La conservazione dei documenti digitali nel nuovo CAD e negli standard

Maria Guercio
Università degli studi di Urbino
m.guercio@mclink.it

Roma, 8 luglio 2011

i temi

1. I processi di conservazione: quadro concettuale e normativo
2. Lo standard UniSincro per l'interoperabilità dei volumi di conservazione
3. Standard internazionali e misurazione di qualità per l'accreditamento di depositi per la conservazione digitale

I processi di conservazione: quadro concettuale e normativo

2001-2009

- Il problema della conservazione digitale è stato trattato a lungo dal legislatore italiano in termini di **conservazione a breve-medio termine** ed è stato circoscritto nella sostanza alla questione della validità giuridica della riproduzione sostitutiva dei documenti analogici.
- La legislazione di riferimento ha comunque offerto **indicazioni operative utili (anche se non complete)** a processi di conservazione a lungo termine, anche se non è stata finora utilizzata a questo fine.

2010 - …

- Le disposizioni del nuovo CAD hanno integrato e completato il quadro di riferimento:
  - accreditamento e certificazione
  - coordinamento delle responsabilità
  - manuale di conservazione
  - disciplina delle copie
  - continuità operativa
- La regolamentazione tecnica in corso di discussione è destinata ad ampliare notevolmente le indicazioni di merito (standard, sistema di conservazione, modelli di responsabilità, ecc.)

concetti chiave: autenticità

- "la capacità del documento di essere ciò che dichiara, senza falsificazioni e manipolazioni"
  - È a rischio nei processi di trasmissione e di conservazione
  - È riconducibile ai concetti di **identità** e di **integrità**
  - L'autenticità in ambito digitale non è verificabile in termini di bit nel caso della conservazione a lungo termine, ma può essere **presunta** sulla base dei requisiti cumulativamente rispettati da un sistema di conservazione: più alto è il numero dei requisiti previsti e rispettato, più alto è il grado di presunzione dell'autenticità

autenticazione/validazione

- La dichiarazione dell'autenticità di un documento da parte di chi sia autorizzato in un determinato sistema giuridico a produrre tale dichiarazione (pubblico ufficiale, notaio, autorità di certificazione):
  - può essere inclusa nel documento
  - in ambiente digitale si traduce in un **metodo per provare l'autenticità del documento in un momento dato** (firma digitale, sigillo informatico, timbro elettronico, ecc.)

validazione nel tempo del documento digitale

- E' un tema centrale e di non facile gestione
- Firme digitali e sigilli informatici sono strumenti cruciali per la validità giuridica dei documenti, sono utilizzabili nella gestione dei processi conservativi, ma non sono in grado di essere conservati funzionalmente se non per un arco temporale limitato: non sono quindi idonei/sufficienti a garantire la persistenza delle memorie digitali:
  - gli istituti di conservazione in Nord America non accettano in versamento documenti cifrati o firmati digitalmente anche se utilizzano meccanismi di cifratura e firma per gestire l'integrità dei trasferimenti e dei pacchetti di archiviazione all'interno del deposito di conservazione

l'autenticità è assicurata da un sistema documentario affidabile **integrato** da un **sistema di conservazione**

- L'autenticità è assicurata dalla **integrità e dalla identificazione univoca e certa dei documenti e delle informazioni** per la loro formazione e gestione che ne consentono la comprensione con riferimento al contesto originario di produzione
- L'autenticità è verificabile se il sistema documentario e i modi concreti di gestione sono **documentati** in modo **completo in tutte le fasi del ciclo di gestione del documento**
- La conservazione digitale è gestibile **a costi ragionevoli** se le procedure sono pianificate e applicate sin dalla formazione dei documenti attraverso la creazione **precoce** e continuamente aggiornata di un sistema di conservazione digitale

le strategie di Adobe per la validità giuridica a lungo termine del documento digitale

- Le strategie individuate da Adobe includono **l'incorporazione** delle risposte di verifica e controllo da parte di chi deve verificare la validità del documento:
  - 1. **incorporazione nel pdf delle risposte sul controllo delle revoche** (server OCSP) con indicazione di data e ora dal server che le crea: es. un consorzio di produttori farmaceutici richiede il controllo incorporato come requisito per una soluzione 'leggera'
  - 2. **incorporazione nel pdf del controllo affidabile di data e ora** in connessione con la produzione dell'impronta del documento
  - 3. **convalida di archivio**: "internalizzazione del processo di autenticazione" mediante la registrazione dei processi di verifica e controlli di validità, revoca e indicatori di data e ora: i metadati sono conservati insieme ai documenti nel sistema di gestione dei documenti (es. il tribunale che accetta documenti legali, moduli e prove "non può contare sul fatto che i certificati siano validi di per sé o sul fatto che una …CA continui ad esistere … Il risultato dei controlli viene documentato e memorizzato nei db e può essere referenziato nel sistema di gestione dei contenuti che ospita i documenti … Il documento può essere considerato valido per un periodo indefinito, coincidente con l'esistenza dei sistemi di archiviazione"

gli interrogativi cruciali

- In questo contesto **quali sono i requisiti** che garantiscono l'esercizio della funzione documentaria in quanto memoria **affidabile per il futuro**? Quanto sono **variabili** in relazione alla tipologia di documento?
- **Quanto è rilevante e in che cosa** consiste la conservazione? Quale **livello di perdita** è accettabile)?
- **Chi** esercita la funzione conservativa in un ambiente digitale? Quali sono i **profili di competenza** necessari? Esiste un modello di **costi**? E' adeguato l'attuale **contesto organizzativo**, il modello, le strutture e gli **strumenti operativi di tutela** esistenti?
- Quali sono i criteri di **affidabilità dei depositi digitali di conservazione**? Quanto **precocemente** e in che forma deve avvenire la custodia?
- Quali sono le **interazioni efficaci** tra ente produttore e struttura di conservazione nella definizione dei **requisiti di versamento**?
- E soprattutto **come si misura, si controlla e si certifica** la fattibilità e l'adeguatezza di chi ha la responsabilità della conservazione?
- E' **compatibile il quadro normativo nazionale con gli standard**?

che cosa si intende per conservazione di documenti digitali

- La funzione in grado di assicurare che gli utenti del futuro possano:
  - identificare, ricercare, trattare, interpretare, utilizzare documenti digitali in un ambiente caratterizzato dalla modifica costante della tecnologia e in condizioni che assicurino la presunzione di autenticità dei documenti medesimi
- Si caratterizza più decisamente rispetto al passato in termini di **gestione del rischio** (speriamo non dell'**incertezza**)
- Richiede un continuo **aggiornamento delle policy**, delle **attrezzature**, degli **standard di rappresentazione**
- Si configura come una **funzione diffusa e condivisa** di *cura del digitale* (*digital curation)*:
- Il nodo centrale della **sostenibilità della funzione** è la **documentazione dei processi di conservazione**

che cosa implica la conservazione di documenti digitali

- interventi di mantenimento dei documenti e delle loro caratteristiche significative (*significant properties* e/o informazioni di rappresentazione?) con specifica attenzione
  - alla completezza, coerenza e accuratezza degli **elementi descrittivi/identificativi delle entità documentarie e delle relazioni di contesto** che danno al documento significato (**nel settore pubblico e in quello privato**)
  - all'adozione di corrette e precoci politiche per gestire il trasferimento di **custodia** e la **selezione**
  - alla **documentazione** nel tempo dei processi e delle attività di gestione e tenuta in tutte le fasi di vita
  - alla definizione e gestione di **architetture** sostenibili

la definizione di conservazione digitale negli standard ISO

- "L'insieme dei principi, delle politiche, delle disposizioni e delle strategie finalizzate a **prolungare l'esistenza di un documento o di una risorsa digitale** grazie alla sua tenuta in condizioni adatte all'uso nella forma originale e/o in un formato persistente che garantisca l'integrità della **configurazione logica** e del **contenuto**" (Standard ISO 14721 – Open Archive Information System)

la conservazione digitale in particolare: i passaggi critici all'interno di un'organizzazione

- **policy interne** a ciascuna organizzazione utilizzando nel caso dei sistemi documentari attivi l'opportunità di predisporre manuali di gestione del sistema documentario (dpr 445/2000 per le pp.aa, ma il nuovo CAD si applica in parte ai privati), con crescente attenzione alla tenuta dei documenti e all'adozione di **manuali della conservazione (DI CUI LA SICUREZZA COSTITUISCE SOLO UNA DIMENSIONE RILEVANTE MA PARZIALE)**
- adozione di **formati** standard nella fase di formazione dei documenti
- individuazione di **responsabilità** certe, *diffuse,* coordinate e documentate

le norme di riferimento

Decreto del Ministro dell'economia e delle finanze 23 gennaio 2004: Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto

Deliberazione CNIPA 19 febbraio 2004: conservazione 'sostitutiva'

Dlgs 20 febbraio 2004, n. 52

Regole tecniche ai sensi dell'articolo 71 CAD in corso di elaborazione (bozza in via di ridefinizione)

CAD 82/2005 e successive modifiche, in particolare dlgs 235/2010

considerazioni generali sull'iter e sullo stato della normativa nazionale

- Percorso lungo e complesso con riferimento
  - alla normativa sulla validità giuridica del documento
  - alle disposizioni sulla conservazione 'sostitutiva' (processo di digitalizzazione di documenti analogici)
- Riduzione delle indicazioni sulla conservazione a lungo termine alle disposizioni sulla conservazione 'sostitutiva'
- Difficoltà del giurista in assenza di un quadro consolidato e di esperienze: inevitabile tendenza a rapportare problemi e soluzioni alla dimensione analogica

le esigenze principali del legislatore

- fornire **indicazioni e procedure che assicurino l'autenticità, l'integrità, la non modificabilità** dei *dati e dei singoli documenti* conservati anche da un ente terzo per ragioni giuridiche e per un *arco temporale limitato* (senza quindi considerare in alcun modo i nodi tecnologici e organizzativi della **conservazione a lungo termine di archivi digitali**),
- l'esigenza di stabilire **modalità che assicurino la conformità all'originale**
  - **di documenti digitali nativi** non più conservabili nella stessa forma e nello stesso formato e
  - di **documenti digitali che costituiscono la riproduzione di documenti analogici** che si vorrebbe destinare successivamente alla distruzione

i principi generali - 1

- distinzione tra **archiviazione informatica** (intesa come semplice attività di memorizzazione su supporti digitali senza ulteriori prescrizioni) e **conservazione sostitutiva** (definita nel dlgs 235/2010 come **conservazione** senza ulteriori attributi), finalizzata a rendere il documento non modificabile né deteriorabile e, quindi, capace di mantenere nel tempo le sue caratteristiche originarie di autenticità e integrità,
- **libertà dell'utente** nel definire le modalità operative del processo (anche in risposta all'eccesso di dettagli tecnici delle disposizioni precedenti, ovvero delle deliberazioni Aipa 15/1994 e 24/1998) e assenza di autorizzazioni preventive

i principi generali - 2

- definizione di **regole tecniche** per la conservazione mediante l'utilizzo dell'impronta del documento e l'apposizione all'insieme dei documenti da conservare del relativo riferimento temporale e della firma digitale da parte del responsabile della conservazione (che in alcuni casi deve avere la veste del pubblico ufficiale), con funzioni di **file di chiusura** del **lotto di conservazione (ma anche come strumento di validità temporale opponibile** a terzi ai sensi del dpcm 30 marzo 2009),
- distinzione tra **riversamento diretto** o **indiretto** dei documenti a seconda che si tratti o meno di modificare la rappresentazione informatica del contenuto e della forma del documento per ragioni di obsolescenza tecnologica (migrazione) o semplicemente per evitare la perdita di efficienza dei supporti (copiatura): nel nuovo CAD si propone una **specifica disciplina** delle copie e si distinguono **copia informatica per immagine** e **duplicato**

i principi generali - 3

- definizione del concetto di **riferimento temporale opponibile a terzi** utilizzando strumenti diversi: marcatura temporale, segnatura di protocollo, posta certificata, predisposizione di lotti per la conservazione,
- individuazione delle modalità per **l'esibizione dei documenti** (criticità dell'obbligo di ricorrere a contrassegni elettronici nel caso di esibizione analogica di documenti digitali),
- identificazione dei compiti e delle responsabilità del **responsabile della conservazione** che includono la realizzazione secondo principi di sicurezza documentati di un sistema informativo relativo ai documenti digitali e la definizione e gestione dell'ambiente applicativo, con specifica attenzione alla tipologia dei documenti da conservare, alle copie di sicurezza e all'eventuale delega di funzioni a terzi. Il nuovo CAD prevede il coordinamento con il responsabile del sistema di gestione dei documenti

circoscrivere le responsabilità per la conservazione

- La responsabilità per la funzione conservativa ha bisogno di specifiche indicazioni sulle forme e sui limiti del suo esercizio, stabilendo ad esempio che
  - la **delega** sia assicurata mediante un atto formale di designazione
  - le **procedure specifiche di conservazione** (ottenute ad esempio mediante la stesura e approvazione congiunta di un **manuale di conservazione**) non siano riducibili alle sole procedure di sicurezza, ma siano capaci di collegare la conservazione alla gestione (il manuale di gestione) con attenzione per le informazioni della fase attiva quali le specifiche modalità di organizzazione e tracciamento dei flussi o la gestione dei fascicoli ibridi.

qualche suggerimento per il manuale della conservazione

- Il manuale operativo della conservazione può assumere la finalità di definire un intervento di pianificazione delle procedure necessarie per la conservazione (vedi anche articoli 50 bis e 51 del CAD)
- Riferimento utile: le **misure operative per la conservazione e la sicurezza** previste per i certificatori accreditati che gestiscono le firme elettroniche ai sensi del CAD (dpcm 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici): articoli 31 (piano della sicurezza), 32 (sistema di controllo), 33 (sistema di qualità del certificatore), 34 (organizzazione del personale addetto alla certificazione), 35 (requisiti di competenza ed esperienza del personale) e 36 (manuale operativo).

la conservazione nell'articolo 44 del Codice

- Le indicazioni si limitano a considerazioni generiche ma corrette (anche se riferite ai singoli documenti e non ai contesti archivistici di produzione e tenuta)
    - **identificazione certa** del soggetto che ha formato il documento o che lo ha acquisito
    - **integrità**
    - **leggibilità** e agevole reperibilità dei documenti e delle informazioni identificative inclusi i dati di registrazione e classificazione originari
    - rispetto delle **misure di sicurezza**

nodi organizzativi: la cooperazione tra responsabili (articolo 44, comma 1bis)

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che **opera d'intesa con il responsabile del trattamento dei dati personali** di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, **con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi** di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

nodi organizzativi: deleghe e limiti del responsabile (articolo 44, comma 1ter)

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 del presente articolo, **ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche**.

i conservatori accreditati: articolo 44 bis

1. I soggetti **pubblici e privati** che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi per conto di terzi ed **intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato**, in termini di qualità e sicurezza, chiedono **l'accreditamento presso DigitPA**.
2. **Si applicano, in quanto compatibili**, gli articoli 26 (requisiti dei certificatori), 27 (certificatori qualificati), 29 (accreditamento, ad eccezione del comma 3, lettera a) e 31 (vigilanza).
3. I **soggetti privati** di cui al comma 1 sono costituiti in **società di capitali con capitale sociale non inferiore a euro 200.000**.

i conservatori accreditati: il riferimento all'articolo 29 sulla qualificazione

1. La qualificazione implica la capacità di
   - dimostrare **l'affidabilità organizzativa, tecnica e finanziaria** necessaria,
   - utilizzare **personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie** per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore tecnologico, della dimestichezza con procedure di sicurezza appropriate ed essere in grado di rispettare le norme previste
   - applicare **procedure e metodi amministrativi e di gestione adeguati** e **conformi a tecniche consolidate** (standard internazionali?)
   - utilizzare **sistemi affidabili e che garantiscono la sicurezza tecnica e crittografica dei procedimenti in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale**

continuità operativa: articolo 50 bis - 1

1. In relazione ai **nuovi scenari di rischio**, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i **piani di emergenza** in grado di assicurare la **continuità delle operazioni** indispensabili per il servizio e il ritorno alla normale operatività.
2. Il Ministro per la pubblica amministrazione e l'innovazione **assicura l'omogeneità delle soluzioni** di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

continuità operativa: articolo 50 bis - 2

3. A tali fini, le pubbliche amministrazioni definiscono :

- a) il **piano di continuità operativa**, che fissa gli obiettivi e i principi da perseguire, descrive le **procedure per la gestione** della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle **potenziali criticità** relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la **funzionalità** del piano di continuità operativa **con cadenza biennale**;
- b) il piano di ***disaster recovery,*** che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di *disaster recovery* delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.
- 4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di **appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere** di DigitPA

sicurezza dei dati, dei sistemi, delle infrastrutture delle pp.aa.: articolo 51

1. Le norme di sicurezza (???) definite nelle regole tecniche di cui all'articolo 71 garantiscono **l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati**. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1-*bis*. DigitPA, ai fini dell'attuazione del comma 1:

- a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
- b) promuove intese con le analoghe strutture internazionali;
- c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

2-*bis*. Le Amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.

alcuni aspetti centrali

- Il ritardo nel riconoscimento della centralità del problema ha lasciato margini ampi alla scelta delle singole amministrazioni
- E' indispensabile definire **linee d'azione**, approvare **policy** adeguate e adottare **infrastrutture** commisurate alle dimensioni e ai mezzi delle diverse istituzioni di conservazione e delle diverse della produzione documentaria (**depositi** digitali e **manuali** per la produzione di documenti digitali e per la loro conservazione, nonché per la gestione delle responsabilità specifiche)
- Il CAD ha una **impostazione ancora riduttiva** nel ricondurre la conservazione a problemi di sicurezza

i nodi da sviluppare nella regolamentazione tecnica

- La normativa di riferimento include alcune importanti indicazioni generali e di principio che andrebbero sostenute e allargate nella regolamentazione tecnica e in norme di accompagnamento:
  - **manuale di gestione** integrati da **manuali della conservazione** (strumenti di documentazione dei processi adottati)
  - **regole per l'interoperabilità** nella trasmissione (segnatura in XML): open data e cooperazione applicativa finalizzati a favorire automazione nei processi di trasmissione nello spazio e nel tempo

le potenzialità del nuovo CAD

Le innovazioni positive includono:

- il riconoscimento della necessità di **discipline particolari** (da approvare con decreto ad hoc del Presidente del Consiglio dei ministri) per la conservazione sostitutiva di particolari tipologie di documenti analogici originali (**garanzie di controllo nel processo di formazione**);
- **l'ancoraggio al protocollo informatico** delle **caselle di posta certificata** (**garanzie di controllo nel processo di formazione**);
- la norma che stabilisce **uno stretto collegamento tra le responsabilità** in materia documentaria tra il responsabile del servizio di protocollo e archivio e il responsabile della conservazione (**garanzie di continuità nella catena delle responsabilità**);
- le norme sull'obbligo dei **piani di continuità operativa e di disaster recovery** e di **sicurezza** (**garanzie di protezione dei contenuti digitali**)

il manuale della conservazione

- Il manuale della conservazione non è indicato in modo esplicito nella normativa (anche se è citato come **strumento di supporto** dal dpcm 30 marzo 2009 che approva le nuove regole tecniche in materia di firme digitali)
- E' possibile (opportuno) **integrarlo nel manuale di gestione** dei documenti nella forma di un allegato
- Il manuale di gestione (previsto dal dpcm 31 ottobre 2000) include parti rilevanti dei processi di conservazione che non dovranno essere sottovalutate (come è stato finora)

la conservazione nel manuale di gestione

- regole di **selezione, versamento** e **conservazione**
- **sicurezza** (diritti di accesso, protocollo di emergenza, gestione dei supporti)
- **conservazione del registro di protocollo** informatico (periodicità coerenti con le esigenze della sicurezza, responsabilità distinte)
- uso e validità giuridica nel tempo della **firma digitale** (natura e titolarità, procedure di sicurezza soprattutto con riferimento al controllo degli accessi: identificabilità degli utenti, mantenimento dei file di log, verifica della firma,ecc.)
- procedure per la **conservazione a norma (anticipata? sostitutiva?)**
- uso di **formati** per i documenti in grado di garantire leggibilità nel tempo, interscambiabilità, immutabilità e persistenza e compatibilità con i meccanismi di firma (html, xml, pdf-a.tiff, txt)

lo standard UniSincro per l'interoperabilità dei lotti/volumi di conservazione

la conservazione “anticipata” e le sue criticità

- La normativa nazionale non risolve il nodo di una **sedimentazione archivistica** governata e razionale, ma si limita a stabilire obblighi di **interoperabilità dei servizi di firma e di marcatura**
- E’ necessario definire le modalità per la creazione dei volumi/lotti di conservazione con particolare (ma non esclusivo) riferimento ai documenti firmati digitalmente a cura del responsabile della conservazione (**lotti o volumi di conservazione** gestiti con **indici di conservazione** riferiti alla procedura di chiusura dei documenti memorizzati a fini di conservazione sostitutiva e alla creazione e gestione di **file di chiusura** previsti dalle delibere Cnipa)

volumi o lotti di conservazione

- Nei sistemi di conservazione sostitutiva un volume o un lotto di conservazione è costituito **dall'insieme dei file** oggetto di conservazione e da un **file ausiliario (indice o file di chiusura)** che contiene informazioni identificative per ogni file conservato (almeno un codice identificativo e l'impronta).
- A fini di integrità l'indice deve essere firmato digitalmente dal responsabile della conservazione e corredato di un riferimento temporale opponibile ai terzi, che può essere una marca temporale.
- L'indice, con firma e riferimento temporale, è finalizzato ad assicurare **l'inalterabilità** di ogni file memorizzato nel sistema di conservazione (grazie all'impronta), la sua **identificazione** mediante un codice univoco e la **data certa** di memorizzazione nel sistema mediante la marcatura temporale.
- Si tratta di uno strumento definito dalla delibera Cnipa del 2004 e sviluppato dai fornitori dei servizi di conservazione sostitutiva al fine di assicurare **garanzie di controllo** al processo di acquisizione e tenuta di file digitali firmati.

consolidamento di documenti sottoscritti e conservazione

- Poiché un volume o un lotto di conservazione è obbligatoriamente corredato di un riferimento temporale opponibile ai terzi (marcatura temporale), tale procedura viene utilizzata non solo al fine di digitalizzare documenti analogici ma anche per risolvere il problema del **consolidamento** (processo di apposizione di una marca temporale a un documento dopo averne verificato la validità in termini di certificato non scaduto, non revocato o sospeso e integrità del contenuto) dei documenti informatici sottoscritti (considerata la difficoltà organizzativa e tecnologica delle amministrazioni e dei privati).
- "Tuttavia, poiché in un volume si accumulano un certo numero di documenti e solo al termine dell'accumulo si applicano la firma del RdC ed il riferimento temporale, **può trascorrere un tempo significativo tra la sottoscrizione del documento ed il riferimento temporale**. Se una revoca o una scadenza di certificato capita in quell'intervallo, si perde il valore probatorio" (Baudizzone)

l'indice di conservazione o file di chiusura: contenuti e formato

- Le disposizioni regolamentari (dpcm 31 marzo 2009) non danno indicazioni specifiche sulle modalità operative di tale processo né sul formato del cosiddetto "**file di chiusura**" (il termine **indice** è citato in forme scarsamente comprensibili tra i compiti del responsabile della conservazione ed è frutto della inconsapevolezza di chi ha scritto quelle norme).
- **L'interoperabilità** è quindi a rischio sia in relazione a **servizi forniti da fornitori diversi per quanto riguarda l'apposizione di firme e di marcature temporali** sia con **riferimento a sistemi di indicizzazione** utilizzati nel tempo anche da parte dello stesso fornitore.

lo standard UNI SInCRO

- Lo standard SInCRO è stato elaborato dalla **Commissione UNI-DIAM** e in particolare dal comitato sulla gestione dei documenti e degli archivi per iniziativa di fornitori preoccupati per la qualità nel tempo dei servizi offerti (Ferri e Baudizzone)
- Ha la finalità di definire una **struttura di dati in XML** che consenta di predisporre sia le informazioni identificative minime (previste dal legislatore) che una **infrastruttura generale in grado di integrare e gestire** tutte le informazioni archivistiche necessarie al processo di formazione e tenuta dei documenti digitali in modo da assicurare l'interoperabilità tra sistemi e la conservazione a lungo termine
- **Presuppone un corretto processo a monte di analisi archivistica dei documenti da digitalizzare e conservare e un adeguato sistema di tenuta dei documenti negli archivi correnti**

lo standard UNI SInCRO: le ragioni

- Le regole tecniche per la conservazione sostitutiva descrivono gli aspetti procedurali e indicano le responsabilità degli attori di questo specifico processo, ma non forniscono **dettagli tecnici** sulle **modalità di rappresentazione dei dati e documenti oggetto di conservazione**, e non contengono alcuna specifica disposizione mirata a conseguire o a promuovere forme d'interoperabilità.
- Gli articoli 3 e 4 in particolare (dedicati alla conservazione sostituiva di documenti informatici ed analogici) **si limitano a prescrivere**
  - l'uso della firma digitale e di un riferimento temporale per perfezionare il processo,
  - con l'intervento del responsabile della conservazione eventualmente integrato o sostituito da quello di un pubblico ufficiale.
  - Tecnicamente l'obbligo è limitato alla apposizione della firma digitale e del riferimento temporale "*sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi*".
- Libertà troppo ampia; rischi di auto-referenzialità e perdita degli investimenti già nel medio periodo

lo standard UNI SInCRO: gli scenari applicativi

evoluzione dei sistemi

- l'assenza d'interoperabilità rende difficile e costosa la migrazione verso nuovi sistemi e soluzioni tecnologiche, vincolando di fatto i soggetti possessori di archivi digitali ai fornitori di servizi e alle loro scelte, con ciò limitando l'auspicabile fluidità delle dinamiche di mercato

accesso ai documenti

- necessità di poter esibire (ad esempio in sede giudiziale, ma anche a mero scopo di consultazione da parte degli aventi diritto) i documenti conservati: in assenza d'interoperabilità e di standard di riferimento si richiedono laboriose perizie per leggere i dati generati da applicazioni *ad hoc*.

lo standard UNI SInCRO – obiettivi specifici

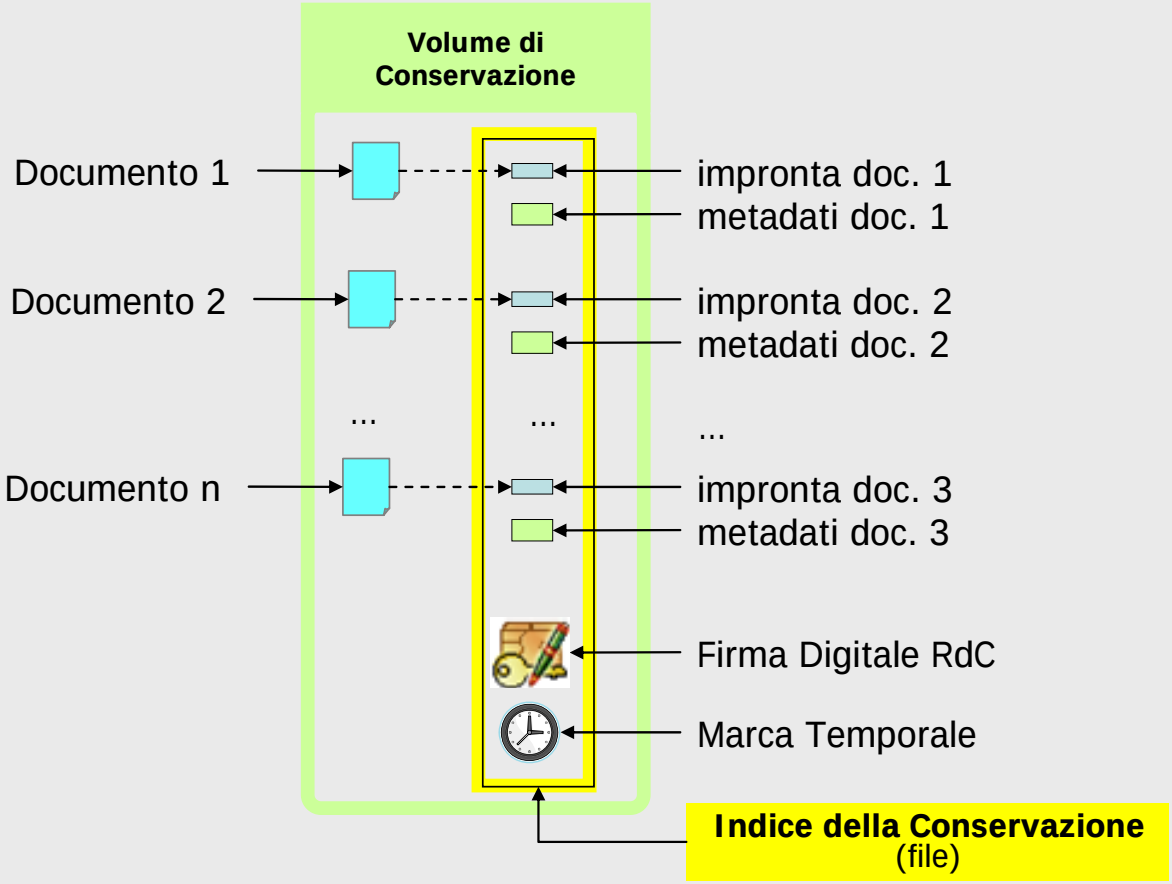
- La norma definisce la struttura dell'insieme di dati a **supporto del processo di conservazione a norma**: in particolare, precisa e integra alcune disposizioni contenute nella deliberazione CNIPA 19 febbraio 2004, n. 11, individuando gli **elementi informativi necessari alla creazione dell'Indice di Conservazione** (il cosiddetto "file di chiusura") e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML.
- L'obiettivo della norma è di consentire agli operatori del settore di utilizzare una **struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione**, grazie all'adozione dello Schema XML appositamente elaborato.

lo standard UNI SInCRO: i vantaggi

- L'adozione di questo standard nello sviluppo di sistemi di conservazione "anticipata" è finalizzato a favorire:
  - **l'interoperabilità** nei sistemi attivi tra produttori diversi e a fini di esibizione
  - **l'aggiornamento** grazie alla presenza di uno schema di metadati aperto alle integrazioni nelle fasi successive di gestione
- E' **indipendente dal fornitore e dall'applicazione**

lo standard UNI SInCRO: il volume di conservazione (VdC) e indice della conservazione (IdC)

(slide di Umberto Ferri)



Standard internazionali e misurazione di qualità per l'accreditamento di depositi per la conservazione digitale

definizione di deposito per la conservazione digitale

Identifica i servizi e l'ente responsabile per la memorizzazione, l'accesso e la conservazione di documenti digitali di diversa natura e complessità insieme ai metadati necessari per descrivere, gestire e rendere disponibili i documenti medesimi

il nodo cruciale non è tecnologico

Da JISC, *Infokit Digital Repository*, 2010
http://www.jiscinfonet.ac.uk/infokits/repositories//index_html

- "What goes into a repository is currently less an issue of technological or software ability, and more a policy decision made by each institution or administrator"

- Il vantaggio principale viene identificato nella presenza di **metadati** minimi obbligatori e conformi a **standard** per ogni documento preso in carico

criteri di creazione (TRAC e NESTOR)

- Le raccomandazioni del documento RLG-NARA, Task Force on digital repository certification, *Audit checklist for certifying digital repositories* (www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf) individuano 4 aree di riferimento:
  - *organizzazione interna*: policy per la conservazione, documentazione delle finalità, responsabilità, procedure e risorse, gestione della qualità (ISO 9000), pianificazione delle risorse
  - *cooperazione con i produttori e gli utenti finali*: definizione della comunità di riferimento, criteri di selezione, linee guida per l'acquisizione, accordi e cooperazione con i produttori, politiche per l'accesso, servizi di consultazione
  - *gestione tecnica del sistema*: conformità agli standard (es. ISO 15489:2001 sul RM, ISO 17799:2005 sulla sicurezza dell'informazione, ISO OAIS 14721), documentazione dei processi tecnici (disegno di sistema delle funzioni conservative della DL), garanzie di autenticità e integrità del sistema, ambiente HW e SW adeguato, fattibilità della migrazione, flessibilità e modularità)
  - *gestione tecnica degli oggetti digitali* (metadati descrittivi, digestione, di conservazione e accesso, vocabolari controllati, codici di identificazione persistenti, autenticità e integrità degli oggetti, formati di archiviazione controllati, disponibilità a lungo termine degli oggetti)

requisiti essenziali negli standard internazionali

- conformità allo **standard OAIS** in quanto capace di fornire un modello funzionale (per l'archiviazione e l'accesso) e informativo (per la gestione dei metadati descrittivi e conservativi) adeguato
- chiara **responsabilità amministrativa**
- **adeguatezza organizzativa e procedurale** del deposito
- **sostenibilità finanziaria** dell'intervento nel lungo periodo
- idoneità della **infrastruttura tecnologica**
- **sicurezza** del sistema

La finalità è quella di assicurare il grado necessario di affidabilità del sistema mediante il riconoscimento di **procedure esplicite e formalizzate**

i profili di responsabilità

- amministratore generale e amministratori di settore;
- record manager e archivisti;
- specialisti ICT (sia nel disegno che nell'implementazione dei sistemi);
- personale per la gestione dei servizi di base e per la sicurezza
- esperti di gestione del rischio;

standard ISO 16363 per la certificazione dei depositi (draft): documentazione dei processi - 1

Governance e stabilità

3.1.1. Mandato istituzionale: documentazione delle finalità, responsabilità, gestione della qualità

3.1.2. Piano strategico del deposito; documentazione delle decisioni amministrative (RM), *disaster recovery*, continuità della funzione (trasferimento delle competenze); sostenibilità finanziaria e pianificazione delle risorse

3.1.3. Policy e linee direttive per la conservazione;

Struttura organizzativa

3.2. Definizione dei ruoli e delle responsabilità; conformità agli standard; profili professionali adeguati e aggiornati

standard ISO 16363 per la certificazione dei depositi (draft): documentazione dei processi - 2

Accountability procedurale

3.3.1. Definizione degli ambiti di intervento

3.3.2. Protocolli, accordi di servizio, flussi di lavoro, manuali operativi interni al deposito

3.3.3. Storia documentata di tutti i cambiamenti relativi agli eventi, alle procedure, agli strumenti software e hardware

3.3.4. Strumenti di audit del deposito e certificazioni

3.3.5. Documentazione relativa alle misure che assicurano l'integrità dei contenuti digitali conservati

3.3.6. Documentazione dei processi di auto-valutazione e di certificazione

standard ISO 16363 per la certificazione dei depositi (draft): documentazione dei processi - 3

Sostenibilità finanziaria

3.4.1. Documentazione di bilancio e contabile

3.4.2. Audit documentati

3.4.3. Documenti sulla gestione del rischio

Contratti e licenze

3.5.1. Accordi di deposito

3.5.2. policy sulla gestione dei diritti

standard ISO 16363 per la certificazione dei depositi (draft): documentazione sulla gestione degli oggetti – 1

Acquisizione di pacchetti di versamento (SIP)

4.1.1. identificazione dei contenuti e delle proprietà destinate alla conservazione (sulla base di specifiche procedure e di documentazione delle scelte effettuate)

4.1.2. identificazione delle informazioni di contesto obbligatorie

4.1.3. specifiche adeguate per il riconoscimento e il futuro trattamento (se possibile automatico) dei documenti da acquisire

4.1.4. meccanismi di verifica rispetto al depositante (controllo della provenienza)

4.1.5. meccanismi di verifica della completezza e accuratezza del trasferimento

4.1.6. strumenti di verifica della sufficienza delle informazioni acquisite per la conservazione degli oggetti anche in termini dei bit che li costituiscono

4.1.7. efficienza dei processi di comunicazione tra deposito e produttore nella fase di trasferimento

4.1.8. documentazione sulle attività di acquisizione in grado di affrontare audit esterni

standard ISO 16363 per la certificazione dei depositi (draft): documentazione sulla gestione degli oggetti - 2

predisposizione di pacchetti di archiviazione (AIP)

4.2.1. esistenza di definizioni precise per ciascun pacchetto di definizione o almeno per ciascuna tipologia con specifico riferimento alle modalità di impacchettamento (identificatori delle componenti e dell'entità complessiva)

4.2.2. informazioni sulle modalità di costituzione dell'AIP nel deposito rispetto a quanto trasferito (SIP)

4.2.3. documentazione sulle decisioni prese per la destinazione finale degli oggetti (conservazione, scarto): procedure, motivazioni

4.2.4. utilizzo di regole per identificatori univoci di ogni AIP all'interno del deposito e per documentare le loro eventuali trasformazioni

4.2.5. strumenti in grado di assicurare informazioni di rappresentazione autorevoli degli oggetti digitali (tipi di file e informazioni rilevanti e persistenti per assicurare la comprensibilità degli oggetti per le rispettive comunità di riferimento)

i parametri della certificazione dei depositi nei progetti internazionali

- La certificazione è un processo ordinato di interventi di verifica sul corretto funzionamento di un sistema di conservazione.
- Riguarda innanzitutto la **capacità di provare la credibilità del deposito e dei suoi contenuti**
- Poiché un sistema è il risultato di una combinazione di elementi o parti, anche di altri sistemi, la sua certificazione dovrà esprimersi attraverso una **successione di atti di verifica** che insistono sul sistema investendo tutte le sue parti.
- Un programma di certificazione, per essere efficace, deve dunque avere **confini certi** ed essere **ripetibile**
- Certezza e sistematicità sono tuttavia difficili da garantire nell'ambiente aperto e dinamico della conservazione digitale

autovalutazione, auditing e requisiti

- Necessità di distinguere tra l'**auto-valutazione** (progetto DRAMBORA) e l'auditing esterno a cura di terzi (progetto MOIMS)
- Necessità di definire parametri interni ed esterni al processo:
  - **attributi e checklist** (TRAC)
  - **costi e tempi** del processo di certificazione
  - **durata** della validità e modalità di gestione delle 'scadenze'

raccomandazioni e standard: lo stato dell'arte

- Dalle linee guida CCSDS allo standard ISO 16363 (draft)
- I principali attori del processo:
  - NARA-RLG-OCLC (2002-2007: TRAC)
  - CCSDS (2003-2011: MOIMS, ISO, PTAB)
  - DCC (2004-2009: DRAMBORA)
  - ADRI (
  - NESTOR (2006: criteri di accreditamento)
  - DINI-CNI (2006-2007: soft certification)

che cosa si certifica

- **Persone**: livelli di formazione e competenze interdisciplinari, aggiornamento
- **Programmi**: mandato istituzionale, risorse finanziarie, staff, infrastrutture di servizio, gestione e conservazione dei depositi, sviluppo dei patrimoni digitali conservati, accesso
- **Processi**: livello di normalizzazione e controllo delle procedure (ISO 14721, standard sulla sicurezza)
- **Dati**: normalizzazione nella gestione dei contenuti e dei metadati (ISO 9000, metadati descrittivi e amministrativi, norme sulla interoperabilità, ad esempio UniSincro per i volumi/lotti di conservazione

  Non tutti i depositi sono uguali: *open-access repository*, depositi istituzionali, depositi digitali per la conservazione, archivi digitali di livello locale, regionale, nazionale e internazionale.

  In molti casi la conservazione non è un obiettivo prioritario né necessario. In altri invece è un obbligo (come nel caso degli archivi nazionali)
- **Standard di riferimento** in corso di approvazione è lo standard 16363 (draft)

gli elementi di valutazione per la certificazione - 1

- **mandato istituzionale** coerente con le finalità anche in termini di garanzia di continuità in caso di trasformazioni istituzionali
- **personale competente** ed esperto per tutti i compiti affidati (tecnologici, organizzativi, archivistici) adeguato in numero e riconosciuto nelle responsabilità
- strumenti e meccanismi per garantire l'**aggiornamento professionale** del personale
- procedure e linee d'azione coerenti inclusive di meccanismi di **verifica** e aggiornamento sul piano **tecnologico e organizzativo**
- strumenti di verifica e monitoraggio interni finalizzati a sostenere la **continuità** della funzione conservativa
- valutazione esterna periodica sulle **funzionalità del deposito**
- **documentazione** dei cambiamenti intervenuti nel deposito con riferimento alle procedure, al software, all'hardware e in relazione alle strategie di conservazione adottate
- strumenti per la verifica **dell'integrità** delle risorse digitali conservate
- **pianificazione** delle attività al fine di garantire la sostenibilità del deposito

gli elementi di valutazione per la certificazione - 2

- **accordi di deposito** con eventuali altri depositi federati
- **funzioni, attività e procedure di acquisizione** degli oggetti digitali che includano:
  - elementi e attributi per ciascuna tipologia di oggetti (identificati secondo standard internazionali)
  - definizione sulla base di accordi scritti con i soggetti produttori che depositano/versano i documenti/archivi delle procedure e delle modalità di gestione e di accesso
  - linee guida per l'acquisizione
  - requisiti per un controllo fisico degli oggetti depositati
  - verifica della completezza e accuratezza degli elementi informativi
  - disponibili (secondo i parametri indicati dal modello OAIS)
  - documentazione delle responsabilità per la conservazione
  - utilizzo di sistemi che garantiscano la identificazione univoca degli oggetti e i legami con le informazioni di rappresentazione
  - utilizzo di meccanismi indipendenti di verifica dell'integrità dei contenuti del deposito

gli elementi di valutazione per la certificazione - 3

- esistenza e documentazione di **strategie di pianificazione** della funzione conservativa e di migrazione/gestione che includano i riferimenti ai registri dei formati secondo gli standard internazionali
- gestione dei **metadati** descrittivi e gestionali/amministrativi
- **politiche per l'accesso** in grado di garantire risposte certe e documentate
- sistemi di **tracciamento** dei file di log in grado di testimoniare le criticità degli accessi
- strumenti in grado di garantire **l'esibizione di documenti autentici**
- **infrastruttura tecnologica** adeguata in termini di sistemi operativi, funzioni di backup, ridondanza (almeno 3 copie) e collocazione sicura delle copie, garanzie per il loro allineamento, meccanismi di verifica delle perdite e delle manipolazioni, processi di migrazione, di documentazione dei processi di gestione del ciclo di vita e del loro impatto sulla conservazione

gli elementi di valutazione per la certificazione - 4

- **sistemi di sicurezza** di alta qualità che includano:
  - l'analisi sistematica dell'ambiente, dei dati, del personale, degli impianti e delle attrezzature, delle esigenze
  - meccanismi di implementazione
  - un sistema chiaro di ruoli, responsabilità e autorizzazioni
  - piani scritti di disaster recovery regolarmente verificati
  - processi per la continuità del servizio

come si certifica - 1

- Sulla base di un modello di riferimento (OAIS)
- In relazione a parametri definiti (TRAC, DRAMBORA e RAC)
- Con il supporto di buone pratiche per le quali sono ancora in via di definizione i parametri di misurazione (progetto PTAB)

come si certifica - 2

- Con l'ausilio di **standard e linee guida** di carattere quantitativo e qualitativo (standard ISO 9000, ma anche standard 27001:2005 sulla sicurezza)
- Con il supporto di **documentazione pre-definita in via normativa** o sulla base di **routine di dominio** (esempio manuale di gestione per la qualità del sistema di gestione documentario del deposito)
- Con **nuovi strumenti** (ad esempio il manuale operativo della conservazione).

chi certifica

- Mancano **figure professionali**
- Mancano **esperienze consolidate** (in corso di elaborazione nell'ambito del progetto europeo APARSEN)
- Servono **metodologie miste** sia dal punto di vista delle discipline che degli strumenti (serve una combinazione di interventi di autovalutazione condotti sulla base di *check-list* standard e fasi di controllo affidate a programmi collaudati esterni di accreditamento e monitoraggio che prevedano la presenza di competenze distinte ma in grado di cooperare)

i principi guida

- documentazione (o evidenza),
- trasparenza,
- adeguatezza,
- misurabilità,
- connessione a reti/standard internazionali, ma anche conformità a pratiche/legislazioni nazionali

le prospettive di sviluppo

- standard internazionali per la definizione di criteri e requisiti per la valutazione dei depositi,
- conformità alle normative e ai contesti nazionali specifici nel processo effettivo di *audit* e accreditamento
  - sviluppo di una **cornice generale** e **comune** di **criteri validi sul piano internazionale**,
  - esecuzione in contesti nazionali o comunque definiti dei processi di valutazione e verifica che conducono all'accreditamento dei depositi,
  - costituzione di **reti** e **consorzi locali** di depositi accreditati e possibilmente federati

indicazioni di approfondimento

qualche indirizzo

- **Per la conservazione digitale:**
- http://www.interpares.org (*progetto InterPARES*)
- http://www.casparpreserves.eu (*progetto Caspar*)
- http://JISC-REPOSITORIES@JISCMAIL.AC.UK (*lista per i depositi digitali)*
  http://www.ukoln.ac.uk/repositories/digirep/index/JISC_Digital_Repository_Wiki *(rete per depositi digitali)*
- http://www.si.umich.edu/CAMILEON/ *(Creative archiving at Michigan and Leeds emulating the old on the new)*
- http://www.sdsc.edu/NARA *(progetto del National Archives di Washington*
- http://www.erpanet.org (*Erpanet*)
- http ://www.dpconline.org (*Digital preservation coalition, UK)*
- http://www.digitaleduurwaamheid.nl *(Digital preservation testbed, NL)*
- http://www.pro.gov.uk/about/preservation/digital/pronom/default.htm (TNA: PRONOM File Format Database) e
  http://droid.sourceforge.net/wiki/index.php/Introduction (DROID)
- *RLG-OCLC. Attributes of a Trusted Digital Repository. Meeting the Needs of Research Resources*, Aug. 2001; *Audit Checklist, February 2007*
- http://www.digitalpreservation.gov/formats/intro/format_eval_rel.shtml *(sui formati secondo la Library of Congress)*
- http://ec.europa.eu/idabc/en/document/3428/556 *(The IDABC PEGSCO Recommendations on Open Document Formats can be found on the IDABC website - as well as further information on related IDABC activities)*
- http://www.jisc.ac.uk/whatwedo/programmes/programme_preservation/2008sigprops.aspx *(Progetto INSPECT)*
- http://repinf.pbworks.com (*REPINF: interoperabilità tra depositi digitali)*
- http://www.jiscinfonet.ac.uk/infokits/repositories//index_html (*JISC, Infokit Digital Repository, 2010)*

standard ISO di riferimento

- ISO 15489-1:2001 Information and Documentation – Records Management – Part 1: General
- ISO 15489-2: 2001 Information and Documentation – Records Management – Part 2: Guidelines
- ISO 18492:2005 Long-term preservation of electronic document-based information
- ISO 23081-1:2006 Information and Documentation – Records management processes – Metadata for records – Part 1: Principles
- ISO 23081-2:2007 Information and Documentation – Records management processes – Metadata for records – Part 2: Implementation issues
- ISO 14721:2003 Space Data and information transfer systems – Open archival information system – Reference model
- ISO 15801:2004 Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability
- ISO/IEC 17799:2005 Information technology – Code of Practice for Information security management
- ISO/IEC 27001:2005 Information Technology Security techniques – Information security management systems
- ISO 19005-1:2006 Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)
- ISO 11799:2003 Information and Documentation – Document Storage requirements for Archive and Library Materials, deserves a reference in the storage chapters below
- ISO 16363 (in corso di approvazione): certificazione dei depositi di conservazione digitale

i principali progetti internazionali in corso - 1

- DCAPE (Distributed Custodial Archival Preservation Environment) project
  - http://salt.unc.edu/dcape
- DIGITAL CURATION CENTRE (DCC)
  - http://www.dcc.ac.uk
- DELOS
  - http://www.dpc.delos.info
- DRIVER Action plan for an International Repository Organisation
  - http://www.driver-repository.eu/
- PLANETS
  - http://www.planets-project.eu/
- CASPAR
  - http://www.casparpreserves.eu/
- INTERPARES
  - http://www.interpares.org
- DRAMBORA
  - http://www.repositoryaudit.eu
- INSPECT (Investigating the Significant Properties of Electronic Content Over Time)
  - http://www.jisc.ac.uk/whatwedo/programmes/programme_rep_pres/inspect.aspx
- REPINF
  - http://repinf.pbworks.com
- ARCHIVEMATICA
  - http://www.archivematica.org