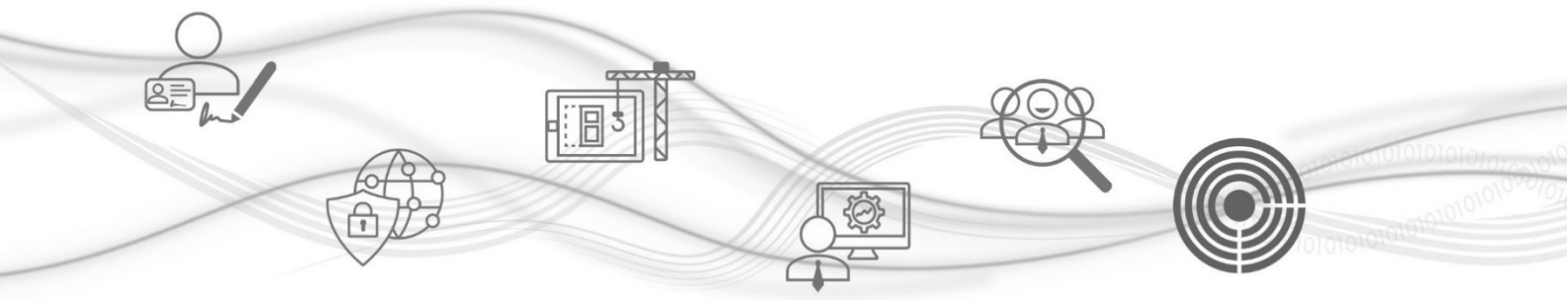
Allegato 1

Policy e Practice Statement del Servizio qualificato di conservazione di firme elettroniche qualificate e sigilli elettronici qualificati



Categoria	**LTA**	Codice Documento	**NAM_LTA_PO**	**Namirial S.p.A.**
Redatto da	**E. Giunta – E. Luzi**	Nota di riservatezza	**Documento pubblico**	Il Legale Rappresentante
Verificato da	**Davide Coletto**	Versione	**1.4**	**Massimiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**02/12/2025**	_____

MASSIMILIANO PELLEGRINI
18/12/2025 12:13:52 UTC+0100

Namirial
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia
Tel. +39 071 63494 | www.namirial.com

Contents

Storia delle modifiche

V.1.4	
Data	02/12/2025
Motivo	Aggiornamento
Cambiamenti	Modifiche in tutti i paragrafi Par. 5.2 Aggiunta di un nuovo modello di Conservazione di firma e sigilli qualifiati (modello WTS)

V.1.3	
Data	05/11/2024
Motivo	Aggiornamento
Cambiamenti	Modifiche in tutti i paragrafi

V.1.2	
Data	10/09/2024
Motivo	Aggiornamento
Cambiamenti	Modifiche sostanziali in tutti i paragrafi

V.1.1	
Data	15/05/2024
Motivo	Aggiornamento
Cambiamenti	Modifiche minori in tutti i paragrafi

V.1	
Data	08/09/2023
Motivo	Prima versione
Cambiamenti	-

1. Scopo e ambito del documento

Il presente documento costituisce la policy e practice statement del servizio fiduciario qualificato di Namirial per la **conservazione di firme elettroniche qualificate e sigilli elettronici qualificati** ed è incluso come Allegato 1 del Manuale del Conservatore del Servizio di Conservazione Long Term Archiving - LTA.

Questa policy e practice statement è stata sviluppata in conformità ai requisiti dello standard ETSI TS 119 511, che delinea i requisiti di policy e sicurezza per i fornitori di servizi fiduciari che offrono la conservazione a lungo termine di firme digitali o di dati utilizzando tecniche di firma digitale.

La presente policy e practice statement descrive il servizio fiduciario qualificato di conservazione delle firme e dei sigilli elettronici qualificati offerto da Namirial, il quale è implementato sui modelli ***Preservation service with storage*** **[WST]** e ***Preservation service with temporary storage*** **[WTS]** individuati nello standard ETSI 119 511 e descritti nel paragrafo *5. Modello di conservazione*. La policy include gli obiettivi di conservazione, le politiche e le prassi attuate, in particolare le misure adottate e le modalità di estensione dell'affidabilità delle firme e dei sigilli oltre il loro periodo di validità tecnologica, e indica l'applicabilità del servizio.

La presente policy è rivolta a tutti i clienti che hanno sottoscritto il servizio di conservazione Namirial e, più in generale, a tutte le parti interessate.

1.1 Identificazione e aggiornamento delle politiche

Il *Reference Identifier* della presente policy è il seguente:

Reference Identifier	OID: 1.3.6.1.4.1.36203.0.0.19511.1.1

Il documento viene aggiornato insieme al Manuale del Conservatore del Servizio di Conservazione Long Term Archiving - LTA, al fine di riflettere le modifiche normative e gli aggiornamenti al servizio.

1.2 Identificativi univoci del servizio

Il servizio di conservazione è identificato tramite appositi identificativi indicati di seguito:

- **System OID** (identificativo univoco del sistema): **1.3.6.1.4.1.36203.7.1.0**

- **Process OID WST** (identificativo del profilo di conservazione basato sullo standard OAIS e sul modello WST): **1.3.6.1.4.1.36203.7.1.1**
- **Process OID WTS** (identificativo del profilo di conservazione basato sullo standard OAIS e sul modello WTS): **1.3.6.1.4.1.36203.7.1.2**

1.3 Rapporto con il Manuale del Conservatore

Il presente documento *Policy e Practice Statement per il Servizio qualificato di conservazione di firme elettroniche qualificate e sigilli elettronici qualificati* è un allegato del Manuale del Conservatore ed è specifico per il servizio fiduciario qualificato di conservazione di firme elettroniche qualificate e di sigilli elettronici qualificati ai sensi dell'art. 34 e art. 40 del Regolamento (UE) n. 910/2014 (Regolamento eIDAS).

Questo documento è sottoposto ad audit da parte di un Organismo di Valutazione della Conformità (CAB) accreditato e alla vigilanza dell'AgID.

Per la conservazione dei dati, come previsto dallo standard ETSI TS 119 511, tale servizio qualificato utilizza il servizio di conservazione di dati e documenti informatici le cui policy sono descritte nel Manuale del Conservatore disponibile e pubblicato al link https://www.namirial.com/it/documentazione/#archive.

1.4 Storia delle versioni e gestione delle modifiche

Il presente documento è gestito e aggiornato in conformità con la normativa vigente ed è soggetto all'approvazione di AgID come organismo di vigilanza.

2. Riferimenti

Sono riportati nel presente paragrafo i riferimenti normativi e gli standard cui il servizio è conforme.

Normativa:

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - **GDPR**);

- **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014** on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS**)

Standard:

- **ISO 9001** Quality management systems – Requirements;
- **ISO/IEC 27001** Information technology - Security techniques - Information security management systems – Requirements;
- **ISO/IEC 27017** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- **ISO/IEC 27018** Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- **ISO/IEC 22313** Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301;
- **ISO 14721 Space data and information transfer systems** - **Open archival information system** (**OAIS**) Reference model;
- **ISO 14641** Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications;
- **NF 461** Système d'archivage électronique;
- **NF Z42-013** Archivage électronique - Recommandations et exigences;
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 511** 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;
- **ETSI TS 119 172-4** Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists;
- **UNI 11386:2020 Standard SInCRO** Support for Interoperability in Preservation and Recovery of Digital Objects - Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali;

- **ISO 16363** Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

3. Definizioni e acronimi

Le definizioni fondamentali per comprendere il funzionamento del servizio sono le seguenti:

Termini	Definizioni
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
AgID	Agenzia per l'Italia Digitale.
Affidabilità (trustworthiness)	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento.
Archival Information Package (AIP)	Pacchetto informativo composto dalla trasformazione di uno o più Submission Information Package (SIP) in conformità allo standard OAIS. Corrisponde, nella terminologia ETSI, ad un POC (Preservation object container), generato dal sistema di conservazione e contenente le evidenze del processo.
Autenticità (authenticity)	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
Certificato qualificato (Qualified certificate)	È un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica).
Certification authority (CA)	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata (private key)	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave pubblica (public key)	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale

	apposta sul documento informatico dal titolare delle chiavi asimmetriche.
Comunità di riferimento (designated community)	Gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere l'informazione conservata, secondo lo standard OAIS. Una comunità di riferimento può essere composta anche da più comunità di utenti
Contenitore dell'oggetto di conservazione (Preservation object container)	Contenitore che include un set di oggetti, dati e metadati facoltativamente correlati che forniscono informazioni sugli oggetti dati e, facoltativamente, istruzioni per la conservazione che ne specificano il contenuto e le relazioni.
Data object	Dati binari/ottetti gestiti da un'applicazione (ad esempio, trasformati, sottoposti a digest o firmati) e a cui possono essere associate informazioni aggiuntive come un identificatore, la codifica, la dimensione o il tipo.
Deletion Package	Pacchetto generato dal servizio a seguito dell'esecuzione di un processo di eliminazione di oggetti.
Dispositivo sicuro per la creazione della firma (QSSDC)	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza.
Dissemination Information Package (DIP)	Pacchetto informativo inviato dal servizio di conservazione all'utente in risposta ad una sua richiesta in conformità allo standard OAIS. Corrisponde, nella terminologia ETSI, ad un POC (Preservation object container), generato dal sistema di conservazione su richiesta dell'utente e contenente l'oggetto conservato e le evidenze di conservazione.
Eliminazione degli oggetti (Deletion)	Operazione con cui si eliminano gli oggetti conservati.
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenze di conservazione (preservation evidence)	Evidenze prodotte dal servizio di conservazione che possono essere utilizzate per dimostrare che uno o più obiettivi di conservazione sono stati raggiunti per un determinato oggetto di conservazione.
Firma elettronica qualificata (Qualified electronic signature)	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Formato (format)	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Funzione di hash (hash function)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Identificativo univoco (Object identifier)	Riferimento univoco (OID – object identifier) e permanente dato a tutti gli oggetti che operano nel perimetro del servizio (cioè oggetti di conservazione, evidenze di conservazione, pacchetti informativi, tipologie documentali, accounts, ecc.).
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Index of the Archival Information Package	Indice dell'Archival Information Package, struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO (UNI 11386). Corrisponde, nella terminologia ETSI, all'evidenza di conservazione (preservation evidence).
Index of the Submission Information Package	Indice del Submission Information Package, struttura dell'insieme dei dati a supporto del processo di versamento del Submission Information Package e definita nello specifico dal Provider.
Index of the Dissemination Information Package	Indice del Dissemination Information Package, struttura dell'insieme dei dati a supporto del processo di distribuzione del Dissemination Information Package e definita nello specifico dal Provider.
Incremento delle evidenze della conservazione (preservation evidence augmentation)	Incremento di dati rispetto a un'evidenza di conservazione esistente per estendere il periodo di validità di tale evidenza.

Information Package	Pacchetto Informativo, contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare in conformità allo standard OAIS che prevede pacchetti informativi di diversa natura che interagiscono con il Sistema di conservazione (SIP, AIP, DIP, etc). Corrisponde, nella terminologia ETSI, al Preservation Object Container (POC).
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati.
Long-term preservation	Estensione dello stato di validità di una firma elettronica o di un sigillo per lunghi periodi di tempo e/o l'estensione della fornitura di prove dell'esistenza di dati per lunghi periodi di tempo, nonostante l'obsolescenza della tecnologia crittografica come algoritmi crittografici, dimensioni delle chiavi o funzioni di hash, compromissioni delle chiavi o perdita della capacità di verificare lo stato di validità dei certificati a chiave pubblica.
Marca temporale (time-stamp)	dati in formato elettronico che collegano altri dati elettronici a un istante specifico, fornendo la prova che tali dati esistevano in quel momento.
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel Sistema di conservazione.
Modello di conservazione (Preservation model)	Si distinguono tre modelli di archiviazione per il servizio di conservazione: 1) Servizi di conservazione con archiviazione [WST – with storage]. In questo caso, i dati da conservare sono memorizzati dal servizio di conservazione, mentre le evidenze e i dati conservati sono consegnati su richiesta del servizio di conservazione al cliente della conservazione. Il servizio di conservazione memorizza gli oggetti dati inviati (SubDO – Submitted Data Object) e gli oggetti di conservazione (PO – Preservation Object) e le evidenze di

	conservazione associate. L'oggetto (o gli oggetti) di conservazione è derivato dal SubDo (o dagli oggetti) mediante incremento o mediante la costruzione di un contenitore di oggetti di conservazione (POC - Preservation Object Container). 2) Servizi di conservazione con archiviazione temporanea [WTS – with temporary storage]. In questo caso, i dati da conservare sono memorizzati lato cliente. Il servizio di conservazione conserva i dati o un hash dei dati da conservare solo temporaneamente. Le evidenze vengono prodotte in modo asincrono. Una volta prodotte, le evidenze vengono conservate per un certo periodo di tempo per consentire al cliente di recuperarle. 3) Servizi di conservazione senza archiviazione [WOS – without storage]. In questo caso, i dati da conservare sono memorizzati lato cliente. Il servizio di conservazione non memorizza né il SubDO né le evidenze di conservazione. Le evidenze vengono prodotte in modo sincrono e sono incluse nella risposta. Il servizio di conservazione conserva solo le tracce delle sue azioni per poter fornire una documentazione delle sue attività.
Obiettivo di conservazione (Preservation goal)	Uno dei seguenti obiettivi raggiunti durante l'arco di tempo della conservazione: estendere per lunghi periodi di tempo lo stato di validità delle firme digitali, fornire prove dell'esistenza dei dati per lunghi periodi di tempo o aumentare le evidenze di conservazione fornite dall'esterno.
Periodo di conservazione (Preservation period)	Nel caso di un servizio di conservazione con archiviazione [WST], il periodo di conservazione è la durata durante la quale il servizio di conservazione conserva i Preservation objects (PO). I PO possono essere costituiti dagli oggetti inviati (SubDO) e dai PO derivati dagli oggetti inviati tramite la creazione di un POC che include le evidenze associate o tramite incremento.
Policy di conservazione delle evidenze (Preservation evidence policy)	Insieme di regole che specificano i requisiti e il processo interno per generare o come validare un'evidenza di conservazione.

Policy di convalida della firma (Signature validation policy)	Nel caso di conservazione di firme digitali in cui il servizio di conservazione raccoglie i dati di convalida necessari per determinare lo stato della firma digitale, la policy di convalida delle firme è indicata nel profilo di conservazione. In questo caso, la policy di validazione descrive le regole seguite per ottenere i dati di validazione.
Oggetto da conservare (submission data object)	Oggetto originario da conservare fornito dall'utente.
Oggetto di conservazione (Preservation object - POC)	Oggetto dati inviato, elaborato da o recuperato da un servizio di conservazione.
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Profilo di conservazione (Preservation profile)	Un profilo di conservazione identifica un insieme di dettagli di implementazione che specificano come vengono generate e convalidate le evidenze di conservazione e che sono pertinenti a un modello di conservazione e a uno o più obiettivi di conservazione.
Revision Package	Pacchetto di Revisione, pacchetto informativo inviato dall'utente al servizio secondo un formato predefinito al fine di apportare una revisione ai dati precedentemente conservati dal servizio. È associato, nella terminologia ETSI, al concetto di Preservation evidence augmentation, in quanto consente di incrementare i dati di un'evidenza di conservazione esistente per estenderne il periodo di validità.
Schema di conservazione (Preservation schema)	Uno schema di conservazione è un insieme generico di procedure e regole pertinenti a un modello di conservazione e a uno o più obiettivi di conservazione che delinea le modalità di creazione e convalida delle evidenze di conservazione. Può essere supportato da uno o più profili di conservazione.
Servizio di conservazione	Servizio che garantisce la ricezione, l'archiviazione, il recupero e la cancellazione di dati e documenti elettronici al fine di assicurarne la durata e la leggibilità, nonché di

	preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione.
Servizio di conservazione qualificato per firme e sigilli qualificati (Qualified preservation service for qualified electronic signatures and seals)	Un servizio di conservazione qualificato per le firme elettroniche qualificate fornito da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'attendibilità della firma elettronica qualificata oltre il periodo di validità tecnologica.
Sigillo elettronico qualificato (Qualified electronic seal)	Un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici.
Signature Report (or Validation Report)	Documento informatico esito della verifica della firma qualificata o del sigillo qualificato, contenente dati riferiti al certificato qualificato utilizzato per l'apposizione della firma/sigillo e conservato insieme alle evidenze di conservazione come elemento di prova.
Submission Information Package (SIP)	Pacchetto informativo inviato dall'utente al servizio secondo un formato predefinito e in conformità allo standard OAIS. Corrisponde, nella terminologia ETSI, ad un POC (Preservation object container), inviato al sistema dall'utente e contenente l'oggetto da conservare e i suoi metadati descrittivi.
Submission Report	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei SIP inviati dal Produttore e validati dal sistema stesso.
Titolare di firma (Certificate holder)	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica.
Utente (user)	Persona, ente o sistema che interagisce con il servizio.

4. Trusted roles

Il personale individuato e preposto all'erogazione e controllo del servizio di conservazione di firme e sigilli qualificati è organizzato secondo quanto indicato all'interno dello standard ETSI 319 401 e a quanto definito da AgID in materia di

qualificazione dei fornitori di servizi fiduciari ai sensi eIDAS. In particolare, sono definite le seguenti figure organizzative:

RUOLO	NOMINATIVO	CONTATTI
Responsabile del Servizio di Conservazione	Davide Coletto	d.coletto@namirial.com
Responsabile della Funzione archivistica di conservazione	Eleonora Luzi	e.luzi@namirial.com
Responsabile per l'aggiornamento della documentazione depositata presso l'Agenzia	Davide Coletto	d.coletto@namirial.com
Responsabile della sicurezza dei sistemi per la conservazione	Mario Veltini	m.veltini@namirial.com
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Nicola Bruni	n.bruni@namirial.com
Responsabile dei sistemi informativi per la conservazione	Mario Veltini	m.veltini@namirial.com
Responsabile dei servizi tecnici e logistici	Alessandro Mandolini	a.mandolini@namirial.com
Responsabile delle verifiche e delle ispezioni	Luigi Enrico Tomasini	l.tomasini@namirial.com

Responsabile del trattamento dei dati personali	Luca Santalucia	l.santalucia@namirial.com

Le competenze dei ruoli sopra indicati sono descritte nel documento *Namirial S.p.A. - Trusted roles e struttura organizzativa dei servizi qualificati e fiduciari Namirial S.p.A.* , anch'esso aggiornato e trasmesso all'Agenzia per l'Italia Digitale.

5. Modello di conservazione

Il servizio fiduciario qualificato per la conservazione di firme e sigilli qualificati di cui al presente documento è basato sul servizio di conservazione di dati e documenti informatici il cui profilo generale di conservazione applicato è accuratamente descritto nel Manuale del Conservatore, pubblicamente disponibile online - insieme al presente documento - sul sito web di Namirial S.p.A. Il profilo generale di conservazione adottato da Namirial si applica per tutto il periodo di conservazione degli oggetti conservati e per tutto il periodo di conservazione delle evidenze.

Il profilo di conservazione è basato sullo schema OAIS, utilizzato nel contesto del servizio fiduciario di conservazione di firme e sigilli qualificati per implementare, a seconda delle esigenze di processo, un modello di conservazione con *storage* o con *storage* temporaneo (WST - *preservation service with storage e WTS – preservation service with temporary storage*, come descritto nella specifica ETSI TS 119 511).
Tale profilo è stato sviluppato utilizzando nel processo le tecniche di firma digitale (firme o sigilli elettronici qualificati automatici e time-stamp qualificati) fornite da Namirial stessa, dato il suo status di eIDAS Qualified Trust Service Provider di firme e marche temporali qualificate.

5.1 Modello WST

Nel dettaglio, il profilo WST applicato nell'ambito del Qpres fornito da Namirial prevede l'acquisizione di oggetti digitali (SubDO – *Submission data object*) contenuti, come Oggetti di Conservazione (PO – *Preservation objects*), in pacchetti

informativi (POC – *Preservation object container*), producendo evidenze di conservazione in accordo con la policy sulle evidenze di conservazione. Il cliente del servizio invia uno o più SubDO e riceve un identificativo univoco di oggetto.

5.2 Modello WTS

Nel dettaglio, il profilo WTS applicato nell'ambito del Qpres fornito da Namirial prevede l'acquisizione di oggetti digitali (Data object) nella forma di documenti in formato elettronico a cui può essere associata una firma qualificata o un sigillo qualificato, accompagnati da informazioni aggiuntive, qualora sia necessario, producendo evidenze di conservazione in accordo con la policy sulle evidenze di conservazione. Il cliente del servizio invia i dati e riceve un identificativo univoco di una operazione asincrona da monitorare. Una volta completata l'elaborazione, il servizio genera un *Preservation object* soggetto al processo di conservazione e il cliente riceve il relativo identificativo univoco di oggetto.

5.3 Fasi del processo

Durante il periodo di conservazione, il cliente può richiedere una o più prove di conservazione e pacchetti informativi (POC) contenenti gli oggetti conservati.

Il servizio fornisce la possibilità di eliminare i POC conservati: in caso di cancellazione delle prove di conservazione, i SubDO corrispondenti e i POC derivati vengono eliminati.

Il servizio consente di generare una nuova versione di un POC già elaborato: il collegamento tra le diverse versioni è tracciato nel POC; dunque, tale funzionalità permette di specificare la differenza rispetto alla versione precedente.

Il servizio contatta il QTSP interno Namirial (Certification e Time-stamping Authority) per apporre le informazioni necessarie a creare le evidenze di conservazione.

Il servizio di conservazione monitora gli algoritmi crittografici utilizzati per la generazione delle evidenze di conservazione e incrementa le stesse evidenze, se necessario, tramite l'acquisizione di un nuovo POC.

Tutte le variazioni al profilo sopra descritto sono specificate e tracciate nella descrizione del profilo, debitamente versionata nel presente documento. In

questo modo, è possibile identificare quale versione del profilo è stata applicata in quale momento.

6. Obiettivi funzionali

Gli obiettivi di conservazione perseguiti realizzano la conservazione a lungo termine di firme, sigilli e della prova di esistenza di dati e sono i seguenti:

1. la fornitura di prova di esistenza di oggetti digitali sul lungo periodo, indipendentemente dal fatto che tali dati siano firmati o meno, mediante tecniche di firma digitale;

2. la conservazione sul lungo periodo della capacità di convalidare firme elettroniche qualificate e sigilli elettronici qualificati, di mantenerne il relativo stato di validità e di ottenere un'evidenza dell'esistenza (proof of existence) dei dati sottoposti a firma o sigillo elettronico. Questo obiettivo garantisce il mantenimento dello status delle firme e dei sigilli corrispondente al momento dell'invio al servizio di conservazione, anche a lungo termine e anche qualora la chiave di firma venga compromessa, il certificato scada o si verifichino attacchi crittografici all'algoritmo di firma o all'algoritmo di hash utilizzato.

   In particolare, questo obiettivo è garantito dal fatto che tutti i dati di convalida necessari sono raccolti, verificati e protetti utilizzando tecniche di firma digitale.

3. l'incremento delle evidenze di conservazione generate dal servizio di conservazione (*augmentation*).

Per poter estendere lo stato di validità di una firma digitale sul lungo periodo, il servizio di conservazione fornisce una prova di esistenza di:

1. firma o sigillo;

2. dati soggetti a tale firma o sigillo; e

3. dati di convalida (percorsi dei certificati, informazioni sulla revoca).

Il sistema di conservazione di Namirial conserva questi oggetti nel loro insieme attraverso il meccanismo dei pacchetti delineato nel successivo paragrafo e a seconda del modello di servizio utilizzato, mantiene:

- i documenti firmati digitalmente con le loro firme, con i metadati e i dati di convalida associati (modello WST)
- o i dati ricevuti con i metadati e i dati di convalida associati (modello WTS).

Tutti gli oggetti del sistema sono identificabili attraverso un identificativo univoco.

7. Descrizione del profilo di conservazione

7.1 Oggetti sottoposti a conservazione

Alla base del profilo impiegato vi è il modello concettuale OAIS, che si basa sull'utilizzo di pacchetti informativi (Information Packages), differenziati in base alla fase del processo di conservazione. Questa unità corrisponde al Preservation object container, elemento generale che si declina – in questo specifico contesto – nelle forme:

- Submission Information Package (SIP);
- Archival Information Package (AIP);
- Dissemination Information Package (DIP); e (ove necessario)
- Revision Package;
- Deletion Package.

7.2 Formati

I formati di input, di firma digitale, di output e delle evidenze supportati sono i seguenti:

- Formati di input: PDF, PDF/A, XML, TXT, TIFF, JPG, EML, OOXML e ODF (elenco non esaustivo);
- Formati di firma: estensioni CAdES (.p7m), PAdES (.pdf) e XAdES (.xml) e/o una marca temporale;
- Formati di output: ZIP, XML, CAdES, TSD.

7.3 Pacchetti informativi (POCs)

7.3.1 Submission Information Package (SIP)

Il Submission Information Package (SIP) è costituito da un archivio zip non compresso, composto dagli oggetti di conservazione e un file SIP Index finalizzato alla descrizione delle informazioni relative all'oggetto stesso.

Il file Indice, in formato XML, assicura l'identificazione del soggetto che ha prodotto il SIP e l'identificazione dell'applicativo che lo ha prodotto.

7.3.2 Archival Information Package (AIP)

L'Archival Information Package (AIP) generato nel processo di conservazione del sistema è una specializzazione del pacchetto informativo ed è composto dalla trasformazione di uno o più Submission Information Package.

Un AIP contiene:

- gli oggetti informativi individuati per la conservazione;
- un Indice dell'Archival Information Package (AIPIndex) che rappresenta le Informazioni sulla Conservazione.

La struttura dati dell'Indice del AIP è conforme allo standard italiano SInCRO (UNI 11386) riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

7.3.3 Revision Package

L'incremento dei dati rispetto a un'evidenza di conservazione esistente per estendere il periodo di validità di tale evidenza avviene tramite l'utilizzo del Pacchetto di revisione.

Un pacchetto di revisione consente all'utente o al sistema di aggiornare e aggiungere informazioni a un oggetto precedentemente inviato in conservazione, tramite il versamento al servizio di un nuovo SIP contenente il riferimento univoco (Id) del SIP originario.

Una volta acquisito il nuovo SIP, il servizio crea una nuova evidenza di conservazione – generando un nuovo AIP – che riporta al suo interno un riferimento univoco all'evidenza di conservazione del precedente AIP.

Per poter essere accettato dal sistema, un pacchetto di revisione deve contenere il tipo di modifica richiesta, che può essere:

- Rettifica: intervento volto alla correzione di elementi presenti nel SIP originario;
- Integrazione: intervento volto ad aggiungere informazioni al SIP originario;
- Annotazione: intervento volto ad apporre una registrazione sintetica al contenuto del SIP originario.

7.3.4 Dissemination Information Package (DIP)

Il Dissemination Information Package (DIP) è generato dal servizio al fine di recuperare gli oggetti conservati e le evidenze di conservazione associate. Può essere richiesto dall'utente nelle seguenti modalità:

- DIP distribuito a seguito di ricerca di un singolo oggetto, in risposta alla richiesta dell'utente;
- DIP distribuito a seguito di ricerca di più documenti, anche appartenenti a più AIP, in risposta alla richiesta dell'utente. Il pacchetto contiene tutti i file richiesti e i relativi file indici degli AIP di tutti i pacchetti;
- DIP distribuito in risposta alla richiesta di cessazione del servizio (in tal caso il DIP contiene uno o più AIP, divisi per anno di riferimento).

Il DIP è costituito da un archivio zip che contiene una serie di elementi a seconda del modello impiegato.

Nel modello WST, il DIP contiene:

- Gli oggetti digitali conservati nel sistema richiesti dall'utente.
- L'Indice del relativo SIP.
- Il Submission Report (SR)
- Il Signature Report associato al documento analizzato dal Sistema
- Uno o più files Indice del AIP firmati dal Responsabile del Servizio di Conservazione e marcati temporalmente, associati ai suddetti oggetti richiesti dall'utente.
- File Indice del DIP: file XML firmato digitalmente dal Responsabile del Servizio di Conservazione, che contiene l'hash dell'Indice del AIP e l'hash di ogni singolo file.

Nel modello WTS, il DIP contiene:

- Gli oggetti digitali – formati dal Signature Report generato dal sistema, con i relativi metadata associati - conservati nel sistema richiesti dall'utente;
- L'Indice del relativo SIP.
- Il Submission Report (SR)
- Uno o più files Indice del AIP firmati dal Responsabile del Servizio di Conservazione e marcati temporalmente, associati ai suddetti oggetti richiesti dall'utente.
- File Indice del DIP: file XML firmato digitalmente dal Responsabile del Servizio di Conservazione, che contiene l'hash dell'Indice del AIP e l'hash di ogni singolo file.

7.3.5 Deletion Package

Il Deletion package viene generato dal servizio a seguito dell'esecuzione di un processo di eliminazione di oggetti conservati.

Il Deletion Package contiene:

- la proposta di eliminazione;

- un report con l'elenco degli oggetti, con indicazioni di codifiche minimali quali traccia degli stessi (Id oggetto, hash), in conformità al trattamento dati;
- L'Indice del Deletion package, contenente – tra le varie informazioni - l'esito dell'accettazione della proposta (*approved* o *rejected*) e l'elenco delle fasi. Tale indice viene sottoscritto digitalmente sia dal Responsabile del Servizio di Conservazione sia dall'utente per approvazione.
- eventuali allegati del processo autorizzativo.

7.4 Periodo di conservazione

Il periodo di conservazione è la durata in cui il servizio di conservazione conserva gli oggetti (PO). Il periodo di conservazione, nell'ambito del servizio, è definito associando al SIP una data (*deletion date*) che indica il termine di conservazione dopo il quale viene avviato il processo di eliminazione dell'oggetto e delle evidenze associate. Tale data può:

- essere fornita dall'utente nella fase di generazione e invio del SIP;
- essere associata agli oggetti conservati in maniera automatica dal sistema.

Durante questo periodo, il servizio di conservazione crea e incrementa – qualora necessario - le evidenze di conservazione per raggiungere l'obiettivo di conservazione.

8. Processo di conservazione

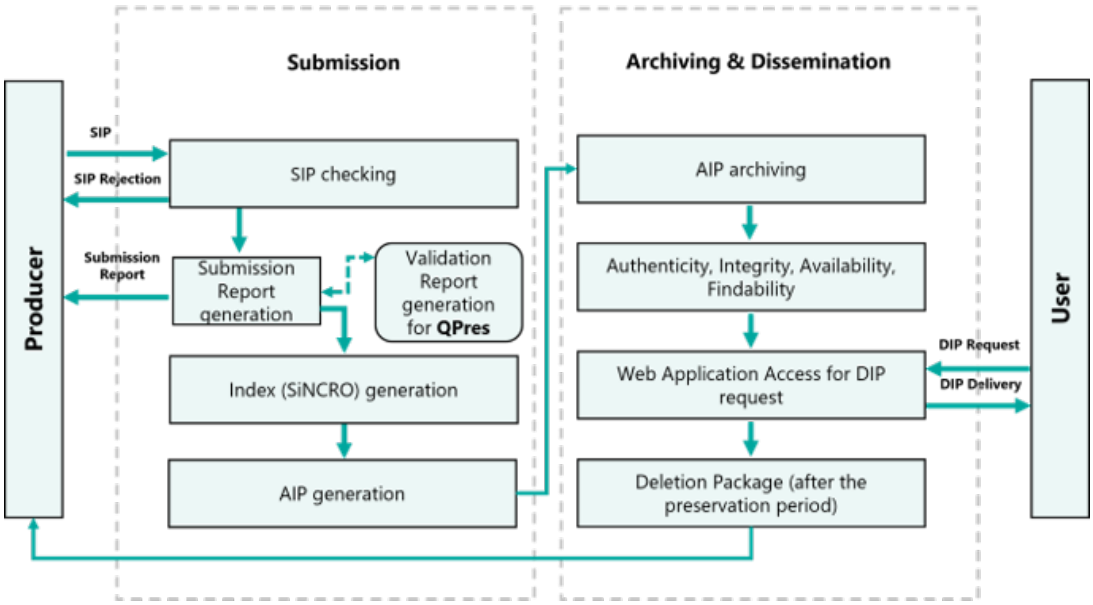
Il versamento dei pacchetti (contenenti gli oggetti da conservare) al servizio da parte di un utente, nonché ogni distribuzione di documenti dal servizio ad un utente autorizzato, avvengono nella forma di una o più trasmissioni distinte (sessioni) ossia tramite lo scambio (versamento o distribuzione) di pacchetti informativi.

Come evidenza dell'avvenuta conservazione, il servizio genera uno specifico pacchetto informativo (AIP), al fine di garantire il mantenimento dell'integrità, dell'autenticità e immodificabilità degli oggetti conservati.

Tutte le operazioni descritte nel seguente processo sono tracciate tramite log.

8.1 Versamento e acquisizione

8.1.1 Modello WST



Il sistema prevede le seguenti **modalità di trasmissione** dei SIP da parte dell'utente:

1. Tramite Web Services (processo sincrono);
2. Tramite sFTP e successivo caricamento all'interno del sistema (processo asincrono);

Tutte le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP). Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi.

Le specifiche e il modello-dati adottati per il SIP sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio di:

- un identificativo Id (GUID) assegnato al SIP in caso di caricamento con esito positivo in modo da identificarlo in maniera univoca;
- una Eccezione, se si sono verificati degli errori durante il caricamento.

Nel processo di presa in carico dei SIP, il servizio effettua una **serie di controlli di coerenza su ciascuno** e sugli oggetti in esso contenuti e genera un esito di presa in carico. Le verifiche, in particolare, prevedono il **controllo della validità della firma** dei file contenuti nel SIP, l'estensione e il formato degli oggetti, nonché un insieme di controlli sul contenuto del pacchetto.

Il servizio effettua inoltre un'analisi dedicata ai certificati qualificati, generando un apposito Signature Report, quale esito della verifica delle firme qualificate e/o dei sigilli qualificati. Tale report in formato XML o JSON è firmato digitalmente dal servizio e riporta i dati riferiti ai certificati qualificati utilizzati per l'apposizione delle firme/sigilli e viene mantenuto insieme alle evidenze di conservazione come elemento di prova. Il Signature Report è recuperabile dall'utente tramite richiesta del Dissemination Information Package (DIP).

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive, il SIP viene acquisito dal servizio, altrimenti l'esito evidenzia il rifiuto definitivo.

In caso di **presa in carico (accettazione)**, il sistema genera il **Submission Report**, quale esito di tutte le verifiche effettuate sul SIP a partire dalla sua ricezione. Il Submission Report ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare. Tale rapporto contiene il riferimento ad uno o più SIP.

Il Submission Report è generato in formato XML e riporta l'esito dei check una volta ricevuto il SIP da parte del servizio, tra cui la verifica della firma dei file contenuti nel SIP, nonché gli elementi identificativi dell'utente versante, del sistema e del pacchetto.

Inoltre, il Submission Report contiene il riferimento temporale in formato UTC (Tempo Universale Coordinato) ed è firmato digitalmente dal Responsabile del servizio di conservazione.
Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio è sincronizzato con il protocollo NTP Time.nist.gov.

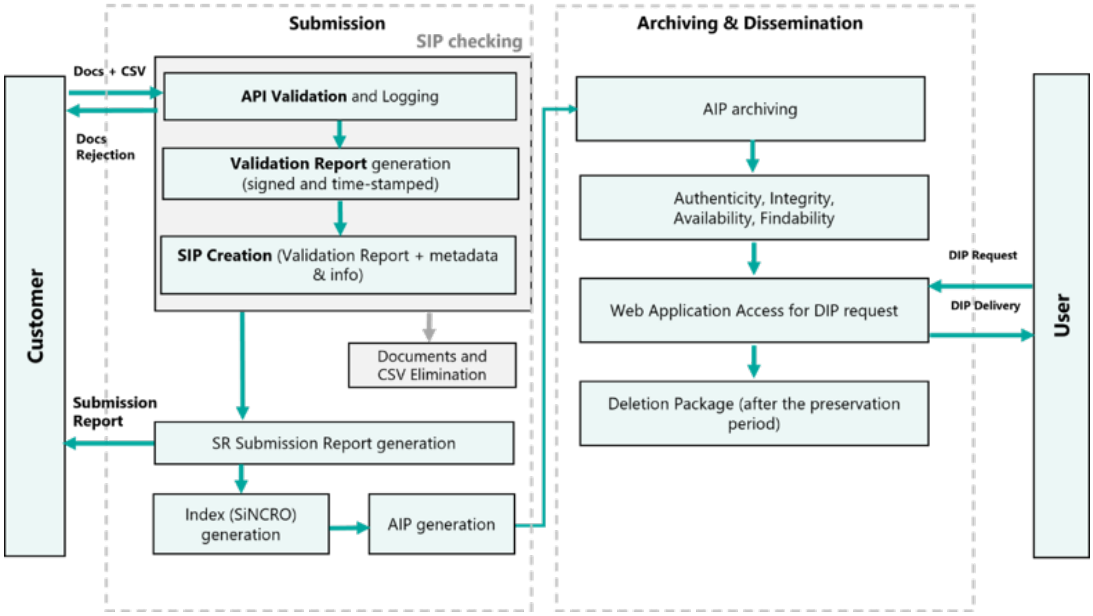
Namirial consente all'utente di avere a disposizione i Submission Report con le seguenti modalità:

- attraverso comunicazione via mail, secondo l'indirizzo di posta elettronica configurato nell'anagrafica dell'utente;
- tramite chiamata al web service del servizio;
- tramite accesso alla piattaforma web del servizio da parte di un utente autorizzato.

Tutti i Submission Report generati, rimangono sempre a disposizione per la consultazione ed esibizione.

Durante le verifiche di coerenza possono essere riscontrate anomalie che generano il **rifiuto dei SIP**, che viene comunicato all'utente tramite canale sicuro.

8.1.2 Modello WTS



Il sistema prevede le seguenti **modalità di trasmissione** dei Data object (documenti su cui sono apposti firme/sigilli qualificati in associazione ad informazioni aggiuntive) da parte dell'utente:

1. Tramite Web Services (processo sincrono);
2. Tramite sFTP e successivo caricamento all'interno del sistema (processo asincrono);

Tutte le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP). Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi.

Il servizio procede all'analisi dei Data object, alla verifica delle firme/sigilli qualificati e alla generazione del Signature Report, quale esito della verifica delle firme qualificate e/o dei sigilli qualificati. Il Signature Report è in formato XML o JSON, firmato e marcato temporalmente dal servizio, riporta i dati riferiti ai certificati qualificati utilizzati per l'apposizione delle firme/sigilli e viene mantenuto insieme alle evidenze di conservazione come elemento di prova. Il Signature Report è recuperabile dall'utente tramite richiesta del Dissemination Information Package (DIP).

Le informazioni ricavate da tale analisi, insieme al Signature Report, vengono inserite dal servizio in un SIP dedicato.

Contestualmente all'invio del SIP, i Data object originari vengono eliminati dal perimetro del sistema, in accordo al modello *with temporary storage* (WTS).

Qualora specifiche condizioni relative al trattamento dati, motivi di riservatezza, privacy o prestazioni lo richiedano, le fasi di presa in carico, l'analisi dei Data object, la verifica dei certificati qualificati e la creazione del SIP possono essere installate all'interno del perimetro del Cliente.

Le specifiche e il modello-dati adottati per il SIP sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio di:

- un identificativo Id (GUID) assegnato al SIP in caso di caricamento con esito positivo in modo da identificarlo in maniera univoca;
- una Eccezione, se si sono verificati degli errori durante il caricamento.

Nel processo di presa in carico dei SIP, il servizio effettua una **serie di controlli di coerenza su ciascuno** e sugli oggetti in esso contenuti e genera un esito di presa in carico. Le verifiche, in particolare, prevedono il **controllo della validità della firma** dei file contenuti nel SIP, l'estensione e il formato degli oggetti, nonché un insieme di controlli sul contenuto del pacchetto.

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive, il SIP viene acquisito dal servizio, altrimenti l'esito evidenzia il rifiuto definitivo.

In caso di **presa in carico (accettazione)**, il sistema genera il **Submission Report**, quale esito di tutte le verifiche effettuate sul SIP a partire dalla sua ricezione. Il Submission Report ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare. Tale rapporto contiene il riferimento ad uno o più SIP.

Il Submission Report è generato in formato XML e riporta l'esito dei check una volta ricevuto il SIP da parte del servizio, tra cui la verifica della firma dei file contenuti nel SIP, nonché gli elementi identificativi dell'utente versante, del sistema e del pacchetto.

Inoltre, il Submission Report contiene il riferimento temporale in formato UTC (Tempo Universale Coordinato) ed è firmato digitalmente dal Responsabile del servizio di conservazione.
Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio è sincronizzato con il protocollo NTP Time.nist.gov.

Namirial consente all'utente di avere a disposizione i Submission Report con le seguenti modalità:

- attraverso comunicazione via mail, secondo l'indirizzo di posta elettronica configurato nell'anagrafica dell'utente;
- tramite chiamata al web service del servizio;
- tramite accesso alla piattaforma web del servizio da parte di un utente autorizzato.

Tutti i Submission Report generati, rimangono sempre a disposizione per la consultazione ed esibizione.

Durante le verifiche di coerenza possono essere riscontrate anomalie che generano il **rifiuto dei SIP**, che viene comunicato all'utente tramite canale sicuro.

8.2 Preparazione e gestione dell'AIP

La generazione dell'AIP determina l'effettiva conservazione degli oggetti digitali con le evidenze di conservazione ad essi associate. Questa procedura avviene tramite la schedulazione di un job automatico secondo tempistiche configurabili. Il rapporto tra SIP e AIP può essere uno a uno o molti a uno.

8.3 Cifratura degli oggetti di conservazione

Gli oggetti informatici vengono crittografati con crittografia lato server e chiavi gestite da Amazon S3 (SSE-S3), servizio fornito da Amazon AWS, in qualità di datacenter Namirial.

Quando si utilizza la crittografia lato server, Amazon S3 esegue la crittografia di un oggetto prima di salvarlo su disco nei suoi data center e lo decripta al momento della richiesta da parte del Cliente.

La crittografia lato server protegge i dati at rest. Amazon S3 cifra ogni oggetto con una chiave univoca. Come ulteriore protezione, cifra la chiave stessa con una chiave master che ruota regolarmente. La crittografia lato server di Amazon S3 utilizza una delle crittografie a blocchi più potenti disponibili per cifrare i dati, ossia Advanced Encryption Standard a 256 bit (AES-256).

8.4 Preparazione e gestione del DIP

L'utente può richiedere uno o più DIP durante l'esercizio del servizio o in caso di disattivazione ai fini della migrazione verso un altro servizio.

Alla richiesta del DIP il servizio restituisce tramite canale crittografato (su protocollo HTTPS) il pacchetto in formato di cartella compressa .zip costituito dagli oggetti digitali e dalle evidenze di conservazione previsti dalla richiesta di distribuzione.

Nel caso di modello WTS il DIP contiene il Signature Report generato dal sistema, i relativi metadati associati e le prove di conservazione.

8.5 Eliminazione degli oggetti conservati (Deletion)

L'eliminazione degli oggetti consiste nell'operazione con cui si pone termine alla conservazione degli stessi, rimuovendoli dal servizio. Tale processo viene avviato:

- al termine del periodo di conservazione degli oggetti;
- su richiesta del cliente per specifici pacchetti/oggetti;
- in caso di disdetta del servizio da parte del cliente.

L'utente ha la facoltà di confermare la proposta di eliminazione; qualora non confermi, ha la facoltà di richiedere l'estensione del periodo di conservazione.

In caso di disdetta, successivamente alla consegna verso l'utente degli oggetti conservati, il sistema procede con la cancellazione.

Tali operazioni vengono gestite in maniera automatica, tramite job e schedulazioni che avviano il processo di verifica del periodo di conservazione, delle proposte di eliminazione, delle autorizzazioni e dell'eliminazione degli oggetti.

Quale esito dell'avvenuta procedura di eliminazione, il servizio genera un Deletion package.

Richiesta e approvazione e procedura sono tracciati.

8.6 Interazioni con il servizio

L'interazione con il servizio da parte dell'utente può avvenire tramite integrazione informatica e accesso web tramite interfaccia. A seconda delle funzionalità richiesteè possibile:

- inviare oggetti al servizio;
- verificare l'esito positivo del versamento attraverso la fruizione del Submission Report generato dal servizio;
- ricercare i propri oggetti tramite chiavi univoche (metadati);
- consultare gli oggetti conservati;
- effettuare il download degli oggetti conservati;
- effettuare il download dei Dissemination Information Package (DIP) ai fini dell'esibizione delle evidenze di conservazione.

L'organizzazione di riferimento degli utenti, all'interno del contratto, indica i soggetti abilitati ad accedere alla piattaforma (utenti), cui Namirial fornisce delle credenziali univoche basate su un doppio fattore di autenticazione (conformi a quanto previsto per il LoA livello substantial). In caso di necessità di aggiungere nuovi utenti, i soggetti indicati

dall'organizzazione in sede contrattuale possono richiedere l'attivazione di nuovi utenti. Tali soggetti hanno la facoltà di richiedere anche la revoca delle credenziali. Nel caso dell'interfaccia web, al primo accesso l'utente dovrà cambiare la password secondo le disposizioni vigenti in materia di trattamento dei dati. Ogni utente è responsabile del controllo esclusivo della propria password di accesso che non è recuperabile o visibile al personale Namirial in quanto anonimizzata.

Inoltre, per ragioni di sicurezza, il servizio disattiva temporaneamente le utenze di consultazione inattive da oltre sei mesi. Per la riattivazione dell'utenza, l'utente dovrà procedere con la procedura di rinnovo password raggiungibile dalla pagina di login.

9. Policy sulle evidenze di conservazione

In conformità con la ETSI 119 511, Allegato A, requisito OVR-A-04, il certificato qualificato specifico associato alla firma o al sigillo dell'evidenza di conservazione è l'identificatore digitale del servizio come definito nel paragrafo 5.5.3 della specifica ETSI TS 119 612, che identifica in modo univoco e inequivocabile il servizio fiduciario di conservazione di firme e sigilli qualificati per il suo riferimento negli elenchi di fiducia secondo l'articolo 22 del Regolamento eIDAS. Lo stato qualificato e il certificato specifico in uso sono presenti nell'elenco di fiducia dell'Italia.

La policy applicata in materia di evidenze di conservazione si basa sulla norma italiana UNI 11386 (SInCRO) (Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali), che definisce la struttura dell'Indice di Conservazione come componente strategica del processo.

Questo standard tecnico definisce uno schema XML che identifica la struttura dell'insieme di dati a supporto del processo di conservazione e recupero degli oggetti digitali. Questo insieme di dati, denominato Indice di conservazione (PIndex), è un file associato agli oggetti sottoposti a conservazione. L'impronta informatica degli oggetti è calcolata tramite algoritmo crittografico SHA-256 (SHA-256 WithRSAEncryption) al fine di generare Hash irreversibili e unici.

L'Indice XML è protetto mediante firma o sigillo qualificato e marca temporale qualificata, generati anch'essi con algoritmo SHA-256, emessi da Namirial in qualità, rispettivamente, di Certification Authority (CA) e di Time Stamping Authority.

La convalida dell'evidenza di conservazione è possibile verificando la firma e la marca temporale apposte sull'Indice di Conservazione (PIndex) attraverso uno

strumento di convalida di firme e sigilli elettronici qualificati. Inoltre, leggendo l'XML, è possibile verificare l'integrità dell'HASH degli oggetti inviati e tutti i dati relativi all'utente che ha versato l'oggetto. Se la firma o il sigillo e la marca temporale sono convalidati, lo stato qualificato del servizio può essere accertato verificando la presenza del certificato come identificatore digitale del servizio per un servizio fiduciario di conservazione di firme e sigilli qualificati nell'elenco di fiducia.

L'indice AIP include anche gli OID, come definiti nel paragrafo 1.2, che in modo unico identificano il sistema di conservazione e il modello di riferimento adottato (WST o WTS), garantendo la piena tracciabilità del processo di conservazione.

Se le evidenze di conservazione necessitano di un aggiornamento o di un'estensione (*augmentation*), secondo quanto richiesto nel requisito OVR-7.15-03 del TS 119 511, il servizio qualificato di conservazione di firme e sigilli fornisce il Revision Package.

10. Policy di convalida della firma

Come evidenziato nel paragrafo *Modello di conservazione* - a seconda del modello utilizzato - il servizio:

1. conserva l'intero documento firmato. Il paragrafo *Versamento e acquisizione - Modello WST* descrive come gli oggetti versati nel sistema di conservazione vengono controllati prima di diventare oggetti conservati.
2. conserva il Signature Report e le informazioni aggiuntive associate. Il paragrafo *Versamento e acquisizione - Modello WTS* descrive come i Data object analizzati dal sistema vengono impiegati per la generazione del Signature Report e dei dati associati inseriti nel SIP.

Gli oggetti firmati conservati, mantenendo tutte le loro proprietà, possono essere convalidati attraverso tutti gli strumenti di convalida disponibili (Namirial fornisce anche il proprio software gratuito per eseguire questa operazione).

Firme e sigilli conservati dal servizio fiduciario qualificato sono conformi al livello B-LTA come definito negli standard europei ETSI per il formato delle firme, secondo ETSI EN 319 122-1 (CAdES), par. 6.1, punto d) (vedi NOTA 4), ETSI EN 319 132-1 (XAdES), par. 6.1, punto d) (vedi NOTA 4), ETSI EN 319 142-1 (PAdES, par. 6.1, punto d) (vedi NOTA 4), ETSI EN 319 162-1 (ASiC, par. 5.1, punto d) (vedi NOTA 3).

11. Condizioni generali di contratto

Namirial fornisce, in relazione al proprio servizio qualificato di conservazione di firme elettroniche qualificate e sigilli elettronici qualificati, uno specifico documento di termini e condizioni, il quale deve essere accettato tramite sottoscrizione da parte del cliente del servizio stesso.

Le condizioni generali di contratto contengono la disciplina generale del servizio, le relative definizioni, gli obblighi e gli adempimenti delle parti, i livelli di servizio, durata e recesso, modalità di trattamento dei dati personali, dettagli sul servizio e, ove necessario, i riferimenti alla documentazione descrittiva specifica.