



ENTAKSI SOLUTIONS

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 Signature Validation Policy

Entaksi Solutions SpA

Indice

Informazioni sul documento	1
Revisioni e relative distribuzioni	1
Approvazione del documento	1
1. Introduzione	2
1.1. Identificazione del documento	2
1.2. Aggiornamento del documento	2
1.3. Approvazione e pubblicazione	2
2. Definizioni e abbreviazioni	3
2.1. Definizioni	3
2.2. Abbreviazioni	5
3. Riferimenti	6
3.1. Riferimenti normativi	6
3.1.1. Long-Term Preservation	6
3.1.2. Normativa italiana sulla conservazione digitale	7
3.1.3. Certificazioni	7
3.1.4. Protezione dei dati personali	8
3.1.5. Altre disposizioni	8
3.2. Riferimenti informativi	8
4. Ruoli e responsabilità	9
4.1. Politiche di validazione delle firme nel Servizio di Conservazione eCON	10
4.1.1. Strategia di validazione	10
4.1.2. Politiche di validazione	10
4.1.3. Descrizione delle politiche	10
Politica di validazione delle firme eCON 2022-01	10
5. Altre disposizioni	10
5.1. Conformità e audit	11

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN eCON 20210628 Signature Validation Policy
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	<i>Firmato digitalmente</i>

© 2021 Entaksi Solutions

Le informazioni contenute nel presente documento sono di proprietà di Entaksi Solutions, sono fornite ai destinatari in via riservata e confidenziale e non possono essere usate per fini produttivi, né comunicate a terzi o riprodotte, per intero o in parte, senza il consenso scritto di Entaksi Solutions.

1. Introduzione

Questo documento descrive la politica di validazione delle firme elettroniche implementata nel Servizio di Conservazione eCON fornito da Entaksi Solutions SpA, via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT) (website: <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.

1.1. Identificazione del documento

Questo documento è identificato dal seguente OID:

OID	Descrizione
1.3.6.1.4.1.57823.1.4	MAN eCON 20210628 Signature Validation Policy 1.0.0

Gli OID che identificano le specifiche policy di validazione sono specificati 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

3.1.1. Long-Term Preservation

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

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

3.1.2. 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".

3.1.3. 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.

3.1.4. 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).

Altri ruoli sono definiti nei documenti "MAN SIG 20210708 Preservation Service Policy" e "MAN SIG 20210708 Preservation Service Practice Statement".

4.1. Politiche di validazione delle firme nel Servizio di Conservazione eCON

Le politiche di validazione delle firme elettroniche utilizzate nel Servizio di Conservazione eCON sono disponibili in un formato elettronico interpretabile dalla procedura di validazione.

Il Servizio di Conservazione eCON interpreta automaticamente la descrizione di una politica di validazione delle firme usando il formato elettronico secondo le specifiche tecniche descritte in ETSI EN 319 102-1 V1.1.1 (2016-5).

Le politiche di validazione delle firme sono descritte in un file XML che stabilisce le regole e le politiche applicate durante il processo di validazione.

4.1.1. Strategia di validazione

La validazione delle firme opera secondo quanto indicato in ETSI EN 319 102-1 V1.1.1 (2016-5) capitolo "5.6 Validation process for Signatures providing Long-Term Availability and Integrity of Validation Material".

Durante la procedura di validazione tutti i materiali necessari per la validazione a lungo termine delle firme vengono raccolti dando come risultato un rapporto di validazione che contiene tutti questi materiali raccolti e l'insieme delle prove di esistenza della firma nel momento della validazione.

4.1.2. Politiche di validazione

Le politiche di validazione delle firme di Entaksi sono identificate dai seguenti OID:

OID	Descrizione
1.3.6.1.4.1.57823.2.3.1	eCON Signature Validation Policy 2022-01

4.1.3. Descrizione delle politiche

Le politiche descrivono un processo che valida le firme elettroniche indicando se queste sono delle firme elettroniche avanzate (AdES), delle firme elettroniche avanzate realizzate con un certificato qualificato (AdES/QC) o delle firme elettroniche qualificate (QES). Tutti i certificati e le loro relative catene di validità a supporto della firma sono validate utilizzando la lista fiduciaria degli Stati membri dell'UE (questo comprende il certificato del firmatario, i certificati utilizzati per validare lo stato di validità del certificato, le CRL, le risposte OCSP e le marche temporali).

Le politiche contengono regole e parametri di validazione che potrebbero cambiare nel tempo seguendo le raccomandazioni descritte nelle versioni più aggiornate di ETSI TS 119 312 V1.4.1 (2021-08).

Politica di validazione delle firme eCON 2022-01

La "Politica di validazione delle firme eCON 2022-01" è identificata dall'OID 1.3.6.1.4.1.57823.2.3.1 e contiene le regole e i parametri di validazione aggiornati a gennaio 2022.

Il file XML che descrive la policy di validazione delle firme è disponibile al seguente indirizzo: <https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.2.3.1>

Il file XML che descrive la policy di validazione delle firme segue i requisiti definiti in ETSI EN 319 102-1 V1.1.1 (2016-5). La procedura di validazione prende questo file in input per applicare le regole e i parametri di validazione definiti in questo file e produce un report di validazione secondo il formato definito in ETSI TS 119 102-2 V1.1.1 (2016-5).

Questa politica di validazione delle firme usa il modello "shell" nel quale tutti i certificati devono essere validi al momento della validazione.

5. Altre disposizioni

5.1. 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.

Altre disposizioni sono definite nei documenti "MAN SIG 20210708 Preservation Service Policy" e "MAN SIG 20210708 Preservation Service Practice Statement".