

Manuale della Conservazione di CompEd Servizi

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	11/07/2017	Roberto Baudizzone	Responsabile Servizi Conservazione
Verifica	12/07/2017	Andrey Romanov	Responsabile Sviluppo Manutenzione
Verifica	12/07/2017	Marco Piccirilli	Responsabile Sicurezza
Verifica	12/07/2017	Roberto Monti	Responsabile Sistemi Informativi
Verifica	12/07/2017	Domenico Rossi	Responsabile Dati Personali
Verifica	12/07/2017	Giuliano Maggi	Responsabile funzione Archivistica
Approvazione	12/07/2017	Renzo Gaggero	Presidente

REGISTRO DELLE VERSIONI

Rev.	Data	Autore	Descrizione
1.0	04/10/2013	Roberto Baudizzone	Prima versione omologata CompEd Servizi
1.9.1	12/11/2015	Roberto Baudizzone	Prima versione revisionata in base allo schema AgID
1.9.2	15/01/2016	Roberto Baudizzone	Organigramma definitivo, altri ritocchi
1.9.3	01/02/2016	Roberto Baudizzone	Ulteriori ritocchi
1.9.4	17/02/2016	Roberto Baudizzone	Inserimento testo alternativo per le immagini, indicazione sito secondario su cloud Aruba
2.0.0	04/03/2016	Roberto Baudizzone	Finalizzazione per presentazione AGID
2.0.1	11/05/2016	Roberto Baudizzone	Ritocchi cap. 4 ("affidamento")
2.0.2	11/07/2017	Roberto Baudizzone	Ritocchi Cap. 8 in occasione di cambio infrastruttura

Sommario

SOMMARIO	2
1 SCOPO E AMBITO DEL DOCUMENTO	4
1.1 INTRODUZIONE E MODELLO DI RIFERIMENTO	4
1.2 ORGANIZZAZIONE DEL DOCUMENTO: CONVENZIONI TIPOGRAFICHE.....	6
1.3 ORGANIZZAZIONE DEL DOCUMENTO: ALLEGATI.....	6
2 TERMINOLOGIA E GLOSSARIO	7
3 NORMATIVA E STANDARD DI RIFERIMENTO	16
3.1 NORMATIVA DI RIFERIMENTO	16
3.2 STANDARD DI RIFERIMENTO.....	17
4 RUOLI E RESPONSABILITÀ	18
4.1 MANAGEMENT: IL RESPONSABILE DELLA CONSERVAZIONE (RdC)	19
4.2 ADMINISTRATION: I RUOLI E LE RESPONSABILITÀ IN COMPED SERVIZI.....	20
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE	22
5.1 ORGANIGRAMMA.....	23
5.2 STRUTTURE ORGANIZZATIVE.....	24
5.2.1 <i>Modalità di commercializzazione</i>	24
5.2.2 <i>La funzione Marketing/Commerciale</i>	25
5.2.3 <i>La funzione Progettazione e Sviluppo</i>	26
5.2.4 <i>La funzione Esercizio</i>	26
5.2.5 <i>Helpdesk</i>	27
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE	27
6.1 OGGETTI CONSERVATI	29
6.2 PACCHETTO DI VERSAMENTO – PdV [SIP]	29
6.3 PACCHETTO DI ARCHIVIAZIONE – PdA [AIP] E RELATIVO INDICE IPdA	31
6.3.1 <i>Struttura del PdA con IPdA in formato SInCRO</i>	31
6.4 PACCHETTO DI DISTRIBUZIONE – PdD [DIP] E RELATIVO INDICE IPDD	32
7 IL PROCESSO DI CONSERVAZIONE (PDC)	32
7.1 MODALITÀ DI ACQUISIZIONE DEI PACCHETTI DI VERSAMENTO PER LA LORO PRESA IN CARICO	34
7.2 VERIFICHE EFFETTUATE SUI PACCHETTI DI VERSAMENTO (PdV) E SUGLI OGGETTI IN ESSI CONTENUTI.....	37
7.3 ACCETTAZIONE DEI PdV E GENERAZIONE DEL RdV	39
7.4 RIFIUTO DEL PdV E MODALITÀ DI COMUNICAZIONE DELLE ANOMALIE.....	41
7.5 PREPARAZIONE E GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE (PdA)	41
7.6 ESIBIZIONE: PREPARAZIONE E GESTIONE DEL PACCHETTO DI DISTRIBUZIONE.....	44
7.6.1 <i>PdD coincidente con PdA</i>	48
7.6.2 <i>PdD non coincidente con un PdA</i>	48
7.6.3 <i>Trasmissione dei Pacchetti di Distribuzione</i>	48
7.7 PRODUZIONE DI DUPLICATI E COPIE INFORMATICHE, EVENTUALE INTERVENTO DEL PUBBLICO UFFICIALE.....	49
7.7.1 <i>Intervento del Pubblico Ufficiale</i>	50
7.8 SCARTO DEL PACCHETTI DI ARCHIVIAZIONE.....	50
8 IL SISTEMA DI CONSERVAZIONE	51
8.1 COMPONENTI LOGICHE	52
8.1.1 <i>Moduli di Input</i>	52

8.1.2	<i>Front-end Produttore/Utente</i>	53
8.1.3	<i>Ingest</i>	53
8.1.4	<i>Access</i>	54
8.1.5	<i>Data Management</i>	54
8.1.6	<i>Administration</i>	55
8.1.7	<i>Service Library</i>	56
8.2	COMPONENTI TECNOLOGICHE	57
8.3	COMPONENTI FISICHE	57
8.3.1	<i>Il sito primario</i>	58
8.3.2	<i>Il sito secondario</i>	59
8.4	PROCEDURE DI GESTIONE ED EVOLUZIONE	59
8.4.1	<i>Conduzione e manutenzione del SdC</i>	59
8.4.2	<i>Gestione e Conservazione dei Log</i>	60
8.4.3	<i>Monitoraggio</i>	60
8.4.4	<i>Change Management</i>	61
8.4.5	<i>Verifica periodica di conformità a normativa e standard di riferimento</i>	61
9	MONITORAGGIO E CONTROLLO	62
9.1	PROCEDURE DI MONITORAGGIO	62
9.1.1	<i>Monitoraggio processi</i>	62
9.1.2	<i>Notifica & Logging</i>	63
9.2	VERIFICA INTEGRITÀ DEGLI ARCHIVI	63
9.3	SOLUZIONI ADOTTATE IN CASO DI ANOMALIE.....	65
9.3.1	<i>Gestione anomalie di funzionamento</i>	65
9.3.2	<i>Gestione anomalie di integrità</i>	66

1 Scopo e ambito del documento

Il presente **Manuale di Conservazione** (nel seguito \Rightarrow **MdC**), redatto in conformità alle \Rightarrow **Regole Tecniche** (DPCM 3/12/2013) ed allo *schema* (v. 2.1) predisposto da \Rightarrow **AgID** per i soggetti che richiedono l'Accreditamento per l'attività di Conservazione dei Documenti Informatici, descrive dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del \Rightarrow **Sistema di Conservazione (SdC)**.

Torna al [sommario](#)

1.1 Introduzione e Modello di riferimento

Le attuali \Rightarrow **Regole Tecniche** in merito di conservazione di documenti informatici sono fortemente ispirate al modello \Rightarrow **OAIS** (*Open Archival Information System*), con l'innesto di alcuni importanti vincoli (soprattutto in merito alla definizione delle responsabilità, dell'interoperabilità, della garanzia di inalterabilità dei dati conservati) che contribuiscono significativamente a guidare l'implementazione da parte dei progettisti.

Le attività fondamentali di cui si compone l'intero processo di conservazione sono svolte da un complesso di regole, procedure, tecnologie che costituiscono il *Sistema di Conservazione*.

Il \Rightarrow **SdC** di **CompEd Servizi**, è basato su un insieme di applicazioni e componenti software installate su una infrastruttura (hardware, software di base, risorse di rete, servizi esterni).

Il software applicativo per la Conservazione, sviluppato interamente da **CompEd Software Design** (azienda del gruppo di cui fa parte anche **CompEd Servizi**), è globalmente denominato **Century**.

L'implementazione di **Century** è dunque basata fortemente sul modello **OAIS**, avvalendosi inoltre della riduzione della complessità di tale modello offerta dal perimetro delle **Regole Tecniche**.

Nel seguito di questo manuale faremo continuo riferimento al modello **OAIS** con le entità funzionali in esso definite, rappresentate in questo diagramma:

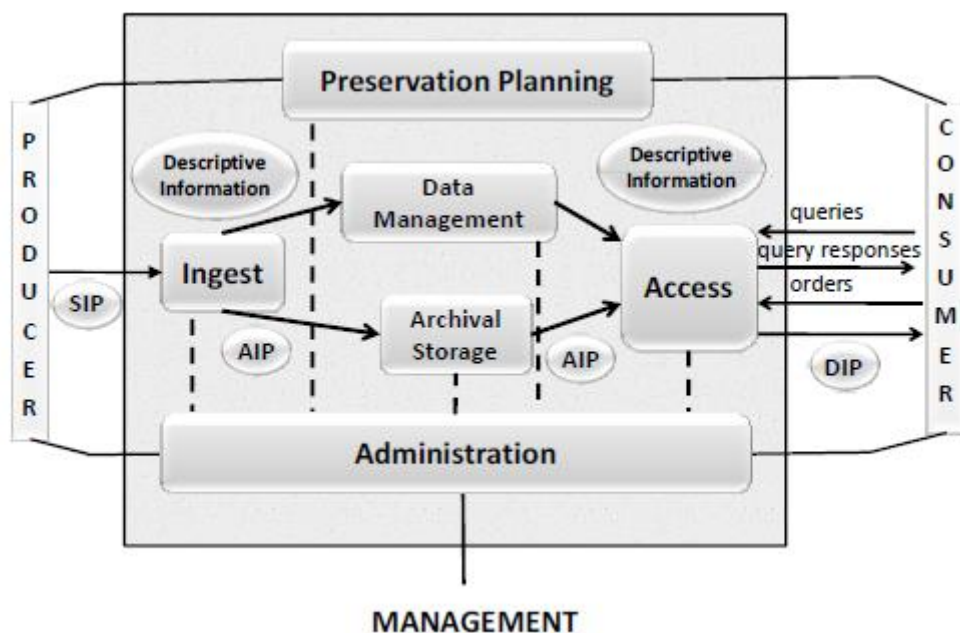


Fig. 1- Modello di riferimento dello standard OAIS (questa figura è tratta direttamente dallo standard)
Relazioni ed interdipendenze tra le entità funzionali del sistema e dei ruoli esterni

Nel diagramma si notano, oltre alle entità funzionali rappresentate dai blocchi rettangolari (⇒ **Ingest**, ⇒ **Access**, ⇒ **Data Management**, ⇒ **Archival Storage**, ⇒ **Preservation Planning**, ⇒ **Administration**), gli oggetti informativi che prendono forma e circolano nel sistema: si tratta degli oggetti ovali del disegno, in particolare quelli contrassegnati dalle sigle ⇒ **SIP**, ⇒ **AIP**, ⇒ **DIP**.

In particolare si desidera qui richiamare la coincidenza concettuale tra alcuni elementi previsti dal modello **OAIS** ed altri previsti – con diversa denominazione – nell’ambito delle **Regole tecniche**:

OAIS - Sigla	OAIS - Esteso	DPCM - Sigla	DPCM 3/12/2015 - Esteso
⇒ SIP	Submission Information Package	⇒ PdV	Pacchetto di Versamento
⇒ AIP	Archival Information Package	⇒ PdA	Pacchetto di Archiviazione
⇒ DIP	Dissemination Information Package	⇒ PdD	Pacchetto di Distribuzione
⇒ Producer	Producer	⇒ Produttore	Produttore
⇒ Consumer	Consumer	⇒ Utente	Utente

Nel seguito del documento useremo spesso queste definizioni come sinonimi, indicandole con la versione italiana (definita nelle **Regole Tecniche**) seguita quasi sempre dall’equivalente **OAIS** racchiuso tra parentesi quadre ed in colore verde. Ad esempio: **PdV** [**SIP**].

Torna al [sommario](#)

1.2 Organizzazione del documento: convenzioni tipografiche

Nel presente **⇒** **MdC** si adottano alcune convenzioni tipografiche:

- Elemento riportato in **grassetto**: indica che nella [sezione Terminologia e glossario](#) esiste una specifica entrata che descrive l'elemento. Quando non eccessivamente ridondante è prefissato dal simbolo **⇒** (**freccia**) che guida direttamente all'elemento corrispondente del glossario.
- Elemento riportato in **grassetto** di colore verde: indica un elemento, presente nella tabella [Terminologia](#), preso dal modello di riferimento **OAIS**. Quando non eccessivamente ridondante è prefissato dal simbolo **⇒** (**freccia**) che guida direttamente all'elemento corrispondente del glossario.
- Elemento in **grassetto corsivo**: indica un nome di società del gruppo **CompEd** (ad esempio **CompEd Software Design** o **CompEd Servizi**) oppure il nome di un prodotto di **CompEd** (ad esempio **Century** o **DigitalSign**)

Torna al [sommario](#)

1.3 Organizzazione del documento: allegati

Questo **MdC** descrive tutti gli aspetti validi in generale, per tutti i clienti del servizio.

Alcune specificità variabili in particolari servizi ed alcune informazioni sensibili sul piano della riservatezza industriale sono stralciate ed incluse in alcuni allegati.

Di seguito la lista degli allegati, cui si fa riferimento nel presente documento:

- **Specificità del contratto**

Torna al [sommario](#)

2 Terminologia e Glossario

Glossario dei termini e Acronimi	
A2A	Leggere "A to A" – Application to Application; indica una comunicazione diretta tra due applicazioni, senza intervento umano.
AA	Area di Accumulazione – nella terminologia di ⇒ Century l'AA è uno spazio di storage ove vengono accumulati gli oggetti che vengono immessi in un Canale tramite i PdV ; la ⇒ Policy del ⇒ Canale determina il momento in cui dal contenuto della AA si produce un nuovo ⇒ PdA .
Access	Un'entità funzionale prevista dal modello ⇒ OAIS : contiene i servizi e le funzioni necessarie a rendere disponibili agli ⇒ Utenti [Users] le informazioni contenute nell'archivio e ad offrire i relativi servizi Si veda la descrizione di questa implementazione .
Administration	Un'entità funzionale prevista dal modello ⇒ OAIS : contiene i servizi e le funzioni necessarie a controllare e gestire il funzionamento delle altre entità funzionali. Si veda la descrizione di questa implementazione .
AgID	Agenzia per l'Italia Digitale, http://www.agid.gov.it/agid
AIP	Archival Information Package - Nel modello ⇒ OAIS è l'equivalente del ⇒ PdA
API	Application Program Interface – espressione generica che indica un set di metodi e funzioni richiamabili a livello programmatico per richiedere servizi applicativi al sistema che espone (rende disponibile) la API
Archival Storage	Area di memorizzazione, basata su <i>file system</i> , in cui ⇒ Century memorizza principalmente i ⇒ PdA completi.
CA	Certification Authority – soggetto che emette ⇒ certificati digitali mediante una propria chiave privata associata ad un <i>Certificato di CA</i> .
CAD	Codice dell'Amministrazione Digitale – il D.L. 7 marzo 2005, n. 82 con tutte le successive integrazioni e modificazioni.
Canale (di Conservazione)	Rappresenta una sequenza di PdA generata nel tempo, contenenti oggetti omogenei (dello stesso ⇒ produttore e di una tipologia logicamente comune). Se ne veda l'introduzione in questa sezione .
CDP	CRL Distribution Point – attributo contenuto in ogni ⇒ certificato , rappresenta uno o più indirizzi Internet presso i quali è possibile reperire le informazioni sull'eventuale stato di sospensione o revoca del certificato stesso (una ⇒ CRL o un

	servizio ⇒ OCSP)
Century	Il software applicativo di CompEd che implementa il ⇒ SdC
Certificato (digitale)	<p>Una struttura dati (file) che contiene una chiave pubblica ed informazioni di identificazione del soggetto titolare della corrispondente chiave privata. È firmato digitalmente dal ⇒ Certificatore, mediante una speciale chiave privata corrispondente ad una specifica ⇒ Certification Authority che lo emette.</p> <p>Consente di ⇒ verificare una firma elettronica.</p> <p>Ogni certificato reca indicazioni della data ed ora di emissione, nonché data ed ora di scadenza (per una durata variabile, tipicamente, da 1 a 10 anni, funzione della lunghezza della chiave oggetto di certificazione e delle scelte del certificatore).</p> <p>Un certificato, anche nel periodo di validità, può essere sottoposto a sospensione o revoca (ad esempio se il titolare della chiave privata associata al certificato perde il possesso del dispositivo di firma, oppure se esso non fa più parte dell'organizzazione – ente, azienda – che compare nel certificato stesso).</p> <p>Lo stato di revoca può essere accertato consultando una Lista di Sospensione/Revoca (⇒ CRL) pubblicata dal ⇒ Certificatore stesso, oppure con una richiesta puntuale ad un servizio ⇒ OCSP (Online Certificate Status Protocol).</p>
Certificato qualificato	Un particolare tipo di ⇒ certificato digitale , conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, permette di verificare ⇒ firme digitali e ⇒ firme elettroniche qualificate
Certificatore	<p>Un soggetto che eroga servizi di emissione di ⇒ certificati digitali e/o ⇒ qualificati, mediante diverse ⇒ Certification Authority. Normalmente si sottintende, almeno nel quadro giuridico del ⇒ CAD, un Certificatore Qualificato, ossia un Certificatore abilitato ad emettere ⇒ Certificati Qualificati.</p> <p>In Italia tutti i Certificatori Qualificati sono anche <i>Accreditati</i>.</p>
Consumer	Nel modello ⇒ OAIS è l'equivalente dell' ⇒ Utente .
Context (Information)	Dal modello ⇒ OAIS , informazione che consente di documentare la relazione tra un oggetto conservato ed il suo ambiente (ad esempio, nel nostro caso, l'appartenenza di un ⇒ PdA ad un certo ⇒ Canale , assegnato ad uno specifico ⇒ Produttore).
CRL	Certificate Revocation List – Lista di Sospensione/Revoca – una lista, gestita da una ⇒ CA , che contiene l'elenco dei numeri di serie dei ⇒ Certificati (ovviamente tutti emessi da quella CA) per i quali sono stati emessi provvedimenti di revoca o di sospensione ancora attivi
Data Management	Un'entità funzionale prevista dal modello ⇒ OAIS : contiene i

	<p>servizi e le funzioni necessarie a popolare, mantenere a rendere accessibili una grande varietà di informazioni. Ad esempio cataloghi ed indici di quanto può essere ricercato nell'archivio.</p> <p>Si veda la descrizione di questa implementazione.</p>
Dissemination API	<p>Una particolare => API esposta da => Century, che implementa funzioni dedicate all'esibizione: immissione => query, ottenimento liste di risultati, accesso a singoli oggetti, produzione => PdD, ...</p>
DIP	<p>Dissemination Information Package - Nel modello => OAIS è l'equivalente del => PdD</p>
Esercizio	<p>Una funzione di CompEd Servizi che presiede alla gestione operativa del sistema di conservazione in tutti i suoi aspetti dinamici. Si veda la sezione dedicata.</p>
Esibizione	<p>L'operazione tramite la quale il => SdC mette un contenuto (o un insieme di contenuti) a disposizione dell' => Utente.</p> <p>Si veda la sezione dedicata.</p>
Firma digitale	<p>Dalla definizione del => CAD:</p> <p><i>Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare 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.</i></p> <p>In pratica è una stringa di bit calcolata su un insieme di dati (più esattamente sulla sua impronta o codice => hash), in base ad una chiave privata e verificabile tramite il => certificato qualificato intestato al sottoscrittore; consente di accertare l'origine e l'integrità dei dati a cui è applicata. Comunemente si usa questa espressione come sostanziale sinonimo di => Firma Elettronica Qualificata, dato che – almeno in Italia- non esiste un esempio concreto di firma digitale che non sia qualificata.</p>
Firma elettronica avanzata	<p>Dalla definizione del => CAD:</p> <p><i>Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.</i></p>
Firma elettronica qualificata	<p>Dalla definizione del => CAD:</p> <p><i>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.</i></p> <p>Comunemente si usa più spesso l'espressione => Firma</p>

	Digitale , che pure formalmente non è necessariamente basata su un dispositivo sicuro (smartcard o HSM), ma nel contesto italiano la firma digitale non esiste senza tale dispositivo, sono quindi da considerare quasi sinonimi.
Fixity (Information)	Dal modello => OAIS , l'informazione utilizzata per assicurare la non modificabilità di un contenuto (nel nostro caso sarà il valore dell'impronta – => hash – di un oggetto, riportata nel => IPdA e nel => IPdD).
freccia	=> simbolo usato nel testo di questo manuale per fornire un collegamento diretto alla entry corrispondente di questo glossario
Giornale di Controllo	Una particolare sequenza di registrazioni corrispondenti ad eventi particolarmente significativi che avvengono nel => SdC . Queste registrazioni vengono conservate in uno specifico => Canale di sistema.
GUI	Graphic User Interface – una interfaccia utente grafica, in => Century è quasi sempre una interfaccia web utilizzabile mediante un <i>browser</i> collegato al <i>web server</i> esposto dall'applicazione.
Hash	Funzione crittografica che consente di ricavare, da un contenuto binario di qualunque lunghezza, una stringa di bit di dimensione fissa e ridotta (chiamata <i>impronta</i> o <i>digest</i> , talvolta <i>codice hash</i>), tale consentire il rilevamento (mediante ricalcolo e verifica) qualunque modifica apportata al dato originale. Alla base della tecnologia della => firma digitale , l'impronta di ogni oggetto conservato è anche riportato nel => IPdA e nel => IPdD .
Information Package	Versione originale => OAIS del => Pacchetto Informativo .
Ingest	Un'entità funzionale prevista dal modello => OAIS : contiene i servizi e le funzioni necessarie ad accettare i => PdV [SIP] e produrre i => PdA [AIP] . Si veda la descrizione di questa implementazione .
Interrogazione	(Denominata => Query nella terminologia => OAIS) – un'operazione (finalizzata alla => Esibizione) eseguita da un => Utente per ricercare uno o più contenuti che soddisfino i criteri di selezione desiderati
IPdA	Indice del Pacchetto di Archiviazione – struttura dati formata in accordo con lo standard => UNI-SInCRO , si veda la sezione dedicata .
IPdD	Indice del Pacchetto di Distribuzione – struttura dati formata in accordo con lo standard => UNI-SInCRO , si veda la sezione dedicata .
Marca Temporale	Un particolare oggetto digitale emesso da un soggetto (in Italia è di fatto sempre un => Certificatore) ed utile a comprovare l'esistenza di un documento informatico in un istante di tempo ben identificato. Di fatto è una => firma elettronica avanzata apposta dal => Certificatore ad una evidenza informatica

	<p>costituita dall'impronta (=> hash) del documento riferito e dall'informazione di data ed ora.</p> <p>Ottenuta tramite la sottoscrizione di un <i>servizio di marcatura temporale</i>, trasmettendo l'impronta del documento al server del => Certificatore ed ottenendone in ritorno la marca temporale stessa.</p>
MdC	Manuale della Conservazione – questo documento, vedere introduzione
Metadati	<p>[dalle => Regole Tecniche]:</p> <p><i>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; tale insieme è descritto nell'allegato 5 del presente decreto (DPCM 3-12-2013)</i></p>
Modulo di Input	Nell'architettura modulare di => Century un Modulo di Input è un'interfaccia verso il => Produttore , attraverso la quale è possibile immettere i => PdV ed ottenere in ritorno i => RdV
OAIS	Open Archival Information System – lo standard (ISO 14721:2012) di riferimento per la progettazione di un sistema di archiviazione.
OCSP	Online Certificate Status Protocol – è un protocollo (implementato in un servizio) che permette di ottenere informazioni puntuali sullo stato di sospensione o revoca di un => certificato . Si tratta di una modalità alternativa alle liste => CRL per ottenere le stesse informazioni.
Operatori Helpdesk	Persone che prestano il servizio di primo livello agli utenti del servizio di conservazione (e di altri servizi di CompEd Servizi), di regola rispondendo alle richieste di supporto telefonico che pervengono al <i>call-center</i> .
Operatori IT	Persone con competenze sistemistiche che collaborano con => RSI per la conduzione del sistema informatico che costituisce il => SdC e che ne svolgono le mansioni operative (monitoraggio, controllo, configurazione, supporto tecnico, interventi di ogni genere)
Ordine	(Equivalentemente di Order definito del modello => OAIS) – nell'ambito dell'esibizione, può seguire una => interrogazione (Query) : costituisce una richiesta di produzione di un => PdD [DIP] .
Pacchetto informativo	<p>Un contenitore logico di informazioni (documenti, metadati, ...), opzionalmente corredato di informazioni specifiche di conservazione, usato come unità discreta di gestione. Versione tradotta in Italiano de => Information Package del modello => OAIS</p> <p>In concreto si tratta delle tipologie => PdV [SIP], => PdA [AIP],</p>

	⇒ PdD [DIP]
Patch	Aggiornamento parziale del software applicativo; in genere coinvolge uno o più componenti software, modificati per correggere un difetto o per implementare una evoluzione di modesta entità.
PdA	Pacchetto di Archiviazione – equivalente al termine ⇒ AIP (Archival Information Package) definito dal modello ⇒ OAIS . Se ne veda la descrizione .
PdC	Processo di Conservazione – vedere descrizione
PdD	Pacchetto di Distribuzione – equivalente al termine ⇒ DIP (Dissemination Information Package) definito dal modello ⇒ OAIS . Se ne veda la descrizione .
PdV	Pacchetto di Versamento – equivalente al termine ⇒ SIP (Submission Information Package) definito dal modello ⇒ OAIS . Se ne veda la descrizione .
PEC	Posta Elettronica Certificata – un sistema di posta elettronica gestito da Gestori Accreditati che assicura la tracciabilità dei messaggi e l'integrità/autenticità dei contenuti
PiC	Presenza in Carico – l'operazione tramite cui il ⇒ SdC (in particolare l'entità funzionale ⇒ Ingest) acquisisce positivamente un ⇒ PdV
Policy	Nella terminologia di ⇒ Century la Policy di conservazione di un ⇒ Canale è un insieme di informazioni che configura la politica di generazione di un ⇒ PdA a partire dal contenuto della ⇒ AA del Canale stesso. Ad esempio può codificare un intervallo temporale e/o un limite alla quantità di dati accumulati.
Preservation Planning	Un'entità funzionale prevista dal modello ⇒ OAIS : provvede servizi e funzioni volte a mantenere e monitorare l'ambiente con l'obiettivo di assicurare, nel tempo, la leggibilità ed accessibilità delle informazioni archiviate. In questa implementazione non è previsto un modulo specifico per questo scopo, che invece è coperto dalla pianificazione e dalle misure di protezione dell'integrità.
Producer	Nel modello ⇒ OAIS è l'equivalente del ⇒ Produttore .
Produttore	Dalle definizioni delle ⇒ Regole Tecniche : <i>persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si</i>

	<p><i>identifica con responsabile della gestione documentale</i></p> <p>Concettualmente coincidente con il => Producer previsto dal modello => OAIS.</p>
Provenance (Information)	Dal modello => OAIS , l'informazione che indica l'origine del contenuto oggetto di conservazione.
Provisioning	Funzione che presiede alla materiale attivazione del servizio di conservazione, istanziando nel sistema le strutture dati ed aggiornando i parametri operativi necessari. Si veda la sezione dedicata .
QBE	Query By Example – metodologia classica per costruire una => query , che prevede l'inserimento di una o più chiavi di ricerca in una struttura visuale che riproduce la struttura dati dell'archivio in cui si effettua la ricerca, costruendo così l'esempio di una classe di oggetti che si sta ricercando
Quality Assurance	Dal modello => OAIS , funzione dell'entità => Ingest che ha lo scopo di verificare che i contenuti immessi nel sistema soddisfino i requisiti predefiniti.
Query	Versione in Inglese, dal modello => OAIS , di => Interrogazione
RAC	Responsabile della funzione archivistica di conservazione – la persona, di CompEd Servizi , che governa gli aspetti del processo di conservazione legati ai contenuti e ai => metadati associati. Si vedano i dettagli delle diverse figure .
RdC	Responsabile della Conservazione – il soggetto che assume le responsabilità previste dall'art. 8 delle => Regole Tecniche , si veda la sezione dedicata .
RDP	Responsabile Dati Personali – la persona, di CompEd Servizi , che assicura il trattamento dei dati personali nell'ambito del processo di conservazione. Si vedano i dettagli delle diverse figure .
RdR	Rapporto di Rifiuto – struttura dati generata dal sistema in caso un => PdV non sia accettato per mancato superamento delle verifiche di accettazione. Si veda la sezione dedicata .
RdV	Rapporto di Versamento – struttura dati generata dal sistema in caso un => PdV sia correttamente accettato e preso in carico a seguito del superamento delle verifiche di accettazione. Si veda la sezione dedicata .
Reference (Information)	Dal modello => OAIS , informazione che consente l'identificazione univoca di un oggetto conservato.
Regolamento di Servizio	Il documento contrattuale che descrive le modalità di erogazione del servizio di Conservazione
Regole Tecniche	Il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – “Regole tecniche in materia di sistema di conservazione ai

	sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"
Release	Un aggiornamento importante significativo del software applicativo che costituisce il => SdC . A differenza di una => patch , una release implica una completa sostituzione di tutti i componenti software del sistema (o tutti quelli di un sottosistema) e richiede un ciclo di test più intensivo.
RSC	Responsabile del Servizio di Conservazione – la persona, di CompEd Servizi , che gestisce e governa il processo di conservazione. Si vedano i dettagli delle diverse figure .
RSI	Responsabile dei Sistemi Informativi – la persona, di CompEd Servizi , che gestisce e governa il patrimonio hardware e software utilizzato nel processo di conservazione. Si vedano i dettagli delle diverse figure .
RSic	Responsabile della Sicurezza – la persona, di CompEd Servizi , che gestisce e governa le soluzioni tecnologiche e le politiche in materia di sicurezza. Si vedano i dettagli delle diverse figure .
RSM	Responsabile Sviluppo e Manutenzione – la persona, di CompEd Servizi , che gestisce le evoluzioni delle componenti software del Sistema di Conservazione. Si vedano i dettagli delle diverse figure .
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Schema	Nella terminologia di => Century indica un set di => metadati ed il relativo significato. Un => Canale (e quindi i => PdA che lo costituiscono) può gestire documenti organizzati secondo uno o più Schemi.
SdC	Sistema di Conservazione – se ne veda la descrizione .
SDI	Sistema Di Interscambio per la fatturazione elettronica verso la Pubblica Amministrazione
SIP	Submission Information Package – nel modello di riferimento => OAIS è l'equivalente del => PdV
SSL	Secure Socket Layer – un protocollo di comunicazione che permette lo scambio di informazioni cifrate, affidabilmente inaccessibili agli estranei, anche su connessioni pubbliche.
Stage	L'ambiente di Stage è un'istanza del sistema di elaborazione distinta da quella di produzione, che comunque replica al meglio. Suo scopo è testare => patch e => release in modo da far emergere anomalie e consentirne la correzione senza disservizi per l'utenza.

Sviluppo	Una funzione operativa di CompEd Servizi che cura le attività di sviluppo delle tecnologie ed in particolare del software applicativo del => SdC . Si veda la sezione dedicata .
Trigger	L'evento trigger è quello che provoca l'effettivo consolidamento del contenuto della => AA (Area di Accumulazione) associata ad un canale in un => PdA . Tale evento consiste di una scadenza temporale (ad esempio le 23.00 di ogni giorno feriali, oppure le 03.00 del 22 dicembre di ogni anno, oppure le 05.00 di ogni primo giorno del mese) e/o del superamento di una soglia di volume dei dati contenuti nella AA (es. 4 GB)
TSS	Time Stamping Server – un server, gestito da un => Certificatore , che eroga il servizio di => Marcatura Temporale
UNI-SInCRO	Espressione compatta per UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; lo standard adottato per rappresentare gli => IPdA e gli => IPdD
User	Nel modello => OAIS è l'equivalente di => Utente
Utente	Dalle definizioni delle => Regole Tecniche : <i>persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse</i>
UTC	Universal Time, Coordinated – Tempo Universale Coordinato: rappresenta l'orario universale espresso con riferimento al meridiano di Greenwich. È il formato in cui sono espressi gli orari delle => Marche Temporali e gli altri riferimenti temporali usati nell'ambito del processo di conservazione, al fine di eliminare ogni ambiguità dovuta a diverse posizioni geografiche, ora legale, ecc.
VdC	Volume di Conservazione – definizione adottata nell'ambito dello standard => UNI-SInCRO con significato del tutto analogo a Pacchetto di Archiviazione => PdA
Verifica di una firma	Riferito ad una => firma digitale , => qualificata , => avanzata , ecc., consiste di una sequenza di passi volti ad accertare l'autenticità della firma e l'integrità del contenuto digitale che la firma protegge. In sintesi, il sistema che esegue la verifica controlla innanzitutto la conformità degli oggetti agli standard attesi; quindi ricalcola il codice => hash dell'oggetto firmato e lo confronta con il risultato della decifratura della firma mediante la chiave pubblica, estratta dal => certificato di firma: l'identità di questi due risultati indica l'integrità di firma e contenuto. Infine si verifica che il certificato da cui si estrale la chiave pubblica sia stato emesso da una => CA

	<p>appartenente alla lista di riferimento per la tipologia di certificato.</p> <p>Di norma la verifica del certificato si estende sino a valutare lo stato di validità, sia rispetto alla scadenza naturale, sia rispetto ad eventuali provvedimenti di sospensione o revoca (vedere => CRL e => OCSP).</p>
Verifica di una marca temporale	Analoga alla => verifica di una firma , applicata alla => marca temporale .
VPN	Virtual Private Network - una rete di privata, instaurata tra soggetti che utilizzano, come infrastruttura di trasporto, un sistema di trasmissione pubblico e condiviso, tipicamente la rete Internet. Scopo delle reti VPN è offrire alle aziende, a un costo inferiore, le stesse possibilità delle linee private in affitto ma sfruttando reti condivise pubbliche. Per ottenere questo risultato si utilizzano tecnologia di autenticazione e di cifratura (fonte: wikipedia).

Torna al [sommario](#)

3 Normativa e Standard di Riferimento

3.1 Normativa di riferimento

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);

- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna al [sommario](#)

3.2 Standard di riferimento

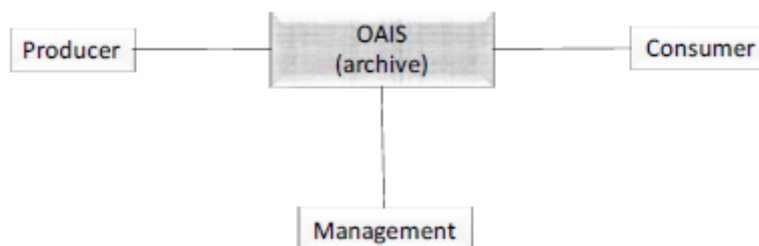
- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al [sommario](#)

4 Ruoli e Responsabilità

Come detto nella [sezione introduttiva](#), **CompEd Servizi** ha adottato pervasivamente il modello \Rightarrow **OAIS**.

Secondo tale modello il \Rightarrow **Sistema di Conservazione** è *circondato* da diversi ruoli:



*Fig. 2 – Modello di riferimento OAIS (figura tratta direttamente dallo standard)
Relazioni tra il Sistema di Conservazione ed i ruoli esterni*

Si noti che tali ruoli sono gli stessi previsti dalle \Rightarrow **Regole Tecniche** (art. 6), con la seguente terminologia:

- a. \Rightarrow **Produttore** \equiv **Producer**
- b. \Rightarrow **Utente** \equiv **Consumer**
- c. \Rightarrow **Responsabile della Conservazione (RdC)** \equiv **Management**

In generale i ruoli qui evidenziati sono ricoperti da persone esterne a **CompEd Servizi**:

- i. il **Produttore** è un soggetto che fa parte dell'organizzazione cliente del servizio, il quale è in possesso dei documenti che intendere affidare al servizio di conservazione;
- ii. l'**Utente** è anch'esso appartenente all'organizzazione del cliente (o un terzo autorizzato), il quale nel tempo accede ai documenti custoditi nell'ambito del servizio di conservazione;
- iii. il **RdC** è una figura appartenente all'organizzazione del cliente, sebbene possa affidare molte delle sue funzioni ad un soggetto appartenente all'organizzazione di **CompEd Servizi**.

All'interno del perimetro del "Sistema" esiste naturalmente un insieme di ruoli che svolgono le attività più operative

- i. Responsabile del Servizio di Conservazione (\Rightarrow **RSC**)
- ii. Responsabile Sicurezza dei Sistemi per la Conservazione (\Rightarrow **RSic**)
- iii. Responsabile funzione Archivistica di Conservazione (\Rightarrow **RAC**)

- iv. Responsabile trattamento dei Dati Personali (**=> RDP**)
- v. Responsabile Sistemi Informativi per la Conservazione (**=> RSI**)
- vi. Responsabile Sviluppo e Manutenzione del Sistema di Conservazione (**=> RSM**)

Nelle prossime sottosezioni dettagliamo le responsabilità di questi ruoli.

Torna al [sommario](#)

4.1 Management: il Responsabile della Conservazione (RdC)

Il ruolo di **=> RdC** è ricoperto da un soggetto (una persona fisica) appartenente all'organizzazione del Cliente.

Le responsabilità di **RdC** sono ben identificate nelle **=> Regole Tecniche** (art. 7). In particolare:

- a) *definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;*
- b) *gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;*
- c) *genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;*
- d) *genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;*
- e) *effettua il monitoraggio della corretta funzionalità del sistema di conservazione;*
- f) *assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;*
- g) *al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;*
- h) *provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;*
- i) *adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;*
- j) *assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;*
- k) *assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;*
- l) *provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;*

m) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

Nel caso di Clienti appartenenti alla Pubblica Amministrazione il **RdC** è nominato all'interno dello stesso Ente, in accordo l'art. 7, commi 3 e 4 delle [=> Regole Tecniche](#).

Nel caso di Clienti rappresentati da aziende private, ove non espressamente comunicato, il ruolo di **RdC** è assunto dal Rappresentante Legale.

Nel caso di Clienti persone fisiche il ruolo di **RdC** è assunto in prima persona dal soggetto stesso.

Il **RdC** affida a **CompEd Servizi** lo svolgimento di tutte o parte le attività connesse con le proprie responsabilità, in accordo con l'art. 6, comma 6 delle **Regole Tecniche**.

Torna al [sommario](#)

4.2 Administration: i ruoli e le responsabilità in CompEd Servizi

La seguente tabella precisa l'assegnazione dei diversi ruoli alle persone fisiche che assumono i rispettivi incarichi, descrivendo sinteticamente i ruoli stessi ed i periodi di copertura del ruolo.

Ove nella tabella il periodo indicato menzioni "ad oggi" indica che il ruolo è tuttora coperto dal soggetto indicato, alla data del presente documento.

Ruolo	nominativo	attività di competenza	periodo	eventuali deleghe
RSC Responsabile del Servizio di Conservazione	Roberto BAUDIZZONE	Definizione ed attuazione delle politiche complessive del SdC, nonché del governo della gestione del SdC stesso; definizione delle caratteristiche e dei requisiti del SdC in conformità alla normativa vigente; corretta erogazione del servizio di conservazione all'ente produttore; gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	dal 01/01/2015 ad oggi	

<p>RSic</p> <p>Responsabile Sicurezza dei sistemi per la conservazione</p>	<p>Ing. Marco PICCIRILLI</p>	<p>Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;</p> <p>segnalazione delle eventuali difformità al RSC e individuazione e pianificazione delle necessarie azioni correttive;</p>	<p>dal 01/01/2015</p> <p>ad oggi</p>	
<p>RAC</p> <p>Responsabile funzione Archivistica di Conservazione</p>	<p>Ing. Giuliano MAGGI</p>	<p>Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</p> <p>definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</p> <p>monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</p> <p>collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.</p>	<p>dal 01/01/2015</p> <p>ad oggi</p>	
<p>RDP</p> <p>Responsabile trattamento Dati Personali</p>	<p>Domenico ROSSI</p>	<p>Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</p> <p>garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza</p>	<p>dal 01/01/2015</p> <p>ad oggi</p>	
<p>RSI</p> <p>Responsabile Sistemi Informativi per la Conservazione</p>	<p>Roberto MONTI</p>	<p>Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</p> <p>monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</p> <p>segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e</p>	<p>dal 01/01/2015</p> <p>ad oggi</p>	

		<p>pianificazione delle necessarie azioni correttive;</p> <p>pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;</p> <p>controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.</p>		
<p>RSM</p> <p>Responsabile Sviluppo e Manutenzione del Sistema di conservazione</p>	<p>Ing. Andrey ROMANOV</p>	<p>Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</p> <p>pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;</p> <p>monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;</p> <p>interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;</p> <p>gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.</p>	<p>dal</p> <p>01/01/2015</p> <p>ad oggi</p>	

Torna al [sommario](#)

5 Struttura Organizzativa per il Servizio di Conservazione

Nelle successive sottosezioni illustriamo sia l'organigramma specifico del servizio di conservazione, sia le strutture organizzative che consentono l'erogazione del servizio.

Torna al [sommario](#)

5.1 Organigramma

Qui di seguito il diagramma descrive visivamente le relazioni tra i diversi ruoli introdotti nella [sezione precedente](#).

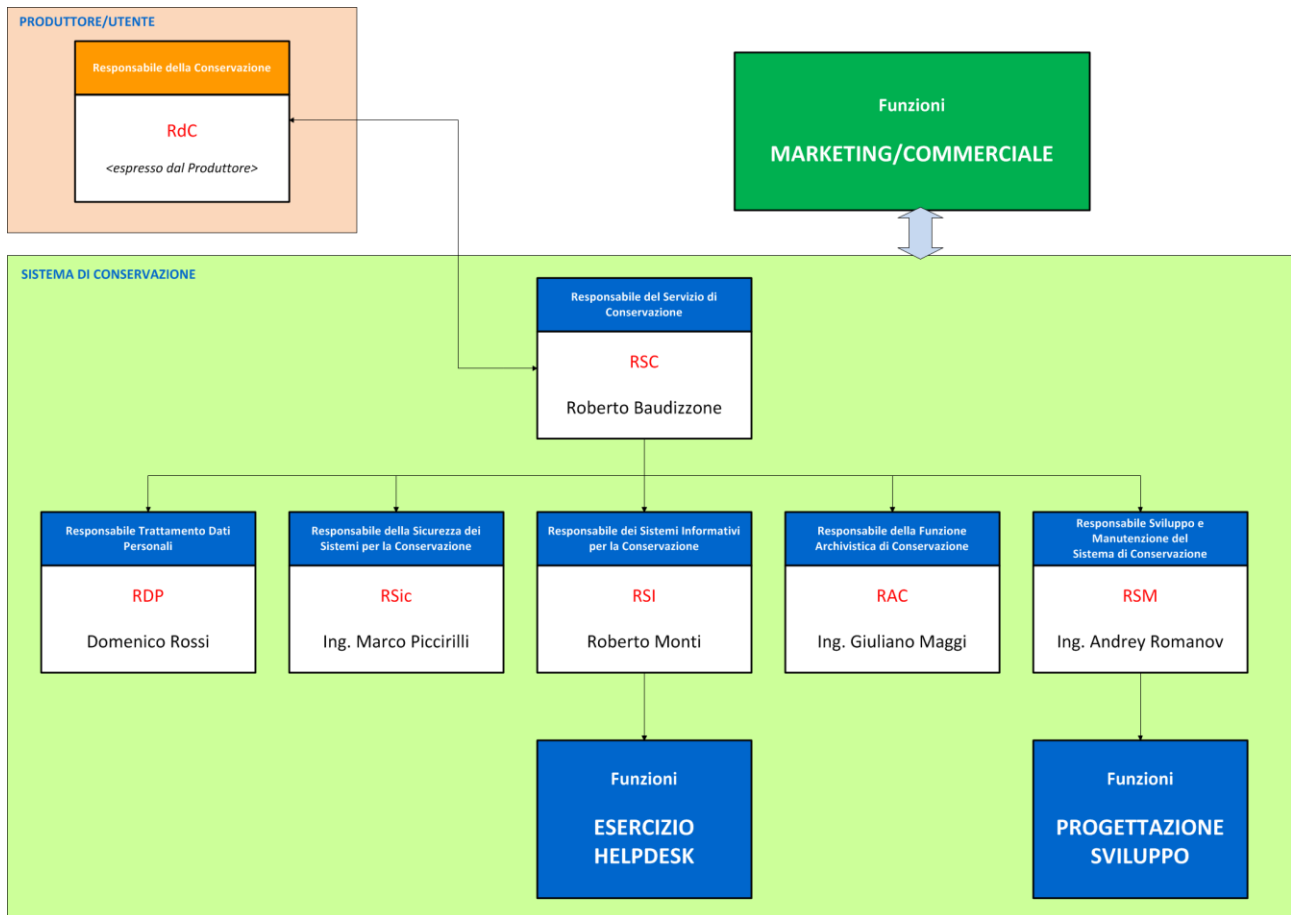


Fig. 3 – Organigramma
I ruoli operativi per la Conservazione in CompEd Servizi

Si evidenzia che il ruolo di Responsabile della Conservazione (\Rightarrow **RdC**) in generale è un ruolo esterno all'organizzazione di **CompEd Servizi**; **RdC** affida le attività specifiche al **Responsabile del Servizio di Conservazione** (\Rightarrow **RSC**). Quest'ultimo opera avvalendosi delle attività (e responsabilità) degli altri ruoli, come definiti in questo documento.

Il diagramma evidenzia l'esistenza di una funzione *Marketing/Commerciale*, non direttamente integrata nel sistema e nelle strutture organizzative strettamente coinvolte nel Processo di Conservazione, ma importante nel determinarne le politiche, come sarà chiarito nella prossima sezione.

L'organigramma visualizza anche l'esistenza di alcune funzioni alle dipendenze di **RSM** e **RSI**, rispettivamente, come chiarito nel seguito.

Torna al [sommario](#)

5.2 Strutture Organizzative

Fermo restando l'organigramma delle funzioni fondamentali definito alla sezione precedente, il servizio prevede alcune strutture operative necessarie all'effettivo funzionamento.

Vale la pena di descrivere brevemente la particolare modalità commerciale adottata da **CompEd Servizi** per l'erogazione dei servizi di Conservazione alla propria clientela.

Torna al [sommario](#)

5.2.1 Modalità di commercializzazione

In generale **CompEd Servizi** offre la Conservazione nell'ambito di pacchetti di servizi che contengono anche altre prestazioni.

Il caso più emblematico è quello collegato alla Fatturazione Elettronica:

- a) Clienti (tipicamente aziende private, ma non esclusivamente) che necessitano di produrre, elaborare e trasmettere fatture elettroniche attive alla Pubblica Amministrazione; **CompEd Servizi** provvede alla gestione del ciclo di vita delle fatture (nel caso più completo sin dalla compilazione manuale della fattura stessa, la sottoscrizione digitale, l'invio attraverso il Sistema Di Interscambio => **SDI**, la gestione dell'esito, ecc.). Il passo finale è appunto la Conservazione della fattura, completa di tutte le ricevute e notifiche collegate.
- b) Clienti (enti della Pubblica Amministrazione) che necessitano di ricevere le fatture elettroniche passive, provenienti dai fornitori attraverso lo **SDI**, quindi consultare, stampare, esportare tali fatture, gestire l'esito committente (accettare una fattura corretta o declinarne una che contiene errori) attraverso lo stesso **SDI**. Anche in questo caso le fatture ricevute, con tutte le notifiche ed esiti, vanno infine sottoposte a conservazione.

Oltre a questi casi ci sono situazioni più concentrate sulla conservazione:

- un servizio di conservazione di documenti contabili, offerto ad aziende e commercialisti;
- un servizio di conservazione di registrazioni giornaliere del protocollo informatico, offerto ad enti pubblici;
- servizi di conservazione offerti a *software house* e *system integrator*, per conto dei loro clienti che utilizzano loro sistemi e applicazioni

Naturalmente esistono progetti *custom*, di conservazione di documenti su specifiche esigenze di aziende, enti, ecc.

Il fattore comune tra queste diverse modalità di erogazione del servizio si riassume in questi punti:

- tariffe molto concorrenziali, adatte anche a piccoli e piccolissimi clienti;
- servizio standardizzato più possibile;
- facilità di accesso ed utilizzo;
- vendita ed attivazione standard.

In alcuni casi, soprattutto quelli relativi alla fatturazione elettronica PA, il \Rightarrow **Produttore** non interviene concretamente a confezionare i \Rightarrow **PdV** ed utilizza servizi applicativi di più alto livello forniti dalla stessa **CompEd Servizi**.

Nelle prossime sezioni vediamo quali funzioni organizzative intervengono a gestire i processi rilevanti per i servizi di conservazione

Torna al [sommario](#)

5.2.2 La funzione Marketing/Commerciale

La messa a punto di una modalità di servizio pacchettizzata parte in generale da un'iniziativa del *Marketing*, che – a seguito di confronti e consultazione con altre funzioni – progetta un pacchetto di servizi.

Per quanto riguarda gli aspetti peculiari della conservazione tale consultazione/approvazione avviene con \Rightarrow **RSC** e \Rightarrow **RSM**, in modo da assicurare la coerenza del progetto.

Importante, a questo livello, è anche la consultazione con lo Studio Legale convenzionato che in ogni caso deve approvare le modalità di erogazione e presentazione dei servizi, avuto riguardo a tutta la normativa vigente.

Sempre questa funzione è responsabile della regia, dell'entrata in produzione dei servizi (dopo valutazione ed approvazione) a seguito dello sviluppo.

La funzione Marketing/Commerciale (in effetti un insieme di persone competenze e responsabilità in queste due aree) non è rappresentata direttamente tra i ruoli "istituzionali" del \Rightarrow **SdC** elencati nella sezione [Ruoli e Responsabilità](#), ma è indicata [nell'organigramma](#) come una funzione esterna.

Torna al [sommario](#)

5.2.3 La funzione Progettazione e Sviluppo

Sulla base dei pacchetti disegnati dalla funzione Marketing/Commerciale è compito di **⇒ RSC** e **⇒ RSM**, che costituiscono la funzione Progettazione e Sviluppo, progettare e realizzare le componenti applicative necessarie ad erogare il pacchetto di servizi, incluse le funzioni di vendita automatizzate e di **⇒ provisioning**.

Il progetto è descritto nei dettagli al [Marketing/Commerciale](#) e – solitamente – al CdA; dopo l'approvazione si avvia l'effettivo sviluppo, quindi la messa in opera in ambiente di stage, il *testing/debugging*, infine il passaggio in produzione, sempre sotto la regia della funzione Marketing/Commerciale.

Oltre a queste attività connesse con l'entrata in servizio di nuovi pacchetti, questa funzione ha le seguenti responsabilità:

- consultazione con la funzione commerciale nell'analisi di requisiti di clienti speciali e definizione di preventivi e specifiche di dettaglio per servizi custom (supporto *pre-sale*);
- consultazione con **⇒ Esercizio** per l'analisi di problemi e soluzioni di anomalie;
- consultazione con **⇒ RSC** per la pianificazione e progettazione di evoluzioni ed estensioni;
- consultazione con **⇒ RSI** per la valutazione di impatti ed opportunità di evoluzioni sugli aspetti tecnologici diversi dal software applicativo;
- realizzazione di ogni **⇒ release** o **⇒ patch** per i componenti del sistema.

Torna al [sommario](#)

5.2.4 La funzione Esercizio

Questa funzione, è responsabile della gestione del funzionamento dell'intero sistema. Governata da **⇒ RSI**, che risponde a **⇒ RSC**, presiede a:

- Monitoraggio dei sistemi, dei processi e dei componenti
- Supervisione dei log e dei messaggi di errore e notifica
- Controllo dei flussi di **⇒ Ingest**
- Controllo delle procedure schedate (in particolare la produzione di **⇒ PdA [AIP]**)
- Eventuale produzione assistita di **⇒ PdD [DIP]** dalle caratteristiche particolari
- Controllo di replica automatica e backup

- Gestione di tutte le procedure di emergenza ed interventi di fix su anomalie

Nei casi di servizi *custom*, ossia diversi dai pacchetti standardizzati, interviene anche attivamente nel [=> provisioning](#), ossia nell'istanziamento e configurazione di tutti i componenti e moduli necessari all'erogazione del servizio stesso.

Torna al [sommario](#)

5.2.5 Helpdesk

Questa funzione è erogata dagli [=> Operatori Helpdesk](#) che erogano il servizio di supporto di primo livello agli utenti.

In generale tale servizio è disponibile telefonicamente e via email; per le problematiche "semplici" (ossia quelle risolvibili correggendo gli errori operativi commessi dagli utenti stessi, o fornendo indicazioni che gli utenti non cercano/trovano autonomamente nella documentazione d'uso) gli operatori Helpdesk provvedono in prima persona. Per i problemi più complessi si aprono ticket verso agli [=> operatori IT](#) che, all'occorrenza, eseguono l'escalation sino ai livelli superiori.

Torna al [sommario](#)

6 Oggetti Sottoposti a Conservazione

In accordo con il [modello OAIS](#) e con le [=> Regole Tecniche](#) sistema Il Sistema di Conservazione di **CompEd Servizi** organizza gli oggetti conservati in unità chiamate [=> pacchetti informativi \[Information Package\]](#).

In particolare si individuano:

- Pacchetto di Versamento – [=> PdV \[SIP\]](#)
- Pacchetto di Archiviazione – [=> PdA \[AIP\]](#)
- Pacchetto di Distribuzione – [=> PdD \[DIP\]](#)

Nelle prossime sottosezioni approfondiamo strutture e scopi di queste unità.

Con particolare riguardo ai Formati documentali ammessi, si precisa che i formati specifici sono concordati con il Produttore e sono oggetto del documento **specificità del contratto**.

Tuttavia valgono alcune regole generali, applicabili dove non diversamente concordato con il produttore.

In primo luogo si osserva che il linea di principio il sistema può gestire qualunque tipologia di dati binari, che vengono immessi, gestiti e restituiti senza restrizioni, ma con ovvie limitazioni riguardo alla relativa possibilità di presentazione con gli strumenti.

Il sistema si affida, per la presentazione, ad un sottosistema denominato **DigitalSign Cloud**: si tratta di una *web application* fruibile da qualunque piattaforma operativa, dedicato a presentare i documenti mediante un rendering in formato immagine che esegue anche l'analisi e la verifica delle eventuali firme digitali apposte al documento.

Si precisa, tuttavia, che il sistema consente di scaricare localmente una copia di ogni oggetto, lasciando quindi all'Utente la libertà di utilizzare qualunque strumento di fruizione/visualizzazione, a partire da quelli di pubblico dominio come Adobe Acrobat/Reader e dagli strumenti integrati nei sistemi operativi, sino a qualunque applicazione specializzata.

Tornando allo strumento integrato nel sistema (**DigitalSign Cloud**) esso è in grado di gestire alcuni formati nativi:

- i. PDF e PDF/A (conformi allo standard ISO/IEC 32000-1:2008)
- ii. XML privi di foglio di stile
- iii. XML che richiedono i fogli di stile ufficiali per la FatturaPA italiana (fatture versioni 1.0 e 1.1, notifiche versione 1.0)

Allo stato attuale il sistema non gestisce i collegamenti diretti a diversi fogli di stile richiamati dal documento stesso, ma su richiesta del cliente è possibile configurare l'uso di fogli di stile particolari come è stato fatto per le fatture.

Per tutti gli altri formati il sistema si appoggia su una preconversione automatica in PDF, utilizzando lo strumento open source LibreOffice. La lista dei formati supportati è documentata qui: https://en.wikipedia.org/wiki/LibreOffice#Supported_file_formats

Questo viewer può gestire (presentare) sia documenti informatici sottoscritti che non sottoscritti. Per quanto riguarda i primi, alla data del presente documento sono accettati tutti i formati descritti nella Delib. CNIPA 45 del 21 Maggio 2009. In particolare i formati CADES, PAdES e XAdES.

Torna al [sommario](#)

6.1 Oggetti conservati

⇒ **Century** è in grado di acquisire (tramite la funzione ⇒ **Ingest**) pacchetti di informazione (nella forma di ⇒ **PdV** [SIP] il cui contenuto informativo [**Content Information**] può essere costituito da qualunque contenuto binario.

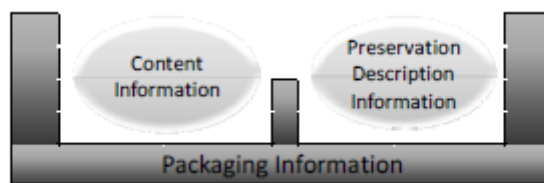


Fig. 4 – Package Information (figura tratta direttamente dallo standard OAIS)
Struttura generale di un pacchetto di informazione

Tuttavia, al fine di consentire la fruizione dei contenuti nel tempo, è indispensabile che l'accordo con il cliente (⇒ **Produttore** [**Producer**]) delimiti le tipologie di contenuti ammesse, descrivendo quindi la comune *knowledge base* relativa a tali contenuti.

Il ⇒ **Regolamento di Servizio**, dunque, descrive i formati ammessi per gli oggetti immessi nel sistema attraverso i ⇒ **PdV**.

Si noti che in alcuni casi tali oggetti, pur essendo forniti – direttamente o indirettamente – dal ⇒ **Produttore**, possono avere una provenienza esterna. È il caso, per esempio, delle fatture elettroniche ricevute da una PA: il **Produttore** è l'ente cessionario/committente che riceve la fattura e la affida a **CompEd Servizi** per la conservazione, ma il documento proviene dal suo cedente/prestatore attraverso un *Sistema Di Interscambio*.

Ebbene, in questo caso il controllo sui formati non è totale nemmeno da parte del **Produttore**, occorre dunque tenere conto di questo contesto. In particolare gli strumenti di presentazione di **Century** possono gestire un certo numero di formati documentati; qualora il documento contenesse un allegato di tipo imprevisto il sistema potrebbe certo esportarlo, ma potrebbe non essere in grado di visualizzarlo direttamente.

Torna al [sommario](#)

6.2 Pacchetto di versamento – PdV [SIP]

Il software applicativo ⇒ **Century**, in considerazione della sua architettura modulare, in generale può montare – al di sopra dell'unità funzionale ⇒ **Ingest**, un numero indefinito di interfacce (definite ⇒ **Moduli di Input**) attraverso le quali i ⇒ **Produttori** possono sottoporre i ⇒ **PdV** [SIP].

Questo significa che il formato dei **PdV [SIP]** può variare da una tipologia di servizio all'altra, come pure da commessa a commessa, in base a specifici accordi con il Cliente/**Produttore**.

Si noti che anche la modalità di sottomissione del **PdV [SIP]** influisce sul formato. Per maggiori dettagli su questo concetto si veda la sezione [Modalità di acquisizione](#).

Riguardo alle tipologie di **PdV** accettate, va precisato che una larga parte dei clienti del servizio di conservazione è anche cliente del servizio di Fatturazione Elettronica PA. In questo caso non è effettivamente il Produttore che confeziona materialmente gli oggetti destinati alla Conservazione, ma:

- i. nel caso della fatturazione ATTIVA (verso la PA) è il software della stessa CompEd Servizi che confeziona le fatture, le firma digitalmente, le recapita attraverso il Sistema di Interscambio, infine le versa nel [=> SdC](#) insieme a ricevute e notifiche;
- ii. nel caso di fatturazione PASSIVA (ricevute da un ente PA) addirittura le fatture provengono dal Sistema di Interscambio al sistema di CompEd Servizi, quindi automaticamente destinate alla conservazione.

A questi casi emblematici si aggiungono diversi casi in cui CompEd Servizi offre ad utenti di piccole dimensioni e limitate capacità informatiche la possibilità di immettere i propri documenti manualmente, attraverso interfacce web molto facili. Ad esempio è in essere un servizio per commercialisti che immettono le scritture contabili dei propri clienti, con un meccanismo analogo a quello delle fatture: una interfaccia web guidata sullo steso portale di erogazione dei servizi.

Quindi, in generale al Produttore non è richiesta la produzione formale di un **PdV**, che invece è confezionato autonomamente dai sistemi – sempre di CompEd Servizi – che interfacciano i clienti.

Ai clienti è invece sempre possibile accedere ai contenuti del [=> RdV](#).

Una casistica diversa rispetto alla pura interfaccia web è un servizio offerto a *software house* e *system integrator*: in questi casi il rapporto contrattuale è in generale con un fornitore (di software o di servizi) che si fa carico del confezionamento del **PdV** e di immetterlo nel **SdC** di CompEd Servizi mediante una interfaccia applicativa ([=> A2A](#)), ad oggi sempre basata su protocollo SOAP.

Le specifiche concordate con il cliente documentano in dettaglio la modalità di immissione di oggetti (documenti e metadati), nonché la modalità di recupero immediatamente successivo del **RdV** e/o delle informazioni diagnostiche.

Il documento **Specificità del Contratto**, in tali casi, descrive sia il formato dei dati immessi, sia quello del **RdV** di ritorno.

Torna al [sommario](#)

6.3 Pacchetto di Archiviazione - PdA [AIP] e relativo indice IPdA

Il [=> PdA \[AIP\]](#) è l'unità di informazione fondamentale per la conservazione.

In generale un **PdA** rappresenta un insieme di documenti, di pertinenza di un [=> Canale](#) di conservazione, costituendo un segmento temporale dell'archivio conservato.

Tecnicamente si tratta di un insieme di file, organizzati in un set di cartelle di *file system* (memorizzate nel [=> Archival Storage](#)) secondo una strategia che ottimizza le prestazioni di accesso ai singoli oggetti, completati da un [=> IPdA](#) - Indice del Pacchetto di Archiviazione (che costituisce la **PDI** – **Preservation Description Information** prevista dal modello [=> OAIS](#)).

Tale **IPdA** – strutturato in piena conformità allo standard **UNI-SInCRO** come richiamato dalle [=> Regole Tecniche](#), tra l'altro:

- contiene informazioni per identificare il [=> Produttore](#) che ha originato gli oggetti contenuti [[=> Provenance](#)];
- contiene informazioni identificative del canale e della collocazione del **PdA** nel **Canale** [[=> Context](#)], con intrinseca definizione dei diritti di fruizione [[Access Rights](#)];
- contiene un riferimento a ciascun oggetto conservato, consentendone l'univoca identificazione e l'automatico reperimento [[=> Reference](#)];
- contiene il valore [=> hash](#) di ogni oggetto, consentendo in ogni istante la verifica di integrità [[=> Fixity](#)];
- contiene l'intero set di [=> metadati](#) associati a ciascun oggetto.

L'intero **IPdA**, in accordo con le **Regole Tecniche**, è [=> firmato digitalmente](#) da [=> RSC](#) (o da soggetto validamente delegato da **RSC**, si veda in proposito la [tabella aggiornata dei ruoli di Administration](#)) e contestualmente corredato di una [=> Marca Temporale](#) per fissare l'istante di firma in modo opponibile ai terzi.

Torna al [sommario](#)

6.3.1 Struttura del PDA con IPdA in formato SInCRO

Ferma restando la piena conformità del IPdA allo standard UNI-SInCRO, i dettagli dell'utilizzo degli elementi MoreInfo per ospitare i metadati di ciascuna tipologia documentale e l'uso degli elementi Agent per ospitare la catena di delega nonché per identificare il Produttore sono analizzati nell'allegato [Specificità del contratto](#).

Torna al [sommario](#)

6.4 Pacchetto di distribuzione – PdD [DIP] e relativo indice IPdD

Sono previste diverse tipologie di \Rightarrow PdD [DIP]

- I. PdD destinato all'esportazione di un intero \Rightarrow PdA [AIP] – in questo caso lo scopo della produzione del PdD è l'esportazione di un intero Pacchetto di Archiviazione; la finalità può essere ad esempio la migrazione verso un diverso Conservatore, la fornitura della copia di un PdA allo stesso Cliente per propri scopi di consultazione/archiviazione privata, ecc.

In questo caso il contenuto del PdD coincide esattamente con quello del PdA, di fatto ne è un *duplicato informatico*.

- II. PdD strutturato, ottenuto per estrazione – in questo caso il contenuto non coincide con quello di un PdA, ma è il risultato di una estrazione da uno o più PdA (comunque appartenenti ad uno stesso \Rightarrow Canale); la qualifica di "strutturato" indica che la forma è la stessa del PdA, quindi corredata di un indice (che in questo caso è denominato \Rightarrow IPdD – Indice Pacchetto di Distribuzione) che ha lo stesso formato \Rightarrow UNI-SInCRO, ma reca precise indicazioni sulla natura di un PdD rispetto a quella di un PdA.

La \Rightarrow firma qualificata (di \Rightarrow RSC o suo delegato) e l'eventuale \Rightarrow marca temporale associate a questo IPdD sono apposte al momento della produzione del PdD stesso.

Torna al [sommario](#)

7 Il Processo di Conservazione (PdC)

Il Processo di Conservazione è affidato, sul piano tecnologico, al software di conservazione denominato **Century**, di **CompEd**.

Century è una implementazione rigorosa dei processi delineati nel [modello di riferimento OAIS](#) e calati nella definizione delle \Rightarrow Regole Tecniche.

Century è un sistema integrato che gestisce flussi di conservazione per una molteplicità di clienti (\Rightarrow Produttori e \Rightarrow Utenti), attraverso una architettura basata sulla gestione indipendente di una molteplicità di \Rightarrow Canali.

I **Canali** sono in generale strumenti "astratti", che possono modellare diverse realtà applicative, ma in prima approssimazione ogni **Canale** è utilizzato per gestire flussi di documenti appartenenti ad uno specifico Cliente, di una determinata tipologia documentale. In altre parole:

- ogni cliente si vedrà assegnare almeno un **Canale**;
- se un cliente, per qualsiasi ragione, ha necessità di gestire flussi documentali separati avrà a disposizione più **Canali**.

Ogni **Canale** prevede, all'interno del sistema:

- un riferimento ad un set di informazioni anagrafiche (che collega il **Canale** ad uno specifico cliente);
- un set di informazioni di configurazione struttura (che definisce i \Rightarrow **metadati** associati ed altre informazioni specifiche sulle modalità di trattamento) [\Rightarrow **schemi**];
- un set di informazioni di configurazione procedurale (che definisce i parametri di funzionamento dell'accumulo, gli eventi che provocano il confezionamento del \Rightarrow **PdA**, ecc.) [\Rightarrow **policy**];
- un'Area di Accumulazione \Rightarrow **AA** (dove confluiscono i \Rightarrow **PdV** [**SIP**], accumulando gli oggetti che verranno sigillati in un **PdA** [**AIP**]);
- una sequenza di **PdA** [**AIP**], indefinitamente lunga, che costituisce la porzione di archivio conservato di pertinenza del **Canale**.

Lo schema sottostante fornisce un'idea visiva dell'organizzazione in **Canali**:

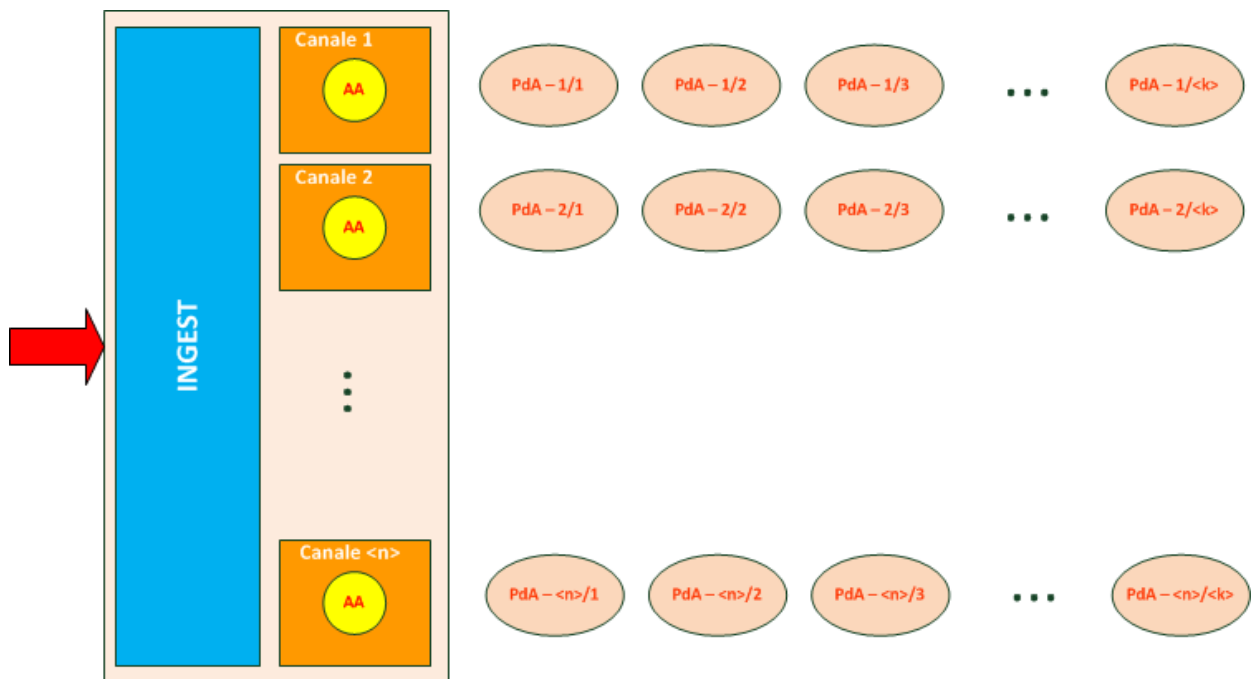


Fig. 5 – Ingest e Canali

Schema logico dell'organizzazione in Canali delle informazioni gestite dal Sistema di Conservazione

L'entità funzionale \Rightarrow **Ingest** (attraverso i diversi \Rightarrow **Moduli di Input**) riceve i **PdV** [**SIP**] dai diversi \Rightarrow **Produttori**, risolve il **Canale** di destinazione ed accumula i contenuti di ciascun pacchetto nella **AA** associata al **Canale** appropriato.

Da qui la funzione **Generate AIP** (interna ad **Ingest**) genera – con il contenuto attuale della **AA**, ed al verificarsi dell'evento \Rightarrow **trigger** codificato nella **policy** – un nuovo **PdA** [**AIP**], mentre la **AA** del **Canale** si svuota, pronta ad accogliere i nuovi **PdV** [**SIP**].

Il **PdA** [**AIP**] così creato va ad aggiungersi alla sequenza di **PdA** che costituisce il patrimonio informativo di quello specifico **Canale**.

Torna al [sommario](#)

7.1 Modalità di acquisizione dei Pacchetti di Versamento per la loro Presa in Carico

In accordo con il [modello di riferimento OAIS](#), l'entità funzionale che acquisisce i \Rightarrow **PdV** [**SIP**] è denominata \Rightarrow **Ingest**.

La figura qui sotto illustra le funzioni logiche dell'**Ingest**, sempre come definite nello standard **OAIS**:

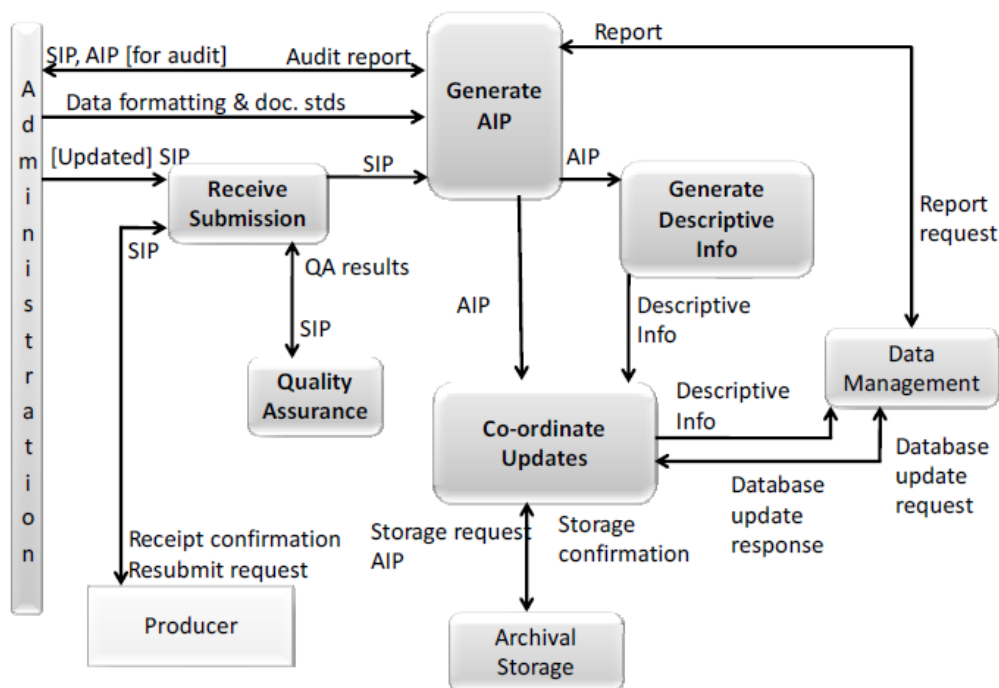


Fig. 6 – *Ingest* (figura tratta direttamente dallo standard **OAIS**)

Diagramma delle funzioni logiche dell'entità funzionale **Ingest**

Century, grazie alla sua architettura molto modulare, mette a disposizione diversi \Rightarrow **Moduli di Input** che rappresentano altrettante interfacce per l'immissione dei **PdV** [**SIP**]:

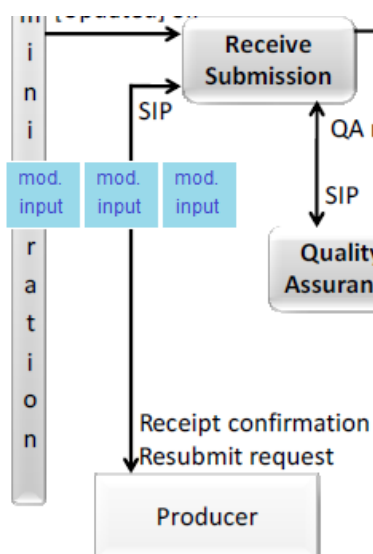


Fig. 7 – I moduli di Input
 Dettaglio della funzione **Ingest** che evidenzia i Moduli di Input di **Century**

Come spiegato nella [sezione dedicata alle modalità di commercializzazione](#), **CompEd Servizi** offre ai propri clienti diversi pacchetti di servizio, che in generale prevedono modalità standard di erogazione e, dunque, fanno riferimento a [=> moduli di input](#) standard (ad esempio, la fatturazione elettronica passiva prevede un modulo di input specifico che preleva i documenti dal database del Portale di Fatturazione PA e li organizza in veri e propri [=> PdV](#), mentre i [=> RdV](#) di ritorno vengono acquisiti dal portale che ne mette le relative informazioni a disposizione degli utenti del servizio).

In altri casi, quando il servizio di conservazione è erogato in modalità *custom*, in fase di negoziazione si mette a punto un documento di specifiche che descrive dettagliatamente i formati del **PdV** e del **RdV**.

In generale un **PdV** [**SIP**] contiene – oltre alla **Content Information** oggetto del versamento (ossia il documento o comunque l'oggetto della conservazione), secondo la terminologia [=> OAIS](#), alcuni elementi di informazione supplementare:

- info di [=> Provenance](#) – elementi di informazione che consentano di identificare il [=> Produttore](#). Queste informazioni potrebbero anche essere intrinseche, ad esempio derivando dall'autenticazione su un servizio esposto in rete;
- info di [=> Context](#) – talvolta, nel traffico prodotto da uno stesso **Produttore**, è necessario distinguere tra diversi [=> Canali](#) assegnati a tale Produttore, come destinazione di un particolare **PdV**;
- info di [=> Reference](#) – al contenuto sono sempre associati alcuni [=> metadati](#), che in generale includono sia elementi utili alla ricerca strutturata, sia estremi di riferimento ed identificazione di ogni documento;

- info di [=> Fixity](#) – al **Produttore** è in genere richiesto di dichiarare alcune informazioni che permettano di verificare l'integrità degli oggetti sottomessi; in taluni casi tali informazioni sono costituiti da una firma digitale, altre volte tra i metadati si include un valore di hash; in caso di trasferimenti basati sulla [=> PEC](#) la **fixity** è implicitamente assicurata dalla firma elettronica apposta dal gestore **PEC** sul messaggio.

L'evento "versamento" è registrato ad almeno due livelli:

- a) in un registro di eventi di sistema, affidato al DB, che traccia ogni operazione di immissione **PdV**
- b) nei log del modulo di input (allo stato attuale è un front-end di accettazione) che traccia i dettagli su utenza, tipo di operazione, documento sottomesso, data e ora

Riguardo alle modalità fisiche di sottomissione di oggetti da conservare, tenendo presente quanto [già introdotto riguardo alla natura dei PdV gestiti](#), si precisa quanto segue:

- I. nel caso di immissione diretta da parte di altri sistemi applicativi CompEd Servizi (ad esempio i servizi di Fatturazione Elettronica PA e di conservazione di scritture contabili) l'immissione avviene attraverso collegamenti telematici, su [=> VPN](#);
- II. nel caso di immissione da parte di Produttori si utilizza ancora una connessione telematica via Internet, comunque sempre su protocollo HTTPS e da parte di utenti autenticati. Opzionalmente al cliente si offre la possibilità di stabilire un circuito **VPN**;
- III. nei casi straordinari di immissione diretta di grandi quantità di dati (circostanza fino ad oggi non verificatasi) è possibile accettare consegne di supporti fisici. In tali casi si assume una consegna diretta dal Produttore, senza intermediari; qualora il ricorso a corrieri sia inevitabile si predilige l'utilizzo di supporti quali hard disk che consentano la crittografia dei dati e si utilizzeranno esclusivamente fornitori approvati da [=> RSC](#); in ogni caso le etichette sui supporti saranno codificate, evitando qualunque riferimento che permetta l'identificazione del Produttore o di una specifica tipologia di dati.

Per ogni PdV acquisito il sistema crea una registrazione di log in cui traccia le informazioni salienti:

- indicazione data/ora
- identificazione del modulo di input (quindi della tipologia di PdV)
- identificazione del produttore e del canale di assegnazione
- estremi di identificazione (ID assegnato dal sistema, eventuale source-id)

Torna al [sommario](#)

7.2 Verifiche effettuate sui Pacchetti di Versamento (PdV) e sugli oggetti in essi contenuti

Con riferimento allo schema \Rightarrow **OAIS** richiamato nella [sezione precedente](#) a proposito dell'entità funzionale \Rightarrow **Ingest**, il sistema implementa una funzione di \Rightarrow **Quality Assurance** che ha lo scopo principale di validare un \Rightarrow **PdV [SIP]** sottomesso dal \Rightarrow **Produttore**:

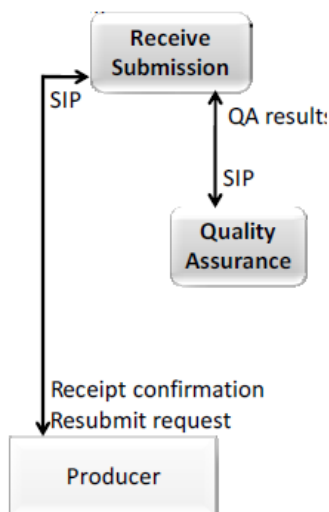


Fig. 8 - Quality Assurance (figura tratta direttamente dallo standard **OAIS**)
 Dettaglio della funzione Quality Assurance nell'ambito dell'entità funzionale Ingest

Sempre ricordando che la funzione **Receive Submission** in \Rightarrow **Century** è implementata da un *array* di \Rightarrow **Moduli di Input** che realizzano diverse interfacce opzionali, l'effettiva \Rightarrow **presa in carico** di un **PdV [SIP]** è condizionata al positivo risultato di una azione di verifica (\Rightarrow **Quality Assurance**).

Le verifiche sono eseguite dal sistema contestualmente all'immissione di un **PdV**: il sistema genera una registrazione di log subito dopo l'acquisizione, indicando l'inizio delle verifiche.

I controlli effettuati, nel dettaglio possono differire secondo l'interfaccia di input attraverso cui avviene la sottomissione del **PdV [SIP]**, ma in generale si esegue:

1. verifica di correttezza formale – il sistema verifica che la struttura dati fatta pervenire all'ingresso sia coerente con le specifiche e sia quindi possibile passare all'estrazione semantica dei contenuti;
2. verifica della \Rightarrow **Provenance** – la verifica di riconoscimento del **Produttore** che sottomette il **PdV** può avvenire in modi diversi in funzione della modalità di immissione.

Ad esempio, i moduli che prevedono il collegamento diretto \Rightarrow **A2A** con il sistema del **Produttore** risolvono di regola questo riconoscimento intrinsecamente, a livello dell'autenticazione sul protocollo di comunicazione e/o tramite la \Rightarrow **VPN** utilizzata per la connessione.

I collegamenti basati sulla [=> PEC](#) usano l'indirizzo **PEC** del mittente – unitamente alla verifica della firma del gestore **PEC** sui messaggi che veicolano i **PdV** – come chiave di autenticazione.

Modalità *custom* più aperte possono prevedere che le strutture dati contenenti i **PdV** siano [=> firmate digitalmente](#) mediante un [=> certificato](#) (eventualmente [=> qualificato](#)) appartenente ad una lista concordata in fase contrattuale.

3. verifica di [=> Reference](#) – il sistema verifica che il set di [=> metadati](#) fornito con il **PdV** corrisponda alle specifiche e codificate nel profilo di configurazione del [=> Canale](#). Le specifiche possono indicare **metadati** obbligatori ed opzionali, come pure restrizioni sui valori presentati da ciascun **metadato** (sia sul piano sintattico che su quello della valorizzazione, come per esempio l'univocità di un identificatore);
4. verifica della [=> Fixity](#) – quale che sia la modalità di identificazione del contenuto (dichiarazione di un valore di [=> hash](#), [=> firma digitale](#) del **PdV** da parte del **Produttore**, affidamento alla **PEC**) il sistema verifica la corrispondenza del contenuto al dato di protezione fornito, calcolando l'**hash** e confrontandolo con il dato dichiarato, oppure effettuando una vera e propria [=> verifica della firma](#) (del **Produttore** o del gestore **PEC**).

In taluni casi (specie se i dati sono originati direttamente da un altro sistema di **CompEd**) il **PdV** non contiene un'informazione aggiuntiva all'origine, mentre il controllo di integrità è eseguito a posteriori dal sistema produttore sulla base del codice **hash** che il sistema inserisce nel [=> RdV](#);

5. verifica dei documenti informatici – per i **PdV** che contengono documenti informatici sottoscritti viene eseguita una [=> verifica](#) puntuale di tutte le [=> firme](#) presenti. Si noti che questa firma non va confusa con quella eventualmente utilizzata per assicurare la **Fixity**, trattata al punto precedente. Se il [=> Regolamento di Servizio](#) indica restrizioni rispetto ai sottoscrittori ammessi per un dato canale, anche l'identità del soggetto sottoscrittore viene verificata contro la lista dei sottoscrittori; inoltre può essere prevista una restrizione sulla validità residua del [=> certificato](#) di firma, l'accettazione o meno di certificati diversi da quelli qualificati Italiani, ecc.;
6. verifica del formato – il sistema identifica il formato di ogni documento contenuto nel **PdV** e verifica che tale formato – per tutti i documenti – corrisponda alle restrizioni eventualmente stabilite in fase contrattuale e codificate nel profilo di configurazione del canale.

Le verifiche qui descritte sono eseguite in sequenza. Il primo risultato negativo in una sequenza di verifica implica l'interruzione della sequenza stessa e l'esito negativo.

Le prossime due sottosezioni illustrano il comportamento del sistema nei due casi (accettazione e rifiuto)

Come detto all'inizio di questa sezione, il sistema registra nel log l'inizio di questa fase di verifiche. L'esito delle verifiche è diverso secondo che le verifiche siano superate o meno, pertanto la registrazione nel log è descritta separatamente nelle prossime sezioni, nel caso di [accettazione](#) o di [rifiuto](#).

Torna al [sommario](#)

7.3 Accettazione dei PdV e generazione del RdV

Se tutte le verifiche descritte nella sezione precedente sono superate con successo il [=> PdV \[SIP\]](#) è accettato dal sistema.

In questo caso viene generato un [=> Rapporto di Versamento \(RdV\)](#), ritornato al [=> Produttore](#), che attesta l'effettiva [=> presa in carico](#) da parte del [=> SdC](#) (in accordo con le [=> Regole Tecniche](#), art. 9 comma 1 lettera 'd').

Il formato specifico del **RdV**, nonché la modalità di consegna dello stesso al **Produttore** dipendono strettamente dalla modalità di interfaccia ([=> Modulo di Input](#)) adottata nel caso specifico, quindi è documentata negli allegati del [=> Regolamento di Servizio](#) o – nel caso di servizio applicativo erogato da un sistema CompEd (ad esempio nel caso di fatturazione elettronica PA) – nella documentazione tecnica del prodotto/servizio.

In generale il **RdV** contiene sempre questi elementi di informazione:

- estremi identificativi del **PdV [SIP]** a cui il **RdV** è riferito
- identificatore univoco assegnato al **RdV**
- riferimento temporale [=> UTC](#) corrispondente alla generazione del **RdV**
- riferimenti ai documenti contenuti nel **PdV [SIP]** e relativi valori [=> hash](#)

In talune circostanze, eventualmente concordate nel **Regolamento di Servizio**, il **RdV** può essere corredato da una [=> firma elettronica qualificata](#), apposta con procedura automatica, da parte di [=> RSC](#).

L'operazione di accettazione è registrata nel registro di sistema sul database, mentre il **RdV** è immesso nel [=> Giornale di Controllo](#) a testimoniare l'avvenuta acquisizione del **PdV**.

Di seguito un esempio di singola registrazione di un PdV, che fornisce alcuni dettagli sul pacchetto stesso:

```

Data/ora versamento 18/12/2015 16:09
      Stato Conservato
      Sistema CompEd Century
      Dominio CS
      Id dominio 1
      Storage main
      Storage id 1
      Canale U03965190659_fe_2012_x_03587610613
      Id canale 1615
      Id pacchetto 4916
      Id Volume 1619
      Nome Volume U03965190659_fe_2012_x_03587610613-800
      Percorso Volume /fe/2012/U03965190659_fe_2012_x_03587610613-800
    
```

Fig. 9 – Pacchetto di Versamento
Esempio di dettagli di un PdV visualizzabili dall'utente

Ad un livello più interno è possibile risalire – sempre dalla normale interfaccia utente di consultazione – tramite il registro (log) di sistema ad informazioni più dettagliate sugli oggetti che compongono un PdV, si veda questo esempio:

Storage uid	eb99695f-3dda-4ed4-a338-accb87f45fa9
Queue	U[redacted]_fe_2012_x_03587610613
Queue id	1615
Packet id	4916
Uploaded time	2015-12-18T15:09:32.454Z

Documents					
Type	Id	Name	Content type	Hash function	Hash
Document metadata	DM_4916	doc_meta_[redacted].xml	text/xml	SHA-256	F3Amgw5gOT+0Zu6UvxEGowNRzS6ITGH9cR/s39ouWjU=
Part metadata	PM_12231	fattura_meta_[redacted].xml	text/xml	SHA-256	hj8AViUCx8QfuocrIPvNwhFmqMKWUESgBfMobjTrtE0=
Part data	PD_12231	fattura_[redacted].p7m	application/pkcs7	SHA-256	92mOJQ39H9M7hWX8rQq58vneRQdJZ38hhzMjDxj5U=
Part metadata	PM_12232	notifica_meta_[redacted].xml	text/xml	SHA-256	/Rox+zaBXqeZJR24tlmsCkYeBEKNB/ohGwzxfOAXZE=
Part data	PD_12232	notifica_[redacted].xml	text/xml	SHA-256	XnATwOoxcvQNOR5p4eodjzjXXbZn3BwkaieOcc7C8Is=
Part metadata	PM_12233	notifica_meta_[redacted].xml	text/xml	SHA-256	Fa/a2+QPOZqYoptl1jzvsHw/ct26wUolfaC87I4ukg0=
Part data	PD_12233	notifica_[redacted].xml	text/xml	SHA-256	oUEZoUfYyVT1iPLEjIrsBaBBE1oIj7IzJenpysgb0E=

Metadata	
document_id	38406
document_description	IT [redacted]

Fig. 10 – log di un Pacchetto di Versamento
Esempio reale (con informazioni anonimizzate) di un log di composizione di un PdV

Torna al [sommario](#)

7.4 Rifiuto del PdV e modalità di comunicazione delle anomalie

A seguito delle [verifiche descritte in una precedente sezione](#) il sistema può decidere di rifiutare un [⇒ PdV \[SIP\]](#).

Nel caso di un mancato superamento delle verifiche il sistema produce un [⇒ Rapporto di Rifiuto \(RdR\)](#) e lo consegna al [⇒ Produttore](#), anche in questo caso con modalità e formato strettamente dipendenti dalla tipologia di interfacciamento adottato, eventualmente descritte negli allegati del [⇒ Regolamento di Servizio](#).

In generale il **RdR** contiene i seguenti elementi di informazione:

- estremi identificativi del **PdV [SIP]** a cui il **RdR** è riferito (NOTA: nel caso di una grave non conformità di formato del **PdV** può essere impossibile estrarre questa informazione, quindi questo elemento sarà 'N/A')
- identificatore univoco assegnato al **RdR**
- riferimento temporale [⇒ UTC](#) corrispondente alla generazione del **RdV**
- informazioni diagnostiche sul motivo del rifiuto.

Anche il **RdR**, analogamente al **RdV**, può eventualmente essere corredato di [⇒ firma qualificata](#) di [⇒ RSC](#), in funzione degli accordi con il [⇒ Produttore](#) e della conseguente modalità di sottomissione concordata.

La circostanza del rifiuto, unitamente alle informazioni diagnostiche risultanti dalla verifica, è annotata nel registro (log) di sistema.

Il **RdR** non è indirizzato al [⇒ Giornale di Controllo](#) (poiché il contenuto del **PdV** rifiutato non entrano a far parte del patrimonio informativo), ma anche il front-end registra la circostanza.

Torna al [sommario](#)

7.5 Preparazione e gestione del Pacchetto di Archiviazione (PdA)

Nell'architettura di [⇒ Century](#), in accordo con il [modello OAIS](#), non esiste un vincolo rigido che impone la corrispondenza *uno a uno* tra un [⇒ PdV \[SIP\]](#) e un [⇒ PdA \[AIP\]](#).

Le esigenze incontrate dal lato del [⇒ Produttore](#) determinano il ritmo di sottomissione e le dimensioni (in termini di numero di oggetti contenuti) dei **PdV**, usualmente con modalità *asincrona* (ossia è il **Produttore** che decide liberamente quando è il momento di sottomettere un insieme di documenti nel **Sistema di Conservazione** in ragione della propria organizzazione e convenienza).

La costruzione dei **PdA** [AIP], invece, segue una strategia organizzativa strettamente connessa alla gestione dell'archivio e – non di rado – da vincoli esterni, di tipo giuridico o di opportunità, comunque diversi da quelli propri del ritmo di alimentazione.

Questa situazione è ben argomentata nella sezione 4.3.2 del modello \Rightarrow **OAIS** (*Data Transformations in the Ingest Functional Area*).

Nel nostro caso possiamo portare un paio di esempi, agli estremi opposti del campo di situazioni reali, utili a chiarire queste esigenze:

Esempio 1 – un piccolo artigiano emette occasionali fatture per servizi prestati al comune in cui opera. Ipotizziamo 1 fattura al mese, 12 in un anno.

La normativa fiscale prevede che le fatture siano materialmente conservate “entro tre mesi dalla scadenza del termine per la presentazione delle dichiarazioni annuali (ex art. 7, co. 4-ter D.L. n. 357/1994)”, quindi con cadenza annuale.

Allora, al fine di non produrre numerosi Pacchetti di Archiviazione costituiti da una sola fattura ciascuno, si configura questo canale a produrre il **PdA** in corrispondenza di una data scadenza temporale (annuale, per esempio il 22 dicembre), ma nel frattempo le fatture sono immesse nel sistema man mano che sono prodotte. Nell'intervallo di tempo tra la \Rightarrow **presa in carico** delle singole fatture e la creazione del **PdA** esse permangono nell'area di accumulazione (\Rightarrow **AA**) del canale, mentre il 22 dicembre tali fatture sono consolidate in un **PdA**.

Esempio 2 – una azienda sanitaria produce ed archivia grandi quantità di referti clinici ogni giorno, provenienti da diversi sistemi produttori che preferiscono immettere i documenti uno per volta, senza farsi carico di alcun contingentamento in **PdV** complessi.

Per avere più presto possibile il riferimento temporale opponibile ai terzi rappresentato dall'inclusione in un **PdA** l'azienda desidera che i referti vengano sigillati in un **PdA** almeno una volta al giorno (alle 23 di ogni notte); inoltre per ragioni di facilità di esibizione e trasferimento, si desidera che la dimensione massima di un **PdA** sia contenuta in 4,7 GB massimi (compatibile con supporti *low cost* come i DVD).

Allora i referti pervengono in **PdV** di un solo documento ciascuno, sono accumulati (nella **AA**) sino al raggiungimento della dimensione massima configurata (es. 4 GB netti) oppure sino alla scadenza dell'orario giornaliero prefissato. Quindi il contenuto della **AA** è consolidato in un **PdA** alle 23.00, oppure al superamento della soglia dimensionale dei 4GB.

Consideriamo dunque questa porzione dell'unità funzionale \Rightarrow **Ingest**:

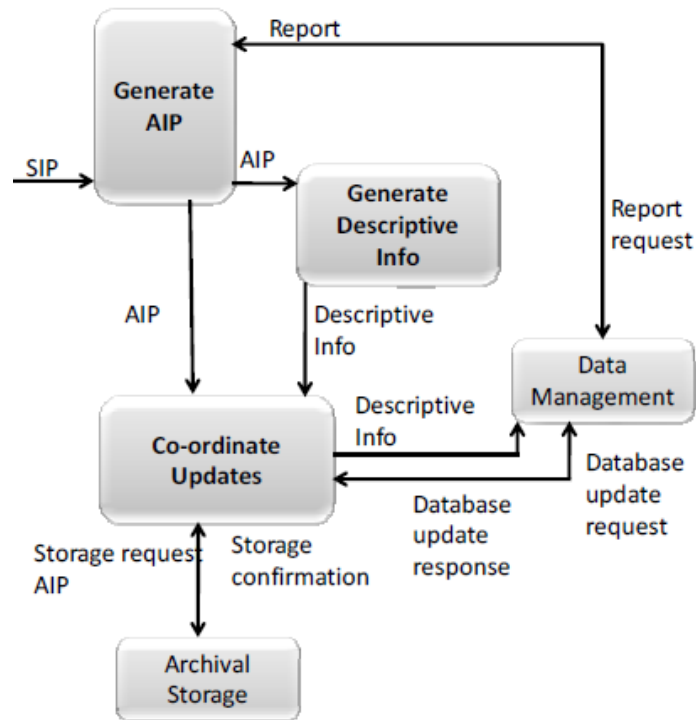


Fig. 11 - generazione PdA [AIP] (figura tratta direttamente dallo standard OAIS)
 Dettaglio della entità funzionale Ingest relativamente alla generazione di un PdA

Come si vede da questa figura è la funzione **Generate AIP** a porre in atto la logica di accumulazione dei PdV [SIP] nella \Rightarrow AA e successivo consolidamento un nuovo PdA [AIP]. Se consideriamo la [figura che illustrava il concetto dei canali](#) e immaginiamo di zoomare ad un maggior livello di dettaglio, esaminando un solo \Rightarrow canale, questa funzione opera così:

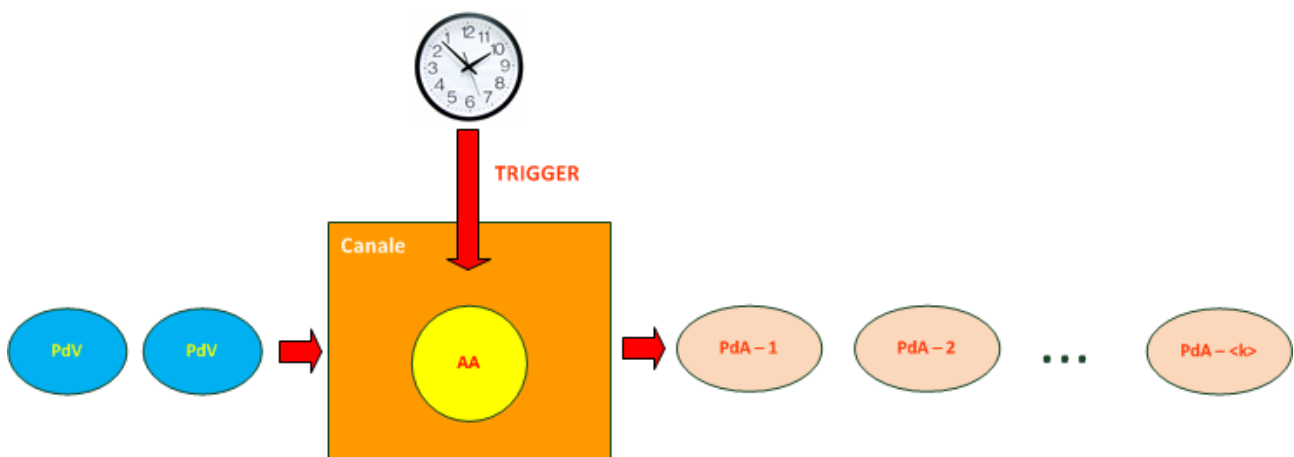


Fig. 12 – Evento trigger
 Schema logico di funzionamento della generazione di PdA a partire dai PdV

I **PdV** provenienti dal **Produttore**, già presi in carico dal **SdC** e già confermati mediante gli appropriati **RdV**, confluiscono in una **Area di Accumulazione (AA)**.

In questa **AA** il sistema già organizza progressivamente gli oggetti estratti da ciascun **PdV** nella forma che costituisce il **PdA**, provvedendo (tramite la funzione **Data Management**) ad aggiornare le tabelle del database con tutti i **metadati** e le altre informazioni di riferimento relative a ciascun oggetto.

Al momento in cui si verificano le condizioni codificate nella **policy** associata al **Canale** – cioè scatta l'evento **trigger** – si eseguono i seguenti passi (*processo di "Chiusura"*):

1. Il contenuto di **AA** viene riletto e verificato, rispetto al contenuto del DB (verifica integrità); in caso di anomalie si solleva un'eccezione urgente nei confronti degli amministratori di sistema e di **RSC**, che prende le opportune misure.
2. Si produce il file **IPdA** (Indice del Pacchetto di Conservazione) in formato **UNI-SInCRO**
3. Si dispone la sottoscrizione del **IPdA** (in genere una **firma qualificata** apposta con procedura automatica da **RSC**, se non diversamente specificato – per servizi *custom* – nel **Regolamento di Servizio**)
4. Si registra il **PdA** come appartenente al proprio **Canale**.

Torna al [sommario](#)

7.6 Esibizione: Preparazione e gestione del Pacchetto di Distribuzione

Come evidenziato dal [modello di riferimento OAIS](#), il servizio prestato ai **Consumer** (ossia agli **Utenti**, in base alla trasposizione nelle **Regole Tecniche** di questo modello) è una delle attività fondamentali di un **SdC**: una volta che gli oggetti sono immessi nel sistema e che il sistema provvede ad organizzarne la tenuta nel tempo, gli **Utenti** effettuano un'attività più o meno regolare di consultazione.

Il processo tramite il quale questa consultazione è posta in essere si definisce **Esibizione**.

Sempre in accordo con il modello **OAIS** tale processo compete all'entità funzionale **Access**:

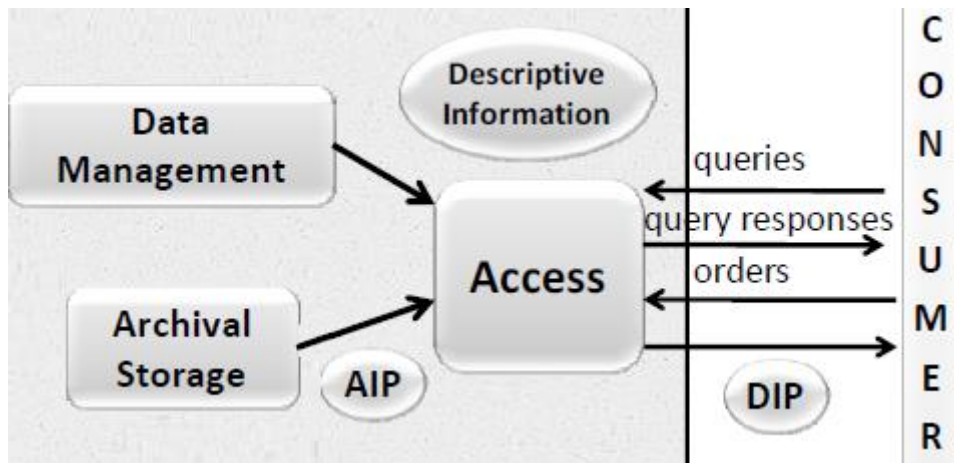


Fig. 13 - Access (figura tratta direttamente dallo standard OAIS)
 Dettaglio del modello di riferimento OAIS relativo all'entità funzionale Access

In termini assolutamente generali gli **Utenti (Consumer)** interagiscono con il sistema sottomettendo \Rightarrow **queries** (cioè **interrogazioni**) ed ottenendo risposte a tali interrogazioni. Da queste risposte l'utente può limitarsi a visualizzare/stampare/esportare semplici copie dei documenti, oppure far seguire veri e propri \Rightarrow **orders** (**ordini**) che determinano la produzione di \Rightarrow **Pacchetti di Distribuzione - PdD [DIP]**.

Naturalmente, come evidenziato dalla figura, l'entità **Access** è alimentata sia dall'entità \Rightarrow **Data Management** (che possiamo considerare, in modo semplificato, come la logica che circonda il database di supporto e fornisce la **Descriptive Information**), sia dallo \Rightarrow **Archival Storage** vero e proprio degli oggetti conservati, che contiene i **PdA [AIP]**.

L'implementazione in \Rightarrow **Century** di questa entità funzionale prevede che l'**Utente** interagisca con il sistema attraverso una interfaccia utente denominata, in termini generali, *Front End*. Si veda lo [schema logico](#).

L'architettura di **Century**, in effetti, è stratificata in modo tale che la vera e propria interfaccia nativa verso **Access** esista sotto forma di una \Rightarrow **Dissemination-API** e che tale \Rightarrow **API** possa essere utilizzata da diversi moduli *front-end* che rappresentano la vera e propria interfaccia operativa verso l'**Utente**.

Il *front-end* dunque può esistere in diverse forme:

- una *web-application* indipendente, facente parte di **Century**, che talune categorie di **Utenti** utilizzano come porta di accesso standard per la consultazione;
- un set di funzionalità di consultazione integrate in una diversa (più ampia) applicazione di **CompEd**; è il caso, per esempio, del **Portale di Fatturazione Elettronica** di **CompEd**: tutte le funzionalità *front-end* verso la consultazione sono integrate nel portale, consentendo all'utente una *user-experience* omogenea rispetto all'ambiente di produzione che utilizza

anche per altre attività, in generale connesse a documenti che debbono anche essere conservati;

- un set di funzionalità di consultazione integrate in una applicazione del cliente: in questo caso – concettualmente del tutto simile al precedente – è il cliente a sviluppare le funzionalità di interrogazione basandole sull'**API** esposta da **Century**, potendo quindi ottimizzare l'operatività e la *user-experience* secondo i propri standard.

Come detto questi diversi contesti hanno in comune il fatto di essere appoggiati sulla **Dissemination-API** esposta da **Century**; comune è dunque anche il repertorio di funzionalità potenzialmente disponibili (usiamo il colore verde, come sempre, per evidenziare termini presi direttamente dal modello \Rightarrow **OAIS**, con particolare riferimento alla figura riportata in calce a questa sezione):

1. autenticazione ed apertura sessione – questa fase consente di riconoscere l'**Utente** che intende accedere alle informazioni in archivio e determinarne i diritti di accesso;

NOTA: questa funzionalità potrebbe essere trasparente per l'utente, nel caso l'applicazione che implementa il *front-end* ed espone il servizio fosse in grado di gestire un *single-sign-on* valido per **Century**;

2. sottomissione di \Rightarrow **query** – questa funzionalità consente di sottomettere al sistema i parametri di interrogazione con l'obiettivo di identificare un insieme di oggetti presenti in archivio che soddisfano i criteri di ricerca;

NOTA: l'applicazione che implementa il *front-end* offrirà in generale strumenti efficaci per la costruzione delle **query**, come maschere \Rightarrow **QBE**, possibilità di raffinamenti successivi, ecc.;

3. presentazione dei risultati dell'esecuzione di una **query** (**Query response**) – il set di oggetti che soddisfano i criteri contenuti in una **query** sono ritornati in forma tabellare, con tutti i metadati e le **Descriptive Info** disponibili; queste possono essere un risultato sufficiente di per sé per gran parte degli scopi dell'Utente, oppure servire come base per richiedere ulteriori servizi;
4. download duplicato – in fase di consultazione informale è piuttosto comune l'esigenza di visualizzare uno specifico documento risultante da una ricerca; l'**API** consente questo download (condizionato ai diritti di accesso), mentre il *front-end* in generale utilizzerà questo servizio per alimentare una visualizzazione/stampa immediata del singolo documento;
5. ordine (**order**) di confezionamento **PdD** [**DIP**] – il risultato di una **query** può essere utilizzato come base per un **order**, ossia per ordinare la produzione di un **PdD**; poiché questa opzione in generale può implicare l'uso di significative risorse di sistema occorre che l'utente disponga di sufficienti diritti e credito residuo (\Rightarrow utilizzo di **billing info**) per avviare effettivamente la produzione.

Oltre a queste funzioni accessibili attraverso l'API standard e – conseguentemente – il *front-end* specifico a disposizione, l'utente può presentare "richieste speciali" (**Special request**) non assecondabili con il normale servizio erogato in modalità automatica.

L'esempio più tipico è la richiesta da parte di un cliente di ottenere un **PdD [DIP]** coincidente con un **PdA [AIP]**, per scopi particolari come il passaggio ad un diverso Conservatore.

In questi casi la richiesta non può essere inoltrata attraverso interfacce automatiche, ma richiede una negoziazione – svolta in sede di definizione contrattuale o anche durante l'esercizio – nonché una descrizione accurata e concordata, per poi essere servita *off-line* dagli **operatori IT**.

Ancora una volta il modello di riferimento **OAIS** (in questo caso tramite uno dei diagrammi estratti dallo standard) è utile a schematizzare i flussi di interazione tra le diverse funzioni dell'entità funzionale **Access**:

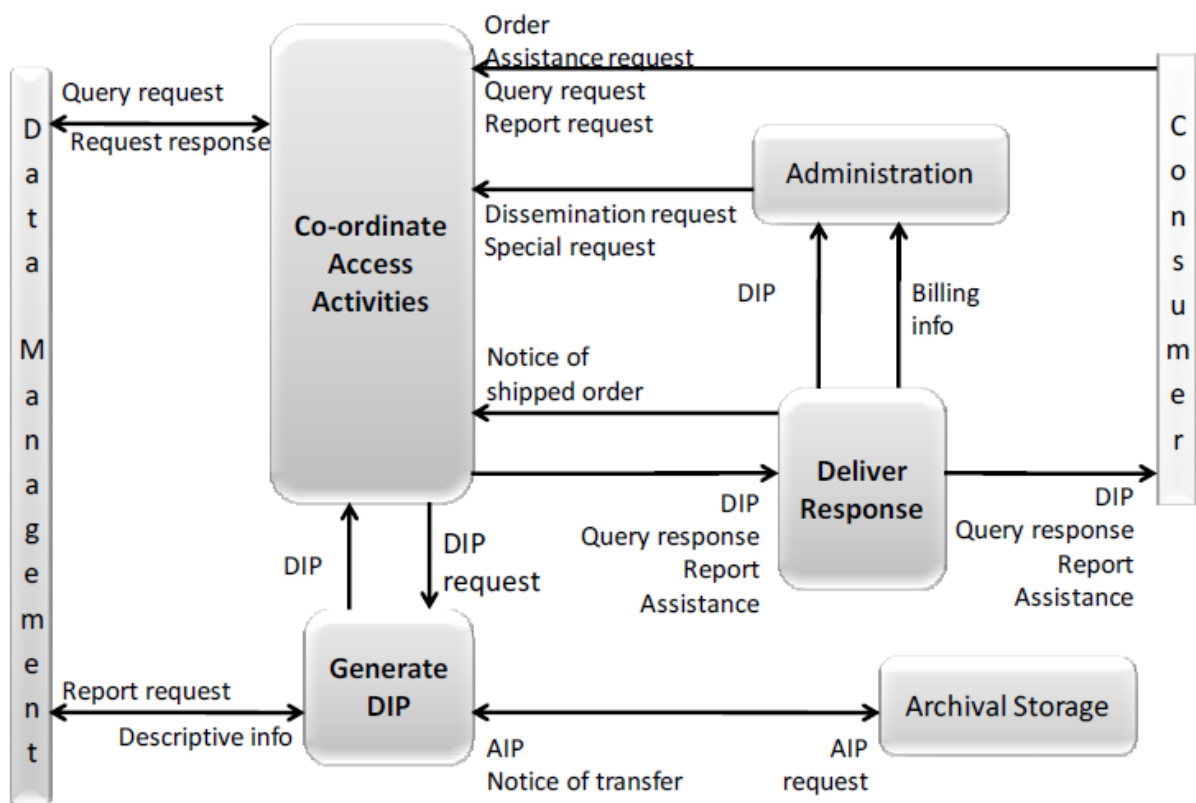


Fig. 14 - Le funzioni di **Access** (figura tratta direttamente dallo standard **OAIS**)
Le funzioni interne all'entità funzionale **Access**

Nel caso in cui l'Utente sottometta – secondo una delle modalità descritte – l'**ordine** di produzione di un **PdD [DIP]** dunque, il sistema risponde con un **PdD** che può assumere diverse forme, descritte nelle prossime sottosezioni.

Torna al [sommario](#)

7.6.1 PdD coincidente con PdA

Questo caso particolare consente l'esportazione integrale di un [=> PdA](#), in generale finalizzato alla migrazione dei documenti verso un diverso [=> Sistema di Conservazione](#) (o alla replica per ragioni di ridondanza).

Su questa modalità c'è relativamente poco da dire: l'intero contenuto del **PdA** viene fisicamente esportato su supporti rimovibili (CD, DVD, Blue Ray, hard disk portatili, unità flash, ...) oppure attraverso *file transfer*.

Sia le modalità di inoltro dell'ordine che le forme di esportazione e consegna possono essere concordate nel [=> Regolamento di Servizio](#) oppure in un apposito modulo d'ordine presentato durante l'esecuzione del servizio stesso.

Le modalità di consegna di **PdD** di questo tipo (e di ogni altro tipo) sono descritte nella sezione [Trasmissione dei Pacchetti di Distribuzione](#).

Torna al [sommario](#)

7.6.2 PdD non coincidente con un PdA

Nella maggioranza dei casi un [=> Utente](#) richiede, attraverso l'interfaccia front-end o la sottostante [=> Dissemination-API](#), l'esibizione di un insieme di documenti che non coinciderà con un intero [=> PdA](#). Per esempio la richiesta potrà avere per oggetto tutti i documenti di una data tipologia, relativi ad un particolare corrispondente, in un certo intervallo di tempo.

Il risultato della selezione è un insieme di documenti che si trovano memorizzati su uno o più **PdA**; quindi il sistema costruisce il [=> PdD](#) in una nuova struttura – del tutto analoga a quella di un **PdA** – e la correda del relativo indice ([=> IPdD](#)) in formato [=> UNI-SInCRO](#).

Le modalità di consegna di **PdD** di questo tipo (e di ogni altro tipo) sono descritte nella sezione [Trasmissione dei Pacchetti di Distribuzione](#).

Torna al [sommario](#)

7.6.3 Trasmissione dei Pacchetti di Distribuzione

I [=> PdD](#) in possono essere consegnati all'Utente essenzialmente in due modalità alternative:

- a) mediante la consegna fisica di supporti fisici rimovibili (es. CD, DVD, Blue Ray, hard disk, memorie flash, ecc.);
- b) mediante il trasferimento telematico di dati.

La prima opzione (nelle sue varianti di formato) si basa di preferenza sulla consegna diretta ad incaricati dello [=> Utente](#), che sono identificati e sottoscrivono un apposito verbale di consegna.

Ove questo non sia possibile si ricorre a personale scelto sulla base di requisiti di affidabilità definiti da [=> RSC](#); in questo caso (ad oggi mai verificatosi) si ricorrerà di preferenza a media che consentono la crittografia del contenuti mediante chiavi scambiate su canali separati, anch'essi cifrati. In ogni caso i media non recano indicazioni che permettano di individuare l'ente produttore, né la natura dei dati contenuti.

La seconda opzione, utilizzata quando i volumi lo consentano, può essere basata sulle normali interfacce di consultazione che per default prevedono l'autenticazione degli utenti e protocollo cifrato HTTPS (è il caso di **PdD** corrispondenti a ricerche selettive, solitamente di piccole dimensioni).

Ove i volumi fossero maggiori (pur nei limiti della trasferibilità telematica) e/o i **PdD** fossero il risultato di procedure di selezione personalizzate si ricorre a trasferimenti via SFTP (protocollo protetto da cifratura); in caso di traffico ricorrente con clienti particolari si ricorre anche a realizzare circuiti [=> VPN](#).

Torna al [sommario](#)

7.7 Produzione di duplicati e copie informatiche, eventuale intervento del Pubblico Ufficiale

In termini generali la produzione di duplicati e copie informatiche di documenti contenuti nell'archivio conservato (più specificamente all'interno di un [=> PdA](#)) rientra nell'attività di [=> Esibizione](#), descritta in una [sezione precedente](#).

L'**Esibizione**, se comporta l'output di una copia fisica (digitale) del documento conservato, produce un duplicato.

Se, diversamente, in sede di esibizione si opta per una *stampa*, si produce una copia informatica.

Si noti che il processo di stampa, operando su una normale stazione di lavoro, implica che la riproduzione del documento sia affidata ad un dispositivo di stampa, che può anche essere virtuale. È tipico l'utilizzo di stampanti virtuali per ottenere copie PDF di documenti in diversi formati. Quindi le funzioni di stampa, del tutto generiche dall'interfaccia utente di [=> Century](#), possono produrre copie analogiche o informatiche.

Torna al [sommario](#)

7.7.1 Intervento del Pubblico Ufficiale

Le normali tipologie di documenti sottoposte a Conservazione da parte dei clienti di **CompEd Servizi** consistono in “documenti informatici” all’origine. Quindi non si pone quasi mai la necessità dell’intervento di un Pubblico Ufficiale al fine di autenticare il riversamento di documenti con alterazione della rappresentazione.

Inoltre si prediligono formati di documenti che offrano garanzia di stabilità e non pongano tale problema per lungo tempo.

Si aggiunga che, nel caso di servizio svolto per i privati, si tratta per la maggior parte di documenti di rilevanza fiscale e tributaria, quindi con un ciclo di vita massimo – prima dello scarto – di soli 10 anni.

Nel caso di documenti delle P.A. la normativa consente che il Pubblico Ufficiale sia espresso nella struttura dello stesso Ente, nel rispetto di alcuni vincoli: pertanto **CompEd Servizi** è disponibile, all’occorrenza, a far intervenire il Pubblico Ufficiale indicato dal cliente (**⇒ Produttore**).

Nei casi in cui l’intervento del Pubblico Ufficiale si renda necessario nel ciclo di vita di documenti forniti da clienti privati il Cliente stesso è libero di indicare un Notaio di propria fiducia, oppure **CompEd Servizi** può mettergli a disposizione un Notaio convenzionato.

Torna al [sommario](#)

7.8 Scarto del Pacchetti di Archiviazione

Nell’ambito di ciascun pacchetto di servizi offerti e, quindi, del relativo **⇒ Regolamento di Servizio**, tra i diversi parametri che costituiscono l’oggetto del servizio stesso figurano anche i tempi globali di conservazione di una tipologia di documenti e le conseguenti modalità di **⇒ scarto**.

Questi parametri sono poi codificati nella **⇒ Policy** di Conservazione associata al **⇒ Canale** o ai canali istanziati nel sistema a seguito dell’attivazione del servizio.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

Nell’imminenza della scadenza del periodo previsto per lo **scarto** (l’anticipo è oggetto di configurazione, ad esempio 30 o 90 giorni), il sistema genera una automatica notifica al **⇒ RSC** per

informarlo. Tale notifica si ripete con cadenza di 5 giorni sino a che non si provveda alla Procedura di Scarto.

La Procedura di Scarto prevede:

1. La produzione di un \Rightarrow **PdD** [**DIP**] coincidente con ciascun \Rightarrow **PdA** [**AIP**] oggetto di **scarto**: scopo principale di questa operazione è poter mettere a disposizione del Cliente una copia di questi **PdA** su supporti rimovibili (opzionale, in funzione del contratto)
2. La produzione di un Verbale di Scarto che riassume i dettagli dell'operazione, compresi i riferimenti del **PdA** oggetto dello scarto, firmato da **RSC**.
3. La registrazione del Verbale di Scarto nel \Rightarrow **Giornale di Controllo**
4. L'invio di comunicazione ufficiale al Cliente dell'avvenuto scarto e delle modalità di consegna delle copie dei **PdD** ricavati dai **PdA** prima dello scarto effettivo (se è stata concordata una consegna di questo tipo).
5. La rimozione dei **PdA** dal sistema, con una tempistica precauzionale (*grace period*) sia per i contenuti effettivi dei **PdA** che dei riferimenti nel database

Torna al [sommario](#)

8 Il Sistema di Conservazione

Il Sistema di Conservazione di **CompEd Servizi**, è costituito da un insieme di componenti di software applicativo installate su una infrastruttura (hardware, software di base, risorse di rete, servizi esterni).

Il software applicativo, sviluppato interamente da **CompEd Software Design** (azienda del gruppo di cui fa parte anche **CompEd Servizi**), è globalmente denominato \Rightarrow **Century**.

Come noto le attuali \Rightarrow **Regole Tecniche** in materia di conservazione digitale sono fortemente ispirate al modello \Rightarrow **OAIS**, con l'innesto di alcuni importanti vincoli (soprattutto in merito alla definizione delle responsabilità, dell'interoperabilità, della garanzia di inalterabilità dei dati conservati) che contribuiscono significativamente ad indirizzare i progettisti dell'implementazione.

L'implementazione di **Century** è dunque basata interamente sul modello **OAIS**, avvantaggiandosi inoltre della riduzione della complessità di tale modello offerta dal perimetro delle **Regole Tecniche**.

Torna al [sommario](#)

8.1 Componenti Logiche

Se si considera l'architettura logica del sistema **Century** è immediato riscontrare la presenza delle strutture fondamentali del [modello di riferimento OAIS](#):

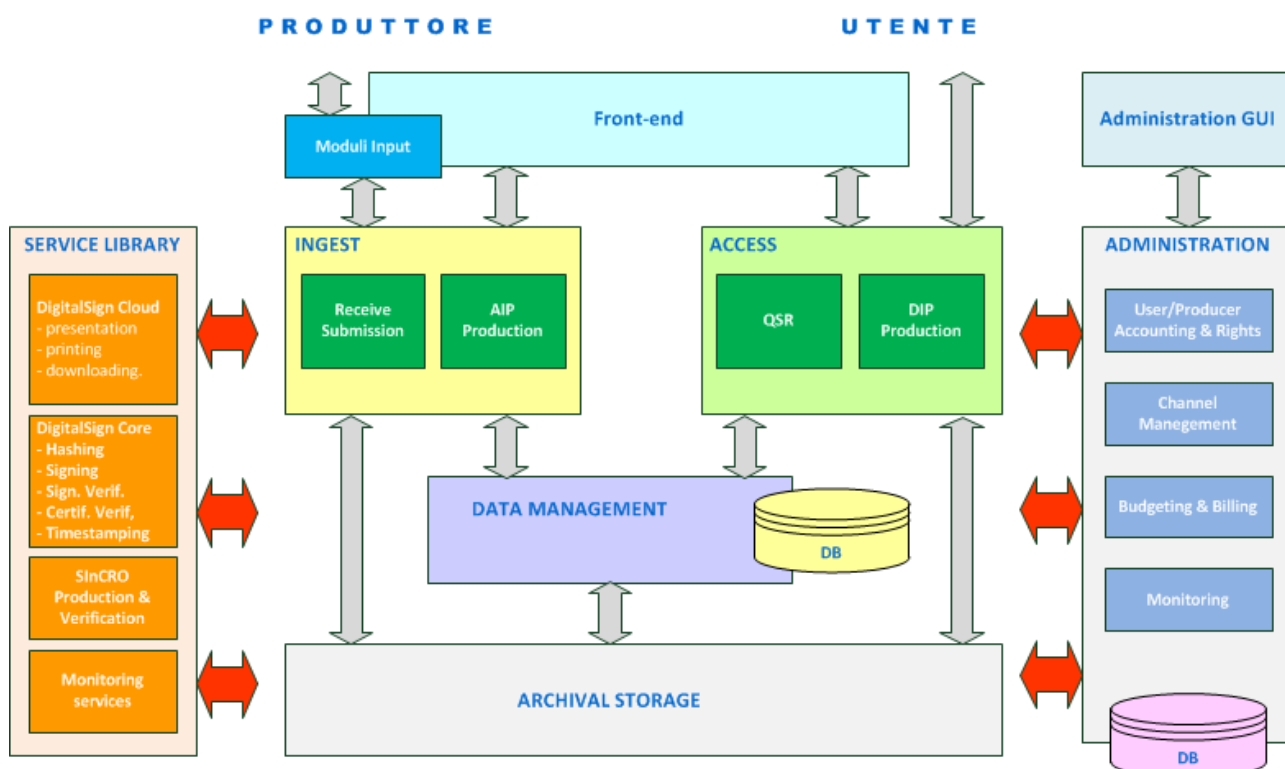


Fig. 15 – Architettura logica di Century

Diagramma illustrante l'architettura logica del sistema di conservazione Century

Nelle prossime sezioni si descrivono le funzioni indicate nel diagramma.

Torna al [sommario](#)

8.1.1 Moduli di Input

I **⇒ moduli di input** implementano le interfacce verso il mondo esterno per l'entità funzionale **⇒ Ingest**: in linea generale acquisiscono i **⇒ PdV [SIP]** e ritornano i **⇒ RdV**.

A questo livello esiste una grande modularità: particolare esigenze di un cliente (o di una categoria di clienti) implicano lo sviluppo di un diverso protocollo di immissione e dunque la realizzazione di un **modulo di input** specializzato.

La figura, sopra, evidenzia che diversi **moduli di input** possono operare con o senza l'intermediazione del *front-end*.

Torna al [sommario](#)

8.1.2 Front-end Produttore/Utente

Si tratta di un'interfaccia utente che consente le interazioni del \Rightarrow **Produttore** (il quale in generale coincide con \Rightarrow **l'Utente**, a meno di ruoli specifici di persone diverse all'interno dell'organizzazione del **Produttore**) con il sistema.

Come evidenziato dalla [figura](#) esiste una parziale sovrapposizione funzionale tra i **moduli di input** e il *front-end*. Il significato di tale sovrapposizione è che in alcuni casi un **modulo di input** interagisce con il sistema del produttore direttamente, in modo specializzato e tipicamente \Rightarrow **A2A**.

In altri casi le funzioni del modulo di input sono implementate nel *front-end*.

Il *front-end* è un componente in rapida evoluzione e può presentarsi in forme diverse. La sua prima, attuale implementazione è integrata in un portale che offre servizi applicativi all'utenza (per la fatturazione elettronica, per l'immissione di registri contabili, per l'immissione del registro giornaliero di protocollo, ecc.); altre istanze svincolate dal portale sono in fase di sviluppo e verranno rilasciate prossimamente.

Il *front-end* offre anche funzionalità di \Rightarrow **interrogazione** del sistema e di \Rightarrow **esibizione**.

Torna al [sommario](#)

8.1.3 Ingest

L'entità funzionale \Rightarrow **Ingest**, come già introdotto nella [sezione dedicata all'acquisizione dei PdV \[SIP\]](#), interfaccia il mondo esterno (per tramite di un \Rightarrow **modulo di input**, eventualmente intermediato da un *front-end*).

Al suo interno contiene diverse funzioni:

1. *Receive-Submission* – presiede alle operazioni di verifica dei \Rightarrow **PdV [SIP]**, nonché alla produzione del \Rightarrow **RdV** ed al passaggio del materiale ricevuto al sottostante modulo di *Channel Management*.

- II. *AIP Production* – questo modulo è responsabile della produzione dei \Rightarrow **PdA** [**AIP**], in base alle \Rightarrow **policy** definite a livello di ciascun *task* di conservazione associato ad un \Rightarrow **canale**. È questo modulo che organizza gli oggetti nell'Area di Accumulazione (\Rightarrow **AA**) del **canale** di pertinenza man mano che vengono estratti dai **PdV**, per poi – al verificarsi delle condizioni di \Rightarrow **trigger** – trasformare il contenuto attuale della **AA** in un vero e proprio **PdA**.

Ingest interagisce anche con il modulo di *Administration/Billing* per verificare che il **PdV** sia accettabile da un punto di vista amministrativo (es. contratto con *budget* sufficiente).

Torna al [sommario](#)

8.1.4 Access

L'entità **Access** implementa le funzioni relative [all'Esibizione](#).

Al suo interno contiene due unità funzionali:

- I. *Query, Search, Retrieval* – si tratta essenzialmente di un motore di ricerca che permette all'**Utente** – in generale attraverso l'interfaccia utente disponibile nel *front-end*, ma eventualmente anche in forma di \Rightarrow **API** – di effettuare ricerche e selezioni di intervalli di documenti, utilizzando tutti i metadati associati agli stessi.

In generale da queste ricerche si ottengono liste di oggetti che soddisfano le condizioni di ricerca e che possono essere usate per operazioni successive. Tra queste la più semplice è la presentazione di un documento o un fascicolo, con opzioni di visualizzazione/rendering avanzate, stampa, download.

- II. *DIP Production* – questo modulo interviene quando la lista di oggetti identificata con una ricerca deve essere convertita in un vero e proprio \Rightarrow **PdD** [**DIP**]: i documenti individuati vengono composti in una struttura dati del tutto analoga a quella di un \Rightarrow **PdA** e corredati di un \Rightarrow **IPdD** in formato \Rightarrow **UNI-SInCRO**, quindi messi a disposizione dell'**Utente** (in modalità variabili, secondo le dimensioni).

Torna al [sommario](#)

8.1.5 Data Management

Il **Data Management** implementa tutte le funzioni di servizio per \Rightarrow **Ingest** ed \Rightarrow **Access** basate sui \Rightarrow **metadati** e sulle altre informazioni strutturate associate ai documenti, ai \Rightarrow **pacchetti informativi**, ai \Rightarrow **canali**.

In un certo senso può essere considerato l'interfaccia tra il *database* ed il resto del sistema: quando **Ingest** acquisisce i \Rightarrow **PdV** è il **Data Management** che popola il database con i metadati e mantiene l'associazione tra ogni documento ed il **canale** di pertinenza, per poi definire il contenuto di ogni singolo \Rightarrow **PdA** generato nel tempo; quando **Access** richiede l'esecuzione di ricerche per ottenere i risultati è ancora **Data Management** che esplora il database e materialmente costruisce la lista di riferimenti, tenendo conto anche dei diritti di accesso in possesso dello \Rightarrow **Utente** che sottomette le richieste.

Torna al [sommario](#)

8.1.6 Administration

La [figura illustrata sopra](#) mostra una unità funzionale **Administration** collocata lateralmente alle altre entità funzionali. Il significato di tale posizione è che **Administration** contiene funzioni e servizi utilizzati costantemente da tutte le altre unità del sistema (le frecce di interazione rosse sono mostrate aperte verso l'interno proprio per indicare che l'interazione è praticamente con tutti gli altri moduli)

I moduli principali di **Administration** sono i seguenti:

- I. *User/Producer Accounting & Rights* – gestisce le comunità di utenti e i relativi diritti di accesso ed operatività
- II. *Channel Management* – tiene traccia di tutti i \Rightarrow **canali** istanziati nel sistema e dell'associazione di ogni canale con un account \Rightarrow **produttore/** \Rightarrow **utente**, gestendo anche i task e le \Rightarrow **policy** di conservazione di ogni canale
- III. *Budgeting & Billing* – provvede servizi relativi al conteggio delle risorse e degli elementi di servizio impegnati/consumati, consentendo un utilizzo controllato (anche sul piano della tariffazione) dei servizi da parte degli utenti.
- IV. *Monitoring* – permette di impostare e lanciare l'esecuzione dei servizi di [monitoraggio](#) delle attività del sistema

Administration prevede anche una *Administration GUI*, distinta dalla \Rightarrow **GUI** del *front-end* dell'utente, a disposizione degli amministratori del sistema.

NOTA: **Administration** usa una porzione di database per gestire le informazioni necessarie per amministrare il sistema. Evidentemente queste informazioni sono ben distinte dalle altre informazioni organizzate nel database da parte di **Data Management** (metadati, relazioni documento/**PdA/Canali**, ecc.).

Il sistema può operare con due database completamente distinti (anche in tecnologie diverse), come pure utilizzare lo stesso database per le due attività.

Torna al [sommario](#)

8.1.7 Service Library

Sempre facendo riferimento allo [schema logico](#) della figura riportata all'inizio di questa sezione, notiamo che sul lato sinistro compare una unità funzionale denominata *Service Library*.

Si tratta di una collezione di strumenti che mettono a disposizione di tutti gli altri moduli i propri servizi, utilizzati in diverse attività. Anche in questo caso le frecce rosse di interazione aperte verso l'interno indicano questa connessione con tutti gli altri moduli.

In particolare identifichiamo:

- i. **DigitalSign Cloud** – è una *web application* di **CompEd** che offre un ambiente visuale molto sofisticato per la presentazione renderizzata di documenti informatici e la gestione di tutto ciò che ha a che fare con la sottoscrizione digitale. In particolare [=> Century](#) lo utilizza per la presentazione di documenti estratti dall'archivio con tutta la relativa collezione di metadati ed informazioni di conservazione, per la verifica visuale delle firme e delle marche temporali, e così via. È previsto l'imminente utilizzo sul *front-end* per offrire ai produttori anche un servizio integrato di firma di documenti prima della composizione automatica dei [=> PdV](#).
- ii. **DigitalSign Core Services** – è una libreria di funzioni crittografiche (su cui si appoggia anche **DigitalSign Cloud**) in grado di apporre e verificare firme digitali di ogni tipo, calcolare hash, apporre e verificare marche temporali, manipolare e verificare certificati; è impiegata per la verifica dei **PdV** e dei **PdA**, per la produzione di [=> IPdA](#) e [=> IPdD](#), per la verifica e monitoraggio degli stessi, ecc.
- iii. **SInCRO Production/Verification** – è un modulo specializzato per la produzione di indici in formato [=> UNI-SInCRO](#), utilizzato per produrre **IPdA** e **IPdD**; le funzioni di verifica sono utilizzate in fase di monitoraggio e presentazione.
- iv. **Monitoring Services** – è un insieme di funzioni al servizio delle attività di [monitoraggio](#). Funzioni di rilettura dei **PdA**, di verifica degli **IPdA**, di controllo di coerenza tra i [=> metadati](#) sigillati degli **IPdA** e le copie degli stessi immagazzinate nel database, funzioni di schedulazione e reporting, ecc.

Torna al [sommario](#)

8.2 Componenti tecnologiche

Il sistema di conservazione è implementato in [=> Century](#): si tratta di una suite di componenti software integrata, sviluppata interamente in Java e – nell'attuale edizione – in tecnologia Adobe Flex (relativamente alla Administration GUI).

Di seguito gli elementi tecnologici principali utilizzati dal codice di **Century**:

- i. Sistema operativo: Century è sviluppato in tecnologia Java, quindi può girare su diversi sistemi operativi; l'implementazione di CompEd Servizi è su Linux Ubuntu
- ii. Java Real Time Environment
- iii. Database: **Century** è compatibile con diversi database, l'implementazione di **CompEd Servizi** è basata su PostgreSQL
- iv. Application Server: Apache Tomcat
- v. Sottosistema di firma digitale e marcatura temporale: DigitalSign Core Services
- vi. Servizio di Firma Digitale Remota Automatica: Aruba/Actalis – in particolare si interfaccia il front-end RSASS implementato da CompEd Servizi (è previsto, a titolo di backup, un meccanismo di firma digitale basato su smartcard interfacciate alla stazione di lavoro locale di [=> RSC](#) via browser, grazie alla tecnologia **DigitalSign Core Service**).
- vii. Servizio di Marcatura Temporale: Aruba/Actalis (è previsto l'utilizzo, a titolo di backup, di servizi alternativi RFC3161 autenticati su https; al momento sono disponibili account Infocert e Trust Technologies).

Il *front-end* attuale, come introdotto nella [sezione dedicata](#), è al momento integrato nel portale di erogazione di servizi (fatturazione elettronica e altri servizi di conservazione). Questo è un sistema tecnologicamente simile a **Century**, basato sul framework **Alchemy** e su una infrastruttura software del tutto simile (Linux, PostgreSQL, Java, Apache Tomcat).

Il Portale offre un'interfaccia utente completamente *web-based, zero-footprint*, basata su HTML-5. Integra anche **DigitalSign Cloud** per la presentazione renderizzata dei documenti.

Torna al [sommario](#)

8.3 Componenti fisiche

Allo stato attuale il SdC di CompEd Servizi è organizzato in questo modo:

- Un sito primario su Virtual Data Center, presso la farm Netalia Srl di Basiglio (MI)
- Un sito secondario su Virtual Data Center, presso la farm Netalia Srl di Empoli (FI)

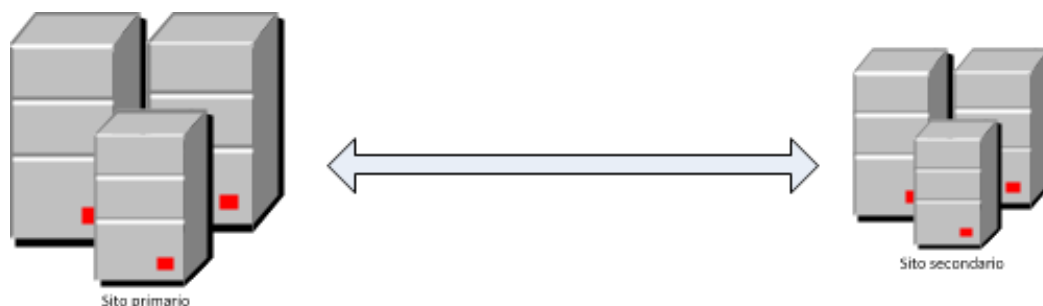


Fig. 16 – Siti di Conservazione
Schema di base della suddivisione in siti (primario e secondario) del SdC

Allo stato attuale il Sito Secondario ha lo scopo di costituire una risorsa di *disaster recovery*, poiché il Sito Primario (come meglio descritto nella prossima sezione) dispone di tutte le misure necessarie ad erogare il servizio in alta affidabilità.

In ogni caso il Sito Secondario è una copia del Sito Primario, sia a livello di risorse che di consistenza dei dati, aggiornati in continuo.

Per maggiori dettagli riguardo alla configurazione fisica dei siti si rimanda al Piano della Sicurezza.

Torna al [sommario](#)

8.3.1 Il sito primario

Il sito primario ospita il sistema di produzione completo:

- Software applicativo **Century**
- Database server
- Storage massivo

Sul piano delle risorse disponibili il sistema consiste di una architettura completamente virtualizzata, descritta nel Piano della Sicurezza.

Torna al [sommario](#)

8.3.2 Il sito secondario

Il sito secondario replica interamente il sito primario, con l'obiettivo di implementare un efficace *disaster recovery*.

Il sistema di D.R. è automaticamente evocato, in caso di necessità, con tempi inferiori ad 1 ora.

Torna al [sommario](#)

8.4 Procedure di gestione ed Evoluzione

Nelle seguenti sottosezioni si espongono i dettagli delle diverse attività.

Torna al [sommario](#)

8.4.1 Conduzione e manutenzione del SdC

La sorveglianza sulla regolare funzionalità del sistema è competenza di [=> RSI](#), che la svolge con la collaborazione degli [=> operatori IT](#) alle sue dipendenze.

Oltre alla gestione dei messaggi di notifica automatici (si veda la sezione relativa al monitoraggio) che informato **RSI** di anomalie rilevate automaticamente, esiste un sistema di "issue tracking" mediante il quale gli operatori di Helpdesk sottomettono i ticket relativi alle anomalie – o presunte tali – segnalate dagli utenti.

Queste anomalie, ove non risolvibili da parte degli [=> operatori IT](#) o comunque quando rivelano l'opportunità di un intervento più profondo, sono condivise con [=> RSM](#).

RSM, **RSI** e [=> RSC](#) prendono in esame le necessità di intervento ed all'occorrenza pianificano una [=> patch](#), ossia la produzione di uno o più componenti modificate del software del sistema, che possono essere installate modularmente senza bisogno di un rilascio integrale.

Le **patch** vengono realizzate e tracciate dal team di sviluppo alle dipendenze di **RSM**, testate in ambiente di stage, quindi rilasciate in produzione dopo il superamento positivo del test (verbale di test).

Ove possibile le **patch** si applicano in parallelo al sistema preesistente, per monitorarne attentamente gli effetti e poterne escludere immediatamente l'applicazione nel caso emergano effetti collaterali non rilevati in fase di test.

In ogni caso la **patch** può risultare applicata positivamente (=> verbale applicazione patch positiva) oppure negativamente (=> *rollback*, verbale, ritorno allo sviluppo).

La caratteristica della patch, rispetto ad una vera e propria [=> release](#) del sistema, è la sua ridotta dimensione ed impatto. Ma viene trattata, pur nei limiti che la contraddistinguono, con le stesse metodologie descritte più avanti nella [sezione Change Management](#).

Torna al [sommario](#)

8.4.2 Gestione e Conservazione dei Log

Il sistema gestisce numerosi *log* di sistema, con diversi livelli di verbosità che si attivano e disattivano prevalentemente quando sia necessario debuggare funzioni specifiche.

Alcuni eventi, tuttavia sono sempre oggetto di logging:

- i. Immissione di un [=> PdV](#)
- ii. Rifiuto di un **PdV**
- iii. Accettazione di un **PdV**
- iv. Produzione di un [=> PdA](#)
- v. Produzione di un [=> PdD](#)
- vi. Esecuzione di una [=> query](#) di esibizione
- vii. Download di un documento
- viii. Modifica alla configurazione di un [=> Canale](#) (inclusa creazione)
- ix. [=> Scarto](#)

Queste informazioni di log sono accumulate su base giornaliera e, quotidianamente, confluiscono in uno speciale **canale** di conservazione chiamato [=> Giornale di Controllo](#), quindi sottoposte a conservazione al pari dei documenti provenienti dall'esterno.

Torna al [sommario](#)

8.4.3 Monitoraggio

Le attività di monitoraggio sono descritte in dettaglio nella successiva [sezione dedicata](#).

Torna al [sommario](#)

8.4.4 Change Management

Naturalmente l'attività di progettazione ed implementazione delle evoluzioni del sistema è pressoché continua.

Le iniziative di intervento in questo senso sono convogliate da [=> RSC](#) (alimentate tipicamente dalla valutazione di ticket da Helpdesk, da richieste di [=> RSI](#), dal marketing, ecc.) che le discute con [=> RSM](#).

La progettazione dell'intervento (si tratti di una semplice patch o di un intervento più massiccio) passa per due documenti:

- Analisi requisiti
- Specifiche di dettaglio

Il documento di specifiche è passato al team di sviluppo che mette in cantiere l'intervento.

Il risultato è sottoposto ad un ciclo di test in ambiente di [=> stage](#) e, dopo tale fase, messo in produzione.

Il piano di *deployment* è scritto specificamente per ogni intervento, tenendo conto dell'impatto atteso (interventi importanti possono avere impatto sulle strutture dati, quindi richiedono l'esecuzione di *tool* di migrazione, a loro volta oggetto di test, valutazione, eventuale *rollback*).

Torna al [sommario](#)

8.4.5 Verifica periodica di conformità a normativa e standard di riferimento

Nel caso del processo di conservazione di **CompEd Servizi** è probabilmente più corretto parlare di "verifica continua" anziché "periodica": [=> RSC](#) in primo luogo ha la responsabilità di tenere controllata l'evoluzione delle norme per esaminare tempestivamente ogni documento normativo che introduca la necessità di cambiamenti.

Per alcuni settori questa attività è facilitata da altri progetti in cui **CompEd** è coinvolta: ad esempio **CompEd** fornisce strumenti di firma digitale e marcatura temporale a diversi altri Certificatori e Conservatori Accreditati, quindi è coinvolta nei periodici *plug-test* europei in materia e partecipa a consultazioni continue con i suoi clienti co-interessati all'argomento, beneficiando dunque delle automatiche ricadute sul livello di aggiornamento dei componenti utilizzati in **Century**.

Quando viene emanato un nuovo documento normativo o uno standard rilevante che implica la necessità di intervento sulle funzionalità del sistema si apre un progetto *ad-hoc* che rientra nel circuito descritto a proposito di [change-management](#).

Torna al [sommario](#)

9 Monitoraggio e controllo

Ricordiamo che gli obiettivi fondamentali del \Rightarrow **SdC** sono i seguenti:

- a) conservare a lungo termine i contenuti informativi affidati al sistema, proteggendone l'integrità e l'utilizzabilità, prevenendo perdite o deterioramenti di ogni tipo (inclusa l'eventuale perdita di valore probatorio dei documenti conservati);
- b) consentire l'accesso alle informazioni da parte degli aventi diritto, mediante le funzioni di ricerca ed estrazione previste;
- c) consentire con continuità il processo di immissione di nuovo materiale nel sistema, prevenendo interruzioni di servizio che possano impedire ai produttori di mettere al sicuro i propri documenti per un tempo più o meno lungo.

Nelle prossime sottosezioni illustriamo le procedure di monitoraggio e controllo messe in atto per raggiungere tali obiettivi.

Torna al [sommario](#)

9.1 Procedure di monitoraggio

Nel \Rightarrow **SdC** sono attuate sia procedure di monitoraggio attivo, che costantemente tengono sotto controllo il funzionamento dei processi fondamentali del sistema, sia un meccanismo di notifica che provvede a segnalare a \Rightarrow **RSI** ed agli \Rightarrow **operatori IT** alle sue dipendenze il rilevamento di anomalie.

Per gli aspetti più sistemistici del monitoraggio si rimanda al *Piano della Sicurezza*.

Torna al [sommario](#)

9.1.1 Monitoraggio processi

Il \Rightarrow **SdC** è servito da due livelli di monitoraggio.

Al livello superiore ci si affida agli strumenti di monitoraggio delle macchine virtuali istanziate, propri di *VMWare*, i quali gestiscono la configurazione cluster in alta affidabilità, provvedendo automaticamente a ripristinare il servizio in caso di caduta ed a notificare anomalie (via email e tramite console).

A più basso livello si impiega lo strumento *MONIT*, il quale offre diversi servizi:

- monitoraggio della CPU rilevando sovraccarichi;
- monitoraggio dello spazio disco, rilevando eventi di eccessivo riempimento;
- monitoraggio dello stato di attivazione di servizi e processi (incluso arresto e riavvio automatico in caso di anomalie e cadute);
- invio notifiche via email relativamente ad ogni anomalia rilevata.

Torna al [sommario](#)

9.1.2 Notifica & Logging

Come già introdotto nella sezione [dedicata ai log](#), il **SdC** provvede ad una gestione particolarmente rigorosa dei log relativi alle operazioni primarie con i pacchetti di informazione.

Oltre a questo, il sistema produce quotidianamente log più tecnici, che anche al livello di configurazione di minima verbosità registrano ogni condizione di errore.

Anche questi log sono indirizzati ad un **canale** di sistema, che conserva nel tempo il flusso delle più significative informazioni generate internamente.

Per le condizioni di errore più critiche, oltre alla registrazione nei log, è previsto l'intervento di un *dispatcher* di notifiche che comunica alla lista dei destinatari predefinita i messaggi di richiamo dell'attenzione. La comunicazione, attualmente, avviene attraverso email ed SMS.

Torna al [sommario](#)

9.2 Verifica integrità degli archivi

Century dispone di alcune funzionalità dedicate alla verifica di integrità e leggibilità, basate su alcune scelte progettuali ed organizzative orientate alla "*integrità intrinseca*".

Vale la pena di richiamare alcune considerazioni preliminari, già discusse in questo manuale:

- i. un [⇒ PdA](#) è sempre corredato di un [⇒ IPdA](#) protetto da una [⇒ firma qualificata](#) ed una [⇒ marca temporale](#) che assicurano l'integrità dell'indice stesso;
- ii. l'**IPdA** contiene un record per ciascun oggetto immagazzinato del **PdA**, ciascun record contiene – tra l'altro – il valore dell'impronta ([⇒ hash](#)) dell'oggetto stesso;
- iii. ogni record del **IPdA** dedicato ad un oggetto conservato contiene anche la lista integrale dei metadati associati a tale oggetto; i metadati sono quindi anch'essi protetti dalla **firma** e dalla **marca temporale** associate al **IPdA**;
- iv. nell'ambito di ogni [⇒ canale](#) la sequenza originale dei **PdA** è ordinata anche mediante il tag VdCGroup, che permette di riconoscere un **PdA** come appartenente ad un canale e determinarne la posizione nella sequenza anche osservando il solo **PdA** fuori da ogni contesto.

Da queste considerazioni discende che:

- a) l'integrità di un singolo **PdA** è immediatamente determinabile anche solo rileggendo il pacchetto stesso, partendo dal relativo **IPdA**, previa verifica della **firma** e della **marca temporale** che li proteggono;
- b) tutto il set di metadati è sempre ricostruibile rileggendo il **PdA**, senza bisogno di consultare un database di appoggio;
- c) l'intera sequenza di **PdA** appartenente ad un **canale** è ricostruibile rileggendo gli **IPdA** anche fuori dal sistema che li gestisce, senza necessità di un database di appoggio;
- d) le informazioni fondamentali che identificano il [⇒ Produttore](#) dei dati contenuti in un **PdA** sono presenti nel **IPdA**, tramite un record Agent specifico (si veda la [struttura del IPdA](#))

Quindi, sebbene **Century** si appoggi – ovviamente – su un database necessario a rendere efficienti le attività di gestione, l'intero contenuto del database può essere automaticamente ricostruito a partire dai **PdA**.

Un apposito processo di verifica periodica gira continuamente (tipicamente nelle ore notturne e nei giorni festivi, in base ad una configurazione di cadenza modificabile) per eseguire la rilettura di tutti i **PdA** a partire dalla lista dei **canali** presenti nel DB: scopo di questa attività è assicurare continuamente l'integrità del DB e la leggibilità dei dati di tutti i **PdA**.

Un ulteriore processo scansiona il *file system* dello storage principale (dove i diversi **canali** sono mappati su folder di sistema) verificando che non esistano canali "orfani" rispetto al database.

Ogni errore rilevato in questa fase, a qualunque livello, provoca una notifica a [⇒ RSI](#) il quale valuta l'anomalia e mette in campo le necessarie contromisure, si veda la [successiva sezione dedicata a questo argomento](#).

Lo stesso processo si esegue anche sui siti diversi da quello primario, con analoghi interventi in caso di rilevazione anomalie.

Quando termina un ciclo integrale di lettura e verifica il sistema genera un report (log) automatico e lo inserisce nel [=> Giornale di Controllo](#).

Evidentemente questo ciclo si completa con frequenza molto maggiore rispetto ai termini di legge; la periodicità effettiva del ciclo dipende dal volume dei dati presenti nel sistema. È compito di [=> RSC](#) valutare continuamente questo periodo risultante e – se ritenuto opportuno – aumentare le risorse del sistema per consentire una frequenza maggiore.

Torna al [sommario](#)

9.3 Soluzioni adottate in caso di anomalie

Nella [sezione dedicata a monitoraggio e controllo](#) abbiamo preso in esame diverse strategie per gestire anomalie di tipo diverso.

Evidentemente anche le contromisure per ovviare alle anomalie differiscono in funzione della tipologia.

In termini generali distinguiamo tra anomalie di funzionamento ed anomalie di integrità, si vedano le successive sottosezioni.

Torna al [sommario](#)

9.3.1 Gestione anomalie di funzionamento

Qualora si verifichi una anomalia di funzionamento, che possa pregiudicare il corretto svolgimento del servizio (ad esempio una difficoltà ad elaborare un [=> PdV](#) in ingresso, oppure in fase di produzione di un [=> PdA](#), o ancora in fase di ricerca finalizzata all'esibizione) la gestione prevede una *checklist* che possiamo sintetizzare in questo modo:

1. Determinazione della gravità del problema (bloccante/non bloccante);
2. Analisi delle cause
3. Definizione dell'intervento
4. Esecuzione intervento

Naturalmente diverse tipologie di intervento richiesto implicano diversi impatti. Seguono gli esempi tipici:

- i. anomalie dovute a situazioni transitorie (ad esempio indisponibilità di servizi remoti o di risorse raggiungibili via rete) => analisi delle cause, eventuale pianificazione intervento migliorativo dell'infrastruttura, sollecito del fornitore;
- ii. anomalie dovute a fuori servizio di componenti software di base del sistema => ripristino della funzionalità, pianificazione intervento sul componente per rimuovere la causa dello stop (esempio: aggiornamento software di terze parti/rollback se l'anomalia è un effetto collaterale di un aggiornamento);
- iii. anomalie dovute a *failure* del software **CompEd** => ripristino della funzionalità tramite riavvio o workaround, ticket verso **RSM** per intervento risolutivo => **patch**

Torna al [sommario](#)

9.3.2 Gestione anomalie di integrità

Quantunque una anomalia di questo tipo non si sia mai verificata, il sistema – come descritto nella [sezione dedicata alle verifiche di integrità](#) – prevede processi automatici di continua rilettura e verifica, emettendo notifiche di allarme in caso di rilevamento anomalie.

In un caso del genere si procederebbe con una immediata analisi del problema ed identificazione del disallineamento. Le prime contromisure prevedono:

- esecuzione di processi di riconciliazione del database a partire dal contenuto dei **PdA** e dei **PdV**;
- sostituzione di unità di memorizzazione dello *storage* (che comunque non pregiudicano l'integrità dei dati, grazie alla configurazione RAID);
- recupero di informazioni danneggiate dagli storage di backup/disaster recovery e ripristino del patrimonio informativo

Da un evento di questo tipo si avvia ovviamente una procedura di indagine che determini le ragioni dell'anomalia e di conseguenza un intervento di risoluzione del problema così scoperto, prevedibilmente con la rimozione del bug e/o con l'introduzione di ulteriori misure di protezione e rilevazione.

Torna al [sommario](#)