# HDC-Bericht

| | |
|---|---|
| **Projektakronym:** | HDC |
| **Förderer:** | Niedersächsisches Ministerium für Wissenschaft und Kultur / Niedersächsisches Vorab |
| **Fördernummer:** | VWZN2941 Humanities Data Centre |
| **Thema:** | Forschungsdatenmanagement |
| **Projektdauer:** | 01.05.2014 – 30.04.2016 |

| | |
|---|---|
| **Nummer des Berichts:** | 3.8 |
| **Titel des Berichts:** | Analyse der Anforderungen aus aktuellen Zertifizierungsstandards |
| **Termin des Berichts:** | M06, Oktober 2014 |
| **Revisions-Nummer:** | 01 |
| **AP-Nummer:** | 8 |
| **AP-Leitung:** | GWDG |
| **Weitergabe:** | Restricted |


| AutorInnen | Partner |
|---|---|
| Claudia Engelhardt | SUB |
| Sven Bingert | GWDG |
| Ulrich Schwardmann | GWDG |

# Inhaltsverzeichnis

# 1. Einleitung

Ziel des Arbeitspakets 8 „Zertifizierung“ in der Designphase des HDC war es zum einen, die derzeit maßgeblichen Standards und Zertifizierungen zur Vertrauenswürdigkeit digitaler Archive bzw. Repositorien hinsichtlich ihrer Implikationen für die Arbeit in den einzelnen Arbeitspaketen zu analysieren und entsprechende Empfehlungen zu geben. Zum anderen ging es auch darum zu eruieren, welche Art der Zertifizierung am Ende der auf die Designphase folgende Aufbauphase des HDC sinnvollerweise zunächst angestrebt werden soll.

Eine Zertifizierung als vertrauenswürdiges digitales Langzeitarchiv dient nicht nur dazu, NutzerInnen wie auch Forschungsförderern Vertrauenswürdigkeit zu demonstrieren und somit die Sichtbarkeit und Akzeptanz der Einrichtung in diesen Zielgruppen zu erhöhen. Die entsprechenden Standards und Richtlinien können auch – gewissermaßen als Checkliste – beim Auf- oder Umbau eines digitalen Archivs genutzt werden, denn sie enthalten die wesentlichen relevanten Kriterien, die dabei idealerweise beachtet werden sollten. Dies macht sie zudem zu einem geeigneten Werkzeug, um zu überprüfen, ob die Infrastruktur, Workflows, organisatorischen Prozesse etc. in einem bestehenden Archiv den Anforderungen an ein vertrauenswürdiges digitales Langzeitarchiv entsprechen (und ggf. Verbesserungen vorzunehmen).[1]

In diesem Bericht wird, im zweiten Kapitel, zunächst das Konzept der Vertrauenswürdigkeit digitaler Archive skizziert, gefolgt von einem kurzen Abriss der Geschichte der für Forschungsdatenzentren und Langzeitarchive zentralen Standards und Zertifizierungen TRAC/ISO 16363, nestor-Siegel/DIN 31644 und Data Seal of Approval (DSA) sowie der Kriterien des World Data Systems. Kapitel 3 gibt einen Überblick über den „European Framework for Audit and Certification of Digital Repositories“. Anschließend werden in Kapitel 4 zusammenfassend die wesentlichen Inhalte der drei erstgenannten Standards dargestellt. Kapitel 5 geht kurz auf die Kosten ein. Kapitel 6 schließlich widmet sich den Anforderungen und Empfehlungen, die sich aus den Kriterien eines ausgewählten Standards für die Konzeption und den Aufbau des HDC ableiten lassen. Hierfür werden die Kriterien des DSA herangezogen, das als erste vom HDC anzustrebende Zertifizierung empfohlen wird.

# 2. Vertrauenswürdigkeit und Zertifizierung digitaler Langzeitarchive

Dobratz und Schoger[2] definieren den Begriff der Vertrauenswürdigkeit digitaler Archive, angelehnt an die Definition der Vertrauenswürdigkeit von IT-Systemen des Internet Security Glossary[3], als „die Eigenschaft eines Systems […], gemäß seinen Zielen und Spezifikationen

[1] Vgl. Engelhardt, Claudia; Recker, Astrid: Trust and the European Framework for Audit and Certification of Digital Repositories. Präsentation anlässlich des DASISH Workshops on Trust and Certification, 16./17. Oktober 2014, Den Haag. http://dasish.eu/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_Intro_trust_and_MoU-Framework_Recker_Engelhardt.pdf

[2] Dobratz, Susanne; Schoger, Astrid: 5.2. Grundkonzepte der Vertrauenswürdigkeit und Sicherheit. In: nestor-Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung. Version 2.3. Hrsg. von Neuroth, Heike et al. Göttingen: nestor c/o Niedersächsische Staats- und Universitätsbibliothek 2010, S. Kap.5:2-Kap.5:8, hier S. Kap.5:2. URN: urn:nbn:de:0008-2010030597

[3] Network Working Group (2007): Internet Security Glossary. Request for Comments: 4949 http://tools.ietf.org/html/rfc4949

zu operieren (d.h. es tut genau das, was es zu tun vorgibt) und dies auch in geeigneter Weise glaubhaft zu machen (z.B. durch eine formale Analyse)“.

Ziel eines digitalen Langzeitarchivs ist es, die in ihm archivierten digitalen Objekte mit ihren Significant Properties, also ihren wesentlichen Eigenschaften, zu erhalten. Dies beinhaltet die Erhaltung der Integrität (die digitale Objekt sind unverändert), der Authentizität (die digitalen Objekt sind echt), der Vertraulichkeit (die Objekte sind geschützt vor dem Zugriff unberechtigter Dritter) sowie der Zugänglichkeit der Objekte.[4] Als Referenzmodell dafür, wie ein System beschaffen sein muss, dass diesen Anforderungen gerecht wird, kann wohl unangefochten das Open Archival Information System (OAIS)[5] angesehen werden.

Das OAIS stellt die grundsätzlichen Funktionen und Verantwortlichkeiten eines Vertrauenswürdigen Archivs dar und schafft eine Terminologie zur Beschreibung der einzelnen Komponenten und Funktionen. Die zentralen Funktionen eines Archivsystems sind nach dem OAIS Übernahme (Ingest), Archivspeicher (Archival Storage) und Zugriff (Access). Flankiert werden diese aufeinander folgenden Phasen von den übergreifenden Aufgaben der Datenverwaltung (Data Management), der Verwaltung des Archivsystems (Administration) sowie der Erhaltungsplanung (Preservation Planning).[6]

Das OAIS beschreibt allerdings nur ein Modell und bleibt demgemäß relativ abstrakt. Es liefert keine Kriterien, nach denen tatsächlich bewertet werden kann, ob und in welchem Grad ein Archiv diesem Modell entspricht. Deshalb haben verschiedene Arbeitsgruppen begonnen, Checklisten und Kriterienkataloge zu entwickeln, anhand derer die Vertrauenswürdigkeit eines digitalen Archivs überprüft werden kann. Einige dieser Kriterienkataloge wurden mit der Zeit zu Standards. Manche dieser Standards wiederum bildeten bzw. bilden die Grundlage für Zertifizierungsverfahren.

Im Folgenden werden zwei Beispiele solcher auf Grundlage des OAIS entwickelten Standards und Zertifizierungen näher betrachtet, die gegenwärtig international bzw. v.a. im deutschsprachigen Raum (im zweiten Beispiel) von Relevanz sind:

- CRL und OCLC veröffentlichten 2007 das Dokument „Trustworthy Repositories Audit & Certification: Criteria & Checklist“ (TRAC).[7] Dieses wiederum war Grundlage für „Audit and Certification of Trustworthy Repositories“[8], das vom CCSDS im September 2011 herausgegeben und im selben Jahr auch als ISO-Standard (**ISO 16363**)[9] veröffentlicht wurde.

[4] Dobratz und Schoger, S. Kap.5:3

[5] Die erste Fassung des OAIS wurde 2002 vom Consultative Committee for Space Data Systems (CCSDS) veröffentlicht. Eine überarbeitete Version erschien 2012 (CCSDS: Reference Model for an Open Archival Information System (OAIS). Recommended Practice. CCSDS 650.0-M-2. Magenta Book, June 2012. http://public.ccsds.org/publications/archive/650x0m2.pdf). Das OAIS wurde zudem als ISO-Standard veröffentlicht (ISO 14721:2012: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=57284). 2012 erschien zudem eine deutsche Übersetzung, die 2013 überarbeitet wurde: nestor-Arbeitsgruppe OAIS-Übersetzung / Terminologie: Referenzmodell für ein Offenes Archiv-Informations-System – Deutsche Übersetzung, Version 2.0. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2013. (nestor-materialien 16). URN: urn:nbn:de:0008-2013082706

[6] Vgl. CCSDS 2012, S. 4ff. sowie nestor-Arbeitsgruppe OAIS-Übersetzung / Terminologie 2013, S. 33ff.

[7] CRL; OCLC: Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC). 2007. http://www.crl.edu/PDF/trac.pdf

[8] CCSCS: Audit and Certification of Trustworthy Digital Repositories. Recommended Practice. CCSDS 652.0-M-1. Magenta Book, September 2011. http://public.ccsds.org/publications/archive/652x0m1.pdf

[9] ISO 16363:2012. Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510

Das Vorliegen des Standards ISO 16363 allein ist jedoch noch nicht ausreichend, um tatsächlich auch eine Zertifizierung durchführen zu können. Es wird auch ein Standard benötigt, der die Durchführung des Zertifizierungsprozesses sowie die notwendigen Kompetenzen auf Seiten der AuditorInnen definiert. Dies ist festgelegt im Standard ISO 16919: "Requirements on Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories"[10], der erst im Herbst 2014 veröffentlicht wurde – weshalb bisher auch noch kein digitales Archiv nach ISO 16363 zertifiziert wurde. Mit dem Vorliegen von ISO 16919 ist eine formale Zertifizierung nach ISO 16363 nun theoretisch möglich.

- Die nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung erarbeitete den „Kriterienkatalog vertrauenswürdige digitale Langzeitarchive", der in der aktuellen Version von 2008[11] vorliegt. Aufbauend auf dieser Arbeit wurde im Jahr 2012 die DIN-Norm **DIN 31644** „Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive"[12] verabschiedet. Auf Grundlage dieser Norm entwickelte die nestor-Arbeitsgruppe ein Verfahren zu erweiterten Selbstevaluierung, das **nestor-Siegel**, das seit 2013 existiert.[13] Erste Einrichtungen, bspw. DANS[14,15], haben mit den Vorbereitungen zur Erlangung des nestor-Siegels begonnen, bisher ist den AutorInnen jedoch keine Institution bekannt, die das Siegel bereits erworben hat.

Neben den beiden genannten gibt es noch weitere Evaluierungsinstrumente, die speziell für Forschungsdatenzentren entwickelt wurden. Zwei, die sich etabliert haben, sind das Data Seal of Approval und die Kriterien des World Data Centre:

- Das **Data Seal of Approval (DSA)** wurde ursprünglich von DANS erarbeitet. Ziel war es, ein Siegel zu entwickeln, das es erlaubt einzuschätzen und zu bestätigen, dass das Datenzentrum in einer Art und Weise betrieben wird, die es ermöglicht, dass die archivierten Daten auch in Zukunft gefunden, verstanden und nachgenutzt werden können. Die erste Version wurde 2008 veröffentlicht; 2009 wurde die Verantwortung für das Siegel an ein internationales Board übergeben.[16] Das DSA erfreut sich zunehmender Popularität, v.a. in der europäischen Community. Im Oktober 2014 hatten bereits 36 Datenzentren das Siegel erlangt, weitere 34 befanden sich im Zertifizierungsprozess.[17] Auch in den geistes- und sozialwissenschaftlichen ESFRI[18]-Initiativen

[10] ISO 16919:2014. Space data and information transfer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57950

[11] nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive Version 2. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2008. (nestor-materialien 8). URN: urn:nbn:de:0008-2008021802

[12] DIN 31644. Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive. http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=147058907&languageid=de&bcrumblevel=3

[13] Vgl. nestor-Siegel für vertrauenswürdige digitale Langzeitarchive. 06.08.2013. nestor. http://www.langzeitarchivierung.de/Subsites/nestor/DE/nestor-Siegel/siegel_node.html

[14] DANS: Data Archiving and Networked Services. http://www.dans.knaw.nl/en

[15] Vgl. Grootveld, Marjan, DIN@DANS. (Präsentation anlässlich des DASISH Workshop on Trust and Certification, 16.17. Oktober 2014, Den Haag). http://dasish.eu/dasishevents/wstrustcertification/2014_10_17_DASISH_trust-ws_nestorSeal_case_study_DANS_Grootveld.pdf

[16] Vgl. About. Data Seal of Approval. http://datasealofapproval.org/en/information/about/

[17] Vgl. Trilsbeek, Paul: Data Seal of Approval. Overview. (Präsentation im Rahmen des DASISH Workshop on Trust and Certification, 16./17. Oktober 2014, Den Haag). http://dasish.eu/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_DSA_Trilsbeek.pdf

bzw. ERICs[19] (insbesondere in CLARIN, DARIAH-EU und CESSDA) etabliert sich das DSA zunehmend als Anforderung an Mitgliedsdatenzentren.[20]

- Das World Data System (WDS) ist eine Einrichtung des International Council for Science (ICSU). Es wurde 2008 eingerichtet, kann jedoch, wenn man seine Vorläufer, die World Data Centres einbezieht, auf eine mehr als 50-jährige Geschichte und entsprechende Erfahrung zurückblicken. Ziel des WDS ist es, naturwissenschaftliche Forschung durch die Koordinierung von Services zur Bereitstellung, Nutzung und Langzeitarchivierung relevanter, qualitätsgesicherter Forschungsdaten zu unterstützen. Dies soll durch eine Infrastruktur aus weltweit verteilten, interoperablen, zertifizierten vertrauenswürdigen Datenzentren gewährleistet werden.[21] Das WDS hat, auf der Grundlage etablierter Standards, zu denen u.a. auch das DSA, DIN 31644 und ISO 16363 gehören, eigene Kriterien für die Zertifizierung von Mitgliedern entwickelt.[22] Im Herbst 2014 wurde die Etablierung einer gemeinsamen Arbeitsgruppe von WDS und DSA bekannt gegeben, deren Ziel die Harmonisierung der beiden Standards und die Erarbeitung eines gemeinsamen Standards zur „basic certification" (siehe nächstes Kapitel) ist.[23]
  Da das World Data System (WDS) sich speziell an die Natur- und Lebenswissenschaften richtet und zudem seine Kriterien aufgrund ihrer Genese sich in den wesentlichen Punkten mit den bisher aufgeführten Standards decken, wird es im Rahmen von AP8 nicht näher betrachtet.

# 3. The European Framework for Audit and Certification of Digital Repositories

Die Arbeit an den verschiedenen Standards und Zertifizierungen fand und findet nicht isoliert voneinander statt. Die entsprechenden Arbeitsgruppen haben sich vielfach ausgetauscht, miteinander kooperiert und sich gegenseitig aufeinander bezogen und tun dies immer noch. Um existierende Standards in Relation zueinander zu setzen und ein „integrated framework" für den Audit und die Zertifizierung von vertrauenswürdigen Repositorien bzw. digitalen Archiven zu schaffen, unterzeichneten die Leiter der CCSDS/ISO-Arbeitsgruppe, des Data Seal of Approval Boards und der nestor/DIN-Arbeitsgruppe ein Memorandum of Understanding zur Etablierung des „European Framework for Audit and Certification of Digital Repositories".[24] Dieser sieht drei Stufen der Zertifizierung vor. Dabei steigen mit der Stufe sowohl der mit der jeweiligen Zertifizierung assoziierte Grad an Vertrauenswürdigkeit, als auch der Auf-

Eine aktuelle Liste der Datenzentren, denen das Siegel zuerkannt wurde (derzeit 38, Stand 19.02.2015), ist auf der DSA-Webseite einsehbar: http://www.datasealofapproval.org/en/assessment/

[18] ESFRI. 07.05.2015. European Commission. http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=esfri

[19] European Research Infrastructure Consortium (ERIC). 16.04.2015. European Commission. http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=eric

[20] Vgl. DASISH workshop on trust and certification. DASISH. http://dasish.eu/dasishevents/wstrustcertification/

[21] Vgl. About. ICSU World Data System. https://www.icsu-wds.org/organization

[22] Vgl. ICSU World Data System: Certification of WDS members. 11 June 2011. https://www.icsu-wds.org/files/wds-certification-summary-11-june-2012.pdf

[23] Vgl. Data Seal of Approval and World Data System to Collaborate. 22.11.2014. Data Seal of Approval. http://datasealofapproval.org/en/news-and-events/news/2013/11/22/dsa-and-wds-collaborate/

[24] Vgl. European Framework for Audit and Certification of Digital Repositories. http://www.trusteddigitalrepository.eu/Trusted%20Digital%20Repository.html

wand (vor allem in Form personeller Ressourcen), der zur Erlangung notwendig ist. Die Stufen sind[25]:

- „basic certification“:
  Hierbei handelt es sich um eine Selbstevaluierung mit Peer-Review. Dies entspricht dem Data Seal of Approval (DSA).
- „extended certification“:
  Stufe 2 entspricht einer erweiterten Selbstevaluierung, d.h. einer Selbstevaluierung, die von externen Gutachtern geprüft wird. Diese kann sowohl nach DIN 31644 (nestor-Siegel) als auch nach ISO 16363 durchgeführt werden.
  Voraussetzung für die Erlangung dieser Stufe ist die „basic certification“.
- „formal certification“:
  Die dritte Stufe beinhaltet ein vollständiges externes Audit. Dieses kann ebenfalls entweder anhand von DIN 31644 oder von ISO 16363 durchgeführt werden. Momentan ist unseres Wissens kein Verfahren für ein formales Audit nach DIN 31644 definiert. Ein Audit nach ISO 16363 ist mit der Veröffentlichung des Standards ISO 16919 im Herbst 2014 theoretisch möglich geworden.
  Ebenso wie für Stufe 2 ist auch für diese Stufe die „basic certification“ Voraussetzung.

Da nach dem Framework eine Selbstevaluierung mit Peer-Review nach dem DSA die Voraussetzung für alle weiteren Stufen ist und das DSA sich zudem, wie oben geschildert, mittlerweile in der Community gut etabliert hat, wird das DSA auch für das HDC als erste anzustrebende Zertifizierung empfohlen.

# 4. Kernthemen in ISO 16363, DIN 31644 und DSA

## ISO 16363/TRAC[26]

Bei der Arbeit an TRAC und am nestor-Kriterienkatalog haben beide Arbeitsgruppen eng zusammengearbeitet und Entwurfsversionen ausgetauscht. Dies führte zu einem formal und inhaltlich sehr ähnlichen Aufbau dieser Dokumente und auch der Standards ISO 16363 und DIN 31644, die sich teilweise aufeinander beziehen. Es werden ähnliche Kriterien angeführt, und auch Prozesse werden in ähnlicher Weise beschrieben. Mit 109 Kriterien ist ISO 16363 allerdings etwas detaillierter als der nestor-Kriterienkatalog/DIN 31644 mit 40 bzw. 34 Kriterien.

Beide Kataloge gliedern die Anforderungen an ein Digitales Langzeitarchiv in die drei Bereiche „Organizational Infrastructure“/„Organisatorischer Rahmen“, „Digital Object Management“/„Umgang mit Objekten“ und „Infrastructure and Security Risk Management“/ „Infrastruktur und Sicherheit“. Im Folgenden werden die drei Bereiche anhand von ISO 16363 be-

[25] Vgl. ebd.
[26] Die Ausführungen in diesem Unterkapitel stützen sich auf das 2011 vom CCSDS veröffentlichte „Audit and Certification of Trustworthy Digital Repositories“ (http://public.ccsds.org/publications/archive/652x0m1.pdf), das die öffentlich zugängliche Version des ISO-Standards 16363 darstellt.

schrieben, das Gesagte trifft aber im Kern auch auf den nestor-Kriterienkatalog/DIN 31644 zu.

Der Bereich *„Organizational Infrastructure“* umfasst 25 Kriterien, die in fünf Kategorien gruppiert sind:

- 3.1. Governance and organizational viability
- 3.2 Organizational structure and staffing
- 3.3 Procedural accountability and preservation policy framework
- 3.4 Financial sustainability
- 3.5 Contracts, licenses, and liabilities

Hier geht es also um die Aspekte und Anforderungen, die für den nachhaltigen Betrieb der Einrichtung selbst von Belang sind. Dazu gehören die Definition eines Leitbildes bzw. der Ziele sowie der Zielgruppe (designated community) des digitalen Archivs. Es muss eine stabile organisatorische Struktur vorhanden sein, in der die Rollen und Verantwortlichkeiten aller Beteiligten klar definiert und in Policies schriftlich festgehalten sind. Hierzu gehören weiterhin eine nachhaltige Finanzierung, qualifiziertes Personal und ein Plan, wie die Daten länger als das Archiv bestehen können, Dokumentation, Transparenz und Qualitätsmanagement. Nicht zuletzt ist eine Reihe von gesetzlichen und vertraglichen Regelungen für Archivierung und Nutzung notwendig, worunter bspw. die Beachtung von Urheberrecht und Datenschutz bei der Nutzung der Objekte fallen.

Das *„Digital Object Management“* umfasst 60 Kriterien, die in sechs Untergruppen aufgeteilt sind:

- 4.1 Ingest: acquisition of content
- 4.2 Ingest: creation of the AIP
- 4.3 Preservation Planning
- 4.4 AIP Preservation
- 4.5 Information Management
- 4.6 Access Management

Es werden, unter Nutzung der Terminologie des OAIS, Ingest, Archivierung und Zugriff (Access) unter den Aspekten der Sicherstellung von Integrität und Authentizität betrachtet. Des Weiteren wird eine formalisierte Datenübernahme vom Produzenten mit definierten Übergabepaketen und festgelegten signifikanten Eigenschaften zur Erhaltung gefordert. Das digitale Langzeitarchiv muss die technische Kontrolle über die Archivdaten haben, um Langzeitarchivierungsmaßnahmen durchführen zu können. Für Objekte, die per Digitalem Rechtemanagement geschützt sind, sind solche Maßnahmen in der Regel nicht möglich. Die Archivablage soll für den Langzeiterhalt geeignet und genau spezifiziert sein, ebenso wie die Datenauslieferung an die Nutzer. Das Datenmanagement muss einem digitalen Langzeitarchiv angemessen sein, dazu gehören persistente Beziehungen zwischen Objekten wie sie mit Hilfe von persistenten Identifikationen (PIDs) möglich sind. Ebenso müssen die erhobenen Metadaten geeignet sein, das Objekt inhaltlich, technisch und strukturell angemessen zu beschreiben.

Unter *„Infrastructure and Security Risk Management“* fallen 24 Kriterien in den zwei Kategorien:

- 5.1 Technical infrastructure risk management
- 5.2 Security Risk Management

Dieser Bereich beschreibt Bedingungen, die die technische Infrastruktur des Datenzentrums erfüllen muss. Sie muss in der Lage sein, die im Bereich „Digital Object Management“ gestellten Anforderungen an Ingest, Archivierung und Access auch in Bezug auf Integrität und Authentizität der Objekte zu erfüllen. Es muss eine geeignete Datenaufbewahrung gegeben sein, bspw. mit Datensicherungsmaßnahmen an verschiedenen Standorten.

### DIN 31644/nestor-Siegel

Die Kriterien des nestor-Siegels[27] entsprechen inhaltlich im Großen und Ganzen denjenigen des nestor-Kriterienkatalogs für vertrauenswürdige digitale Langzeitarchive[28]. Diese wiederum decken sich in ihren Kernaussagen größtenteils mit denen des eben beschriebenen Standards ISO 16363, weswegen auf eine erneute Erläuterung der Inhalte an dieser Stelle mit Verweis auf das vorangegangene Unterkapitel verzichtet wird.

Obwohl der nestor-Kriterienkatalog und das nestor-Siegel sich inhaltlich gleichen, gibt es in der Form doch Unterschiede. So sind die Kriterien des Kriterienkatalogs, ebenso wie die von ISO 16363, in die drei Bereiche „Organisatorischer Rahmen“ (16 Kriterien), „Umgang mit Objekten“ (22 Kriterien) und „Infrastruktur und Sicherheit“ (2 Kriterien) gegliedert, während beim nestor-Siegel nicht mehr explizit auf diese Gliederung Bezug genommen wird. Gleichwohl können auch die 34 Kriterien des Siegels diesen zugeordnet werden („Organisatorischer Rahmen“: 16 Kriterien, „Umgang mit Objekten“: 21 Kriterien, „Infrastruktur und Sicherheit“: 2 Kriterien).

### Data Seal of Approval

Auch in den Kriterien des Data Seal of Approval finden sich die zentralen Punkte von ISO 16363 und DIN 31644 wieder, jedoch in weniger detaillierter Form. Eine Besonderheit des DSA im Vergleich zu den beiden oben beschriebenen Standards ist der spezielle Fokus auf Forschungsdaten. Dabei wird die Einschätzung, ob die Daten in einem Repositorium nachhaltig und sicher archiviert sind, von fünf Prinzipien geleitet:[29]

- Die Daten sind online auffindbar.
- Die Daten sind (im Rahmen der rechtlichen Bestimmungen) zugänglich.
- Die Daten sind in einem gebräuchlichen bzw. brauchbaren Format erhältlich.
- Die Daten sind verlässlich („reliable“).
- Die Daten sind referenzierbar (mittels persistenter Identifikatoren).

[27] nestor-Arbeitsgruppe Zertifizierung: Erläuterungen zum nestor-Siegel für vertrauenswürdige digitale Langzeitarchive. Frankfurt am Main: nestor c/o Deutsche Natioanlbibliothek 2013. (nestor-materialien 17). URN: urn:nbn:de:0008-2013100803

[28] nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive Version 2. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2008. (nestor-materialien 8). URN: urn:nbn:de:0008-2008021802

[29] Vgl. Trilsbeek 2012 sowie
Data Seal of Approval Board 2013: Data Seal of Approval: Guidelines version 2. July 19, 2013. S. 5
http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

Die 16 Richtlinien des DSA konzentrieren sich auf drei Zielgruppen: die Datenproduzenten (Richtlinie 1-3), das Repositorium/Datenarchiv (Richtlinien 4-13) und die Datenkonsumenten (Richtlinien 14-16). Das heißt jedoch nicht, dass die Kriterien 1-3 und 14-16 für das Repositorium irrelevant sind, da es hinsichtlich der beiden Nutzendengruppen in der Rolle des „Enablers“ gesehen wird. D.h. es ist dafür verantwortlich, es den Datenproduzenten und -konsumenten zu ermöglichen (etwa durch entsprechende Policies), die auf sie zutreffenden Kriterien zu erfüllen.[30]

Die die Datenproduzenten betreffenden Richtlinien beziehen sich auf die Qualität der abgelieferten Daten.[31] Sie beinhalten, dass zusammen mit den Daten ausreichend Informationen und Metadaten geliefert werden müssen, damit andere die wissenschaftliche Qualität der Daten einschätzen können. Ferner müssen sie den Formatvorgaben des Repositoriums entsprechen. [32]

Die Richtlinien 4 bis 13, die das Repositorium direkt betreffen, dienen dazu, die ausreichend hohe Qualität der Langzeitarchivierung und des Zugangs zu den Daten festzustellen bzw. zu belegen[33] und thematisieren die Abläufe und Regelungen des Repositoriums sowohl in technischer als auch in organisatorischer Hinsicht. Hierzu gehört zunächst, dass die Langzeitarchivierung Teil seines Leitbildes ist, also als institutioneller Auftrag begriffen wird, und dass es in Übereinstimmung mit rechtlichen Regelungen und Verträgen agiert. Das Repositorium muss einen Plan für die Langzeitarchivierung (inkl. der entsprechenden Erhaltungsmaßnahmen) besitzen, Workflows und Prozesse müssen definiert und dokumentiert sein, die Bewahrung der Integrität und Authentizität der digitalen Objekte muss sichergestellt und die technische Infrastruktur muss geeignet sein, die Aufgaben und Funktionen der LZA gemäß etablierter Standards wie dem OAIS zu unterstützen. Des Weiteren müssen die Verfügbarkeit und der Zugang zu den sowie die Suchbarkeit und Referenzierbarkeit der Daten gewährleistet sein.[34]

Die letzten drei Richtlinien schließlich, die die Datenkonsumenten im Fokus haben, betreffen die Qualität der (Nach)Nutzung der Daten.[35] Diese sollte in Einklang stehen mit den Zugangsregelungen des Repositoriums einerseits und mit den Konventionen der Wissenschaft bezüglich des Austauschs und der Nutzung von Information andererseits. Lizenzen, denen die Daten unterliegen, müssen respektiert werden.[36]

## 5. Kosten

Bei den Kosten für eine Zertifizierung sind hauptsächlich zwei Posten zu berücksichtigen: zum einen mögliche Gebühren, zum anderen der damit verbundenen Personalaufwand.

Für die Erlangung des Data Seal of Approval werden keine Gebühren fällig. Allerdings werden Repositorien, denen das Data Seal of Approval verliehen wird, automatisch Mitglied in

[30] Vgl. ebd.
[31] Vgl. Data Seal of Approval Board 2013, S.5.
[32] Vgl. ebd., S. 11-13.
[33] Vgl. ebd., S. 5.
[34] Vgl. ebd., S. 14-23.
[35] Vgl. ebd., S. 5.
[36] Vgl. ebd., S. 24-26.

der DSA Community, was mit der Verpflichtung verbunden ist, bis zu drei Mal jährlich als Reviewer für die Selbsteinschätzungen anderer DSA-Anwärter zur Verfügung zu stehen.[37] Für die Erlangung des nestor-Siegels wird eine Gebühr von 500 Euro verlangt. [38] Für ISO 16363 konnte keine Angabe bezüglich eventueller Gebühren gefunden werden.

Die Kosten für die Gebühren dürften gegenüber dem Personalaufwand und ergo den Personalkosten, die für die Vorbereitung und Durchführung einer Zertifizierung nötig sind, eher weniger ins Gewicht fallen. Das Personal wird z.B. benötigt, um die entsprechenden Formulare auszufüllen, die notwendige Dokumentation zusammenzutragen bzw., falls noch nicht vorhanden, zu erstellen oder auch, falls noch Infrastruktur oder Arbeitsläufe entwickelt und implementiert werden muss, um die entsprechenden Aktivitäten durchzuführen.[39] Wie in Kapitel 3 beschrieben, steigt der Aufwand für die Zertifizierung mit der jeweiligen Stufe nach dem European Framework for Audit and Certification. Am wenigsten aufwändig sollte demnach die „basic certification“ nach dem DSA, am aufwändigsten ein formales Audit („formal certification“) z.B. nach ISO 16363 sein. Der Aufwand für die Erlangung einer „extended certification“, z.B. nach dem nestor-Siegel, sollte ungefähr dazwischen liegen. Dies deckt sich Angaben aus Erfahrungsberichten. So benötigte der Archaeology Data Service (ADS) etwa 5 Arbeitstage für das Data Seal of Approval. Für das nestor-Siegel und ISO 16363 liegen noch kaum Erfahrungsberichte vor. Im Rahmen des APARSEN-Projektes wurden mehrere Testaudits für ISO 16363 und ein Testaudit für das nestor-Siegel/DIN 31644 durchgeführt. Der Personalaufwand für DIN31644 wurde dabei auf 1,51 PM (Personenmonate) geschätzt, der geschätzte Aufwand für ISO 16363 lag zwischen 2 und 3 PM.[40]

# 6. Abbildung der Kriterien des Data Seal of Approval auf die Aufgaben im HDC

Im folgenden Abschnitt werden die Kriterien (DSA-Guidelines) auf die Arbeitspakete (AP) abgebildet. Einzelne Kriterien können mehrfach auftreten da sie für verschieden Arbeitspakete von Bedeutung sein können. Der Wortlaut der einzelnen Kriterien nebst Erläuterungen findet sich in den DSA Guidelines version 2[41] vom 19 Juli 2013.

Im Anschluss werden die Kriterien und ihre Zuordnung zu den Arbeitspaketen überblicksartig in einer Tabelle dargestellt. Dort ist auch vermerkt, welche Mindeststufe das „Statement of Compliance“, das die (Selbst)Einschätzung hinsichtlich des Implementierungsgrades der einzelnen Kriterien widerspiegelt, jeweils erreicht werden muss.

[37] Vgl. Data Seal of Approval (DSA). Community and Regulations. January 1 2013. S. 4f. http://datasealofapproval.org/media/filer_public/2013/09/27/dsa-regulations_2013.pdf
[38] Vgl. nestor-Siegel für vertrauenswürdige digitale Langzeitarchive 2013. http://www.langzeitarchivierung.de/Subsites/nestor/DE/nestor-Siegel/siegel_node.html
[39] D.h. wenn bei der Planung und dem Aufbau des Datenarchivs die Kriterien der angestrebten Zertifizierung(en) bereits berücksichtigt und soweit möglich umgesetzt wurden, kann sich der Zeitaufwand für die Zertifizierung selbst erheblich verringern.
[40] Vgl. APARSEN: Report on Peer Review of Digital Repositories (Part B of D33.1). 30.04.2012. http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D33_1B-01-1_0.pdf
[41] Data Seal of Approval Board 2013, S. 8ff.

AP1 (Definition des Angebots)

- **Guideline 4:** Das HDC hat ein Leitbild (Mission Statement), in dem die digitale Langzeitarchivierung als Aufgabe benannt (und dann entsprechend im Angebot umgesetzt) wird.

AP2 (Arbeitsabläufe)

- **Guideline 1**: Das HDC macht Vorgaben, welche Metadaten und Kontextinformationen zusammen mit Daten vorm/beim Ingest geliefert werden müssen, damit andere eine qualitative Beurteilung der Daten vornehmen können, und überprüft deren Einhaltung. Das HDC berücksichtigt die Abgabe dieser Kontextinformationen im Ingestworkflow.
- **Guideline 2**: Das HDC erstellt eine Liste mit empfohlenen Datenformaten und stellt diese zur Verfügung. Im Zuge des Ingest findet eine Formatvalidierung statt. Es muss eine Leitlinie für den Umgang mit Objekten, die nicht den Formatvorgaben entsprechen, geben.
- **Guideline 3**: Das HDC macht Vorgaben bezüglich der Metadaten, die bei der Datenübergabe angegeben werden müssen und überprüft deren Einhaltung. Es gibt eine Leitlinie zum Umgang mit Objekten, für die für die LZA nicht ausreichend Metadaten vorliegen.
- **Guideline 5**: Es gibt Richtlinien und Workflows zum Umgang mit sensiblen Daten.
- **Guideline 6**: Das HDC hat eine Preservation Policy. Die Prozesse und Workflows für das Datenmanagement sind dokumentiert.
- **Guideline 7**: Es gibt einen Plan zur Langzeiterhaltung digitaler Objekte. Dieser wird fortlaufend aktuellen Gegebenheiten angepasst (Technology Watch).
- **Guideline 8**: Es gibt klar definierte, dokumentierte Prozesse bzw. Workflows für die Langzeiterhaltung und den Umgang mit den Objekten über den gesamten Objektlebenszyklus hinweg.
- **Guideline 10**: Es gibt Arbeitsabläufe, die sicherstellen, dass NutzerInnen die Daten des HDC finden, nutzen und persistent referenzieren können.
- **Guideline 11**: Es gibt Arbeitsabläufe für die Überprüfung und Erhaltung der Integrität der digitalen Objekte und Metadaten.
- **Guideline 12**: Es gibt Arbeitsabläufe für die Überprüfung und Erhaltung der Authentizität der digitalen Objekte und Metadaten.

AP3 (Technische Infrastruktur)

- **Guideline 5**: Die Infrastruktur gewährleistet eine sichere Lagerung und Zugriffsbeschränkungen für sensible Daten.

- **Guideline 6**: Es gibt dokumentierte Prozesse und Workflows für das Datenmanagement; die technische Infrastruktur ermöglicht deren Umsetzung.
- **Guideline 7**: Die technische Infrastruktur ermöglicht die Umsetzung der Erhaltungsplanung/Erhaltungsmaßnahmen der digitalen Objekte.
- **Guideline 10**: Die technische Infrastruktur ermöglicht, dass NutzerInnen die Daten des HDC finden, nutzen und persistent referenzieren können.
- **Guideline 11**: Die technische Infrastruktur ermöglicht die Überprüfung und Erhaltung der Integrität der digitalen Objekte und Metadaten sowie Versionierung.
- **Guideline 12**: Die technische Infrastruktur ermöglicht die Überprüfung und Erhaltung der Authentizität der digitalen Objekte und Metadaten.
- **Guideline 13**: Die technische Infrastruktur unterstützt die Aufgaben und Funktionen, wie sie in international anerkannten Standards wie dem OAIS beschrieben werden.

AP4 (Werkzeuge)

- **Guidelines 1 & 3**: Auf technischer Ebene müssen Werkzeuge erstellt und bereitgestellt werden, die zur Eingabe bzw. teilweise auch automatischen Erfassung und Qualitätsprüfung von Metadaten sowie zusätzlichen Information dienen und die diese dann den Daten zuordnen können.
- **Guideline 2**: Es müssen Werkzeuge zur Überprüfung der Datenformate und Einbindung in den technischen Ablauf erstellt und in die Infrastruktur eingebunden werden.
- **Guideline 10**: Es gibt Werkzeuge für Suche, Download, OAI-PMH-Harvesting u.a.
- **Guideline 11**: Es gibt Werkzeuge zur Überwachung und Überprüfung der Integrität der digitalen Objekte und Metadaten.
- **Guideline 12**: Es gibt Werkzeuge zur Überprüfung und Erhaltung der Authentizität der digitalen Objekte und Metadaten (z.B. zur Erhaltung von Provenance-Informationen, zur Erhaltung der Verbindung zwischen Metadaten und Daten oder zur Überprüfung der Identität von Datengebern).

AP6 (Geschäftsmodell und Betrieb)

- **Guideline 1:** Entwicklung einer Vorlage für ein Deposit Agreement/eine Datenübernahmevereinbarung
- **Guideline 4:** Es gibt eine Nachfolgeregelung.
- **Guideline 5**: Die Organisations- und Rechtsform ist definiert. Rechtliche Vorgaben werden eingehalten. Es gibt Vorlagen für Vereinbarungen zur Datenübergabe (deposit agreement) und zur Datennutzung (Terms of Use). Die Terms of Use sind öffentlich zugänglich. MitarbeiterInnen werden im Umgang mit sensiblen Daten geschult.
- **Guideline 6**: Das HDC hat eine Preservation Policy.

- **Guideline 8**: MitarbeiterInnen werden geschult (intern oder extern), um ihre Aufgaben gemäß der definierten Worksflows für die Langzeitarchierung und den Umgang mit den digitalen Objekten erfüllen zu können.
- **Guideline 9**: Das HDC übernimmt von den Datenproduzenten die Verantwortung für die Zugänglichmachung und Verfügbarkeit der Daten. Es werden Lizenzverträge oder ähnliche Vereinbarungen (d.h. es gibt entsprechende Vorlagen) geschlossen, die dies besiegeln.
- **Guideline 14**: Es gibt Verträge, Vereinbarungen oder Lizenzen, die die Bedingungen für die Nachnutzung der Daten im Rahmen der rechtlichen Rahmenbedingungen regeln. Es gibt Regelungen bzw. Maßnahmen, die bei Nichteinhaltung von Lizenzen und Vereinbarungen greifen.
- **Guideline 15**: Es wird ein Code of Conduct zur (Nach)Nutzung der Daten unter Berücksichtigung sensibler Daten sowie communityspezifischer Gepflogenheiten erstellt.
- **Guideline 16**: Das HDC eruiert die rechtlichen Rahmenbedingungen für die Nachnutzung von Daten und klärt, welche Lizenzen für die Nachnutzung in Frage kommen. Soweit möglich (d.h. in den Grenzen nationaler rechtlicher Regelungen) werden dabei internationale Standards berücksichtigt.

AP7 (Dissemination, Beratung und Schulung)

- **Guideline 1**: Es wird Beratung und Begleitung, ggf. auch Schulung, der Datengeber vor und während des Ingest-Prozesses in Bezug auf die ausreichende Dokumentation der Daten und des Kontexts ihrer Erstellung, Bearbeitung etc. angeboten.
- **Guideline 2**: Es wird Beratung und Schulung zu den empfohlenen/unterstützten Datenformaten angeboten.
- **Guideline 3**: Es wird Beratung und Schulung zu den beim Ingest geforderten Metadaten angeboten.
- **Guideline 4**: Das Leitbild (Mission Statement) ist öffentlich zugänglich.
- **Guideline 5**: Die Terms of Use sind öffentlich zugänglich.
  Für NutzerInnen werden Beratung und Schulung zu rechtlichen Fragen im Umgang mit Forschungsdaten angeboten.
- **Guideline 14**: NutzerInnen werden über Zugangsregelungen, Lizenzen und Bedingungen zur (Nach)Nutzung der Daten informiert und können bei Bedarf Beratung und Schulung erhalten.
- **Guideline 15**: Der Code of Conducts zur Nachnutzung der Daten wird NutzerInnen zur Verfügung gestellt. Es wird Beratung und Schulung zur verantwortlichen Nachnutzung von Daten, insbesondere sensiblen Daten, angeboten.
- **Guideline 16**: Es wird Beratung und Schulung zu Lizenzen für die Nachnutzung von Daten angeboten.

| | | DSA Guideline 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TP1 | | | | | | | | | | | | | | | | | | |
| | AP1 | | | | | x | | | | | | | | | | | | |
| | AP2 | | x | x | x | | x | x | x | x | | x | x | x | | | | |
| TP2 | | | | | | | | | | | | | | | | | | |
| | AP3 | | | | | | x | x | x | | | x | x | x | x | | | |
| | AP4 | | x | x | x | | | | | | | x | x | x | | | | |
| TP3 | | | | | | | | | | | | | | | | | | |
| | AP5 | | | | | | | | | | | | | | | | | |
| | AP6 | | x | | | x | x | x | | x | x | | | | | x | x | x |
| | AP7 | | x | x | x | x | x | | | | | | | | | x | x | x |
| | AP8 | | | | | | | | | | | | | | | | | |
| | AP9 | | | | | | | | | | | | | | | | | |
| Required statement of compliance | | | 3 | 3 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 4 | 4 | 4 |

**Table 1: Statement-of-Compliance: 3="In Arbeit: wir sind in der Implementierungsphase" 4="Implementiert: Diese Richtlinie wurde komplett für die Bedürfnisse unseres Datenzentrums implementiert."**

## 7. Zusammenfassung

Das Projekt HDC befindet sich aktuell in der Design-Phase, in der die konzeptuelle Entwicklung, mit all den offenen Fragen bezüglich der Angebote und des Geschäfts- und Betriebsmodells im Vordergrund stehen. Der Aufbau einer Infrastruktur mit funktionierenden Werkzeugen zur Realisierung der Angebote ist in einem Folgeantrag vorgesehen. Trotzdem wird mit der Entwicklung von Prototypen in der aktuellen Phase schon der Grundstein für das spätere Datenzentrum gelegt. Daraus ergibt sich schon jetzt die Notwendigkeit, die Kriterien einer Zertifizierung zu kennen und danach zu handeln. Der eigentliche Zertifizierungsprozess ist dann Aufgabe in einem Folgeprojekt.

Die zu erwartenden Kosten für eine DSA-Zertifizierung bestehen dabei ausschließlich aus Personalmitteln. Dabei kann schon über eine komplette Projektlaufzeit auf eine Zertifizierung hin gearbeitet werden. Die Anzahl an benötigten Personenmonaten kann dabei die aus vorherigen Initiativen geschätzten Angaben überschreiten. Es wird empfohlen, in einem Folgeprojekt eine Arbeitsgruppe einzurichten, die auf eine Zertifizierung am Projektende hin arbeitet. Diese Zertifizierungsarbeitsgruppe sollte für die Überwachung und Kommunikation innerhalb der anderen Arbeitsgruppen verantwortlich sein und darauf achten, dass die notwendige Dokumentation erstellt wird.

Als möglichweise erster Schritt wäre weiterhin eine Registrierung bei re3data[42] zu überlegen. re3data, ein von der DFG gefördertes Projekt, versteht sich als ein globales Register von Forschungsdaten-Repositorien. Eine Eintragung in dieser Datenbank würde die Sichtbarkeit des zukünftigen geisteswissenschaftlichen Datenzentrums erhöhen und damit die Nachnutzung von Forschungsdaten fördern. Die Kriterien für eine Eintragung sind: das Forschungsdatenzentrum muss von einer juristischen Person (am besten einer nachhaltigen Institution wie einer Bibliothek oder Universität) betrieben werden, die Zugangsbedingungen sowie die Terms of Use für die Nachnutzung der Daten müssen geklärt sein, es muss eine englische Benutzeroberfläche geben und der Schwerpunkt des Repositoriums muss auf Forschungsdaten liegen.[43]

[42] http://www.re3data.org/
[43] Vgl. Suggest. re3data.org. http://www.re3data.org/suggest/

# Quellenverzeichnis

*Das Abrufdatum aller referenzierten Online-Quellen ist der 12. Mai 2015.*

About. Data Seal of Approval. http://datasealofapproval.org/en/information/about/

About. ICSU World Data System. https://www.icsu-wds.org/organization

APARSEN: Report on Peer Review of Digital Repositories (Part B of D33.1). 30.04.2012. http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D33_1B-01-1_0.pdf

CCSDS: Reference Model for an Open Archival Information System (OAIS). Recommended Practice. CCSDS 650.0-M-2. Magenta Book, June 2012. http://public.ccsds.org/publications/archive/650x0m2.pdf

CCSDS: Audit and Certification of Trustworthy Digital Repositories. Recommended Practice. CCSDS 652.0-M-1. Magenta Book, September 2011. http://public.ccsds.org/publications/archive/652x0m1.pdf

DASISH workshop on trust and certification. DASISH. http://dasish.eu/dasishevents/wstrustcertification/

Data Seal of Approval and World Data System to Collaborate. 22.11.2014. Data Seal of Approval. http://datasealofapproval.org/en/news-and-events/news/2013/11/22/dsa-and-wds-collaborate/

Data Seal of Approval Board 2013: Data Seal of Approval: Guidelines version 2. July 19, 2013. http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

Data Seal of Approval (DSA). Community and Regulations. January 1 2013. http://datasealofapproval.org/media/filer_public/2013/09/27/dsa-regulations_2013.pdf

DIN 31644. Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive. http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=147058907&languageid=de&bcrumblevel=3

Dobratz, Susanne; Schoger, Astrid: Grundkonzepte der Vertrauenswürdigkeit und Sicherheit. In: nestor-Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung. Version 2.3. Hrsg. von Neuroth, Heike et al. Göttingen: nestor c/o Niedersächsische Staats- und Universitätsbibliothek 2010. URN: urn:nbn:de:0008-2010030597

Engelhardt, Claudia; Recker, Astrid: Trust and the European Framework for Audit and Certification of Digital Repositories. (Präsentation anlässlich des DASISH Workshop on Trust and Certification, 16./17. Oktober 2014, Den Haag). http://dasish.eu/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_Intro_trust_and_MoU-Framework_Recker_Engelhardt.pdf

ESFRI. 07.05.2015. European Commission. http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=esfri

European Framework for Audit and Certification of Digital Repositories. http://www.trusteddigitalrepository.eu/Trusted%20Digital%20Repository.html

European Research Infrastructure Consortium (ERIC). 16.04.2015. European Commission. http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=eric

Grootveld, Marjan, DIN@DANS. (Präsentation anlässlich des DASISH Workshop on Trust and Certification, 16./17. Oktober 2014, Den Haag). http://dasish.eu/dasishevents/wstrustcertification/2014_10_17_DASISH_trust-ws_nestorSeal_case_study_DANS_Grootveld.pdf

ICSU World Data System: Certification of WDS members. 11 June 2011. https://www.icsu-wds.org/files/wds-certification-summary-11-june-2012.pdf

ISO 14721:2012. Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=57284

ISO 16363:2012. Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510

nestor-Arbeitsgruppe OAIS-Übersetzung / Terminologie: Referenzmodell für ein Offenes Archiv-Informations-System – Deutsche Übersetzung, Version 2.0. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2013. (nestor-materialien 16). URN: urn:nbn:de:0008-2013082706

nestor-Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive Version 2. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek 2008. (nestor-materialien 8). URN: urn:nbn:de:0008-2008021802

nestor-Arbeitsgruppe Zertifizierung: Erläuterungen zum nestor-Siegel für vertrauenswürdige digitale Langzeitarchive. Frankfurt am Main: nestor c/o Deutsche Natioanlbibliothek 2013. (nestor-materialien 17). URN: urn:nbn:de:0008-2013100803

nestor-Siegel für vertrauenswürdige digitale Langzeitarchive. 06.08.2013. nestor. http://www.langzeitarchivierung.de/Subsites/nestor/DE/nestor-Siegel/siegel_node.html

Network Working Group (2007): Internet Security Glossary. Request for Comments: 4949 http://tools.ietf.org/html/rfc4949

Suggest. re3data.org. http://www.re3data.org/suggest/

Trilsbeek, Paul: Data Seal of Approval. Overview. (Präsentation anlässlich des DASISH Workshop on Trust and Certification, 16./17. Oktober 2014, Den Haag). http://dasish.eu/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_DSA_Trilsbeek.pdf