

Postedoc - Manuale della Conservazione Sostitutiva

Copia Archiviata Elettronicamente	File: MDCPOSTEDOC20
-----------------------------------	---------------------

Copia cartacea Controllata in distribuzione ad enti esterni	N°: 0
Rilasciata a:	
Copia cartacea non Controllata in distribuzione ad enti esterni	N°:

Versione n.	Pagina n.	Motivo della revisione	Data
1.0	tutte	emissione	31/01/2007
1.1	tutte	revisione	04/03/2010
2.0	ultima	Inserimento SLA	02/02/2011

Versione n.	Redazione	Verifica	Approvazione	Data
1.0	Vittorio D'Alessio	Riccardo Fasoli	Gianfranco Godino Virgilio Arciero	31/01/2007
1.1	Riccardo Fasoli	N/A	Virgilio Arciero	04/03/2010
2.0	Riccardo Fasoli	N/A	Virgilio Arciero	02/02/2011

Indice

1	Scopo del documento	4
2	Riferimenti normativi	4
3	Documenti di riferimento	4
4	Definizioni	5
4.1	Definizioni Normative	5
5	Dati di identificazione	6
5.1	Dati identificativi del Responsabile della Conservazione	6
5.2	Dati identificativi della Certification Authority (C.A.)	6
5.3	Dati identificativi dei documenti da trattare	6
5.4	Luogo di conservazione dei documenti	6
6	Compiti e doveri del Responsabile della Conservazione Sostitutiva	7
7	Il servizio	9
7.1	Descrizione del Servizio	9
7.2	Descrizione della organizzazione	10
7.2.1	Ruoli e Responsabilità	10
7.3	Descrizione delle procedure	10
7.3.1	Flussi inviati dal Cliente: il file dati e il file check	10
7.3.2	Memorizzazione del lotto di documenti su storage ad alta affidabilità	11
7.3.3	Formato del File di chiusura	11
7.3.4	Sintesi del processo di Conservazione Sostitutiva	12
7.3.5	Le procedure di sicurezza del riferimento temporale	12
7.3.6	Modalità di apposizione della firma digitale da parte del Responsabile della Conservazione	13
7.3.7	Procedura di esibizione	13
7.4	Descrizione flussi informatici	14
7.4.1	Classi documentali	14
7.5	Descrizione utenti del sistema	17
8	Verifiche periodiche	18
8.1	Definizione della procedura adottata nella verifica dei lotti di documenti	18
8.2	Scadenziario delle verifiche periodiche	18
8.3	Libro dei verbali delle verifiche periodiche	18
9	Procedure di gestione delle copie di sicurezza	19
9.1	Modalità di produzione delle copie di sicurezza	19
9.2	Conservazione delle copie di sicurezza	19
10	Manutenzione del software applicativo	19
11	Procedure di gestione degli eventi catastrofici	19
12	Procedure di gestione della privacy	20
13	Livelli di Servizio	20

1 Scopo del documento

Il presente manuale descrive il sistema di Conservazione Sostitutiva per il Cliente del servizio Postedoc, di qui innanzi denominato come il %Cliente% che intende sottoporre a conservazione sostitutiva, utilizzando l'apposito servizio, i propri documenti.

Esso, in generale, ha lo scopo di:

- descrivere le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo;
- descrivere come è stato implementato il processo di conservazione e gli aspetti operativi per arrivare alla produzione del dispositivo contenente la documentazione digitale;
- descrivere il processo di apposizione della Firma Digitale, della Marca Temporale e tutti gli aspetti procedurali inerenti la registrazione dei dispositivi sostitutivi,
- descrivere le procedure di verifica dei documenti e di gestione delle copie di sicurezza.

Il documento recepisce le indicazioni fornite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA, dal 29 dicembre 2009 Digit PA), e in particolare le %Regole Tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali+ (Deliberazione n.11/2004 del 19 febbraio 2004), e le successive %Note Esplicative delle Regole Tecniche per la riproduzione e conservazione dei documenti su supporto ottico+.

Nota: Tutte le modifiche apportate al presente Manuale sono riportate a pagina 2.

2 Riferimenti normativi

- [1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) . Codice dell'amministrazione digitale
- [2] Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004 e relative note esplicative
- [3] Decreto Legislativo 20 febbraio 2004, n.52
- [4] Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009

3 Documenti di riferimento

Codice Documento	Descrizione
MUPOSTEDOC15	Manuale Utente

4 Definizioni

4.1 Definizioni Normative

Termine/Acronimo	Definizione
Documento	Per documento si intende la rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.
Documento analogico	Per documento analogico si intende un documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia.
Documento analogico originale	Per documento analogico originale si intende un documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Funzione di hash	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.
Riferimento temporale	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici da una procedura informatica.
Marca temporale	Una marca temporale (art. 1 DPCM [4]) è un'evidenza informatica risultato di una procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.
TSA	Time Stamping Authority. Ente terzo che emette i certificati di marcatura temporale
TSS	Time Stamping Service. Servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA. Questo servizio deve rispettare i requisiti del RFC 3161 e il titolo IV del DPCM 13 gennaio 2004

5 Dati di identificazione

5.1 Dati identificativi del Responsabile della Conservazione

Ai fini dell'esecuzione del Servizio, Postecom è Responsabile della Conservazione nella persona del Dirigente responsabile della Service Centers Unit, che agisce ai sensi dell'art. 5 della Deliberazione CNIPA. [2]

Il Dirigente espletterà tutte le funzioni inerenti al processo di Conservazione Sostitutiva ed in particolare i processi di apposizione di firme digitali e marche temporali, essendo dotato di un certificato qualificato emesso secondo la normativa vigente in tema di firma digitale. Tale certificato, installato su dispositivo HSM (Hardware Security Module), è utilizzato dal processo di certificazione dei lotti di documenti da sottoporre a Conservazione Sostitutiva.

In base a quanto previsto all'art.5 comma 3 della deliberazione CNIPA [2] il Responsabile della Conservazione, per la parte operativa delle attività, si avvale a sua volta di personale appartenente alla struttura di Gestione Applicativa della Service Centers Unit di Postecom.

Postecom si riserva, a proprio insindacabile giudizio, di sostituire il Responsabile della Conservazione.

5.2 Dati identificativi della Certification Authority (C.A.)

I certificati di firma digitale utilizzati dal processo di Conservazione Sostitutiva nonché le marche temporali sono rilasciate dalla Certification Authority di Postecom (Dname: CN=Postecom CA1, OU=CA e Sicurezza, O=Postecom s.p.a., C=IT), accreditata presso il CNIPA secondo la normativa vigente.

5.3 Dati identificativi dei documenti da trattare

I documenti da sottoporre a conservazione sostitutiva fanno riferimento alle classi documentali definite per il Cliente, i cui attributi sono conformi allo standard di definizione riportato al capitolo 7.4.1.

5.4 Luogo di conservazione dei documenti

I documenti sono conservati in appositi dispositivi di storage all'interno del Centro Servizi Postecom, in Viale Europa 190, 00144 - Roma.

6 Compiti e doveri del Responsabile della Conservazione Sostitutiva

La deliberazione CNIPA [2] attribuisce al responsabile del procedimento di conservazione sostitutiva (art. 5) precisi compiti e specifiche responsabilità. In conformità a quanto riportato nella norma appena citata viene effettuata una classificazione dei compiti del Responsabile della Conservazione; nella tabella seguente sono riportati da un lato i compiti del Responsabile della Conservazione e, in modo corrispondente, le modalità con cui tali compiti vengono eseguiti:

Responsabile della conservazione	Realizzazione del compito
<p>Compiti organizzativi: definisce i requisiti del sistema di conservazione, organizza il contenuto dei supporti di memorizzazione e gestisce le procedure di sicurezza e tracciabilità che garantiscono la corretta conservazione e consentono l'accessibilità di ciascun documento conservato.</p>	<p>Tali compiti sono svolti da personale di Postecom appartenente alla struttura di Gestione Applicativa della Service Centers Unit, tramite le funzionalità rese disponibili dal software del sistema di conservazione. L'elenco dei nominativi è tenuto aggiornato dalla struttura Risorse Umane di Postecom.</p>
<p>Compiti di registrazione delle attività: archivia e rende disponibili, con l'impiego di procedure elaborative, per ogni supporto di memorizzazione le seguenti informazioni:</p> <ol style="list-style-type: none"> 1. descrizione del contenuto dei documenti; 2. estremi identificativi del Responsabile della Conservazione; 3. estremi identificativi delle persone delegate dal Responsabile della Conservazione, con l'indicazione dei compiti assegnati; 4. indicazione delle copie di sicurezza. 	<p>Tali compiti sono svolti da personale di Postecom appartenente alla struttura di Gestione Applicativa della Service Centers Unit, mediante funzionalità rese disponibili dal software del sistema di conservazione.</p>
<p>Compiti di manutenzione e controllo del software del sistema di conservazione: mantiene e rende accessibile un archivio del software dei programmi utilizzati per il processo di conservazione.</p>	<p>Tali compiti sono svolti da personale di Postecom, appartenente alla struttura Software Development Unit, mediante l'utilizzo di un sistema di gestione del software, con il quale viene mantenuto il versioning del software realizzato.</p>
<p>Compiti di verifica del sistema: verifica la corretta funzionalità del sistema e dei programmi in gestione.</p>	<p>Questa attività è svolta da Postecom. Periodicamente il personale di Postecom appartenente alla struttura di Gestione Applicativa della Service Centers Unit, effettua le verifiche come al par. 8</p>
<p>Compiti inerenti alla sicurezza: garantisce le misure necessarie per la sicurezza fisica e logica del sistema di conservazione sostitutiva e per la realizzazione delle copie di sicurezza.</p>	<p>La sicurezza fisica e logica fa riferimento alla sicurezza dei sistemi e delle reti di Postecom e nel rispetto di quanto riportato nel Piano della sicurezza di Postecom. Le attività di creazione delle copie di sicurezza sono effettuate da personale di Postecom, della struttura dei Servizi Sistemistici della Service Centers Unit, secondo quanto riportato al par. 0 del presente manuale.</p>

<p>Compito di richiedere la presenza del Pubblico Ufficiale quando previsto dalla normativa: richiede l'intervento del Pubblico Ufficiale nei casi previsti, assicurando allo stesso l'assistenza e le risorse necessarie allo completamento delle attività al medesimo attribuite.</p>	<p>Allo stato attuale, in fase di conservazione sostitutiva, le tipologie di documenti in oggetto non necessitano dell'intervento del Pubblico Ufficiale.</p>
<p>Compito di definire e documentare le procedure di sicurezza per la apposizione del riferimento temporale</p>	<p>Questo compito è realizzato in base a quanto descritto al par. 7.3.5 del presente manuale</p>
<p>Compiti di verifica periodica di leggibilità: verifica periodicamente la validità e la coerenza dei supporti generati e garantisce l'assistenza alle persone da lui eventualmente delegate</p>	<p>Questo compito è svolto dal personale Poste.com, della struttura di Gestione Applicativa della Service Centers Unit, secondo quanto indicato al par. 8 del presente manuale.</p>

Nota:

Il Responsabile della Conservazione non è responsabile del contenuto dei singoli Documenti né degli indici (attributi) associati a ciascun Documento. La conformità dei documenti trasmessi ai corrispondenti originali è assicurata da formale autorizzazione alla Conservazione Sostitutiva da parte del Cliente, eseguita mediante la sottoscrizione del contratto per la fornitura del servizio.

7 Il servizio

7.1 Descrizione del Servizio

La realizzazione del Servizio presenta le caratteristiche sinteticamente descritte di seguito.

- ✓ Invio dei Documenti da parte del Cliente, secondo formati indicati da Postecom;
- ✓ Acquisizione dei documenti e relativi attributi attraverso un collegamento telematico;
- ✓ Archiviazione e indicizzazione dei documenti sulla base degli attributi definiti;
- ✓ Esecuzione del processo di Conservazione Sostitutiva che può essere riassunto nell'esecuzione delle seguenti operazioni:
 - generazione dell'impronta (*hash*) del Lotto di Documenti,
 - memorizzazione dell'impronta del Lotto di Documenti nel File di chiusura,
 - apposizione della Firma Digitale al File di chiusura,
 - richiesta di una Marca Temporale associata al File di chiusura firmato,
 - memorizzazione del Lotto di Documenti, del File di chiusura firmato digitalmente e della Marca Temporale su supporto con caratteristiche di alta affidabilità e alta permanenza del dato, per un periodo temporale di 10 anni.
- ✓ Realizzazione di un'apposita interfaccia che permetta al Cliente di:
 - effettuare ricerche all'interno del repository documentale, sulla base degli indici definiti,
 - visualizzare i risultati della ricerca,
 - visualizzare il documento risultante dalla ricerca effettuata,
 - effettuare il download di uno o di tutti i documenti risultanti dalla ricerca effettuata,
 - verificare, in caso di esibizione dei documenti, la Marca Temporale e la Firma Digitale del lotto di documenti in cui ogni documento è stato inserito

7.2 Descrizione della organizzazione

7.2.1 Ruoli e Responsabilità

La presente sezione illustra le responsabilità e i passi del processo di Conservazione Sostitutiva. Nella tabella sono indicati: nelle colonne i ruoli, nelle righe i passi del processo (le azioni), nelle intersezioni le responsabilità:

	Cliente	Responsabile Conservazione Sostitutiva
Generazione flussi dati relativi a documenti da sottoporre a Conservazione Sostitutiva	R	
Invio dei flussi dati al sistema di Conservazione Sostitutiva	R	
Ricezione, da parte del sistema di Conservazione Sostitutiva, dei flussi dati contenenti documenti e attributi	C	R
Verifica della consistenza dei flussi dati		R
Archiviazione documenti e memorizzazione degli stessi su Storage ad Alta affidabilità		R
Esecuzione del processo di Conservazione Sostitutiva dei lotti di documenti digitali (apposizione di Marca Temporale e Firma Digitale)		R
Verifica avvenuta Conservazione	C	R
Verifica Marca Temporale e Firma Digitale applicata sui Lotti	R	C
Ricerca e visualizzazione dei documenti conservati tramite interfaccia WEB	R	C
Esibizione dei documenti conservati	R	C
Generazione e archiviazione in luogo sicuro dei supporti di backup		R
Verifica periodica dell'effettiva leggibilità dei documenti conservati		R

R per il responsabile primario

C per chi collabora alla realizzazione dell'attività.

7.3 Descrizione delle procedure

7.3.1 Flussi inviati dal Cliente: il file dati e il file check

Ogni flusso dati è inviato al sistema di Conservazione Sostitutiva dal Cliente utilizzando il canale di trasmissione concordato. Ogni flusso è costituito da:

- ✓ un file dati: contenente il file attributi e i documenti da conservare,
- ✓ un file check, chiamato anche file di controllo: contenente la dimensione in byte del file dati e la sua impronta hash.

Prima di elaborare il flusso, il sistema Postecom verificherà la coerenza tra i due file trasmessi che avranno le seguenti caratteristiche.

- ✓ **File dati**, in formato archivio **zip**, contenente a sua volta:
 - un File Attributi, in formato XML, denominato **index.xml**,
 - un numero variabile di documenti.
- ✓ **File check**, in formato XML, contenente la dimensione in byte del File dati e la sua impronta hash, denominato **chk.xml**. Viene utilizzato per verificare l'integrità di ogni flusso spedito.

Il file **index.xml** all'interno del File dati conterrà tutti i valori degli attributi di ogni singolo documento, e il riferimento (path) del singolo documento all'interno del File dati stesso. I valori inseriti in tale file, per ogni documento, saranno corrispondenti agli indici definiti per la classe documentale (vedi capitolo 7.4.1).

7.3.2 Memorizzazione del lotto di documenti su storage ad alta affidabilità

I lotti di documenti vengono memorizzati su storage ad alta affidabilità. All'atto della scrittura, per ogni lotto di documenti viene calcolata l'impronta hash utilizzando l'algoritmo standard SHA-1. Il processo di memorizzazione su storage ad alta affidabilità viene effettuato, oltre che per il lotto di documenti, anche per il file di chiusura e per la Marca Temporale.

7.3.3 Formato del File di chiusura

Il formato del File di chiusura è il seguente:

```
Archivio lotto: azienda-nomeclasse-20100101-00000001.zip
Impronta archivio : da39a3ee5e6b4b0d3255bfef95601890afd80709
Algoritmo impronta archivio: SHA-1
Data conservazione: 2010-01-01 01:02:39.0
ID Lotto: 1234
Check file: azienda-nomeclasse-20100101-00000001-chk.xml
Classe Documentale: nomeclasse
Numero documenti: 123
Responsabile Conservazione: COGNOME NOME
Titolo Responsabile Conservazione: RESPONSABILE CONSERVAZIONE SOSTITUTIVA
Organizzazione Responsabile Conservazione: POSTECOM SPA/05838841004
```

Si possono riconoscere le seguenti informazioni:

- nome del file dati (Archivio lotto)
- impronta hash del file dati (Impronta archivio)
- algoritmo utilizzato per il calcolo dell'impronta (Algoritmo impronta archivio)
- data conservazione
- identificativo univoco del lotto (ID Lotto)
- nome del file di check (Check file)
- identificativo della classe documentale di appartenenza del lotto (Classe Documentale)
- numero totale dei documenti presenti (Numero documenti)
- Nome, Titolo e Organizzazione di appartenenza del Responsabile della Conservazione

7.3.4 Sintesi del processo di Conservazione Sostitutiva

Il processo di Conservazione sostitutiva, eseguito nelle modalità sopra esposte, esegue quindi le seguenti attività:

- ✓ verifica del flusso dati sorgente (file ZIP) mediante il file di controllo del flusso dati (file CHK);
- ✓ calcolo dell'impronta (chiave hash) del flusso dati sorgente (file ZIP);
- ✓ scrittura del file di chiusura, contenente la chiave hash del lotto (file TXT);
- ✓ firma digitale del file di chiusura (file TXT.P7M)
- ✓ associazione di una marca temporale al file di chiusura (file TSR)
- ✓ creazione di un file archivio compresso, in formato ZIP, contenente:
 - il flusso dati sorgente (file %zip+);
 - il file di controllo del flusso dati (file %chk.xml+);
 - il file di chiusura in chiaro (file %txt+);
 - il file di chiusura firmato digitalmente (file %txt.p7m+);
 - la marca temporale associata al file di chiusura (file %tsr+);
 - il file di notifica di avvenuta conservazione (file %cert.xml.p7m+).

Il nome del file archivio sarà determinato dall'identificativo numerico univoco del lotto di documenti memorizzato nel sistema di conservazione.

Esempio:

Postecom riceve il seguente flusso (file zip + file di check):

azienda-nomeclasse-20100201-cod00001.zip
azienda-nomeclasse-20100201-cod00001-chk.xml

Al termine del processo di conservazione il sistema genera il file *NNNN.zip* contenente i seguenti file:

azienda-nomeclasse-20100201-cod00001.zip
azienda-nomeclasse-20100201-cod00001-chk.xml
azienda-nomeclasse-20100201-cod00001.txt
azienda-nomeclasse-20100201-cod00001.txt.p7m
azienda-nomeclasse-20100201-cod00001.tsr
azienda-nomeclasse-20100201-cod00001-cert.xml.p7m

7.3.5 Le procedure di sicurezza del riferimento temporale

Il sistema utilizza, per soddisfare il requisito di apposizione del riferimento temporale richiesto per la procedura di conservazione prevista dalla deliberazione CNIPA [2] (art. 5 comma 1 lett. g), le Marche Temporalmente fornite dal servizio di Time Stamping di Postecom. Le marche temporali emesse sono firmate da un certificato emesso mensilmente dalla TSA di Postecom accreditata presso il CNIPA.

La generazione di una Marca Temporale è ottenuta attraverso una sottoscrizione digitale apposta su una evidenza informatica e fornisce la prova dell'esistenza di tale evidenza informatica al momento di generazione della marca stessa. Apporre una marca temporale ai documenti informatici sottoscritti digitalmente permette di verificare la firma oltre il periodo di validità del certificato di sottoscrizione.

Le marche temporali utilizzate nel processo di Conservazione Sostitutiva sono di tipo *detached* (ovvero sono contenute in un file distinto da quello per il quale si richiede il servizio di marcatura temporale) e hanno una validità di 20 anni dall'emissione in quanto conservate dall'ente certificatore Postecom per l'intero periodo come indicato nel relativo DPCM [4].

7.3.6 Modalità di apposizione della firma digitale da parte del Responsabile della Conservazione

Le chiavi crittografiche corrispondenti al certificato qualificato del Responsabile della Conservazione per l'apposizione della firma digitale sono memorizzate in un dispositivo HSM conforme alla normativa vigente relativa ai dispositivi sicuri per la creazione della firma digitale.

La firma digitale del Responsabile della Conservazione è apposta tramite una procedura automatica la cui attivazione è effettuata tramite l'inserimento di un pin da parte del responsabile medesimo, il quale in questo modo afferma la propria volontà nell'apposizione della firma stessa sui singoli File di chiusura.

7.3.7 Procedura di esibizione

L'esibizione dei documenti conservati avviene da parte di personale autorizzato del Cliente mediante l'interfaccia di una applicazione di esibizione documenti che il sistema rende disponibile mediante un apposito indirizzo web.

L'interfaccia permette ad un utente abilitato di ricercare ed eventualmente visualizzare i documenti di una determinata tipologia sottoposti al processo di Conservazione Sostitutiva presenti all'interno dell'archivio. A seguito dell'accesso a tale funzionalità è possibile visualizzare la lista di tutte le classi documentali per le quali l'utente può effettuare le ricerche. Successivamente, selezionando la tipologia di interesse, viene visualizzata una form, costruita dinamicamente in base alle caratteristiche della classe documentale, per l'inserimento di tutti i parametri del documento in base ai quali effettuare la ricerca.

Alla conferma dell'utente l'applicazione esegue la ricerca visualizzando la lista di documenti che rispondono ai parametri selezionati.

Per ciascun documento della lista viene mostrato:

- un link che consente la visualizzazione di tutte le informazioni disponibili per il documento;
- un link che recupera il documento dall'archivio.

Visualizzando tutte le informazioni disponibili per il documento è possibile, tramite apposito link, recuperare l'intero Lotto di Documenti sottoposto a Conservazione Sostitutiva (vedi capitolo 7.3.4) e successivamente verificarne la Firma Digitale e la Marca Temporale.

7.4 Descrizione flussi informatici

7.4.1 Classi documentali

Una classe documentale definisce tutte le caratteristiche di un tipo di documento da sottoporre a conservazione. A partire dalla definizione della classe documentale vengono generati i file **DTD** e **XSD** da utilizzare per la validazione del file XML che descrive i documenti dei lotti da archiviare.

Una classe documentale è definita dai seguenti parametri:

- ✓ nome,
- ✓ descrizione,
- ✓ periodo di conservazione,
- ✓ insieme di attributi.

Gli attributi sono definiti utilizzando la notazione standard XML

La definizione di una classe documentale genera un file XSD. Si riporta di seguito un esempio di file XSD relativo ad una classe documentale denominata **fattatt** (fatture attive):

fattatt

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
<xs:simpleType name="simpleFile">
<xs:restriction base="xs:string">
<xs:pattern value="[a-zA-Z0-9_][a-zA-Z0-9_\-\.\.]{0,255}"/>
</xs:restriction>
</xs:simpleType>
<xs:element name="fattatt">
<xs:complexType>
<xs:choice maxOccurs="unbounded">
<xs:element name="documento">
<xs:complexType>
<xs:sequence>
<!-- numero_fattura -->
<xs:element name="numero_fattura" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="20"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- data_fattura -->
<xs:element name="data_fattura" type="xs:date" />
<!-- codice_cliente -->
<xs:element minOccurs="0" name="codice_cliente" >
<xs:simpleType>
```

```
<xs:restriction base="xs:string">
<xs:maxLength value="20"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- ragione_sociale -->
<xs:element name="ragione_sociale" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="100"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- partita_iva -->
<xs:element name="partita_iva" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="20"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- codice_fiscale -->
<xs:element name="codice_fiscale" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="16"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- importo_euro -->
<xs:element minOccurs="0" name="importo_euro" >
<xs:simpleType>
<xs:restriction base="xs:decimal">
<xs:maxInclusive value="999999999999999.9999"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- codice_protocollo -->
<xs:element minOccurs="0" name="codice_protocollo" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="20"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- numero_movimento -->
<xs:element minOccurs="0" name="numero_movimento" >
```

```
<xs:simpleType>
<xs:restriction base="xs:integer">
<xs:maxInclusive value="9999999999"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- id_ged -->
<xs:element minOccurs="0" name="id_ged" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="40"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- sottoclasse -->
<xs:element minOccurs="0" name="sottoclasse" >
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:maxLength value="3"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<!-- file -->
<xs:element name="file">

<xs:complexType>
<xs:simpleContent>
<xs:extension base="simpleFile">
<xs:attribute name="size" type="xs:integer" />
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:choice>
</xs:complexType>
</xs:element>
</xs:schema>
```

7.4.1.1 Il file degli attributi

La definizione della classe documentale permette di generare il corrispondente file XML contenente gli attributi dei singoli documenti.

Segue un esempio di file XML per la classe documentale "fattatt":

```
<?xml version="1.0" encoding="UTF-8" ?>
<fattatt>
<documento>
<numero_fattura>XXXXXXXXXXXXXXXXXXXX</numero_fattura>
<data_fattura>2000-01-01</data_fattura>
<codice_cliente>XXXXXXXXXXXXXXXXXXXX</codice_cliente>
<ragione_sociale>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</ragione_sociale>
<partita_iva>XXXXXXXXXXXXXXXXXXXX</partita_iva>
<codice_fiscale>XXXXXXXXXXXXXXXXXX</codice_fiscale>
<importo_euro>9999999999999999.9999</importo_euro>
<codice_protocollo>XXXXXXXXXXXXXXXXXXXX</codice_protocollo>
<numero_movimento>9999999999</numero_movimento>
<id_ged>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</id_ged>
<sottoclasse>XXX</sottoclasse>
<file size="123456789">d_1_f_1.txt</file>
</documento>
</fattatt>
```

7.4.1.2 Il file di controllo

Il file di controllo serve a verificare l'integrità e l'avvenuto trasferimento del file di dati del lotto. Equivale a un file XML che deve avere la seguente struttura:

```
<?xml version="1.0" encoding="UTF-8"?>
<file_chk>
  <file_size>[size file di dati]</file_size>
  <file_hash type="MD5">[hash file di dati]</file_hash>
</file_chk>
```

7.5 Descrizione utenti del sistema

Di seguito si descrivono brevemente i diversi profili utente che hanno accesso ai documenti sottoposti al processo di Conservazione Sostitutiva. La descrizione completa delle funzionalità per il Cliente si trovano all'interno del documento MU_POSTEDOCWEB01.

- **Utenza di Invio documenti**

Postecom al momento dell'attivazione del servizio fornisce al Cliente una utenza abilitata all'invio dei Lotti di Documenti.

- **Utenze di Ricerca, Visualizzazione e Esibizione dei documenti**

Postecom al momento dell'attivazione del servizio fornisce al Cliente un pacchetto di utenze abilitate alla ricerca, visualizzazione e esibizione dei documenti, comprensivo della verifica della Firma Digitale e della Marca Temporale, per conto del Cliente. Tali utenze utilizzano l'interfaccia web del servizio.

8 Verifiche periodiche

8.1 Definizione della procedura adottata nella verifica dei lotti di documenti

Il Responsabile delle Conservazione Sostitutiva con cadenza annuale controllerà la consistenza e l'integrità dei lotti di documenti e dei relativi file attributi, file di indice e file di chiusura, eseguendo o delegando l'esecuzione di una procedura di controllo che interesserà un adeguato campione dei Lotti sottoposti a Conservazione Sostitutiva.

La procedura sarà effettuata sui dati presenti all'interno del sistema di storage e sulle copie di sicurezza custodite dal Responsabile della Conservazione.

8.2 Scadenziario delle verifiche periodiche

Si distinguono due procedure di verifica:

- ✓ Verifica dell'integrità e della consistenza dei lotti di documenti generati dal Processo di Conservazione;
- ✓ Verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei lotti.

La prima procedura è eseguita dal Responsabile della Conservazione, come descritto in precedenza nel paragrafo 8.1.

Per la seconda procedura il Responsabile della Conservazione, con cadenza annuale verificherà che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile sul mercato un visualizzatore aggiornato e conforme alle specifiche del singolo formato di file.

8.3 Libro dei verbali delle verifiche periodiche

Tutte le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni, nonché tutti gli avvenimenti importanti o ritenuti tali dal Responsabile della Conservazione ai fini del corretto svolgimento del processo di conservazione sostitutiva saranno opportunamente tracciati su un apposito Libro dei Verbali.

9 Procedure di gestione delle copie di sicurezza

9.1 Modalità di produzione delle copie di sicurezza

Il sistema prevede un apposito processo per la generazione di copie di sicurezza nel rispetto della vigente normativa.

Ciascuna copia di sicurezza contiene uno o più lotti di documenti, unitamente ai corrispondenti file attributi, file di chiusura firmati digitalmente e marche temporali.

9.2 Conservazione delle copie di sicurezza

Le copie di sicurezza verranno generate in unica copia (su richiesta duplice copia):

- ✓ Una copia sarà custodita dal Responsabile della Conservazione, che provvederà a conservarla opportunamente, impegnandosi a mantenerne la riservatezza e a verificarne periodicamente la leggibilità;
- ✓ Opzionalmente e previo accordo tra il Cliente e Postecom potrà essere generata una seconda copia di sicurezza, su supporto removibile, che verrà consegnata al Cliente.

Le copie in possesso di Postecom vengono memorizzate in apposito dispositivo di storage presso il bunker della CA. L'edificio all'interno del quale viene ospitato il suddetto dispositivo è dotato di un sistema di protezioni fisiche descritte nel documento Piano della Sicurezza della Certification Authority.

10 Manutenzione del software applicativo

Il personale delegato dal Responsabile della Conservazione della struttura di Software Development Unit ha cura di mantenere le versioni aggiornate del SW per la generazione dei Lotti di Documenti sottoposti a Conservazione Sostitutiva.

A tale scopo, tutto il software realizzato per il processo di conservazione sostitutiva e per i processi ad esso collegati si trova all'interno di un sistema di gestione del software in grado di mantenere il versioning del codice sorgente sviluppato.

11 Procedure di gestione degli eventi catastrofici

In caso di evento catastrofico che pregiudichi, in tutto o in parte, il repository primario dei dati sottoposti a conservazione (ovvero il sistema di storage ad alta affidabilità), Il Responsabile della Conservazione provvederà, utilizzando le copie di sicurezza in suo possesso, al corretto ripristino dell'intero archivio.

Un'apposita procedura preleverà i dati da tutte le copie di sicurezza generate, ne verificherà l'integrità, e procederà nuovamente al salvataggio di tutti gli elementi (Lotto di Documenti, File di Indice e File Attributi) su un nuovo sistema di Conservazione Sostitutiva, ovvero su quello preesistente, dopo aver sostituito le parti danneggiate dall'evento catastrofico.

Il verificarsi dell'evento catastrofico e l'evoluzione della procedura di ripristino dell'archivio saranno tempestivamente notificati al Cliente e registrati sul Libro dei Verbali.

12 Procedure di gestione della privacy

Per quanto riguarda l'accesso ai dati da parte di personale Postecom si farà riferimento alle procedure di gestione della privacy presenti nella documentazione ufficiale della società Postecom.

Per quanto riguarda l'accesso ai dati da parte di personale del Cliente, e in particolare al personale che avrà accesso all'interfaccia web di ricerca, visualizzazione e esibizione dei documenti, si farà riferimento alle procedure di gestione della privacy del Cliente.

Allo scopo e per le sole finalità legate all'esecuzione del servizio, il Cliente nomina il Responsabile della Conservazione e la struttura di Gestione Applicativa Postecom quali Responsabili del Trattamento dei dati, ai sensi del Dlgs 196/2003: "Codice in materia di protezione dei dati personali", e li autorizza ad accedere e visualizzare i documenti sottoposti a Conservazione Sostitutiva ai fini e per i soli scopi di verifica della leggibilità dei documenti conservati.

13 Livelli di Servizio

Di seguito si descrivono i livelli di servizio che Postecom deve garantire nell'espletamento delle attività affidategli. Le tempistiche descritte fanno riferimento alle modalità operative per l'erogazione del servizio Postedoc, in conformità a quanto previsto dalla normativa vigente.

Attività e tempistiche		Livelli di servizio	Ambito di applicazione
1	Tempistiche di lavorazione dei <u>flussi documentali</u> ricevuti: archiviazione dei documenti e inoltro degli stessi al processo di conservazione sostitutiva.	Lavorazione di ogni flusso documentale entro 1 giorno lavorativo dalla data di ricezione	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 5.000.
2	Segnalazione della presenza di anomalie nei <u>flussi documentali</u> ricevuti.	Comunicazione della presenza di anomalie nel flusso documentale, tramite risposta ad interrogazione web o web services, entro 1 ora dall'orario di ricezione.	99% dei flussi documentali standard inviati dall'organizzazione.
3	Modalità e tempistiche di rendicontazione degli esiti del processo di Conservazione Sostitutiva da parte di Postecom dei singoli <u>flussi documentali</u>	Generazione dei file esiti del processo di Conservazione Sostitutiva e messa a disposizione all'organizzazione entro le ore 13 del giorno lavorativo successivo alla data di ricezione del flusso documentale.	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 5.000.
4	Modalità e tempistiche di archiviazione elettronica dei documenti	Archiviazione dei documenti tale da consentirne la ricerca on-line (ad evento), secondo le chiavi di ricerca concordate, entro le ore 13.00 del giorno successivo alla data di ricezione del flusso documentale.	99% di ciascun flusso ricevuto contenente un numero di documenti minore o uguale a 5.000.
5	Modalità di conservazione sostitutiva dei documenti.	Conservazione sostitutiva secondo i requisiti previsti dalla normativa nonché dalle procedure condivise e descritte nell'apposito "Manuale della conservazione".	100% di tutti i flussi ricevuti