JLIS.it
Italian Journal of Library and Information Science
Rivista italiana di biblioteconomia, archivistica e scienza dell'informazione

La certificazione dei depositi digitali: il *Data Seal of Approval*

Stefano Allegrezza

Introduzione

Negli ultimi anni sta diventando sempre più incalzante la necessità di affidare i propri archivi digitali ad aziende ed enti che forniscono servizi di archiviazione e conservazione a lungo termine; tuttavia questa operazione presuppone un'implicita fiducia nell'affidabilità del fornitore e di conseguenza comincia ad essere impellente l'individuazione di criteri sulla base dei quali valutare i depositi digitali. Nel panorama italiano esistono norme ben precise per le pubbliche amministrazioni, che devono necessariamente affidare i loro archivi digitali a conservatori che abbiamo ottenuto l'accreditamento da parte dell'Agenzia per l'Italia Digitale (AgID), ma non vi sono regole altrettanto stringenti per le aziende o per le singole persone che possono decidere di consegnare i propri archivi a qualsiasi conservatore digitale, anche non accreditato. Inoltre, nulla vieta di rivolgersi al mercato europeo od internazionale, dove le legislazioni sono differenti. Ecco, quindi, che diventa importante individuare delle modalità condivise a livello internazionale per valutare l'affidabilità di un deposito digitale al fine di «provare la credibilità del deposito e dei suoi contenuti» (Guercio 2013, 107).

JLIS.it Vol. 6, n. 3 (September 2015)
DOI: 10.4403/ jlis.it - 11132

Le iniziative internazionali sulla certificazione dei depositi

La comunità internazionale ha cominciato ad interrogarsi sui criteri da prendere in considerazione per valutare l'affidabilità dei depositi digitali fin dagli anni '90; infatti, già nel 1994 la Commission on Preservation & Access (CPA) e il Research Library Group (RLG) Task Force on Archiving of Digital Information cominciarono a lavorare congiuntamente per descrivere ed esplorare la natura di un deposito digitale affidabile; i risultati di questa ricerca vennero pubblicati nel 1996 nel rapporto *Preserving Digital Information: Report of the Task Force on Archiving of Digital Information* (Garrett e Waters 1996). Nel 2002 venne pubblicato il rapporto *Trusted digital repositories, attributes and responsibilities* come risultato di un lavoro condotto da gruppi di ricerca di Research Library Group (RLG) e Online Computer Library Center (OCLC) (RLG-OCLC 2002). Nel contempo sono stati avviati numerosi studi e progetti che hanno portato alla definizione di linee-guida, criteri e strumenti necessari per guidare un processo di valutazione dell'affidabilità di un deposito: tra questi vanno certamente ricordati il *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC), il *Catalogue of Criteria for Trusted Digital Repositories* (NESTOR Catalogue), il *Repository Audit Method Based on Risk Assessment* (DRAMBORA) rilasciato nel 2007 dal Digital Curation Centre (DCC) e Digital Preservation Europe (DPE). Dall'evoluzione dello studio NESTOR è nato lo standard tedesco DIN 31644: *Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive* (in inglese: "Information and documentation - Criteria for trustworthy digital archives") che è stato rilasciato nel 2012 dal gruppo di lavoro DIN su *Trustworthy Digital Archives*; si basa su una serie di 34 criteri e le prime certificazioni di conformità a questo standard sono state rilasciate nel 2014. Analogamente, dall'evoluzione della checklist predisposta dal gruppo di lavoro RLG-NARA (RLG-NARA 2007) e di quella predisposta nell'ambito

del progetto NESTOR è nato lo standard ISO 16363: *Space data and information transfer systems - Audit and certification of trustworthy digital repositories*, che costituisce uno dei principali riferimenti in tema di certificazione dei depositi digitali. Ufficialmente riconosciuto standard nel 2012, si pone «l'ambizioso obiettivo di dar vita ad uno standard internazionale riconosciuto» (Guercio 2013, 122) coerente con il modello ISO 14721 (*Open Archival Information System* – OAIS)[1]. Lo standard è piuttosto complesso e prevede più di cento criteri che analizzano i tre principali aspetti di un archivio digitale sulla base di un approccio espressamente "operativo": l'infrastruttura organizzativa del deposito, la gestione degli oggetti digitali e la gestione del rischio. Allo standard ISO 16363 è collegato lo standard ISO 16919: *Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*, che fornisce le linee-guida per i valutatori. Accanto a questi due standard, che forniscono le basi per una certificazione di livello avanzato, vi è il *Data Seal of Approval* che è utilizzato per una certificazione di livello base (ma, come vedremo più avanti, assai utile) e che costituisce l'argomento principale di questo articolo. Di particolare rilievo per lo scenario europeo è stata l'iniziativa che ha portato alla definizione dello *European Framework for audit and certification of digital repositories*[2]. L'8 luglio 2010 David Giaretta (presidente del Repository Audit and Certification Working Group (RAC) del Consultative Committee for Space Data Systems – CCSDS), Henk Harmsen (a capo del progetto *Data Seal of Approval* – DSA) e Christian Keitel (a capo del gruppo di lavoro DIN "Trusted Archives – Certification"), hanno sottoscritto un *Memorandum of Understanding* (MoU)[3] allo scopo di fissare un insieme di condizioni per la certificazione dei depositi digitali, favorendo la cooperazione

[1] L'ultima versione dello standard è stata pubblicata nel 2012 con il titolo: ISO 14721:2012 *Space data and information transfer systems, Open archival information system (OAIS), Reference model*.

[2] Il sito web di riferimento è http://www.trusteddigitalrepository.eu.

[3] Il *Memorandum of Understanding to Create a European Framework for Audit and Certification of Digital Repositories* è disponibile all'indirizzo http://www.trusted digitalrepository.eu/Memorandum%20of%20 Understanding.html.

tra i principali standard e distinguendo chiaramente i processi di *auditing* esterni da quelli interni (APARSEN 2012). Sulla base di questo accordo sono stati individuati tre livelli di certificazione: *basic*, *extended* e *formal* (si veda la Figura 1).

La *basic certification* costituisce il livello base; si tratta di una certificazione che si fonda sull'auto-valutazione ed è concessa ai depositi che ottengono la certificazione *Data Seal of Approval*.

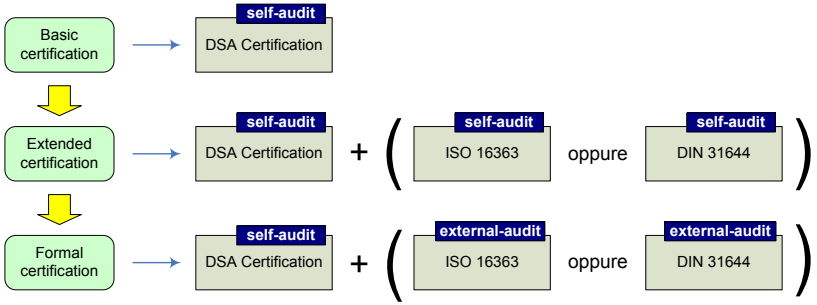

Figura 1. I livelli di certificazione

Gli altri due livelli di certificazione sono entrambi basati sullo standard ISO 16363 o sul suo corrispettivo tedesco DIN 31644.

L'*extended certification* rappresenta il secondo livello di certificazione e viene rilasciato ai depositi che, dopo aver ottenuto la *basic certification*, si sottopongono ad un'auto-valutazione basata sulla norma ISO 16363 o sulla corrispondente norma tedesca DIN 31644, rivista da *auditor* esterni e pubblicamente disponibile. Questa valutazione è molto approfondita: vengono presi in considerazione vari elementi, come il mandato istituzionale, l'infrastruttura tecnologica, il personale impiegato, i metodi adottati per il trattamento degli oggetti digitali e la loro gestione. È importante notare che l'*extended certification* può essere rilasciata solo dopo che il deposito ha ottenuto la *basic certification*: il *Data Seal of Approval* rappresenta dunque un passaggio iniziale ed obbligato senza il quale non si può giungere agli altri due livelli di certificazione.

La *formal certification* rappresenta la certificazione di livello più elevato ed è rilasciata ai depositi che, oltre ad aver conseguito la *basic certification* (anche in questo caso il punto di partenza è sempre il *Data Seal of Approval*) si sottopongono ad un *full external audit* (ovvero una procedura di verifica da parte di un *auditor* esterno), anche in questo caso sulla base della norma ISO 16363 o della corrispondente norma tedesca DIN 31644.

In definitiva, i tre livelli permettono ai depositi di avere a disposizione un percorso di certificazione graduale, che parte dall'auto-valutazione sulla base dei criteri del *Data Seal of Approval*, passa attraverso una successiva e più approfondita auto-valutazione basata sullo standard ISO 16363 o DIN 31644 e si conclude con una valutazione ancora sulla base degli standard ISO 16363 o DIN 31644 ma effettuata da *auditor* esterni. In ogni caso, il punto di partenza è costituito dal *Data Seal of Approval* ed è per questo motivo che è importante conoscerlo più in profondità.

Il Data Seal of Approval

Le origini del *Data Seal of Approval* (DSA) risalgono al 2007 quando il comitato del Data Archiving and Network Services (DANS)[4] decise di avviare un progetto che avesse come obiettivo la definizione di Linee guida per l'auto-valutazione dei depositi digitali. L'idea si deve a Laurents Sesink, Renè van Horik e Henk Harmsen, i quali presentarono una prima stesura delle Linee guida (*Data Seal of Approval: Quality guidelines for digital research*) ad una conferenza internazionale nel 2008. Le Linee guida furono sviluppate inizialmente per essere utilizzate nei Paesi Bassi, ma presto risultò evidente che potevano essere molto utili anche nel contesto internazionale. Di conseguenza, nel 2009 la gestione del *Data Seal of*

[4] DANS è un istituto della Royal Netherlands Academy for Arts and Science (KNAW) e della Netherlands Organization for Scientific research (NWO); ha come obiettivo la promozione dell'accesso ai dati digitali della ricerca scientifica e del loro riuso nei Paesi Bassi.

Approval venne trasferita ad un organismo internazionale, il *DSA Board*[5], che da allora è responsabile dello sviluppo delle Linee guida. La prima versione delle *DSA Guidelines* è stata pubblicata il 1° giugno 2010 ed ha costituito la base su cui sono state rilasciate le prime certificazioni nel triennio 2010-2013[6]. Il 19 luglio 2013 è stata pubblicata la seconda versione, valida per il biennio 2014-2015[7].

È importante notare che le *DSA Guidelines* non sono il frutto di un lavoro isolato ma sono state prodotte in sintonia con le più importanti linee guida internazionali, come *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive* sviluppato da NESTOR; *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) pubblicato dal Digital Curation Centre (DCC) e da Digital Preservation Europe (DPE); *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC) del *Research Library Group* (RLG). Inoltre, sono state prese in considerazione anche *Foundations of Modern Language Resource Archives* del Max Planck Institute (Wittemburg, Peter et al. 2006) e *Stewardship of Digital Research Data: A Framework of Principles and Guidelines* (Research Information Network 2008).

Le *DSA Guidelines* si basano su cinque principi fondamentali, che, nel loro insieme, determinano se i dati versati nel deposito digitale possono essere considerati come archiviati in maniera "sostenibile" [8]:

[5] Il *DSA Board* è eletto tra i membri dell'Assemblea Generale (l'organo di governo della comunità DSA, a sua volta formata da tutte le organizzazioni che hanno uno o più depositi certificati DSA) dai membri stessi; ha il compito, tra gli altri, di gestire la procedura di valutazione DSA.

[6] La prima versione è disponibile all'indirizzo http://datasealofapproval.org/media/filer_public/2013/09/27/guidelines_01-june-2010.pdf. Si noti che questa prima versione era applicabile solo a depositi digitali destinati alla conservazione dei dati della ricerca, mentre questa limitazione è scomparsa con la seconda versione.

[7] La nuova versione è disponibile all'indirizzo: http://datasealofapproval.org/media/filer_public/2013/09/27/ guidelines_2014-2015.pdf.

[8] Si riporta di seguito l'originale in lingua contenuta nella versione 2 delle *DSA Guidelines*: 1) The data can be found on the Internet. 2) The data are accessible, while

1. i dati devono essere resi disponibili su Internet;
2. i dati devono essere accessibili tenendo conto della normativa in materia di tutela della privacy e del diritto d'autore;
3. i dati devono essere disponibili in un formato utilizzabile;
4. i dati devono essere affidabili;
5. deve essere possibile creare riferimenti ai dati (ad esempio, mediante l'utilizzo di *persistent identifier*).

Per quanto riguarda i soggetti coinvolti, esse si focalizzano su tre tipologie di *stakeholder*:

- il *data producer*, ovvero colui che produce gli archivi digitali;
- il *data repository*, ovvero il deposito digitale, responsabile della loro conservazione;
- il *data consumer*, ovvero colui che usufruisce di tali archivi.

Per quanto riguarda la certificazione dei depositi digitali, le *DSA Guidelines* prevedono sedici linee-guida (o criteri) che prendono in esame, in un'ottica qualitativa, gli aspetti della creazione, conservazione e riuso degli oggetti digitali conservati. La documentazione prodotta dal deposito digitale per dimostrare la propria conformità ai criteri richiesti deve essere pubblica, facilmente accessibile on line e preferibilmente scritta in lingua inglese. Se tale documentazione è ancora sotto forma di bozza, allora va indicato un termine di tempo per la loro pubblicazione on line, verificabile dal *DSA Board*. Ai fini della certificazione (con conseguente rilascio del "sigillo"), per ciascuna delle sedici linee

taking into account relevant legislation with regard to personal information and intellectual property of the data. 3) The data are available in a usable format. 4) The data are reliable. 5) The data can be referred to.

guida è previsto un livello di minimo di conformità, che deve essere soddisfatto, su una scala di valori composta da quattro livelli:

- livello 0: linea guida non applicabile (in questo caso occorre fornire la motivazione);
- livello 1: linea guida non ancora presa in considerazione (in questo caso occorre fornire una spiegazione);
- livello 2: linea guida in fase di studio a livello teorico (in questo caso occorre fornire un URL che rinvia alla documentazione provvisoria);
- livello 3: linea guida in fase di implementazione (in questo caso occorre fornire l'URL che rinvia alla documentazione di supporto);
- livello 4: linea guida completamente implementata (in questo caso occorre fornire l'URL che rinvia alla documentazione di supporto).

Per ottenere la certificazione del deposito, le *DSA Guidelines* richiedono una conformità almeno di livello 3 per le linee guida 1, 2, 7, 8, 10, 11, 12, 13, mentre per le rimanenti è richiesto il livello 4.

Le sedici linee guida

È interessante prendere brevemente in esame le sedici linee guida previste dal *DSA Guidelines* nella versione attualmente in uso (la versione n. 2, valida per gli anni 2014-2015). Esse sono suddivise in tre categorie: linee guida relative ai *data producer*, relative ai *data repository* e relative ai *data consumer*[9].

Guidelines relating to data producers:

1. The data producer deposits the data in a data repository with sufficient information for others to assess the quality of the data and

[9] Si riporta qui la versione in lingua inglese, non essendovi ancora una traduzione ufficiale in lingua italiana.

compliance with disciplinary and ethical norms (livello di conformità richiesto: 3).
2. The data producer provides the data in formats recommended by the data repository (livello di conformità richiesto: 3).
3. The data producer provides the data together with the metadata requested by the data repository (livello di conformità richiesto: 4).

Guidelines related to data repositories:
4. The data repository has an explicit mission in the area of digital archiving and promulgates it (livello di conformità richiesto: 4).
5. The data repository uses due diligence to ensure compliance with legal regulations and contracts including, when applicable, regulations governing the protection of human subjects (livello di conformità richiesto: 4).
6. The data repository applies documented processes and procedures for managing data storage (livello di conformità richiesto: 4).
7. The data repository has a plan for long-term preservation of its digital assets (livello di conformità richiesto: 3).
8. Archiving takes place according to explicit work flows across the data life cycle (livello di conformità richiesto: 3).
9. The data repository assumes responsibility from the data producers for access and availability of the digital objects (livello di conformità richiesto: 4).
10. The data repository enables the users to discover and use the data and refer to them in a persistent way (livello di conformità richiesto: 3).
11. The data repository ensures the integrity of the digital objects and the metadata (livello di conformità richiesto: 3).
12. The data repository ensures the authenticity of the digital objects and the metadata (livello di conformità richiesto: 3).
13. The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS (livello di conformità richiesto: 3).

Guidelines related to data consumers:
14. The data consumer complies with access regulations set by the data repository (livello di conformità richiesto: 4).
15. The data consumer conforms to and agrees with any codes of conduct that are generally accepted in the relevant sector for the exchange and proper use of knowledge and information (livello di conformità richiesto: 4).
16. The data consumer respects the applicable licences of the data repository regarding the use of the data (livello di conformità richiesto: 4).

Per ciascuna linea guida, le *DSA Guidelines* forniscono informazioni pratiche (sotto forma di domande) sia per l'attività di auto-valutazione che per quella di revisione da parte del *DSA Board*. Innanzitutto, prima di cominciare la vera e propria attività di auto-valutazione è necessario fornire informazioni riguardo la struttura organizzativa del deposito digitale, delle attività in capo allo stesso e delle sue funzioni, con particolare riguardo a quelle procedure che potrebbero non essere adatte per una revisione paritaria[10]. La descrizione dovrà preferibilmente riferirsi ai termini e alle funzioni previste dallo standard ISO:14721, che viene preso come riferimento. Se alcune delle funzioni del deposito digitale dovessero essere affidate a terze parti, esse devono essere esplicitate in dettaglio in maniera da identificare il livello di controllo che il deposito ha nei confronti della terza parte, descrivendo anche la natura del rapporto che intercorre tra i due soggetti (sia a livello organizzativo che contrattuale). Vi devono anche essere riferimenti ad eventuali certificazioni (*Data Seal of Approval* od altre) possedute dalla terza parte.

Analizziamo sinteticamente i vari requisiti. L'assunto di base è che il rispetto delle linee guida da parte dei *data producer* e dei *data consumer* sia una responsabilità attribuibile al *data repository*. In altre

[10] Si tratta della cd. linea guida n. 0 - "Repository Context", che va ad aggiungersi alle altre sedici linee guida.

parole, un *data repository* è designato come *Trusted Digital Repository* (TDR) se è conforme alle linee guida dalla n. 4 alla n. 13 e se permette ai *data producer* e ai *data consumer* il rispetto delle linee guida dalla n. 1 alla n. 3 e dalla n. 14 alla n. 16 (Dillo e de Leeuw 2014).

Le prime tre linee guida sono relative al *data producer*. La linea guida n. 1 richiede che il *data producer* depositi, oltre agli oggetti digitali, anche le informazioni necessarie per valutare la loro qualità e la loro conformità alle norme disciplinari ed etiche (ad esempio, le informazioni relative ai diritti di proprietà degli oggetti digitali "versati"). La linea guida n. 2 richiede che il *data producer* fornisca gli oggetti digitali in uno dei formati elettronici raccomandati dal *data repository*. A tal fine il deposito deve pubblicare una lista dei formati accettati, specificando quali procedure verranno adottate nel caso in cui il *data producer* fornisca oggetti digitali in formati che non sono compresi in tale lista. La linea guida n. 3 attribuisce al *data producer* la responsabilità di fornire, oltre ai dati, anche i relativi metadati (in accordo con le specifiche fornite dal *data repository*, che dovrà fornire linee-guida e *tool* per produrre correttamente i metadati e dovrà anche indicare qual è la procedura adottata dal deposito se non vengono rispettate le indicazioni fornite).

Le successive dieci linee guida sono relative al *data repository*. La linea guida n. 4 richiede che il *data repository* abbia un'esplicita *mission* nell'area dell'archiviazione digitale e che tale *mission* venga chiaramente divulgata. La linea guida n. 5 richiede che il *data repository* impieghi la dovuta accortezza per assicurare la conformità delle procedure adottate alle norme giuridiche e ai contratti, comprese eventualmente le disposizioni in materia di protezione dei dati personali. A tal fine deve essere specificato il modo in cui il *repository* rispetta la normativa vigente e devono essere descritti i tipi di contratto che vengono sottoscritti con il *data producer* e il *data consumer*. La linea guida n. 6 richiede che il *data repository* utilizzi processi documentati e procedure per gestire le operazioni di *storage* degli oggetti digitali; ad esempio, il deposito deve descrivere le

procedure relative al monitoraggio dei sistemi di *storage*, quelle relative al *back-up* dei dati, quelle relative alla gestione del rischio e della sicurezza. La linea guida n. 7 richiede che il *data repository* abbia un piano per assicurare la conservazione a lungo termine del patrimonio digitale, ad esempio per contrastare il fenomeno dell'obsolescenza tecnologica. La linea guida n. 8 richiede che i processi di archiviazione avvengano secondo prestabiliti flussi di lavoro durante tutto il ciclo di vita dei dati; a tal fine è necessario che vengano descritti tali flussi di lavoro e le procedure utilizzate per il trattamento degli oggetti digitali. La linea guida n. 9 richiede che il *data repository* si assuma le responsabilità in merito all'accesso e alla disponibilità nel tempo degli oggetti digitali; a tal fine, devono essere sottoscritti con il *data producer* degli appositi contratti e devono essere presenti piani per la gestione delle situazioni critiche. La linea guida n. 10 richiede che il *data repository* permetta agli utenti di ricercare ed utilizzare gli oggetti digitali (ad esempio, rendendoli disponibili in formati standard e mettendo a disposizione funzionalità di ricerca) e di creare riferimenti a essi in maniera persistente (ad esempio, utilizzando *persistent identifiers*). La linea guida n. 11 richiede che il *data repository* assicuri l'integrità degli oggetti digitali e dei metadati (ad esempio, utilizzando meccanismi quali *checksum* e *versioning*). La linea guida n. 12 richiede che il *data repository* assicuri l'autenticità degli oggetti digitali e dei metadati, ad esempio monitorando eventuali modifiche degli oggetti stessi. La linea guida n. 13 richiede che l'infrastruttura tecnologica sia conforme ad uno degli standard archivistici accettati a livello internazionale (come l'ISO 14721); poiché l'infrastruttura tecnologica fornisce le basi per la realizzazione di un *Trusted Digital Repository*, il deposito deve indicare quali standard sono stati presi come riferimento ed esplicitando quali procedure sono ad esso conformi e quali invece si allontanano dalle indicazioni dello standard.

Le ultime tre linee guida riguardano il *data consumer*. La linea guida n. 14 richiede che questo si conformi alle regole per l'accesso ai dati stabilite dal *data repository*, ad esempio sottoscrivendo accordi di

licenza o contratti diversificati a seconda del tipo di utente. La linea guida n. 15 richiede che il *data consumer* si conformi ai codici di condotta per lo scambio e l'utilizzo delle informazioni che sono generalmente accettati in un determinato settore (ad esempio, quelli per la protezione dei dati sensibili). Infine, la linea guida n. 16 richiede che il *data consumer* rispetti le licenze previste dal *data repository* riguardo l'utilizzo delle risorse digitali; a tal fine il *data repository* è tenuto ad informare il *data consumer* delle licenze adottate (ad esempio, *Creative Commons*).

In sostanza le *DSA Guidelines* prendono in considerazione tutti gli aspetti che rendono un deposito digitale affidabile (Dillo 2014): in primo luogo, la sua missione dovrebbe essere quella di garantire, non solo ora ma anche in futuro, l'accesso ai dati digitali che gli sono stati consegnati in custodia; in secondo luogo, il deposito dovrebbe essere costantemente tenuto sotto controllo, con operazioni di manutenzione che prendano in considerazione le possibili minacce ed i rischi; infine, dovrebbe essere continuamente sottoposto a processi di *audit* e certificazione: l'affidabilità non è qualcosa che si raggiunge una volta e poi si può dare per scontata per sempre.

La procedura di certificazione

La procedura di certificazione è piuttosto "snella" e prevede tre fasi: innanzitutto il deposito digitale che intende "certificarsi" deve inviare una richiesta compilando un *application form* presente sul sito web del *Data Seal of Approval*[11]. Una volta ricevuta la richiesta, il *DSA Board* rende disponibile l'accesso ad una procedura on line di auto-valutazione (*DSA online tool*) che il deposito utilizzerà per fornire evidenza del rispetto delle sedici linee guida. Infine, la documentazione prodotta viene valutata dal *DSA Board*, che ha il compito di verificare la correttezza delle risposte fornite e la conformità del deposito ai parametri minimi richiesti. Al termine di

[11] L'*application form* è disponibile all'indirizzo https://assessment.datasealofapproval.org/apply.

questa valutazione, se l'esito è favorevole, viene rilasciato il "Data Seal of Approval", ovvero il "sigillo di approvazione dei dati" il cui logo potrà essere pubblicato nella home-page del sito web del deposito (si veda la Figura 2); l'auto-valutazione verrà poi pubblicata sul sito del *Data Seal of Approval*. Ovviamente il sigillo di approvazione viene rilasciato sulla base di una particolare versione delle linee guida e potrà essere utilizzato sul sito web del deposito a tempo indeterminato. Tuttavia, se il deposito vuole mantenere aggiornata la sua certificazione, dovrà nel tempo sottoporsi nuovamente ad ulteriori procedure di auto-valutazione[12] sulla base delle nuove versioni del *Data Seal of Approval* che saranno via via rilasciate (ricevendo i relativi "sigilli" se l'esito sarà favorevole)[13].

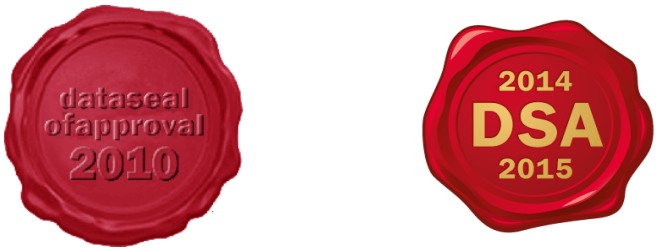

Figura 2. I "sigilli" rilasciati sulla base della prima (a sinistra) e della seconda (a destra) versione delle *DSA Guidelines*

Considerazioni finali

La certificazione dei depositi digitali rappresenta il principale strumento attraverso il quale un deposito digitale può dimostrare la propria affidabilità e creare fiducia negli utenti. In questo senso il *Data Seal of Approval* costituisce un buon punto di partenza: la realizzazione di una auto-valutazione basata sulle sedici linee guida

[12] A tal fine, i depositi certificati verranno contattati automaticamente quando è disponibile un aggiornamento delle linee guida del *Data Seal of Approval*.
[13] Il sigillo che viene attualmente rilasciato è attribuito sulla base della versione 2 delle linee guida e mostra all'interno del logo la scritta "2014-2015".

non richiede molto tempo (solitamente sono necessari da due a quattro giorni; ovviamente il tempo necessario dipende molto dalla documentazione già presente e dal suo livello di divulgazione), ma è molto utile per evidenziare i punti di forza e di debolezza del deposito; in ogni caso costituisce una solida base per una successiva certificazione di conformità agli standard ISO 16363 o DIN 31644. Anche il fatto che si tratti di un'autovalutazione sottoposta ad un processo di revisione tra pari (peer-review) - e non dall'alto verso il basso - viene percepito come un fattore positivo ed in grado di fornire maggiori garanzie di correttezza ed imparzialità rispetto a valutazioni effettuate da *auditor* esterni. Infine, il *Data Seal of Approval* è già piuttosto diffuso a livello internazionale: agli inizi del 2015 sono circa quaranta i depositi che hanno già ottenuto il sigillo di approvazione ed altrettanti hanno avviato le procedure per ottenerla[14]. È, pertanto, lecito aspettarsi che diventi ben presto una delle certificazioni imprescindibili per i depositi digitali che aspirano ad essere riconosciuti come una fonte affidabile di dati.

[14] La comunità DSA sta crescendo rapidamente e si dimostra particolarmente attiva: alla prima conferenza internazionale che si è tenuta a Firenze il 10 dicembre 2012 (prima del convegno internazionale "Cultural Heritage Online: Trusted Digital Repositories & Trusted Professionals") hanno partecipato oltre 40 persone, provenienti da tutto il mondo; si è trattato di un momento importante di confronto nel quale sono stati presi in esame i *case study* rappresentati dai primi depositi che avevano ricevuto il *Data Seal of Approval*. La seconda conferenza internazionale si è tenuta l'8 ottobre 2013 in Ann Arbor, Michigan, nel campus della University of Michigan. La terza conferenza internazionale si è tenuta il 24 settembre 2014, ad Amsterdam, nei Paesi Bassi, ed è stata presieduta da Ingrid Dillo del Data Archiving and Networked Services (DANS), il deposito digitale che sviluppò il concetto di *Data Seal of Approval* e il relativo progetto.

Bibliografia

APARSEN. 2012. Deliverable D33.1B, *Report on peer-review of digital Repositories*, WP 33. http://www.alliancepermanentaccess.org/wpcontent/uploads/downloads/2012/04/ APARSEN-REP-D33_1B-01-1_0.pdf

Centre for Reserch Libraries, *Core Criteria*. http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re

Data Seal of Approval, *DSA Guidelines, version 2 (2014-2015)*, http://datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

Dillo, Ingrid and Lisa de Leeuw. 2014. *Data Seal of Approval: Certification for sustainable and trusted data repositories*. http://datasealofapproval.org/media/filer_public/2014/10/03/20141003_dsa_overview_defweb.pdf

DIN 31644, *DINI Certification Document and Pubblication Service* edoc.hu-berlin.de/series/dini-schriften/2010-3-en/PDF/dini-zertifikat-2010-3-en.pdf

DRAMBORA, *Digital Repository Audit Method Based on Risk Assessment* http://www.repositoryaudit.eu/about

Garrett, John e Donald Waters. 1996. *Preserving Digital Information: Report of the Task Force on Archiving of Digital Information*. (Washington, DC: Commission on Preservation and Access, and Mountain View, CA: RLG , 1996) http://www.rlg.org/ArchTF/index.html

Giaretta, David. 2011. *Advanced digital preservation*, Springer Verrlag, Berlin-Heidelberg.

Guercio, Maria. 2011. *Misurare e certificare la conservazione. Nuovi profili, nuove competenze*, in *Un futuro per il presente, politiche strategie e strumenti della conservazione digitale*, Bologna, PARER. http://parer.ibc.regione.emilia-romagna.it/saperi/copy_of_presentazioni/seminario-un-futuro-per-il-presente-presentazione-di-mariella-guercio

Guercio, Maria. 2013. *Conservare il digitale. Principi, metodi e procedure per la conservazione a lungo termine di documenti digitali*, Laterza, Roma.

Keitel, Christian. 2012. *DIN standard 31644 and Nestor Certification*, Buden-Wurttemberg. http://www.rinascimento-digitale.it/conference2012/paper_ic_2012/keitel_paper.pdf

ISO 14721:2012, *Space data and information transfer systems, Open archival information system (OAIS) -- Reference model*.

ISO 16363:2012, *Audit and certification of trustworthy digital repositories*.

ISO 16919:2014, *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories*.

NESTOR, *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive* http://www.langzeitarchivierung.de

Research Information Network. 2008. *Stewardship of Digital Research Data: A Framework of Principles and Guidelines.* http://www.rin.ac.uk/system/files/attachments/Stewardship-data-guidelines.pdf

RLG-OCLC. 2002. Report, *Trusted digital repositories, attributes and responsibilities*, Mountain View, California. http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

RLG-NARA. 2005. *An Audit Checklist for the Certification of Trusted Digital Repositories*, Mountain View, California. http://library.oclc.org/cdm/ref/collection/p267701coll33/id/408

RLG-NARA. 2007. *Trustworthy Repositories Audit and Certification: Criteria and checklist*. www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

Wittemburg, Peter et al. 2006. *Foundations of Modern Language Resource Archives.* Max-Plack- Institute for Psychilingustics. http://arxiv.org/ftp/cs/papers/0606/0606006.pdf

STEFANO ALLEGREZZA. Università degli Studi di Udine. stefano.allegrezza@uniud.it.

Allegrezza, S. "La certificazione dei depositi digitali: il *Data Seal of Approval*". *JLIS.it*. Vol. 6, n. 3 (September 2015): Art: #11332. DOI: DOI: 10.4403/ jlis.it - 11132

ABSTRACT: In recent years, it has become increasingly common to entrust records to digital repositories; this assumes an implicit confidence in the repositories reliability, and therefore is urgent to identify the criteria on which to evaluate them. The Data Seal of Approval is a set of sixteen criteria that can be used to ensure that archived data can still be found, understood and used in the future. It is a basic level of certification but it is very useful to highlight the strengths and weaknesses of the deposit; in any case, it constitutes a solid basis for further certification of compliance to ISO 16363 or DIN 31644. The aim of this article is to provide an overview of Data Seal of Approval in the wider context of digital repositories' certification..

KEYWORDS: Digital Archives; Digital Repositories; Digital preservation; Trusted Digital Repositories; Data Seal of Approval.

Submitted: 2015-05-29

Accepted: 2015-06-25

Published: 2015-09-15