

---

Susanne Fröhlich

## Normen und Standards der digitalen Archivierung

Spricht man über Normen und Standards im Archivbereich, darf heutzutage die digitale Archivierung nicht mehr außer Acht gelassen werden. Auch, oder gerade auf diesem Gebiet entstehen immer mehr qualifizierte Vorgaben, deren Umsetzung und Einhaltung eine dauerhafte Aufbewahrung von digitalem, archivwürdigem Schriftgut garantieren sollen. Da eine Auflistung aller möglichen relevanten Vorschriften den Rahmen dieses Beitrages bei Weitem sprengen würde, werden nur die derzeit in Österreich bzw. im deutschsprachigen Raum primär verwendeten Normen auszugsweise vorgestellt<sup>1</sup>. Es sei dazu gleich zu Beginn darauf hingewiesen, dass alle im folgenden zitierten Vorschriften, Dokumente und Internetlinks mit Status „Frühjahr 2014“ angeführt werden. Über etwaige Weiterentwicklungen und/oder Aktualisierungen möge sich der interessierte Leser selbst auf dem Laufenden halten.

Grundsätzlich muss man im digitalen Umfeld, anders als vielleicht aus der analogen Archivierung geläufig, zwischen mehreren Anforderungsgruppen von Standards unterscheiden. Nicht nur die interne Struktur der aufzubewahrenden Daten selbst unterliegt gleichförmigen Regelungen, auch die physischen Komponenten und sogar die organisatorischen Bedingungen digitaler Systeme sind mit Hilfe genormter Maßnahmen umzusetzen. Da digitale Archive im Gegensatz zu ihren analogen Vorläufern noch über keine lange Tradition verfügen, ist es umso wichtiger, mit Hilfe genormter Vorgänge ein gewisses Vertrauen für und in digitale Langzeitarchivsysteme aufzubauen. Im Weiteren bedingt der technische Fortschritt ein höheres Maß an standardisierten Abläufen, welche nicht zuletzt (Arbeits)Prozesse automatisieren, beschleunigen und vereinfachen sollen.

In diesem Sinne lässt sich in Bezug auf digitale Archivierung eine grobe Dreiteilung anzuwendender Normen vornehmen:

- Archivfachliche Anforderungen zur (analogen und digitalen) deskriptiven Metadatenhaltung<sup>2</sup>;
- technische Vorgaben, welche sich wiederum in drei Bereiche gliedern lassen: physische Komponenten, logische Komponenten sowie „fachliche“ Anforderungen an technische Metadaten, Datenerzeugung oder Datenstruktur;
- allgemein übergreifende Standards, die sonstige Rahmenbedingungen für digitale Archive festlegen, wie z. B. Referenzmodelle, Kriterienkataloge, Transport- und Transformationsschemata, organisatorische Maßnahmen etc.

---

1 Eine Übersicht über alle geläufigen (Metadaten)Standards findet sich bei „Seeing Standards“: <http://www.dlib.indiana.edu/~jenlrile/metadatamap/>.

2 Die technisch-organisatorischen Rahmenbedingungen für analoge Archive werden hier nicht berücksichtigt.

## Archivische Fachnormen

Auf diese erste Gruppe archivfachlicher Normen, wie z. B. ISAD(G), ISAAR(CPF) oder ISDIAH, die im Archivalltag allgegenwärtig sind, sei nur kurz verwiesen, da ihre detailliertere Vorstellung Gegenstand anderer Beiträge des vorliegenden Scribium-Bandes ist. Es wird als selbstverständlich vorausgesetzt, dass diese Normen auch für digitale Archive die Grundlage einer seriösen Erschließungsarbeit bilden und somit die deskriptive (Meta)Datenhaltung eines jeden Archives auch zukünftig prägen werden. Im Hinblick auf digitale Systeme sei jedoch darauf hingewiesen, dass sich bereits innerhalb der genannten „I-Standards“ in Teilbereichen weitere, quasi schon als „technische“ Normen angesehene Regelungen finden, deren Anwendung in Bezug auf digitale Daten empfohlen wird. Exemplarisch mögen hier die ISO-Normen für Ländercodes, Sprachcodes oder Datumsangaben genannt werden<sup>3</sup>, welche nicht zuletzt eine internationale Interpretier- und Lesbarkeit von Informationen erleichtern. In Zeiten von Cloudanwendungen, Portallösungen und transparenter Internetbenutzung ist der Vorteil strukturierter Metadaten nicht von der Hand zu weisen.

Zu den genannten Fachnormen gibt es jeweilige Entsprechungen für die digitale Datenhaltung. Diese so genannten „E-Normen“ wurden in internationalen Gemeinschaftsprojekten entwickelt und veröffentlicht und haben sich durch die praktische Umsetzung in fast allen großen digitalen Archiven und auch Archivportalen bereits zu anerkannten, gültigen Standards ausgebildet:

Archivstandard				Beschriebenes Objekt
analog		digital		
ISDIAH	<=>	EAG	<=>	Archivinstitution
ISAAR (CPF)	<=>	EAC-CPF	<=>	Archivgutprovenienz
ISAD (G)	<=>	EAD	<=>	Archivgut

3 Weitere Informationen können den Archivstandards selbst entnommen werden. Für Gesamtübersichten siehe: <http://www.ica.org/10206/standards/standards-list.html> bzw.

ISAD (G) - General International Standard Archival Description - 2nd ed.; ICA, 2000.

ISAAR(CPF) - International Standard Archival Authority Record for Corporate Bodies, Persons and Families, 2nd ed., ICA, 2007.

ISDIAH - International Standard for Describing Institutions with Archival Holdings. 1st ed.; ICA, 2008,

oder International Organization for Standardization (ISO): <http://www.iso.org/iso/home/standards.htm>

ISO 8601 - Data elements and interchange formats - Information interchange - Representation of dates and times, 2nd ed., Geneva: International Standards Organization, 2000.

ISO 3166-2 - Codes for the representation of names of countries and their subdivisions - Part 2: Country subdivision code, Geneva: International Standards Organization, 1998.

ISO 639-2 - Codes for the representation of names of languages, Alpha-3 code, Geneva: International Standards Organization, 1998.

So findet sich das Pendant zu ISAD(G) in der Norm EAD (Encoded Archival Description), welche durch die Library of Congress (LOC) gewartet wird<sup>4</sup>. EAD ist ein XML-Schema, das zur Beschreibung archivfachlich-deskriptiver Metadaten und in weiterer Folge zu deren Weiterverwendung oder „Transport“ dient. Als „Transport“ sei hier die durch das Format XML gewährleistete internationale Anwendbarkeit und Umwandlung digitaler Daten innerhalb und außerhalb unterschiedlicher Archivsysteme verstanden. Mit Hilfe von EAD können Daten über Schnittstellen in verschiedenste Umgebungen eingebracht und/oder ausgetauscht werden. So können über vordefinierte „Datenmappings“ Metadaten z. B. aus einem Archivinformationssystem in ein Portal eingebracht werden oder innerhalb digitaler Archive für den Archivar in ein „lesbares“ Format übergeführt werden.

Das Gegenstück zu ISAAR (CPF) stellt EAC-CPF (Encoded Archival Context – Corporate bodies, Persons, and Families) dar<sup>5</sup>. EAC ist ebenfalls ein XML-Standard, der die formale Beschreibung von Archivgutprovenienzen unterstützt. Das dritte Element ISDIAH, die Beschreibung von Archivinstitutionen, findet seine Entsprechung im Standard EAG (Encoded Archival Guide), welcher unter anderem vom Bundesarchiv veröffentlicht wird<sup>6</sup>.

## Technische Vorgaben

Als zweite Normenserie kommen Anforderungen für sichere, langfristige IT-Systeme aus dem rein technischen Bereich zum Tragen. Die erste Komponente betrifft den „physischen“ Teil der Archive – die Hardware –, also Server, Festplatten, Rechner und sonstige Speichermedien, aber auch den lokalen Speicherort – das Rechenzentrum – selbst. Analog zum gängigen Archivdepot müssen auch digitale Standorte Vorkehrungen gegen mechanische Störungen, technische Defekte, Schadstoffe oder elektromagnetische Einwirkungen treffen. Ebenso sind gleichbleibende Außenbedingungen, wie z. B. eine stabile Luftfeuchtigkeit, Temperatur, Stromversorgung oder Lichteinspeisung, Grundvoraussetzungen. All dies wird heutzutage in modernen Rechenzentren gerne unter dem Begriff „Green IT“ zusammengefasst und dient dem Zweck, erhöhtes Umweltbewusstsein, Nachhaltigkeit und Effizienz zu demonstrieren.

Weiters sind allgemeine Richtlinien für die äußere Sicherheit von digitalen Speichern, wie z. B. feuerpolizeiliche Vorkehrungen, Katastrophenszenarien oder

---

4 Für Informationen zur LOC allgemein siehe: <http://www.loc.gov/>, zu den Archivnormen finden sich Unterlagen auf: <http://www.loc.gov/standards/> und <http://www.loc.gov/ead/>.

5 Die von der Staatsbibliothek zu Berlin gehostete Homepage findet sich unter: <http://eac.staatsbibliothek-berlin.de>.

6 Für eine Übersicht zu den E-Standards siehe: [http://www.bundesarchiv.de/archivgut\\_online/standards\\_werkzeuge/index.html](http://www.bundesarchiv.de/archivgut_online/standards_werkzeuge/index.html); Details zu EAG siehe: [http://www.bundesarchiv.de/archivgut\\_online/standards\\_werkzeuge/02255/index.html](http://www.bundesarchiv.de/archivgut_online/standards_werkzeuge/02255/index.html).

spezielle Zutrittsberechtigungen für Mitarbeiter zu berücksichtigen. Als Beispiele zu diesem Komplex seien hier auszugsweise folgende Normen genannt<sup>7</sup>:

- Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 1: Allgemeine Konzepte (deutsche Fassung); *ÖVE/ÖNORM EN 50600-1: 2013 06 01*;
- Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2–3: Überwachung der Umgebung (deutsche Fassung) prEN 50600-2-3:2013; *DIN EN 50600-2-3\*VDE 0801-600-2-3: 2013 08*;
- Einrichtungen der Informationstechnik – Sicherheit – Teil 23: Große Einrichtungen zur Datenspeicherung (IEC 60950-23:2005); *ÖVE/ÖNORM EN 60950-23:2006 11 01*;
- Risikomanagement für Organisationen und Systeme – Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement – Umsetzung von ISO 31000 in die Praxis; *ONR 49002-3: 2014 01 01*;
- Wertbehältnisse – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand – Teil 2: Datensicherungsräume und Datensicherungscontainer (deutsche Fassung); *DIN EN 1047-2:2009+A1:2013*;
- die gesamte *ISO/IEC 27000-Reihe* (auch *ISO/IEC 27000-Familie* oder im Englischen kurz auch *ISO27k* genannt), welche derzeit bereits über 20 Normen zur IT-Sicherheit vereint<sup>8</sup>.

Ergänzend sollte hier noch auf individuelle rechtliche und/oder organisatorische Vorschriften für Archive und/oder Betreiber von Rechenzentren hingewiesen werden. So gelten z. B. für alle IT-Beschaffungen im Bundesbereich die „*Allgemeinen Vertragsbedingungen der Republik Österreich für IT-Leistungen (AVB-IT)*“<sup>9</sup> als unwiderrufliche Grundlage zur Umsetzung von IT-Projekten, wozu unter anderem auch das „Digitale Archiv Österreich“ zählt.

Der zweite Teilbereich der technischen Vorgaben für digitale Systeme/Archive umfasst alle „logischen Komponenten“, wie Software inklusive Schnittstellen, die Datenhaltung an sich und den Datenschutz. Hier finden sich Reglementierungen, die die für Archive so wichtige Vollständigkeit, Authentizität und Integrität der Daten sicherstellen sollen. Dazu gehören z. B. Anwendungen zur Integritäts- und Virenprüfung, Signaturnachweise, Tools zur Formaterkennung oder Schemaprüfung ebenso wie Maßnahmen gegen „äußere“ Einflüsse, wie Datenschutz- und

7 Eine ausführlichere Aufzählung findet sich auf den Webseiten des Austrian Standards Institute ([www.austrian-standards.at](http://www.austrian-standards.at)) sowie des Deutschen Normungsinstitutes ([www.din.de](http://www.din.de)).

8 Siehe hierzu neben der ISO-Homepage auch Auflistungen auf: <http://www.27000.org/> (Download am 20. 2. 2014) oder <http://www.iso27001security.com/> (Download am 20. 2. 2014).

9 Das erste Gesamtdokument wurde 2004 erstellt, 2007 erfolgte eine Neufassung, der 2011 eine komplette Überarbeitung folgte. Seitdem sind die Vorgaben auch schriftlich in drei Teilbereiche (Hardware, Software und Projektentwicklung) getrennt. Details hierzu siehe: <http://www.bbg.gv.at/kunden/beratung/vergabekompetenz-center/gesetze-verordnungen/oesterreichische-vergabevorschriften/allgemeine-vertragsbedingungen-der-republik-oesterreich-fuer-it-leistungen-avb-it/>.

Datensicherheitskonzepte, Firewalls, Rollen- und Rechteverwaltungen, aber auch die Backup-Haltung von Daten und Szenarien zur allfälligen Datenwiederherstellung im Katastrophenfall. Jegliche Beschädigung und Manipulation von Daten muss genauso vermieden werden wie Datenverlust oder Datenmissbrauch. Auf diesem Gebiet stellen jedoch nicht nur Normen und Standards Regulative dar, es gilt vielmehr auf qualitativ hochwertige, aktuell gewartete Softwareprodukte und komplexe administrative Konzepte („Policies“) Wert zu legen.

Die dritte Gruppe der „technischen“ Normen deckt analog zu den oben erwähnten archivfachlichen Standards die Vorgaben zur deskriptiven, technischen Metadatenhaltung der zu archivierenden Objekte ab. Sie sind insbesondere in Bezug auf das für Langzeitarchive notwendige „Preservation Planning“ von wesentlicher Bedeutung. Nicht nur der „Inhalt“ der archivierten Objekte an sich ist auf lange Sicht sicher zu stellen, auch – oder vor allem – die Benutzbarkeit der Daten, sprich die Erhaltung von Interpretier- und Lesbarkeit, ist essentiell. Um dies zu gewährleisten, benötigt man detaillierte Informationen zu technischen Objektkomponenten, wie z. B. Format, Schriftart, Dateigröße, Auflösung und vieles andere mehr. Im digitalen Kontext spricht man von „signifikanten Eigenschaften“, welche für jedes Informationsobjekt ausgewählt, festgelegt und dauerhaft unverändert erhalten werden müssen.

Als Standard im deutschsprachigen Umfeld hat sich diesbezüglich der PREMIS-Katalog (vormals „Preservation Metadata: Implementation Strategies“, aktuell „Preservation Metadata Maintenance Activity“) durchgesetzt, welcher Empfehlungen, Vorschläge und Best-Practices zur Implementierung von Metadaten enthält. Als Einzeldokument ist das „Data Dictionary for Preservation Metadata“ hervorzuheben<sup>10</sup>. Ergänzt wird die technische Metadatenhaltung durch die so genannte PRONOM-Registry, eine Datenbank, die die praktische Umsetzung von Formatmigrationen unterstützt. Diese Registry ist auch Teil des „Digitalen Archivs Österreich“ und dient als Ausgangspunkt für die im System implementierten, intern durchführbaren Preservationprozesse. Als dazugehörige Softwaretools werden vorrangig DROID (Digital Record Object Identification)<sup>11</sup> oder auch JHOVE (JSTOR/Harvard Object Validation Environment) zur Formaterkennung verwendet<sup>12</sup>.

Möchte man die angeführten Maßnahmen, die im Normalfall zeitverzögert nach der Datenerzeugung oder sogar erst im Zuge einer möglichen Archivierung greifen, auf den Produktivbetrieb, also auf den „vorarchivischen“ Bereich ausdehnen, wäre die Einhaltung diverser Normen schon bei der Datenerzeugung

---

10 PREMIS-Gesamtdokumentation siehe: <http://www.loc.gov/standards/premis/>.

11 Die PRONOM-Registry wurde vom englischen Nationalarchiv in Zusammenarbeit mit diversen Herstellern digitaler Archivsoftware, insbesondere Tessella, entwickelt und wird auch durch die National Archives aktualisiert und gewartet. Als Softwaretool wurde DROID entwickelt. Informationen hierzu siehe: <http://www.nationalarchives.gov.uk/PRONOM/Default.aspx> und <http://www.nationalarchives.gov.uk/information-management/projects-and-work/droid.htm>.

12 JHOVE dient als Softwareframework zur Formaterkennung, Validierung und Charakterisierung digitaler Objekte. Details siehe: <http://jhove.sourceforge.net/#implementation>.

angeraten. Wenn bereits bei der Entstehung digitaler Daten auf gewisse Standards Rücksicht genommen wird, schafft dies enorme Erleichterungen im Lifecycle-Management und bringt Vorteile für Datenübernahmen in digitale Archive ebenso wie für zukünftige Migrationsprojekte oder die Archivbenutzung (Stichwort: Suche). Als Beispiel einer genormten Datenerstellung sei hier das wohl bekannteste und weitest verbreitete Archivformat – PDF/A – genannt: *ISO 19005-2:2011, Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)*<sup>13</sup>. Als aktuelle Version ist seit 2012 PDF/A-3 auf dem Markt, das weitere Verbesserungen für die langfristige Aufbewahrung von Dokumenten enthält (z. B. sind Attachments als ZIP-Files integrierbar, zusätzliche Metadaten verfügbar etc.)<sup>14</sup>.

Im erweiterten Kontext können zur Erstellung strukturierter deskriptiver und technischer Metadaten wiederum spezifische nationale und/oder regionale Vorschriften herangezogen werden. Es gibt die Möglichkeit, die Erzeugung von Digitalisaten zu reglementieren<sup>15</sup>, Maßnahmen des Record-Managements anzuwenden<sup>16</sup> oder auch allgemein gültige Vorschriften zur Aktenführung wie z. B. Büroordnungen, Schlagwortkataloge oder dergleichen zum Einsatz zu bringen<sup>17</sup>.

## Allgemeine Standards für digitale Archive

Im Zuge der fortschreitenden Entwicklung von und der Beschäftigung mit digitaler Datenhaltung haben sich in den letzten zwei Jahrzehnten rasch eine Reihe von Konventionen entwickelt, welche – vereinfacht ausgedrückt – mehr oder weniger „Rahmenbedingungen“ für digitale Langzeitarchive festlegen bzw. deren Qualität und Vollständigkeit aufzeigen sollen. Einige dieser Empfehlungen haben sich zu (international) anerkannten Standards ausgebildet und sind in der Zwischenzeit auch offiziell zu solchen (ISO/DIN-Normen) erhoben worden. Teilweise handelt es sich um sehr eng gesteckte, themenbezogene Normen, meistens sind es jedoch „Mischformen“ aus fachlichen, technischen und administrativen Handhabungen, deren notwendiges Zusammenspiel im Kontext digitaler Archivierung nie außer Acht gelassen werden darf. Nur die konsequente Einhaltung

13 Als Überblick siehe hierzu den Internetauftritt der PDF/A-Association, früher PDF/A-Competence Center: <http://www.pdfa.org/?lang=de>.

14 Siehe hierzu auch den Vortrag von Dietrich von Seggern auf der diesjährigen AÜS-Tagung: [http://www.staatsarchiv.sg.ch/home/auds/18/\\_jcr\\_content/Par/downloadlist\\_1/DownloadListPar/download\\_9.ocFile/Praesentation%20von%20Seggern.pdf](http://www.staatsarchiv.sg.ch/home/auds/18/_jcr_content/Par/downloadlist_1/DownloadListPar/download_9.ocFile/Praesentation%20von%20Seggern.pdf) (Download am 24. 3. 2014).

15 Als Beispiel: ISO/TR 13028/2010-12 – Information und Dokumentation – Anleitung für die Implementierung von Verfahren zur Digitalisierung von Schriftgut.

16 Als Beispiel: DIN ISO 15489-1/2002-02 Information und Dokumentation – Schriftgutverwaltung – Teil 1: Allgemeines. Oder auch: MoReq („Model Requirements for the Management of Electronic Documents and Records“, seit der Version MoReq2010 „Modular Requirements for Records Systems“) ist der europäische Standard für das elektronische Records-Management. Die Richtlinie wurde im Rahmen des IDA-Programmes der Europäischen Kommission entwickelt und vom DLM-Forum veröffentlicht.

17 Als Beispiel sei hier die Empfehlung für zu verwendende Amtsformate in Österreich angeführt: Dokumentenformate 1.0.2, Konvention, BLSG. Wien, 2005 <http://reference.e-government.gv.at/uploads/media/formate-1-0-2-2005-01-26.pdf> oder auch die Büroordnung des Bundes: <http://www.bka.gv.at/DocView.axd?CobId=33038>.

möglichst vieler Standards wird auf Dauer ein umfassendes, qualitatives und vertrauenswürdiges Langzeitarchiv garantieren können.

### *OAIS-Referenzmodell*

Den Ausgangspunkt für zahlreiche Umsetzungsvarianten digitaler Archivierung bildet das mittlerweile international anerkannte „*Open Archival Information System – Reference Model (OAIS-Modell)*“ der NASA. Das ursprünglich für die Auswertung und die langfristige Erhaltung von Satellitendaten erstellte Modell wurde ab den 1990er Jahren zur theoretisch fundierten Grundlage sämtlicher Diskussionen zum Thema digitale Langzeitarchivierung. Ab 1994 fanden rund 20 US-nationale und 17 internationale Fachworkshops statt, in denen an der Ausarbeitung gemeinsamer technischer, fachlicher sowie administrativer Formulierungen und Anforderungen zur digitalen Archivierung gearbeitet wurde. Das abschließende Modell wurde 2000 als Empfehlung und 2003 als ISO-Norm publiziert (*ISO 14721:2003 Space data and information transfer systems – Open Archival Information System – Reference Model; Blue Book*)<sup>18</sup> und hat sich rasch als führendes Rahmenwerk für digitale Großprojekte der vergangenen Jahre etabliert. Es diente europäischen Initiativen, wie z. B. *nestor* (Network of Expertise in long-term Storage and availability of digital Resources in Germany) oder *PLANETS* (Preservation and Long-term Access through networked Services), ebenso als Vorgabe wie dem „Digitalen Archiv Österreich“ des Österreichischen Staatsarchivs.

Im deutschen Sprachraum hat sich insbesondere die *nestor*-Arbeitsgruppe „OAIS-Übersetzung/Terminologie“ mit dem OAIS-Modell befasst und 2012 erstmals eine vollständige deutsche Übersetzung veröffentlicht. Bereits 2013 erfolgte die Publikation einer korrigierten Version<sup>19</sup>. Auf Basis der von *nestor* erarbeiteten Dokumentation ist im Jänner 2014 ein Normen-Kommentar im deutschen Beuth-Verlag erschienen, herausgegeben von Sabine Schrimpf: „*Das OAIS-Modell für die Langzeitarchivierung. Anwendung der ISO 14721 in Bibliotheken und Archiven.*“<sup>20</sup> Hiermit liegt erstmals eine Gesamtfassung des OAIS-Modells in englischer und deutscher Sprache vor, ergänzt durch einen historischen Abriss und praktische Anwendungsbeispiele.

Doch wie schon der Name ausdrückt, ist das OAIS-Modell lediglich als „Referenz“, als bestmögliche Maximumvariante der digitalen Datenhaltung, zu betrachten. Es können je nach individueller Gestaltung der Archivorganisation Teilbereiche ergänzt und/oder weggelassen werden ohne die Integrität des Modells oder die Vertrauenswürdigkeit des Archives zu beeinträchtigen. OAIS bietet vor allem

---

18 The Consultative Committee for Space Data Systems (CCSDS): <http://public.ccsds.org/publications/default.aspx> Aktuelle OAIS-Version: ISO 14721:2012, CCSDS 650.0-M-2: Reference Model for an Open Archival Information System (OAIS). Magenta Book. Juni 2012. <http://public.ccsds.org/publications/archive/650x0m2.pdf>.

19 *nestor*-materialien 16, Referenzmodell für ein Offenes Archiv-Informations-System – Deutsche Übersetzung 2.0. Frankfurt am Main, 2013 [http://files.d-nb.de/nestor/materialien/nestor\\_mat\\_16-2.pdf](http://files.d-nb.de/nestor/materialien/nestor_mat_16-2.pdf).

20 Bestellseite des Beuth-Verlages: <http://www.beuth.de/de/publikation/das-oais-modell-fuer-die-langzeitarchivierung/186561465>.

einen Rahmen für ein gesteigertes Verständnis und Bewusstsein archivischer Konzepte inklusive einer gemeinsamen Terminologie, die zur langfristigen Erhaltung digitaler Informationen und zum Zugriff auf diese nötig ist. Es gestattet auch nicht-archivischen Organisationen erfolgreich am Prozess der Langzeitarchivierung mitzuwirken, umreißt Konzepte zur Beschreibung und zum Vergleich des Aufbaus und der Tätigkeiten bestehender und zukünftiger Archive und vermittelt Vorgaben zu verschiedenen möglichen Langzeiterhaltungsstrategien und -techniken. Es kann als Voraussetzung zur Gegenüberstellung divergierender Datenmodelle von archivierter digitaler Information herangezogen werden und zeigt Möglichkeiten auf, um auch die Langzeiterhaltung nicht-digitaler Information (z. B. physischer Datenträger) abzudecken.

Der wesentlichste Punkt ist aber die Definition des OAIS selbst: „Ein OAIS ist ein Archiv, das aus einer Organisation, die Teil einer größeren Organisation sein kann, aus Menschen und Systemen besteht, das die Verantwortung übernommen hat, Information zu erhalten und sie einer vorgesehenen Zielgruppe zugänglich zu machen. Es erfüllt eine Reihe von Verantwortlichkeiten.“<sup>21</sup> Die oft getätigte Annahme und landläufige Vorstellung, dass ein digitales Archiv „eine rein technische Angelegenheit“ ist, wird damit dezidiert abgelehnt und die gleichwertige Aufteilung zwischen technischen, fachlichen, administrativen und personellen Zuständigkeiten betont. Ein OAIS ist keine technische Lösung, sondern ein organisatorisches Gesamtkonzept.

Allerdings ist das OAIS-Modell nicht dafür geeignet, daraus konkrete Angaben zu nicht-funktionalen Anforderungen, wie Zuverlässigkeit, Änderbarkeit, Übertragbarkeit, oder Vorschläge zu allgemeinen Prinzipien, wie Dokumentation, Transparenz, Messbarkeit oder Angemessenheit, abzuleiten. Es gibt kein bestimmtes Design und auch keine bestimmte Art der Umsetzung vor. Im Zuge der Implementierung können Funktionen nach Bedarf gruppiert, maximiert, minimiert oder herausgebrochen werden. Es müssen nicht alle Module gleichzeitig oder qualitativ gleichwertig entwickelt werden, sondern können zeitlich nacheinander und in unterschiedlichen Ausbaustufen langfristig zu einem komplexen Ganzen führen. Weiters stellt OAIS keine direkten Zusammenhänge zwischen abstrakten (Policy-) und konkreten (Praxis-)Einheiten her und erscheint dem Laien durch das Fehlen von tauglichen Beispielen, Best-Practices sowie etwaiger „Checklisten“ anfänglich oft kompliziert und undurchschaubar. Doch genau durch diese modularen, nicht taxativ festgeschriebenen Rahmenbedingungen ist das OAIS-Modell vielseitig einsetz- und anwendbar und sollte für jedes anspruchsvolle digitale Archiv das fachliche Fundament darstellen.

## *EDIAKT II*

Als spezieller Österreich-Bezug soll in diesem Beitrag das sogenannte *EDIAKT II-Schema* („Electronic Data Interchange Format“ für elektronische Akten) als nationaler Standard nicht unerwähnt bleiben. Die 2005 publizierte „Empfehlung“ der

---

21 Siehe nestor-materialien 16, Seite 2.



österreichischen Kooperation Bund-Länder-Städte-Gemeinden (BLSG) beschreibt den Aufbau und die Integration von EDIAKT II für gültige elektronische Akten quer über alle in Österreich installierten ELAK- und KIS-Systeme<sup>22</sup>. Das XML-Schema dient zum Austausch digitaler Informationen innerhalb von Verwaltungen und Behörden im Produktivbetrieb ebenso wie als „Transportmittel“ zwischen Fachanwendungen sowie nicht zuletzt als Containerformat zur Übernahme von Daten in Archivsysteme.

Das „Digitale Archiv Österreich“ (digLA) ist derzeit darauf ausgerichtet, ausschließlich gültige EDIAKT II-Pakete aus dem Elak-im-Bund-System auszusondern und über eine passende Ingest-Schnittstelle zu archivieren. Durch die XML-Struktur des Standards ist es möglich, die verschiedensten Ausprägungen der Aktenführung (Layer), von Inhalten (Content in allen denkbaren Formaten) und von Metadaten zu vereinheitlichen und (technisch) genormt in das digitale Archiv einzulagern. Die Inhaltsdaten bleiben bei diesem Prozess unverändert, deren Qualität muss allenfalls nachträglich durch andere (archivfachliche) Normen geprüft werden. Durch die Verwendung von EDIAKT als abgestimmtes Übergabeformat können aktuell Ingestabläufe großteils automatisiert gestaltet und zukünftig Migrationen leichter durchgeführt werden.

Seit einiger Zeit wird in der Arbeitsgruppe am Nachfolgeschema „EDIDOC“ (Electronic Data Interchange Format for Documents)<sup>23</sup> gearbeitet, eine Verabschiedung des Standards als Empfehlung oder Konvention sollte im Laufe des Jahres 2014 erfolgen. Der Umstieg bzw. die „Umrüstung“ des digLA auf das Format EDIDOC ist in Diskussion bzw. in Planung, kann aber erst nach offizieller Freigabe des neuen Schemas erfolgen. Diesbezüglich bedarf es auf Grund der komplexen Strukturen innerhalb des digitalen Archivs nicht unerheblicher Anpassungen der Software (Workflows, Schnittstellen, Schemavalidierungen) sowie der Fachprozesse. Im Weiteren wird die parallel laufende Entwicklung der EDIDOC-Tools (Creator/Viewer) abgewartet.

## METS

Ein weiteres XML-Transport- oder Austauschformat, das mittlerweile vielfach in digitalen Archiven zum Einsatz kommt, ist METS (Metadata Encoding and Transmission Standard). Der Standard wird von der Library of Congress gehostet<sup>24</sup>. Im Gegensatz zu den bereits bei den Archivnormen erwähnten I- und E-Standards erlaubt METS den Austausch von deskriptiven, administrativen, technischen und strukturellen Metadaten digitaler Objekte innerhalb einer einzigen Norm. Die METS-Struktur besteht aus sieben Hauptabschnitten, in welche je nach Bedarf entweder direkt Metadatenfragmente aus anderen Systemen (anderen Normen) eingepflegt oder Verweise auf externe Angaben angeführt werden können.

22 Dokumente zu EDIAKT II: <http://reference.e-government.gv.at/Veroeffentlichte-Informationen.601.0.html>.

23 Den Entwurf zum EDIDOC-Schema findet man auf der BKA-WIKI Seite: <https://www.ag.bka.gv.at/at.gv.bka.wiki-bka/index.php/Portal:Ediakt>.

24 Siehe hierzu: <http://www.loc.gov/standards/mets/>.

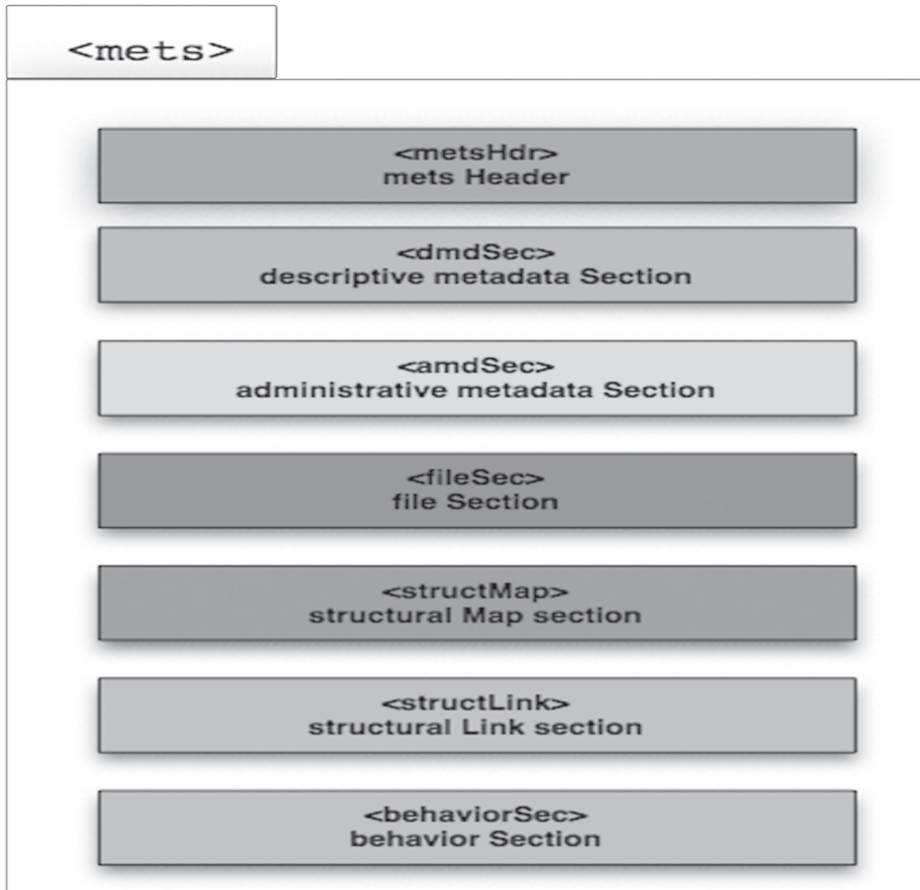


Abbildung entnommen aus: *Metadata Encoding And Transmission Standard - Primer And Reference Manual*, Seite 1<sup>25</sup>.

Der Vorteil von METS besteht darin, dass nicht alle Ebenen gleichmäßig befüllt werden müssen, sondern entsprechend der jeweiligen Ausformung digitaler Informationspakete nur die benötigten Sektionen genutzt werden können. So kann ein METS-Dokument im Kontext des Open Archival Information System-Referenzmodells entweder als Liefereinheit der Datenübernahme (Submission Information Package, SIP), als Archivierungseinheit (Archival Information Package, AIP) oder als Bereitstellungseinheit (Dissemination Information Package, DIP) verwendet werden. Das „Digitale Archiv Österreich“ z. B. nutzt die METS-Struktur als unterstützendes Containerformat für die DIP-Auslieferung der Metadaten (EAD, PREMIS).

<sup>25</sup> <http://www.loc.gov/standards/mets/METSPrimerRevised.pdf>.

## *DIN-Normen*

In Bezug auf digitale Archivsysteme ist es nicht nur notwendig, sich mit den reinen Fachprozessen wie Datenübernahme (Ingest), Datenspeicherung (Storage) oder Datenzugriff (Access) inhaltlich zu beschäftigen, sondern vor allem die Umsetzung dieser Vorgänge sorgfältig zu dokumentieren und qualitativ abzusichern. Da digitale Objekte im Unterschied zu analogem Schriftgut durch komplexe Erhaltungsstrategien und -prozesse einer schnelllebigeren inneren und äußeren Veränderung unterliegen können bzw. müssen, ist es umso wichtiger, alle getroffenen Entscheidungen genau festzuhalten, sodass langfristige Nachvollziehbarkeit gegeben ist. In diesem Zusammenhang ist immer öfter von Schlagwörtern wie „Vertrauenswürdigkeit“ oder „Zertifizierung“ digitaler Archive die Rede, wodurch die Qualität eines Langzeitarchives auch nach außen hin sichtbar gemacht werden soll. Gefördert wird dieses Bestreben durch die Anwendung von Normen.

Es wurde bereits mehrfach auf die rege Arbeitstätigkeit deutscher Kollegen zu vielen Themen digitaler Archivierung Bezug genommen. Maßgebliche Grundlegendendokumente, welche in diversen Projekten, insbesondere nestor-Arbeitsgruppen, erarbeitet wurden, sind in den letzten Jahren in Arbeitskreisen des Deutschen Instituts für Normung (DIN) aufgegangen und wurden in der Zwischenzeit als DIN-Normen publiziert<sup>26</sup>. Als Hauptgremium beschäftigt sich der Normenausschuss „Bibliotheks- und Dokumentationswesen“ (NA 009 oder kurz NABD) mit den archiv- und bibliotheksspezifischen Themen. Der Unterausschuss NA 009-00-15 AA „Schriftgutverwaltung und Langzeitverfügbarkeit digitaler Informationsobjekte“ mit seinen sechs thematischen Arbeitsgruppen ist für sämtliche digitalen Belange zuständig<sup>27</sup>. Der gesamte Archivierungszyklus wird, wohlgerne immer unter Berücksichtigung des OAIS-Modells, fachlich durchleuchtet und mit entsprechenden Maßnahmen und Richtlinien befüllt. Als Beispiele seien die derzeit relevanten veröffentlichten DIN-Normen 31644 bis 31647 angeführt:

### *DIN 31647 – Information und Dokumentation – Beweiswerterhaltung kryptographisch signierter Dokumente*

Der Norm-Entwurf des Arbeitskreises „Beweiswerterhaltung kryptographisch signierter Dokumente“ befindet sich in der letzten Abstimmungsphase und wird noch im Frühjahr 2014 offiziell erscheinen. Es werden die technischen und sicherheitsrelevanten Anforderungen an die langfristige Aufbewahrung von digital signierten Dokumenten unter Wahrung der Rechtskraft der digitalen Signatur sowie konkrete Funktionen eines generischen Systems zur Beweiswerterhaltung kryptographisch signierter Dokumente beschrieben<sup>28</sup>. Als Instrumente der Datenverschlüsselung sind in der modernen Verwaltung fortgeschrittene qualifizierte

26 DIN-Startseite siehe: <http://www.din.de/cmd?level=tpl-home&contextid=din>.

27 Zum Ausschuss NABD siehe: [http://www.nabd.din.de/cmd?workflowname=InitCommittee&search\\_committee=nabd&contextid=nabd](http://www.nabd.din.de/cmd?workflowname=InitCommittee&search_committee=nabd&contextid=nabd) und <http://www.nabd.din.de/cmd?level=tpl-untergremium-home&contextid=54738855&languageid=de&breadcrumblevel=2&subcommitteeid=54774796>.

28 Details zur Norm siehe: <http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&contextid=54738855&artid=198641541&languageid=de&breadcrumblevel=3>.

elektronische Signaturverfahren (z. B. zur Ermittlung von kryptographischen Hashwerten) und Zeitstempel, welche den technisch gültigen Anforderungen entsprechen, im Einsatz.

Die Signaturen müssen jedoch im Laufe der Zeit „nachsigniert“, d. h. regelmäßig erneuert und auf den aktuellen Stand gebracht werden. Dazu muss die neue Signatur alle vorangegangenen Signaturen und Zeitstempel einschließen, ebenso müssen die dazugehörigen Schlüssel aufbewahrt und langfristig gesichert werden. Die vorliegende Norm versucht all diese Vorgaben abzubilden und grundlegende Anforderungen an die Informationspakete eines digitalen Langzeitarchivs gemäß OAIS-Modell anzuführen, um dauerhaft die Integrität und Authentizität digitaler Objekte sicherstellen zu können. Dies dient insbesondere dem zukünftigen Benutzer digitaler Archive als Beweis, dass das für ihn in späteren Jahren zur Verfügung gestellte Objekt (Nutzungspaket, DIP) inhaltlich noch dasselbe ist wie zum Zeitpunkt der Übernahme in das digitale System<sup>29</sup>.

#### *DIN 31646 – Information und Dokumentation – Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier, PI)*

Um digitale Objekte langfristig „auffindbar“ zu machen, d. h. für Migrationsprozesse ebenso wie zur späteren Benutzung (Stichwort: „dauerhafte Zitierfähigkeit“) zu erhalten, ist die Vergabe eines eindeutigen Identifikators unerlässlich. Diese eindeutig festgelegte Objektbezeichnung, welche sich nie ändern darf, kann fachlich gesehen eine Geschäftszahl oder Aktenzahl, technisch eine URL (Uniform Resource Locator) oder eine UUID (Universally Unique Identifier) sein. All diese Identifier sind aber abhängig von ihrem Standort, sprich Speicherort. Ändert sich dieser, erscheinen auf Webseiten das allseits bekannte „Diese Seite kann nicht angezeigt werden“ oder ähnliche Hinweise. Für digitale Archivobjekte gilt nun dasselbe: Ändert sich der physikalische Speicherort und somit die Referenz auf diesen, kann unter Umständen das Objekt nicht mehr aufgefunden und somit im schlechtesten Fall nicht länger erhalten werden.

Abhilfe dafür soll die aus dem Bibliothekswesen übernommene Vorgehensweise der Vergabe von „persistenten Identifikatoren“ (PI) schaffen. „Persistent“ wird als ein im Kontext wohldefinierter Fachbegriff für „nicht unkontrolliert veränderlich“ verwendet. Das bedeutet, dass Daten, z. B. auch nach (unvorhergesehenem) Beenden eines Programms, vorhanden/gespeichert bleiben und bei erneutem Aufruf des Programms wieder rekonstruiert und angezeigt werden können. Bezüglich der logischen Verbindungen bedeutet Persistenz, dass die reale Verbindung bei Bedarf wiederhergestellt werden kann, ohne dass die zwischenzeitliche Trennung durch die Kommunikationspartner bemerkt wird.

---

<sup>29</sup> Weiterführende Informationen: Steffen Schwalm, Ulrike Korte, Detlef Hühnlein, Vertrauenswürdige und beweiswerterhaltende elektronische Langzeitspeicherung auf Basis von DIN 31647 und BSI TR-03125. GI-Jahrestagung, volume 220 of LNI, page 550–566. GI (2013): <http://subs.emis.de/LNI/Proceedings/Proceedings220/550.pdf>.

Persistente Identifikatoren dienen im Weiteren der eindeutigen, dauerhaften und vor allem standortunabhängigen Adressierung von digitalen Ressourcen. Im Gegensatz zu herkömmlichen Identifiern unterscheiden sie zwischen Identifizierung und Adresse eines Objektes. Im Archivwesen bedeuten Pls weltweit eindeutig vergebene Objektadressen, welche zur dauerhaften Erkennung archivierter Objekte (Dokumente, Bilder, Tonaufnahmen, Videoaufzeichnungen oder Metadatenbeschreibungen) eingesetzt werden. Als Ausformungen solcher Pls können fachlich ISBN, ISSN oder Archivsignaturen sowie technisch URN (Uniform Resource Name) oder im Weiteren PURL (Persistent Uniform Resource Locator) angeführt werden<sup>30</sup>.

Die vorliegende DIN-Norm 31646 dient nunmehr dazu, die Handhabung und Nutzung persistenter Identifikatoren in Bezug auf digitale Archive zu veranschaulichen und den Umgang mit denselben zu verdeutlichen<sup>31</sup>. Als Umsetzungsinstrumente werden so genannte „(Link)Resolver“ vorgeschlagen. Dies sind Systeme, welche in der Lage sind, Metadaten digitaler Informationsobjekte entgegenzunehmen und in Verbindung mit Informationen über Speicherorte dynamische Verweise (Links) auf diese zu erzeugen. Somit ist langfristig über technische und organisatorische Veränderungen hinweg eine verlässliche Identifizierung und Adressierung digitaler Objekte möglich, wodurch Integrität, Authentizität und Vertrauenswürdigkeit digitaler Archive gesichert werden.

### *DIN 31645 – Information und Dokumentation – Leitfaden zur Informationsübernahme in digitale Langzeitarchive*

Lange Zeit hat man sich in den Fachdiskussionen zur digitalen Archivierung vorrangig mit der Datenübernahme, dem Ingest, beschäftigt. Wobei der Begriff „Datenübernahme“ hier nicht erst ab dem Zeitpunkt der physischen Datenabgabe an das digitale Archiv gesehen, sondern um den vor- und zwischenarchivischen Aufgabenbereich (z. B. erste Kontaktaufnahme, Bewertung der zu archivierenden Objekte, Aufbewahrungsfrist etc.) erweitert wird. Als Ergebnis wurde 2004 vom *Consultative Committee for Space Data Systems (CCSDS)* ein erstes Dokument zur Beschreibung des Zusammenspiels zwischen (Akten/Daten-)Produzent und (Langzeit-)Archiv vorgelegt, dessen Überarbeitung 2006 als ISO-Norm veröffentlicht wurde: *ISO 20652:2006 Producer-Archive Interface Methodology Abstract Standard (PAIMAS)*<sup>32</sup>. In 88 Einzelschritten mit festgelegter Reihenfolge wird

30 Nähere Informationen zu persistenten Identifikatoren siehe z. B.: <http://www.persistent-identifier.de/> oder auch: <http://www.langzeitarchivierung.de/Subsites/nesstor/DE/Standardisierung/PI.html> sowie: *nesstor-materialien 13, Kriterienkatalog zur Überprüfung der Vertrauenswürdigkeit von PI-Systemen*. Frankfurt am Main, 2009. [http://files.d-nb.de/nesstor/materialien/nesstor\\_mat\\_13.pdf](http://files.d-nb.de/nesstor/materialien/nesstor_mat_13.pdf).

31 Details zur Norm siehe: <http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=165444031&languageid=de&tbcrumble=3>.

32 Das Gesamtdokument von PAIMAS als Magenta Book von 2004 siehe: <http://public.ccsds.org/publications/archive/651x0m1.pdf>; die ISO-Norm findet sich unter: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39577](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39577).

genau definiert, wann und welche Maßnahmen, Regeln und Vereinbarungen zu treffen sind und wer (Produzent oder Archiv) dafür die Verantwortung trägt.

Für die deutsche Archivlandschaft hat sich erneut eine nestor-Arbeitsgruppe, die AG „Standards für Metadaten, Transfer von Objekten in digitale Langzeitarchive und Objektzugriff“, dieses Themas angenommen und 2008 den Leitfaden „Wege ins Archiv“ veröffentlicht<sup>33</sup>. Auf Basis dieses Dokumentes ist in weiterer Folge im Normen-Arbeitskreis „Ingest“ die DIN 31645 entstanden, welche 2011 erschienen ist<sup>34</sup>. Im Unterschied zu PAIMAS hebt die DIN-Norm die feste Reihenfolge der Übernahmeschritte auf und folgt lediglich einer plausiblen zeitlichen Abfolge. Die definierten Maßnahmen werden nicht mehr durchnummeriert, sondern sind nach Themen gegliedert (Objekte – Prozesse – Management) und als Maximalcatalog anzusehen. Die praktische Realisierung der einzelnen Phasen kann je nach Ausgangssituation, Form der Datenobjekte, Archivorganisation oder Aktenproduzent variieren. Eine angefügte „Checkliste“ der durchzuführenden Planungsschritte sowie praktische Beispiele zu den einzelnen Kriterien ergänzen die DIN-Norm 31645.

Da gerade bei der Informationsübernahme in digitale Archive bereits grundlegende Voraussetzungen für eine spätere automatisierte und effiziente Datenverarbeitung gelegt werden, ist die Anwendung dieses Standards sehr zu empfehlen. Durch die Vorgaben zu dokumentierten Planungs- und Arbeitsschritten, Validierungsprozessen, zur Bestimmung der beteiligten Personen und Hilfsmittel sowie zum anzustrebenden Erfüllungsgrad einzelner Kriterien und den daraus entstehenden Konsequenzen ist die Norm ein weiterer wichtiger Schritt auf dem Weg zu einem vertrauenswürdigen, zertifizierbaren digitalen Langzeitarchiv.

### *DIN 31644 - Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive*

Auch die letzte hier genannte DIN-Norm hat eine Vorgeschichte in einer nestor-Arbeitsgruppe. Die AG „Vertrauenswürdige Archive“ wurde 2004 gegründet und hat 2006 einen ersten „Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ herausgegeben. 2008 erfolgte eine überarbeitete zweite Version<sup>35</sup>, welche schließlich wiederum in einer DIN-Arbeitsgruppe des NABD 15 aufgegangen ist. Durch den Arbeitskreis „Vertrauenswürdige digitale Archive“ wurde der Kriterienkatalog schließlich im Frühjahr 2012 als DIN-Norm 31644 veröffentlicht<sup>36</sup>.

33 Siehe hierzu: nestor-materialien 10, Wege ins Archiv - Ein Leitfaden für die Informationsübernahme in das digitale Langzeitarchiv. Frankfurt am Main, 2008. [http://files.d-nb.de/nestor/materialien/nestor\\_mat\\_10.pdf](http://files.d-nb.de/nestor/materialien/nestor_mat_10.pdf).

34 Details zur Norm siehe: <http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=145158117&languageid=de&breadcrumblevel=3>.

35 Siehe hierzu: nestor-materialien 8, nestor-Kriterienkatalog vertrauenswürdige digitale Langzeitarchive Version II. Frankfurt am Main, 2008. [http://files.d-nb.de/nestor/materialien/nestor\\_mat\\_08.pdf](http://files.d-nb.de/nestor/materialien/nestor_mat_08.pdf).

36 Details zur Norm siehe: <http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=147058907&languageid=de&breadcrumblevel=3>.

In Abweichung von den bisher dargestellten DIN-Standards wird hier das OAIS-Modell lediglich terminologisch referenziert, es stellt keine Bedingung und keinen „Überstandard“ dar. Im Weiteren spricht die Norm nicht nur altbekannte und bewährte Gedächtnisorganisationen, wie Archive oder Museen, an, sondern soll für alle Institutionen, welche sich im digitalen Zeitalter mit langfristiger Datenhaltung beschäftigen (müssen), als Vorgabe dienen. Wie bereits mehrfach angesprochen, ist gerade im digitalen Archivwesen die Beweisführung bezüglich Authentizität und Integrität digitaler Informationsobjekte ein wesentlicher Bestandteil. Die für analoge Datenhaltung – sprich Schriftgutaufbewahrung – zuständigen Einrichtungen konnten sich im Laufe ihres Bestehens einen gewissen Vertrauensvorschuss erarbeiten. Es wird vorausgesetzt, dass sie alle notwendigen Maßnahmen zur Erhaltung des ihnen anvertrauten kulturellen Erbes durchführen. Digitale Archive müssen sich dieses Vertrauen erst erarbeiten, und dazu kann der vorliegende Kriterienkatalog als Unterstützung dienen.

DIN 31644 gilt als Rahmenstandard, der je nach Zielgruppe, (Archivierungs-) Auftrag und/oder Aufbewahrungsdauer unterschiedlich umgesetzt werden kann. Die insgesamt 34 Kriterien sollen dabei helfen, den zukünftigen Archivbenutzer von Fragen nach Vertrauenswürdigkeit zu entlasten; sie können digitalen Archiven im Zuge von Selbstevaluierungen Hinweise auf mögliche Schwachstellen ihrer Archivsysteme geben und fördern dadurch das öffentliche Vertrauen in digitale Archive. Es werden keine expliziten technischen Richtlinien vorgegeben, sodass im Zuge von internen und externen Projekten auch einer weitergehenden (kosteneffizienten) Beteiligung ausführender Dritter nichts entgegensteht. Im Sinne der Norm ist ein digitales Langzeitarchiv dann vertrauenswürdig, wenn es gemäß seinen Zielen und seiner Aufgaben den Erhalt von Daten über einen langfristigen Zeitraum sicherstellen kann und seine Nutzer, Produzenten, Betreiber und Partner ihm dieses zutrauen.

Die aufgelisteten Kriterien teilen sich in mehrere Abschnitte. Die Punkte 1-12 sind primär organisatorischen Rahmenbedingungen zuzuordnen:

Ziele des Langzeitarchives:	K 1: Auswahl der Informationsobjekte und ihrer Repräsentationen
	K 2: Verantwortung für den Erhalt
	K 3: Zielgruppen
Angemessene Nutzung:	K 4: Zugang
	K 5: Interpretierbarkeit
Rechtliche Regelungen:	K 6: Rechtliche und vertragliche Basis
	K 7: Rechtskonformität
Ressourcenplanung:	K 8: Finanzierung
	K 9: Personal
	K 10: Organisation und Prozesse
	K 11: Erhaltungsmaßnahmen
	K 12: Krisen-/Nachfolgeregelung

Die Kriterien 13–32 definieren den Umgang mit den zu erhaltenden digitalen Informationsobjekten und deren Repräsentationen, wobei auch hier nochmals ein paar „Themenkapitel“ eingezogen werden können:

Objekteigenschaften:	K 13: Signifikante Eigenschaften
Integrität:	K 14: Integrität: Aufnahmeschnittstelle
	K 15: Integrität: Funktionen der Archivablage
	K 16: Integrität: Nutzerschnittstelle
Authentizität:	K 17: Authentizität: Aufnahme
	K 18: Authentizität: Erhaltungsmaßnahmen
	K 19: Authentizität: Nutzung
Umgang mit Datenpaketen:	K 20: Technische Hoheit
	K 21: Transferpakete
	K 22: Transformation der Transferpakete in Archivpakete
	K 23: Archivpakete
	K 24: Interpretierbarkeit der Archivpakete
	K 25: Transformation der Archivpakete in Nutzungspakete
	K 26: Nutzungspakete
Datenmanagement:	K 27: Identifizierung
	K 28: Beschreibende Metadaten
	K 29: Strukturelle Metadaten
	K 30: Technische Metadaten
	K 31: Protokollierung der Langzeiterhaltungsmaßnahmen
	K 32: Administrative Metadaten

Die letzten beiden Kriterien weisen abschließend auf technische Vorgaben hin, ohne jedoch, wie bereits erwähnt, genaue technische Spezifikationen anzugeben:

Infrastruktur und Sicherheit:	K 33: IT-Infrastruktur
	K 34: Sicherheit

Mit Hilfe von DIN 31644 können archivische Grundprinzipien, wie Dokumentation, Transparenz, Angemessenheit und Bewertbarkeit, in digitalen Archiven umgesetzt werden. Realisierung und/oder Evaluierung der einzelnen Kriterien können als mehrstufiger Prozess angesehen werden, der gegebenenfalls nach einiger Zeit wiederholt werden sollte/muss. Der Standard dient als Instrument zur ständigen Verbesserung der Konzeption, Planung, Spezifikation, Umsetzung und Implementierung digitaler Archive.

Eine praxisnahe Form des Standards liegt seit 2013 in einem Kommentarband des Beuth-Verlages vor: *Christian Keitel, Astrid Schoger (Hrsg.), Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644. Beuth Verlag GmbH Berlin, Wien,*



Zürich 2013. 112 S., ISBN 978-3-410-23499-9<sup>37</sup>. Der Kommentar umfasst neben einem Vorwort eine kurze Einführung zur Norm sowie die Darlegung zentraler Begriffe, wie z. B. „Informationsobjekt“, „Signifikante Eigenschaften“, oder „Repräsentationen“ (hier auch in terminologischem Bezug zum OAIS-Modell). Es folgen zwei recht ausführliche Kapitel zur Entstehungsgeschichte der nestor-Kriterienkataloge und der internationalen wie nationalen (= deutschen) Diskussionen rund um das Thema „Vertrauenswürdigkeit“ – immer auch einhergehend mit der Folgewirkung einer möglichen Zertifizierung. Im Weiteren wird der Darstellung der Verbindung zu anderen nationalen und internationalen Projekten und Entwicklungen der Langzeitarchivierung sowie dem Thema Zertifizierung Raum gegeben. Im Anschluss folgt die Auslegung der Norm in ihren einzelnen Kriterien, jeweils mit Erläuterungen und/oder Beispielen versehen. Abschließend findet sich, wie bei den Kommentarbänden üblich, der Gesamtabdruck des Standards im Original.

Alles in allem stellt das Buch einen sehr empfehlenswerten Normenkommentar dar. Für alle Einsteiger in die Materie „Langzeitarchivierung“ wird eine gute Informationsgrundlage bezüglich der Bedingungen, die ein funktionales digLA benötigt, geboten, für alle Experten finden sich weiterführende (Literatur-)Hinweise, Erläuterungen und Praxistipps zur Weiterentwicklung digitaler Archive bzw. auch zur Herangehensweise an eine etwaig geplante Zertifizierung.

### Exkurs Zertifizierung

Die seit Mitte der 1990er Jahre parallel geführten Fachdialoge in Gremien, wie dem *Internationalen Archivrat (ICA)*, der *Commission of Preservation and Access*, der *Research Library Group (RLG)* oder dem *Online Computer Library Center (OCLC)*, führten „Glaubwürdigkeit“ und „Vertrauenswürdigkeit“ digitaler Objekte immer öfter im Zusammenhang mit Zertifizierung an. Die Vergabe eines offiziellen „Gütestempels“ sollte auch nach außen hin demonstrieren, dass digitale Archive das sind, was sie zu sein vorgeben. Diesbezüglich wird im Zuge von Zertifizierungen auch nur ein „ganzes“ digitales Archiv als Organisation bewertet und nicht einzelne Dokumente oder technische Lösungen.

Bis Mitte der 2000er Jahre entstanden neben dem nestor-Katalog bzw. der DIN 31644 erste Kriterienkataloge, die sich explizit mit Zertifizierung auseinandersetzen. Bekannt sind insbesondere:

- *Digital Repositories Audit Method Based on Risk Assessment (DRAMBORA)*<sup>38</sup>
- *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*<sup>39</sup>
- *Data Seal of Approval (DSA)*<sup>40</sup>

37 Bestellseite des Beuth-Verlages: <http://www.beuth.de/de/publikation/vertrauenswuerdige-digitale-langzeitarchivierung-nach-din-31644/169654635?SearchID=658511451>.

38 Projektseite siehe: <http://www.repositoryaudit.eu/>.

39 Projektseite siehe: <http://trac.edgewall.org/>; Kriterienkatalog von 2007 unter: [http://www.crl.edu/sites/default/files/attachments/pages/trac\\_0.pdf](http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf).

40 Projektseite siehe: <http://www.datasealofapproval.org/en-qb/>.

Die in TRAC erarbeiteten Vorgaben wurden ab 2008/2009 durch die fast gleichnamige, aber personell anders besetzte Arbeitsgruppe „Repositories Audit and Certification“ (RAC) des CCSDS weitergeführt und als Magenta Book „Audit and Certification of Trustworthy Digital Repositories“ 2011 veröffentlicht. Daraus entstand in weiterer Folge, inhaltlich unverändert, die ISO-Norm 16363:2012 *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*<sup>41</sup>.

Um ein Auseinanderdriften der verschiedenen Initiativen zu verhindern bzw. zukünftige Zertifizierungsprozesse einheitlich zu gestalten, fand in den letzten Jahren eine Abstimmung der drei Großprojekte – TRAC/RAC, DSA und nestor – statt. Obwohl thematisch ident, waren die Kriterienkataloge inhaltlich doch sehr unterschiedlich. Die Anzahl der Kriterien, die Ausrichtung und Zielsetzung sowie die fachlichen Bezugspunkte stammten zu sehr aus dem jeweiligen Entstehungskontext, als dass man die drei Dokumente einfach zu einem hätte zusammenführen können. So einigte man sich auf internationaler Ebene 2007 in einer gemeinsamen Sitzung in Chicago auf „10 allgemeine Grundprinzipien“, die allen Katalogen gemeinsam waren<sup>42</sup>. Auf europäischer Ebene mündete das Bestreben zur Einheitlichkeit 2010 in ein „Memorandum of Understanding to create a European Framework for Audit and Certification of Digital Repositories“<sup>43</sup>.

Somit gibt es mit Stand 2014 drei Möglichkeiten, ein digitales Archiv im deutschsprachigen Raum zertifizieren zu lassen. Das „Data Seal of Approval“, das so genannte „nestor-Siegel“ nach DIN 31644 und die Zertifizierung nach ISO 16363. Das Verfahren ist dreistufig geplant, wobei das DSA immer die Basisbewertung darstellt und DIN/ISO entweder als „extended“- (begutachtete und veröffentlichte Selbstevaluierung) oder „formal“- (formal-extern begutachtete) Zertifizierung durchgeführt werden kann. DIN/ISO werden hierbei gleichwertig behandelt, wobei das nestor-Siegel weitaus kostengünstiger ausfällt<sup>44</sup>. Eine „Ausbaustufe“ zu einem einheitlichen europäischen Siegel ist für die kommenden Jahre in Planung.

## Zusammenfassung

Alle hier vorgestellten Normen, Standards und Richtlinien mögen als weiterführende Informationsquellen und als Anhaltspunkte dienen. Die Aufzählung erhebt keinerlei Anspruch auf Vollständigkeit, da die Anwendung von Standards immer von der individuellen Ausrichtung und den Ansprüchen der jeweils damit

41 Zu CCSDS und Magenta Book siehe: <http://public.ccsds.org/publications/MagentaBooks.aspx>; die ISO-Norm findet sich auf: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_tc\\_browse.htm?commid=46612](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=46612).

42 Grundprinzipien siehe z. B. auf: <http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re>.

43 Informationen zum Memorandum unter: <http://www.trusteddigitalrepository.eu/Site/Trusted%20Digital%20Repository.html>.

44 Informationen zum nestor-Siegel unter: [http://www.langzeitarchivierung.de/Subsites/nestor/DE/nestor-Siegel/siegel\\_node.html](http://www.langzeitarchivierung.de/Subsites/nestor/DE/nestor-Siegel/siegel_node.html).

befassten Organisation abhängt. Ob viel, wenig oder nur auszugsweise mit Hilfe normativer Vorgaben gearbeitet wird, ist oftmals eine Frage von administrativen, fachlichen, technischen, budgetären oder personellen Ressourcen. Die Erarbeitung von standardisierten Rahmenkriterien, deren Dokumentation, Umsetzung und dauerhafte Einhaltung benötigt Zeit, einiges an Engagement und Idealismus und ist nicht selten der Anfang oder die Bedingung einer entscheidenden Änderung von Organisationsstrukturen und -kulturen.

Insbesondere die digitale Archivierung verlangt nicht nur Wissen über bestehende Reglementierungen, sondern sieht sich gezwungen, die alltäglichen Prozesse den neuen Anforderungen ständig anzupassen, um langfristig konkurrenzfähig zu bleiben und auch in den nächsten Jahren alle Bedürfnisse der Archive dauerhaft sicherstellen zu können. In diesem Sinne sollte man sich bewusst werden, dass es durch die Anwendung von international anerkannten, einheitlichen Standards leichter fällt, die grundlegenden Kriterien der digitalen Archivierung kennenzulernen, zu verstehen und nicht zuletzt auch einzelne Punkte bei Bedarf vor Entscheidungsträgern als zwingend notwendig besser vertreten und argumentieren zu können. Der fachliche Austausch in übergeordneten (Entwicklungs-)Gremien, eine vereinfachte Kommunikation mittels einer „gemeinsamen Normensprache“, der daraus entstehende vereinfachte und/oder automatisierte Austausch von Informationen/Daten innerhalb und außerhalb verschiedener (Archiv-)Systeme und die bessere „Kontrollierbarkeit“ (Nachvollziehbarkeit) strukturierter Inhalte können als weitere Vorteile von Normung gesehen werden.

Nichtsdestotrotz ist das Gebiet der digitalen Normen ein neues, aufstrebendes Arbeitsfeld, in dem es gilt, sich stetig weiterzuentwickeln, sich laufend und wiederholt den aktuellen Herausforderungen zu stellen, technische Neuerungen mit einzubeziehen und zukünftig auch auf verändertes Nutzungsverhalten (Stichwort: Social Media, Open Data) verstärkt Rücksicht zu nehmen. Diesbezüglich sind in den kommenden Jahren weitere Entwicklungen von Normen und Standards zur digitalen Archivierung mit Spannung zu erwarten.