autenticazione OAuth2 OpenID Connect (vedi RFC-6749 e http://openid.net/).

Per le comunicazioni cifrate con i servizi esposti dall'infrastruttura sulla rete pubblica il servizio di conservazione eCON usa il protocollo TLS (Transport Layer Security) versione 1.2 o successivi.

Versioni precedenti del protocollo TLS e il protocollo SSL (Secure Socket Layer) sono disabilitati.

Le aree di applicazione di questo protocollo sono:

1. La protezione delle connessioni ai servizi che usano il protocollo HTTP.
2. La sicurezza delle connessioni ai servizi di posta elettronica o altri servizi basati su connessioni TCP.
3. La protezione delle conessioni VPN.
4. La protezione di altri canali di interconnessione tra servizi interni basati sul TLS.

6.4. Registro di audit

Il servizio di conservazione eCON usa la registrazione e la revisione degli eventi come uno dei componenti necessari per il suo sistema di gestione della sicurezza. In questo paragrafo sono fornite le descrizioni dei vari tipi di eventi registrati e revisionati, la frequenza delle verifiche e le procedure di conservazione.

Eventi registrati:

- autenticazioni riuscite e fallite;
- modifiche sulle impostazioni di sicurezza;
- uso dei privilegi o aumento dei privilegi;
- eventi di sistema;
- modifica di entità a livello di sistema;
- tutte le operazioni relative a un specifico identificativo di un'entità conservata;
- attività di sessione;
- attività relative alla gestione degli utenti inclusa la modifica delle password (riuscite e fallite);

Ogni evento registrato riporta le seguenti informazioni:

- data e ora dell'attività;
- indirizzo IP di provenienza (per il registro delle connessioni);
- identificativo dell'utente;
- descrizione dell'attività completata o tentata;
- la richiesta e la risposta del client;
- uso anomalo, ad esempio nel numero di transazioni, picchi di utilizzo, ecc;
- comportamento anomalo dell'applicazione, incluso il ripetuto riavvio dell'applicazione;
- modifiche sui dati dove richiesto dalla conformità con i regolamenti;

Entaksi assicura un adeguato monitoraggio dei registri degli eventi e revisiona questi registri in caso problemi di sicurezza sospettati o riportati.

I registri degli eventi sono conservati per 6 mesi. Il periodo di conservazione può essere ridotto o allungato in funzione dei termini di contratto, delle leggi e dei regolamenti.

La conservazione avviene all'interno del servizio di conservazione eCON. I registri degli eventi sono inviati in conservazione quotidianamente.

I registri degli eventi sono sottoposti all'accesso, alla sicurezza e alla protenzione in base alla natura delle informazioni che possono contenere. Ad eccezione di Entaksi, qualsiasi attività di revisione dei registri, come le verifiche o le ispezioni, viene registrata.

Per qualsiasi domanda o richiesta di assistenza con i registri degli eventi e per segnalare attività sospette l'utente può contattare l'assistenza Entaksi.

7. Cessazione TSP e piani di cessazione

La decisione di cessare il Servizio di Conservazione eCON può essere presa solo dal management di Entaksi Solution SpA.

L'Amministratore Delegato, preso atto del parere dei Soci, dovrà formalizzare la cessazione della fornitura del Servizio di Conservazione eCON e la successiva attivazione del piano di cessazione in un verbale.

Un apposito documento descrive il piano di cessazione e la procedura per affrontare le fasi di cessazione. Il piano è costantemente tenuto aggiornato dalla direzione di Entaksi ed è conforme alla normativa italiana e internazionale sulla conservazione a lungo termine.

Il piano di cessazione sviluppa tutte le attività riassunte nel seguente elenco:

1. **Decisione di cessazione del servizio**: la Direzione di Entaksi Solutions SpA, sentito il parere dei Soci, può dichiarare la cessazione del servizio di conservazione eCON. Contestualmente redige un'apposita relazione in cui spiega il motivo della cessazione, il piano di cessazione e avvia il programma di cessazione.
   Allo stesso tempo, viene interrotta l'acquisizione di nuovi clienti.
2. **Comunicazione alle parti interessate**: durante la procedura di cessazione le parti interessate, elencate nel capitolo Ruoli e responsabilità, sono informate della cessazione del servizio. La comunicazione avviene almeno 60 giorni prima della cessazione effettiva del servizio. La comunicazione deve essere notificata rapidamente a tutte le parti interessate.
   La responsabilità della comunicazione è affidata al Responsabile del Servizio di Conservazione, che approva il contenuto della mail. Il database delle e-mail delle terze parti interessate è mantenuto aggiornato sul sistema.
   Oltre all'invio delle comunicazioni via e-mail, un avviso di cessazione del servizio viene pubblicato sul sito web della società "www.entaksi.eu".
3. **Cessazione dei subappaltatori**: Entaksi attualmente non utilizza subappaltatori per il Servizio di Conservazione eCON, ma ha una specifica procedura interna che regola i rapporti con i fornitori e altri subappaltatori.
4. **Identificazione del sistema di conservazione per la documentazione del servizio**: entro 30 giorni dall'inizio della procedura di cessazione, Entaksi sceglierà un altro servizio di conservazione per depositare la documentazione che prova il funzionamento del Sistema di Conservazione (documentazione tecnica, manuali di servizio, log del sistema, contratti di servizio).
   L'individuazione del servizio segue la procedura di qualificazione del fornitore come indicato nella procedura interna che regola i rapporti con i fornitori. Il TSP individuato viene anche proposto ai clienti come nuovo servizio di conservazione a cui trasferire gli archivi.
5. **Trasferimento dei dati di conservazione a un nuovo sistema di conservazione**: la documentazione che prova la gestione del sistema di conservazione (documentazione tecnica, manuali di servizio, sistema, modello SLA) è selezionata dal

Responsabile della Funzione Archivistica. La lista di consistenza è approvata dal Responsabile del Servizio di Conservazione e dal Responsabile del Trattamento dei Dati Personali, e i Pacchetti di Distribuzione per interoperabilità (PDD) sono preparati dal Responsabile dello Sviluppo e della Manutenzione, che è anche responsabile del completamento della procedura di trasferimento.
Il caricamento avviene entro lo stesso lasso di tempo previsto per i clienti alla data di cessazione.
La comunicazione del nuovo sistema di conservazione designato viene inviata all'AgID dal Responsabile del Servizio di Conservazione secondo la procedura di comunicazione con l'autorità.

6. **Notifica di disdetta da parte del Responsabile del Servizio di Conservazione**: una volta identificato il nuovo fornitore del servizio di conservazione, viene preparata una seconda comunicazione per i clienti, che rende disponibili le specifiche tecniche per gli utenti per preparare i propri PDD da esportare o per permettere che Entaksi trasferisca automaticamente i documenti ospitati direttamente al nuovo fornitore per loro conto.
   L'accesso al servizio di conservazione è garantito fino alla data di cessazione stabilita contrattualmente (6 mesi dalla notifica) per permettere l'esportazione autonoma degli oggetti di conservazione tramite PDD.
   Se l'attività di conservazione termina senza l'indicazione di un sostituto del TSP e non è possibile garantire la conservazione e la disponibilità della documentazione e degli archivi, gli oggetti di conservazione e i relativi documenti sono depositati entro 60 giorni nell'archivio AgID, che ne garantisce la conservazione e la disponibilità, ai sensi dell'art. 37 comma 4-bis del CAD.
7. **Cessazione**: terminato il periodo di 6 mesi per il trasferimento della documentazione, il Responsabile dello Sviluppo e della Manutenzione, su indicazione del Responsabile della Funzione Archivistica e con l'approvazione del Responsabile del Servizio di Conservazione, procede alla cancellazione definitiva degli oggetti conservati. L'eliminazione è estesa a tutte le copie di backup e viene effettuata utilizzando la più aggiornata tecnologia di cancellazione sicura disponibile.

Il piano di cancellazione è referenziato come "MAN eCON 20190918 Piano di cessazione" ed è classificato come "Confidenziale".

8. Altre disposizioni

8.1. Conformità e audit

Il sistema giuridico applicabile è dichiarato nel capitolo Riferimenti.

La configurazione del Servizio di Conservazione eCON è regolarmente controllata dalla direzione per evitare qualsiasi modifica che violi le politiche di sicurezza di Entaksi.

Il Servizio di Conservazione eCON di Entaksi è supervisionato dall'Agenzia dell'Italia Digitale (AgID), che ha la responsabilità di verificare e revisionare periodicamente la conformità del sistema ai requisiti definiti in base alla normativa italiana sulla conservazione digitale.

Inoltre, il sistema è verificato almeno annualmente da un organismo di certificazione accreditato, riconosciuto da Accredia, l'Ente Italiano di Accreditamento.

I verbali di audit e i documenti di controllo sono classificati come confidenziali.
I certificati di conformità e i loro aggiornamenti sono pubblicati sul sito web Entaksi in conformità ai risultati della valutazione.

8.2. Termini e condizioni

Entaksi fornisce un accordo di servizio ("Condizioni generali del servizio") ai potenziali clienti interessati per essere informati su termini e condizioni del servizio di conservazione eCON, prima di formalizzare un rapporto contrattuale.

Il contratto contiene:

- termini e condizioni generali del servizio di conservazione eCON;
- limitazione dell'uso del servizio;
- obblighi del cliente;
- informazioni per le parti coinvolte nel servizio fiduciario;
- il periodo di tempo per il quale vengono conservati i log degli eventi di Entaksi;
- limitazioni di responsabilità;
- limitazioni sull'uso dei servizi forniti, compresa la limitazione per i danni derivanti dall'uso dei servizi che superano tali limitazioni;

- procedure per i reclami e la risoluzione delle controversie;
- se il servizio fiduciario Entaksi è stato valutato conforme alla politica del servizio fiduciario e attraverso quale schema di valutazione della conformità;
- informazioni di contatto di Entaksi;
- qualsiasi impegno riguardante la disponibilità e i Service Level Agreements.

Per quanto riguarda specificamente il sistema di conservazione:

- il riferimento a questo documento e ad altre politiche pertinenti, e il profilo di conservazione supportato;
- un riferimento al manuale dell'utente, che spiega il ruolo dell'autore nel processo di conservazione, le specifiche dei dati da convalidare, come importare i Pacchetti di Versamento (PDV) e richiedere i Pacchetti di Distribuzione (PDD);
- il numero massimo di errori consentito per un singolo PDV da convalidare, e come il sistema notifica gli errori.

Entaksi mette i termini e le condizioni del Servizi di Conservazione eCON a disposizione di tutti i clienti e delle parti interessate, e può trasmettere il documento in forma cartacea o elettronica.

Entaksi non impiega subappaltatori o outsourcer per la fornitura di funzioni di servizio classificate come critiche. Qualsiasi terza parte coinvolta è nominata nel contratto.

Entaksi conserva automaticamente il documento digitale firmato del contratto di servizio sia sul proprio sistema di conservazione che sull'area riservata del cliente. Se il contratto è firmato in forma cartacea procede a digitalizzarlo e archivia entrambe le copie.

I termini e le condizioni sono disponibili in due lingue, italiano e inglese.

8.3. Formato e lingua dei documenti

I documenti del sistema di conservazione eCON come indicati nel capitolo Riferimenti informativi sono disponibili in formato descrittivo in formato PDF.

La politica di validazione delle firme elettroniche è disponibile in formato elettronico.

I documenti sono disponibili in due lingue: inglese e italiano.

A causa dell'interpretazione della lingua ci possono essere piccole differenze tra le due versioni che, comunque, non impattano sul contenuto. In caso di ambiguità la versione in inglese ha la precedenza.

8.4. Protezione dei dati

Nell'ambito del trattamento dei dati personali relativi allo svolgimento delle attività fornite dal sistema di conservazione eCON, Entaksi opera come Titolare del trattamento in virtù di una specifica delega fornita dal cliente.

L'insieme completo delle condizioni relativa al trattamento dei dati personali nel servizio eCON è riportato nel documento "Condizioni Generali del Servizio", capitolo "Trattamento dei dati personali".

L'insieme completo delle condizioni relative al trattamento dei dati personali di Entaksi è riportato nel sito web Entaksi.

8.4.1. Data Breach

Secondo il Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati, articoli 33-34, "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza(...)".

"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.".

Pertanto, non appena Entaksi viene a conoscenza di una violazione dei dati personali trattati, in qualità di titolare o responsabile del trattamento, notificherà la violazione sia al/ai cliente/i che all'autorità di controllo e agli aventi diritto, senza indebito ritardo, **entro 72 ore** dal momento in cui ne è venuta a conoscenza.

L'obbligo non sussiste nel caso in cui il Titolare sia in grado di dimostrare che è improbabile che la violazione rappresenti un rischio per i diritti e le libertà delle persone fisiche come: perdita di controllo dei dati personali o limitazione dei loro diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifrazione non autorizzata della pseudonimizzazione, danno alla reputazione, perdita di riservatezza dei dati personali protetti dal segreto professionale, o qualsiasi danno economico o sociale significativo per il proprietario dei dati.

Passate le 72 entro cui viene rilevata la violazione la notifica deve essere corredata delle ragioni del ritardo e deve essere data in ogni caso la massima disponibilità a collaborare con le autorità competenti.