



ENTAKSI SOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001

ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035

SERVIZI FIDUCIARI QUALIFICATI

ETSI 319 401 | ETSI 319 411-1 e 2 | ETSI 319 421 | ETSI 119 511

FIRME E SIGILLI ELETTRONICI - MARCHE TEMPORALI

CONSERVAZIONE A LUNGO TERMINE

## Manuale

MAN eIDAS 20210628 Preservation Evidence 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 .....	6
3.1.3. Protezione dei dati personali .....	6
3.1.4. Certificazioni .....	6
3.1.5. Altre disposizioni .....	7
3.2. Riferimenti informativi .....	7
4. Ruoli e responsabilità .....	9
4.1. Politica per la gestione delle evidenze di conservazione eCON .....	10
4.1.1. Creazione delle evidenze di conservazione .....	10
4.1.2. Archiviazione delle evidenze di conservazione .....	10
4.2. Estensione della validità dell'evidenza di conservazione .....	11
4.3. Informazioni esplicite sulla politica di gestione delle evidenze di conservazione .....	11
4.4. Uso di altri servizi fiduciari .....	11
5. Altre disposizioni .....	13
5.1. Conformità e audit .....	13

## Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Manuale
Nome documento	MAN eIDAS 20210628 Preservation Evidence Policy
Versione	1.1.0
Data creazione	28/06/2021
Ultima revisione	15/12/2023
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	RSIG	Creazione bozza.	Interno
01/12/2021	1.0.0	Alessia Soccio	RSIG	Revisione e rilascio.	Pubblico
15/12/2023	1.1.0	Alessia Soccio	RSIG	Aggiornamento periodico, revisione presentazione società, revisione formale definizioni e riferimenti normativi, correzioni minori.	Pubblico

## Approvazione del documento

Data	Addetto	Mansione	Firma
15/12/2023	Alessandro Geri	Amministratore Unico	<i>Firmato digitalmente</i>

© 2023 Entaksi Solutions SpA.

Le informazioni contenute nel presente documento sono di proprietà di Entaksi Solutions SpA, 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.

# 1. Introduzione

Questo documento rappresenta la **politica per la gestione delle evidenze di conservazione relative al servizio di conservazione eCON fornito da Entaksi Solutions SpA - Irish Branch**, (di seguito "Entaksi"), una filiale dell'azienda italiana con numero di partita IVA IT01621900479 Entaksi Solutions SpA, che opera in Irlanda con numero di iscrizione al Registro Nazionale del Commercio 909882.

Entaksi è un **Trust Service Provider** per:

- **rilascio di certificati qualificati per firme elettroniche e sigilli;**
- **creazione di marche temporali elettroniche;**
- **conservazione a lungo termine di firme elettroniche e sigilli.**

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 definite da Regolamento UE 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 (di seguito "eIDAS").

## 1.1. Identificazione del documento

Questo documento è identificato dal seguente OID:

Tabella 1. Nome del documento e identificativo.

OID	Descrizione	Permanent Link
1.3.6.1.4.1.57823.1.3	MAN eIDAS 20210628 Preservation Evidence Policy	<a href="https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3">https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3</a>

Gli OID che identificano le specifiche politiche per la gestione delle evidenze di conservazione e sono individuati 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 al seguente link: <https://www.entaksi.eu/documentation.html>.

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**

Autorità che fornisce informazioni sullo stato del certificato.

**Pacchetto**

*Data object* che contiene un insieme di dati ed informazioni aggiuntive opzionali, che descrivono gli oggetti contenuti e, facoltativamente, il loro contenuto e le loro interrelazioni.

**Data object**

Dati binari su cui opera un'applicazione (ad esempio, trasformandoli, selezionandoli o firmandoli) e che possono essere associati a informazioni aggiuntive come un identificatore, l'encoding, la dimensione o il tipo.

**Servizio di conservazione qualificato UE**

Servizio di conservazione che soddisfa i requisiti per il servizio di conservazione qualificato per firme elettroniche qualificate e/o per sigilli elettronici qualificati come stabilito in Regolamento UE no. 910/2014 - eIDAS.

**Record di evidenza**

Unità di dati che può essere utilizzata per provare l'esistenza di un oggetto dati archiviato o di un gruppo di oggetti dati archiviati in un certo momento.

**Durata prevista delle evidenze**

Per un servizio di conservazione con archiviazione temporanea o senza archiviazione, è la durata durante la quale il servizio di conservazione si aspetta che le evidenze di conservazione possano essere utilizzate per raggiungere l'obiettivo di conservazione a lungo termine: il periodo di tempo durante il quale i cambiamenti tecnologici possono costituire un problema.

**Metadati**

Dati relativi ad altri dati.

**Interfaccia di notifica**

Interfaccia fornita dal client di conservazione che supporta il protocollo di notifica.

**Protocollo di notifica**

Protocollo utilizzato da un servizio di conservazione per notificare il client di conservazione.

**Client di conservazione**

Componente o software che interagisce con un servizio di conservazione tramite il protocollo di conservazione.

**Evidenza di conservazione**

Evidenza prodotta dal servizio di conservazione che può essere utilizzata per dimostrare che uno o più obiettivi di conservazione sono soddisfatti per un determinato oggetto di conservazione.

**Preservation Evidence Policy**

Insieme di regole che specificano i requisiti e il processo interno per generare o per validare un'evidenza di conservazione.

**Periodo di conservazione delle evidenze di conservazione**

Il un servizio di conservazione With Temporary Storage (WTS) è il periodo di tempo durante il quale le evidenze prodotte in modo asincrono possono essere recuperate dal servizio di conservazione.

**Obiettivo di conservazione**

Uno dei seguenti obiettivi raggiunti durante il periodo di conservazione: estendere per lunghi periodi di tempo lo stato di validità delle firme digitali, fornire prove dell'esistenza di dati per lunghi periodi di tempo o migliorare le evidenze di conservazione fornite esternamente.

**Interfaccia di conservazione**

Componente che implementa il protocollo di conservazione sul lato del servizio di conservazione.

**Manifesto di conservazione**

Oggetto dati in un contenitore di oggetti di conservazione che fa riferimento agli oggetti dati di conservazione o a informazioni aggiuntive e metadati nel contenitore di oggetti di conservazione.

**Meccanismo di conservazione**

Il meccanismo utilizzato per preservare gli oggetti di conservazione e mantenere la validità delle evidenze di conservazione.

**Oggetto di conservazione**

Oggetto di dati di tipo specifico, che viene sottoposto, elaborato o recuperato da un servizio di conservazione.

**Contenitore di oggetti di conservazione**

Contenitore che contiene un insieme di oggetti dati e metadati opzionalmente correlati che forniscono informazioni sugli oggetti dati e facoltativamente manifesto / manifesti di conservazione specificando il suo contenuto e le relazioni.

**Identificatore dell'oggetto di conservazione**

Identificatore univoco di un / Insieme di oggetto / oggetti di conservazione sottoposti ad un servizio di conservazione .

**Pianificazione della conservazione**

Monitoraggio dei cambiamenti e dei rischi, ad esempio riguardo alle innovazioni nelle tecnologie di archiviazione, accesso e conservazione, nuove strategie di progettazione, ecc..

**Periodi di conservazione**

La durata durante la quale il servizio di conservazione conserva gli oggetti di conservazione inviati e le evidenze associate.

**Profilo di conservazione**

Insieme univocamente identificato di dettagli implementativi pertinenti ad un modello di conservazione e ad uno o più obiettivi di conservazione che specifica come vengono generate e validate le evidenze di conservazione.

**Protocollo di conservazione**

Protocollo per comunicare tra il servizio di conservazione e un client di conservazione.

**Schema di conservazione**

Insieme generico di procedure e regole pertinenti a un modello di conservazione e a uno o più obiettivi di conservazione che descrive come vengono create e validate le evidenze di conservazione.

**Servizio di conservazione**

Servizio in grado di estendere lo stato di validità di una firma digitale per lunghi periodi di tempo e/o di fornire prove dell'esistenza di dati per lunghi periodi di tempo.

**Modello di conservazione degli archivi**

Uno dei seguenti modi di implementare un servizio di conservazione: con archiviazione, con archiviazione temporanea, senza archiviazione.

**Utente di conservazione**

Persona giuridica o fisica che utilizza il client di conservazione per inviare l'oggetto dati di sottomissione.

**Utente della conservazione**

Persona giuridica o fisica vincolata da un accordo con un fornitore di servizi fiduciari per la conservazione a eventuali obblighi sottoscritti.

**Prova di esistenza**

Evidenza che dimostra che un oggetto è esistita in una data / ora specifica.

**Prova di integrità**

Evidenza che i dati non sono stati alterati da quando sono stati protetti.

**Firmatario**

Entità che possiede una firma digitale.

**Oggetto dati di presentazione**

Oggetto dati originale fornito dal client.

**Marca temporale**

Dati in forma elettronica collegati ad altri dati elettronici in un momento specifico, stabilendo una prova che questi dati esistevano in quel momento.

**Time Stamping Authority**

Fornitore di servizi fiduciari che emette la marca temporale utilizzando uno o più marche temporali.

**Time Stamping Service**

Servizio fiduciario per l'emissione di marche temporali.

**Time Stamping Unit**

Insieme di hardware e software gestito come un'unità e dotato di una singola chiave di firma di marche temporali attiva alla volta.

**Elenco dei servizi fiduciari**

Elenco che fornisce informazioni sullo stato e la storia dello stato dei servizi fiduciari da parte dei fornitori dei servizi fiduciari riguardo alla conformità ai requisiti applicabili e alle disposizioni pertinenti della legislazione applicabile.

**Dati di validazione**

dati utilizzati per convalidare una firma digitale.

## 2.2. Abbreviazioni

**AUG**

Augmentation Goal.

**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.

**SigS**

Digital Signature creation Service.

**SubDO**

Submission Data Object.

**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.

La presente policy 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

##### **Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio - eIDAS**

Regolamento UE 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

#### 3.1.2. Normativa italiana sulla conservazione digitale

##### **Codice dell'Amministrazione Digitale (CAD)**

Codice dell'Amministrazione Digitale (Decreto Legislativo del 7 marzo 2005, n. 82, e successive modifiche).

##### **Linee Guida sulla formazione, 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. Protezione dei dati personali

##### **Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati**

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)

##### **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).

#### 3.1.4. Certificazioni

Entaksi ha ottenuto le seguenti certificazioni:

- **ISO 9001:2015:** Sistemi di gestione per la qualità - Requisiti.
- **ISO/IEC 20000-1:2018:** Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio.
- **ISO/IEC 27001:2013:** Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti.
- **ISO/IEC 27017:2015:** Tecnologie informatiche - Tecniche per la sicurezza - Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO/IEC 27002 per i servizi cloud.
- **ISO/IEC 27018:2019:** Tecnologie informatiche - Tecniche per la 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:** Tecnologie informatiche - Tecniche per la sicurezza - Gestione degli incidenti di sicurezza delle informazioni.



- **ISO/IEC 22301:2019:** Sicurezza e resilienza - Sistemi di gestione della continuità operativa aziendale - Requisiti.
- **UNI ISO 37001:2016:** Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo..
- **Regolamento eIDAS per i Prestatori di Servizi Fiduciari Qualificati:**
  - **ETSI EN 319 401:** Electronic Signatures and Infrastructures (ESI) - Policy e requisiti generali per i fornitori di servizi fiduciari.
  - **ETSI EN 319 411-1:** Electronic Signatures and Infrastructures (ESI) - Policy e requisiti di sicurezza per i prestatori di servizi fiduciari che emettono certificati - Parte 1: Requisiti generali.
  - **ETSI EN 319 411-2:** Electronic Signatures and Infrastructures (ESI) - Policy e requisiti di sicurezza per i prestatori di servizi fiduciari che emettono certificati - Parte 2: Requisiti per i prestatori di servizi fiduciari che emettono certificati qualificati UE.
  - **ETSI EN 319 412-1,2,3,5:** Electronic Signatures and Infrastructures (ESI) - Profili dei certificati.
  - **ETSI EN 319 421:** Electronic Signatures and Infrastructures (ESI) - Policy e requisiti di sicurezza per i fornitori di servizi fiduciari che emettono marche temporali.
  - **ETSI EN 319 422:** Electronic Signatures and Infrastructures (ESI) - Protocollo di marcatura temporale e profili di token di marcatura temporale.
  - **ETSI TS 119 511:** Electronic Signatures and Infrastructures (ESI) - Policy e requisiti di sicurezza per i fornitori di servizi fiduciari di conservazione a lungo termine delle firme digitali o dei dati generali utilizzando tecniche di firma digitale.

### 3.1.5. Altre disposizioni

#### **UNI 11386:2020**

Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SInCRO).

#### **ISO/IEC 14721:2012**

"Space data and information transfer systems - Open archival information system (OAIS) - Modello di riferimento", modello di riferimento di sistema informativo aperto per la gestione e l'archiviazione a lungo termine di contenuti informativi.

#### **ISO 15489-1:2016**

Informazione e documentazione - Gestione dei documenti di archivio - Parte 1: Concetti e principi.

#### **ISO 15836-1:2017**

Informazione e documentazione - Il Dublin Core metadata element set - Parte 1: Elementi essenziali.

#### **ISO 16363:2012**

Space data and information transfer systems - Audit e certificazione di depositi digitali.

#### **ISAD(G)**

General International Standard Archival Description, standard per la descrizione di archivi destinati alla registrazione di documenti prodotti da organizzazioni, persone e famiglie.

#### **ETSI TS 119 512 V1.2.1 (2023-05)**

Electronic Signatures and Infrastructures (ESI) - Protocolli per i fornitori di servizi fiduciari di conservazione a lungo termine.

## 3.2. Riferimenti informativi

Il servizio qualificato di conservazione a lungo termine di Entaksi è supportato dalle seguenti policy, dichiarazioni di pratica e manuali::

Tabella 2. Documenti Servizio di Conservazione eCON

Nome del documento	Versione del documento	Valido da
MAN eIDAS 20210628 Preservation Service Policy	1.1.0	01/12/2021
MAN eIDAS 20210628 Signature Validation Policy	1.1.0	01/12/2021
MAN eIDAS 20210628 Preservation Service Practice Statement	1.1.0	01/12/2021

Nome del documento	Versione del documento	Valido da
MAN eIDAS 20210628 Preservation Evidence Policy	1.1.0	01/12/2021
MAN eCON 20151222 Conservazione	1.10.0	01/12/2021
MAN SIG 20200511 Politica per la sicurezza delle informazioni	1.3.0	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	1.4.0	01/12/2021
MAN eCON 20151222 Piano della sicurezza	1.5.0	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 (ReCON).**
- **Vice Responsabile del Servizio di Conservazione (VReCON).**
- **Responsabile della Funzione Archivistica di Conservazione (RARC).**
- **Responsabile del Trattamento dei Dati Personali (RPRI).**
- **Responsabile della Sicurezza dei Sistemi per la Conservazione (RSSC).**
- **Responsabile dei Sistemi Informativi per la Conservazione (RSIC).**
- **Responsabile dello Sviluppo e della Manutenzione del Sistema di Conservazione (RSMC).**

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 (ReCON) 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 in "MAN eIDAS 20210628 Preservation Service Policy" and "MAN eIDAS 20210628 Preservation Service Practice Statement".

## 4.1. Politica per la gestione delle evidenze di conservazione eCON

Questo documento rappresenta la politica per la gestione delle evidenze di conservazione nel sistema di conservazione eCON in formato descrittivo.

La politica per la gestione delle evidenze di conservazione è identificata mediante l'OID 1.3.6.1.4.1.57823.2.2.1 in base alla seguente gerarchia di numerazione:

Tabella 4. Gerarchia OID.

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

### 4.1.1. Creazione delle evidenze di conservazione

Il sistema di conservazione eCON implementa la conservazione a lungo termine delle firme elettroniche mediante la validazione delle firme secondo quanto specificato in "MAN eIDAS 20210628 Signature Validation Policy".

Questa procedura genera un rapporto di validazione che conforme a ETSI EN 319 102-1 nella forma di un documento XML definito in ETSI TS 119 102-2.

Il rapporto di validazione contiene i seguenti elementi relativi alla firma elettronica validata:

- Un elemento **Rapporto di validazione della firma**, che rappresenta il risultato complessivo della validazione della firma e le informazioni supplementari sull'esecuzione della validazione. Questo elemento è descritto in ETSI TS 119 102-2 al paragrafo 4.3.
- Un elemento **Oggetti per la validazione della firma**, che contiene tutti i materiali raccolti durante la procedura di validazione, come le CRL, i riferimenti fiduciari, le risposte OCSP, ecc e la prova di esistenza al momento in cui può essere stabilita per la prima volta. Questo elemento è descritto in ETSI TS 119 102-2 al paragrafo 4.4.
- Un elemento **Informazioni sul validatore**, che identifica l'entità che ha validato la firma. Questo elemento è descritto in ETSI TS 119 102-2 al paragrafo 4.5.
- Un elemento **Firma del rapporto di validazione**, che contiene la firma del rapporto di validazione. Questo elemento è descritto in ETSI TS 119 102-2 al paragrafo 4.6.

Il processo di validazione della firma crea un rapporto di validazione per ogni firma elettronica durante la validazione del Pacchetto di Versamento (PDV).

Tale rapporto viene memorizzato in un registro di archiviazione dedicato ed è correlato con la firma originale mediante il valore dell'impronta SHA-256 del file che contiene la firma.

Ad esempio, se la firma elettronica da validare è un file PDF firmato, il codice di correlazione del rapporto di validazione sarà l'impronta SHA-256 del contenuto del file PDF.

Questa strategia di correlazione consente al sistema di associare il rapporto di validazione alla corrispondente firma elettronica senza aggiungere un codice di correlazione all'insieme dei metadati del documento firmato. Allo stesso tempo, il rapporto di validazione archiviato è libero da ogni legame con il documento originale così che risulta possibile una futura implementazione della conservazione a lungo termine senza archiviazione.

### 4.1.2. Archiviazione delle evidenze di conservazione

Ciascun file nel sistema di conservazione eCON è archiviato in un Pacchetto di Archiviazione (PDA) con un indice nella forma di un file XML conforme allo standard UNI 11386:2020 (SinCRO).

L'indice del PDA contiene le impronte calcolate su ciascun oggetto conservato.

L'indice del PDA è firmato digitalmente con il profilo XaDES\_LTA in modo che l'integrità e la prova di esistenza si estenda a

ciascun oggetto conservato contenuto nel PDA.

Mentre i documenti firmati sono archiviati in un PDA che dipende dai documenti e dai loro metadati, i rapporti di validazione sono archiviati in un PDA su uno speciale registro di archiviazione dedicato per questo scopo.

L'indice del PDA è firmato digitalmente con il profilo XaDES\_LTA in modo tale che l'integrità e la prova di esistenza risulta estesa ad ciascuno degli oggetti conservati nel PDA.

La struttura dati risultante è un albero d'impronte che ha come nodo radice l'impronta firmata digitalmente dell'indice del PDA e come nodi foglia i valori delle impronte degli oggetti conservati. Questi ultimi sono i documenti firmati, per i PDA contenenti documenti, e i rapporti di validazione delle firme per i PDA contenenti rapporti di validazione.

Quindi, per i PDA contenenti oggetti conservati, l'indice del PDA firmato elettronicamente è effettivamente una evidenza di conservazione per gli oggetti conservati inclusi nel PDA, firmati elettronicamente o meno, attraverso i valori delle impronte dei file corrispondenti che fanno parte di un albero di impronte che ha l'impronta dell'indice come radice.

Inoltre, per lo stesso motivo, l'indice firmato elettronicamente di un PDA contenente rapporti di validazione è effettivamente una evidenza di conservazione delle firme elettroniche mediante la prova di esistenza del relativo rapporto di validazione al momento del versamento della firma elettronica.

Con le informazioni contenute nel rapporto di validazione è possibile verificare la validità della firma elettronica nel tempo, finché il sistema di conservazione garantisce l'autenticità del rapporto di validazione e la prova di esistenza alla data del versamento.

## 4.2. Estensione della validità dell'evidenza di conservazione

L'estensione della validità dell'evidenza di conservazione è realizzata sulla firma elettronica dell'indice del PDA nei seguenti due casi:

- quando la marca temporale sta per scadere oppure è a rischio di perdere la sua validità perché il certificato dell'autorità emittente sta per scadere oppure è compromesso o rischia di essere compromesso;
- quando risulta fattibile un attacco crittografico sull'algoritmo di firma o sull'algoritmo per calcolare l'impronta usati nella firma dell'indice del PDA.

Nel primo caso viene eseguito un rinnovo periodico della marca temporale quando l'autorità emittente rinnova il proprio certificato di firma.

Nel secondo caso viene eseguito un ricalcolo dell'albero di impronte dell'intera struttura di dati costruendo un nuovo indice del PDA con un algoritmo aggiornato per il calcolo delle impronte.

## 4.3. Informazioni esplicite sulla politica di gestione delle evidenze di conservazione

L'indice del PDA firmato elettronicamente, ovvero l'evidenza di conservazione, contiene delle informazioni esplicite sul servizio di conservazione, sulla politica di gestione delle evidenze di conservazione e sul profilo di conservazione.

Queste informazioni sono specificate includendo una politica di firma all'interno della firma elettronica dell'indice del PDA.

La politica di firma che viene inclusa è la presente "Politica di gestione delle evidenze di conservazione", che è identificata dall'OID definito in [Identificazione del documento](#) e contiene anche quattro riferimenti di documentazione come attributi XaDES, anch'essi parte dell'insieme degli attributi firmati:

- Un riferimento alla politica di gestione delle evidenze di conservazione.
- Un riferimento al profilo di conservazione utilizzato quando è stato costruito il PDA.
- Un riferimento al servizio di conservazione.
- Un riferimento alla politica di validazione delle firme.

## 4.4. Uso di altri servizi fiduciari

Il servizio di conservazione eCON utilizza servizi di altri fornitori di servizi fiduciari nelle seguenti fasi del processo di conservazione:

- quando viene applicata una marca temporale il servizio invoca il servizio RFC 3161 fornito da un servizio fiduciario qualificato per l'emissione di marche temporali;

- durante la costruzione della catena di validazione dei certificati il servizio raccoglie i certificati dell'autorità di certificazione emittente utilizzando il valore URI contenuto nell'estensione che descrive l'accesso alle informazioni dell'autorità (AIA) che si trova nei certificati;
- durante la validazione delle firme elettroniche il servizio ottiene delle risposte OCSP dal servizio OCSP indicato con un valore URI nell'estensione che descrive l'accesso alle informazioni dell'autorità (AIA) del certificato allo scopo di verificare lo stato di revoca del certificato.

## 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.

Il servizio qualificato di Entaksi per la conservazione a lungo termine di firme, sigilli e dati è delineato nei seguenti documenti:

Tabella 5. Nome e identificativo dei documenti LTP.

OID	Descrizione	Permanent Link
1.3.6.1.4.1.57823.1.1	MAN eIDAS 20210628 Preservation Service Policy	<a href="https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1">https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.1</a>
1.3.6.1.4.1.57823.1.2	MAN eIDAS 20210628 Preservation Service Practice Statement	<a href="https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2">https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.2</a>
1.3.6.1.4.1.57823.1.3	MAN eIDAS 20210628 Preservation Evidence Policy	<a href="https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3">https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.3</a>
1.3.6.1.4.1.57823.1.4	MAN eIDAS 20210628 Signature Validation Policy	<a href="https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4">https://r.entaksi.eu/oids/1.3.6.1.4.1.57823.1.4</a>

Tutti i documenti relativi ai servizi fiduciari qualificati di Entaksi sono disponibili al seguente link:

<https://www.entaksi.eu/documentation.html>.