Fraunhofer
FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

DIGITALE DOKUMENTE NACHHALTIG ZUGREIFBAR MACHEN

DIGITALE DOKUMENTE NACHHALTIG ZUGREIFBAR MACHEN

INS - Innovation mit Normen und Standards

Projektgruppe:

Dr. Klaus-Peter Eckert, Joachim Kaeber
Fraunhofer-Institut für Offene Kommunikationssysteme, FOKUS

Roman Grahle
Deutsches Institut für Normung, DIN

Mai 2015

Gefördert durch das Bundesministerium für Wirtschaft und Energie

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Zusammenfassung

Das durch das BMWi im Rahmen des INS-Programms finanzierte Projekt untersucht, in welchem Umfang und unter welchen Voraussetzungen digitale Dokumente in der Kommunikation zwischen Verwaltung, Unternehmen und Bürgern auf portable Art und Weise erstellt, ausgetauscht und nachhaltig im Rahmen gesetzlicher Vorgaben archiviert und bei Bedarf weiterverarbeitet werden können.

Die Notwendigkeit zur Definition eines übertragbaren Dokumentenbegriffs als Voraussetzung für die Erstellung und Archivierung portabler Dokumente sowie die Implementierung interoperabler Büroanwendungen ist aus Sicht von Forschung und Praxis allgemein akzeptiert. Dabei sind unterschiedlichste offene Dokumentenstandards wie ODF, OOXML, PDF oder ePub in die Überlegungen einzubeziehen. Es existieren bereits Analysen zur Verträglichkeit einzelner Standards. Diese Analysen sind unter Berücksichtigung aktueller Weiterentwicklungen in der Standardisierung, insbesondere in Bezug auf Zertifizierung und Speicherung/Archivierung zu aktualisieren. Dazu sind insbesondere die Arbeitsergebnisse in den zugehörigen ISO Gremien (ISO/IEC JTC 1 SC34, ISO TC 171 SC 2) verfolgt worden.

Ergänzend sind die Arbeitsergebnisse bezüglich der Zertifizierung und Langzeitarchivierung von Dokumenten aus internationalen und nationalen Gremien zusammengestellt. Dabei wird insbesondere auf die Unterschiede und Gemeinsamkeiten der verwendeten Dokumentenbegriffe eingegangen. Im Allgemeinen ist der hier verwendete Dokumentenbegriff erheblich weiter gefasst als in den ISO Gremien. Die allgemeinen rechtlichen und technischen Anforderungen sind in der Studie zusammengestellt und mit den heute bereits vorhandenen speziellen Lösungen bei offenen Dokumentenformaten verglichen worden. Aus dieser Gegenüberstellung sind Handlungsempfehlungen für die Verwendung offener Dokumentenformate zur konformen Archivierung abgeleitet und/oder Standardisierungspotentiale identifiziert worden.

Die politische Relevanz der Ergebnisse wird durch die Analyse der im Umfeld der Einführung der elektronischen Akte (E-Akte) in der Bundesverwaltung bzw. in Ländern und Kommunen vorhandenen Anforderungen bez. Signierung und Archivierung von Dokumenten hergestellt. Insbesondere die nachhaltige Zugreifbarkeit und Langzeitarchivierung sind Themen, die aktuell im Zusammenhang mit elektronischen Dokumenten im Rahmen der Verwaltungsmodernisierung und partizipativer Ansätze diskutiert werden. Der Stand der Diskussion ist unter besonderer Berücksichtigung fachlicher, sicherheitsbezogener und rechtlicher Anforderungen zusammengestellt, wobei Rahmenbedingungen wie DIN 31644/45/46 oder ISO 14721 (OAIS) berücksichtigt sind.

Inhalt

1 Einleitung

Entsprechend den strategischen Vorgaben der Politik müssen durch Forschungsaktivitäten verstärkt neue Modelle der Arbeitsorganisation entwickelt werden, die ein hohes Maß an Partizipation sicherstellen. Im Verwaltungsbereich muss das Ziel der Bundesregierung, eine medienbruchfreie ebenenübergreifende Verwaltung zu etablieren, umgesetzt werden. Das Projekt untersucht dazu, in welchem Umfang und unter welchen Voraussetzungen digitale Dokumente in der Kommunikation zwischen Verwaltung, Unternehmen und Bürgern auf portable Art und Weise erstellt, ausgetauscht und nachhaltig im Rahmen gesetzlicher Vorgaben archiviert und bei Bedarf weiterverarbeitet werden können.

Der weitere Ausbau des E-Government-Angebots des Bundes soll bewirken, dass die Verwaltung erforderliche Informationen durchgängig bereitstellen und Verfahren intern wie extern medienbruchfrei mit offenen Standards durchgängig elektronisch bearbeiten kann. Die vorliegende Studie untersucht dazu einerseits die Anforderungen an Bearbeitungssperren, Signaturen, Speicherung, Austausch und nachhaltige Archivierung elektronischer Dokumente unter Berücksichtigung zugehöriger Mechanismen offener Dokumentenformate wie ODF, OOXML, PDF oder EPUB unter Einbeziehung relevanter struktureller und darstellungsbezogener Dokumenteneigenschaften. Dabei werden existierende Vorarbeiten bez. der Möglichkeiten und Grenzen der Interoperabilität von ODF und OOXML berücksichtigt. Andererseits werden die Bestrebungen der Bundesregierung in Bezug auf die Etablierung der elektronischen Akte und der dort verwendete Dokumentenbegriff betrachtet. Ergänzend untersucht die Studie nationale und internationale Aktivitäten zur nachhaltigen Archivierung von Dokumenten wie OAIS (Open Archival Information System), Arbeitsergebnisse des Kompetenznetzwerks zur Langzeitarchivierung (nestors), sowie Arbeiten von DIN und BSI zur Zertifizierung und Archivierung von Dokumenten und setzt diese Aktivitäten zu den Ansätzen im Bereich offener Dokumentenformate in Beziehung.

Die durchgeführten Arbeiten haben ergeben, dass eine strikte Trennung zwischen der Analyse offener Dokumentenformate einerseits und technischen bzw. rechtlichen Vorgaben in Bezug auf Signierung, Archivierung und Langzeitarchivierung andererseits erforderlich ist. Insbesondere ist der Unterschied zwischen Speicherung/Archivierung und Langzeitspeicherung/-archivierung im Kontext der deutschen Verwaltung als wichtig anzusehen. Archivierung ist die langzeitige, sichere, unveränderbare, vollständige, nachvollziehbare, authentische, integre, beweisfähige und jederzeit verfügbare Aufbewahrung von Dokumenten. Dies betrifft alle Dokumente, die aufbewahrungspflichtig oder aufbewahrungswürdig sind. Archivierung im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung und bezieht sich

darauf, dass Unterlagen einer Behörde, sobald sie für die Zwecke der Behörde nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vgl. §§ 1 und 2 BArchG[1]). In Langzeitarchive der öffentlichen Hand kommen Dokumente aus der öffentlichen Verwaltung demnach erst dann, wenn Bearbeitung und Aufbewahrungspflichten abgeschlossen sind. Der 2009 aufgekommenen Begriff „Langzeitarchivierung" wird in Initiativen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des DIN verwendet. Danach soll es eine vertrauenswürdige elektronische Langzeitspeicherung nur für elektronisch signierte Dokumente mit Nachsignieren zum Erhalt der Beweisfähigkeit geben. Die Langzeitspeicherung wird mit bis zu 100 Jahren definiert und gilt als Vorstufe zur vertrauenswürdigen elektronischen Langzeitarchivierung.
In Bezug auf die vorliegende Themenstellung ist daher untersucht worden, wie weit offene Dokumentenformate und ihre Speicherformate den genannten Anforderungen an Archivierung genügen und ob Unterstützung für Nachsignieren vorhanden ist. Ergänzend wurde geprüft, ob die vorhandenen Konzepte zur Archivierung von „elektronischen, digitalen Unterlagen" so allgemein sind, dass sie die Archivierung offener Dokumentenformate ermöglichen, ohne spezielle Anforderungen an deren Speicherformat zu stellen. Dafür ergibt sich dann jedoch die Notwendigkeit sicherzustellen, dass auch in „bis zu 100 Jahren" Software vorhanden ist, die nachhaltig eine Prüfung und Interpretation/Darstellung der digitalen Dokumente ermöglicht.

[1] Verordnung zur elektronischen Signatur (Bundesministeriums der Justiz und für Verbraucherschutz, 2013)

2 Zielsetzung

Die Studie stellt standardisierungsrelevante Anforderungen an digitale Dokumente zusammen, die deren nachhaltige und gesetzeskonforme Verwendung in elektronischen, medienbruchfreien Verwaltungsprozessen ermöglichen. Die Ergebnisse können sowohl in die internationale Standardisierung offener Dokumentenformate als in nationale Empfehlungen einfließen. Die Verfolgung zugehöriger Standardisierungsaktivitäten, insbesondere in ISO/IEC SC34 stellt einen Schwerpunkt der Arbeiten dar.
Ziel des Projektes ist es daher, die dokumentenbezogenen Voraussetzungen für eine nachhaltige Umsetzung der politisch angestrebten, medienbruchfreien Kommunikation zwischen Bürgerinnen und Bürgern, Unternehmen und Verwaltungen zusammenzustellen und somit ein hohes Maß an Partizipation zu ermöglichen. Dazu sind eine Analyse und Gegenüberstellung der verwendeten Dokumentenbegriffe, der Zertifizierungstechniken und Anforderungen sowie der Archivierungsbegriffe erforderlich.

2.1 Lösungsansatz

Die Notwendigkeit zur Definition eines übertragbaren **Dokumentenbegriffs** als Voraussetzung für die Erstellung und Archivierung portabler Dokumente sowie die Implementierung interoperabler Büroanwendungen ist aus Sicht von Forschung und Praxis allgemein akzeptiert. Dabei sind unterschiedlichste offene Dokumentenstandards wie ODF, OOXML, PDF oder EPUB in die Überlegungen einzubeziehen. Es existieren bereits Analysen zur Verträglichkeit einzelner Standards. Diese Analysen sind unter Berücksichtigung aktueller Weiterentwicklungen in der Standardisierung, insbesondere in Bezug auf Zertifizierung und Speicherung/Archivierung zu aktualisieren. Dazu sind insbesondere die Arbeitsergebnisse in den zugehörigen ISO Gremien (ISO/IEC JTC 1 SC34, ISO TC 171 SC 2) verfolgt worden.
Ergänzend sind die Arbeitsergebnisse bezüglich der **Zertifizierung und Langzeitarchivierung** von Dokumenten aus internationalen und nationalen Gremien zusammengestellt. Dabei wird insbesondere auf die Unterschiede und Gemeinsamkeiten der verwendeten Dokumentenbegriffe eingegangen. Im Allgemeinen ist der hier verwendete Dokumentenbegriff erheblich weiter gefasst als in den ISO Gremien. Die allgemeinen rechtlichen und technischen Anforderungen sind in einer Anforderungsspezifikation zusammengestellt und mit den heute bereits vorhandenen speziellen Lösungen bei offenen Dokumentenformaten verglichen. Aus dieser Gegenüberstellung sind Handlungsempfehlungen für die Verwendung offener Dokumentenformate zur konformen Archivierung abgeleitet und/oder Standardisierungspotentiale identifiziert worden, sofern Standards und Anforderungen zu weit auseinander liegen.

Die politische Relevanz der Ergebnisse wird durch die Analyse der im Umfeld der Einführung der **elektronischen Akte** in der Bundesverwaltung bzw. in Ländern und Kommunen vorhandenen Anforderungen bez. Signierung und Archivierung von Dokumenten hergestellt. Insbesondere die nachhaltige Zugreifbarkeit und Langzeitarchivierung sind Themen, die aktuell im Zusammenhang mit elektronischen Dokumenten im Rahmen der Verwaltungsmodernisierung und partizipativer Ansätze diskutiert werden. Der Stand der Diskussion ist unter besonderer Berücksichtigung fachlicher, sicherheitsbezogener und rechtlicher Anforderungen zusammengestellt, wobei Rahmenbedingungen wie DIN 31644/45/46 oder ISO 14721 (OAIS) berücksichtigt sind.

2.2 Betrachtete Standards und Dokumente

Für die Studie wurden die im Folgenden gelisteten Dokumente betrachtet:
Offene Dokumentenstandards:

- ISO/IEC 26300:2006 Open Document Format inkl. COR 1, COR 2 und AMD 1
- ISO/IEC FDIS 29500 (Ed 3) Information technology - Document description and processing languages - Office Open XML File Formats - Part 1-4
- ISO/IEC TS 30135-4:2014, Digital Publishing - EPUB 3 - Part 4: Open Container Format
- ISO/IEC CD 21320-1.2, Document Container File -- Part 1: Core
- ISO 32000-1 Document management -- Portable document format -- Part 1: PDF 1.7
- ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)
- ISO 19005-3:2012 Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)

Regelungen zur Dokumentenarchivierung

- ISO 14721:2012, Reference Model For An Open Archival Information System (OAIS-V2) entsprechend Consultative Committee for Space Data Systems: OAIS - Recommended Practice, 2012
- BSI Technische Richtlinie TR-03125 - Beweiswerterhaltung kryptographisch signierter Dokumente mit Anlagen TR-ESOR, vgl. auch (BSI - Bundesamt für Sicherheit in der Informationstechnik, 2009)

- Projektergebnisse ArchiSig und ArchiSafe (vgl. Anlage TR-VELS -M.1/.3: ArchiSig-Modul zu TR 03125) sowie Profil für ArchiSafe-konforme Middleware[2]
- DIN 31664 - Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive
- DIN 31665 - Information und Dokumentation - Leitfaden zur Informationsübernahme in digitale Langzeitarchive
- DIN 31666 Information und Dokumentation - Anforderungen an die langfristige Handhabung persistenter Identifikatoren

Regelungen zur elektronischen Akte

- BMI – Organisationskonzept elektronische Verwaltungsarbeit - Baustein E-Akte
- BMI – Organisationskonzept elektronische Verwaltungsarbeit - Baustein E-Langzeitspeicherung
- Bundesgesetzblatt Jahrgang 2013 Teil I Nr. 43: Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften
- BMI, BMWi, BMV: Digitale Agenda 2014-2017, August 2014
- BMI: Regierungsprogramm Digitale Verwaltung 2020, September 2014

[2] Common Criteria Protection Profile for an ArchiSafe Compliant Middleware (BSI - Bundesamt für Sicherheit in der Informationstechnik, 2008)

3 Politischer und gesetzlicher Rahmen

3.1 Regierungsprogramm Digitale Verwaltung 2020

Der Eckpunkt Nr. 5 des Regierungsprogrammes „Digitale Verwaltung 2020"[3] besagt: „Mit dem Programm Digitale Verwaltung 2020 soll die Umsetzung des E-Government-Gesetzes (EGov)[4] im Bund ressortübergreifend koordiniert werden. Eine wichtige Maßnahme ist dabei, die Einführung der elektronischen Aktenführung in der Bundesverwaltung im Rahmen eines ressort-übergreifenden Aktionsplans E-Akte zu unterstützen. Der Aktionsplan E-Akte soll die organisatorischen und fachlichen Aspekte sowie technische Angebote aber auch Vorschläge für Maßnahmen zum Kulturwandel hin zu einer noch bürgernäheren und effizienteren digitalen Verwaltung bündeln. Für die Umsetzung der E-Akte sollen im Rahmen des Programms „Gemeinsame IT des Bundes" wichtige technische Grundlagen erarbeitet werden."
Nach dem E-Government-Gesetz sind Bundesbehörden ab 2020 verpflichtet, ihre Akten elektronisch zu führen. Die elektronische Aktenführung wird als unerlässlich angesehen, um in der digitalen Verwaltung die Nachvollziehbarkeit des Verwaltungshandelns und insbesondere die rechtssichere und gesetzeskonforme Dokumentation der Entscheidungsprozesse weiterhin zu gewährleisten. Die elektronische Akte muss dazu den kompletten Lebenszyklus der elektronischen Informationen berücksichtigen und den Bearbeitungszusammenhang vom Antrag über alle Beteiligungs- und Abstimmungsverfahren bis zur Langzeitspeicherung abbilden.

3.2 Organisationskonzept Elektronische Verwaltungsarbeit

Im Baustein E-Akte[5] werden der Begriff der Akte und die rechtlichen Anforderungen an die Langzeitspeicherung zusammengestellt. Eine E-Akte besteht danach aus der eigentlichen „Akte" als dem formalen Rahmen der enthaltenen Vorgänge und Dokumente. Ein Vorgang ist die kleinste Sammlung von zusammengehörenden Dokumenten aus der Bearbeitung eines Geschäftsvorgangs. Unter Dokumenten werden papiergebundene oder elektronisch erstellte Objekte wie Fax, E-Mail, Datenbankauszüge und andere Dateien, einschließlich aller ergänzenden Angaben wie Metadaten, die zum Verständnis der Informationen notwendig sind, verstanden. Sie bilden die kleinste logische Einheit eines Vorgangs und können aus einem oder mehreren Einzelobjekten

[3] Digitale Verwaltung 2020 (Bundesregierung, 2014)
[4] E-Government Gesetz (Bundesregierung, 2013)
[5] Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Akte (Bundesregierung, 2013)

wie Schriftstücken, PDF- oder Office-Dateien und Bildern bestehen. Im Kontext dieser Studie ist daher der Begriff des „Objekts" relevant.

ABBILDUNG 1: DER DOKUMENTENBEGRIFF IM KONTEXT DER E-AKTE NACH [5]

Bezüglich der Umsetzung von Formvorschriften bei der elektronischen Aktenführung wird auf die Verwendung qualifizierter elektronischer Signaturen verwiesen. Elektronische Dokumente, die einem Schriftformerfordernis, d.h. der eigenhändigen Unterschrift, unterliegen, müssen mit einer qualifizierten elektronischen Signatur versehen werden. Sofern eine dauerhafte Überprüfbarkeit der elektronischen Signatur gefordert wird, ist die Anbringung einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung notwendig. Das Signaturgesetz bildet den zugehörigen rechtlichen Rahmen. Rein rechtlich gilt für qualifiziert elektronisch signierte Dokumente die Vermutung der Echtheit. Sie sind privaten Urkunden gleichgestellt.
Im Organisationskonzept „Elektronische Verwaltungsarbeit" werden im Baustein E-Langzeitspeicherung[6] die Begrifflichkeiten um die Archivierung von Dokumenten definiert. Der Begriff der „Archivierung" bezeichnet dabei die dauerhafte und unveränderbare Aufbewahrung und Erhaltung von Unterlagen durch Archive *nach* Ablauf der Aufbewahrungsfrist, die den Zeitraum bezeichnet, in dem die aktenführende Stelle das Schriftgut nach Abschluss der Bearbeitung für einen möglichen Rückgriff auf dieses Schriftgut für Verwaltungszwecke aufbewahrt. Die Aufbewahrung und Erhaltung von

[6] Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Langzeitspeicherung (Bundesregierung, 2014)

elektronischen Dokumenten während der Aufbewahrungsfrist wird als „Langzeitspeicherung" bezeichnet.

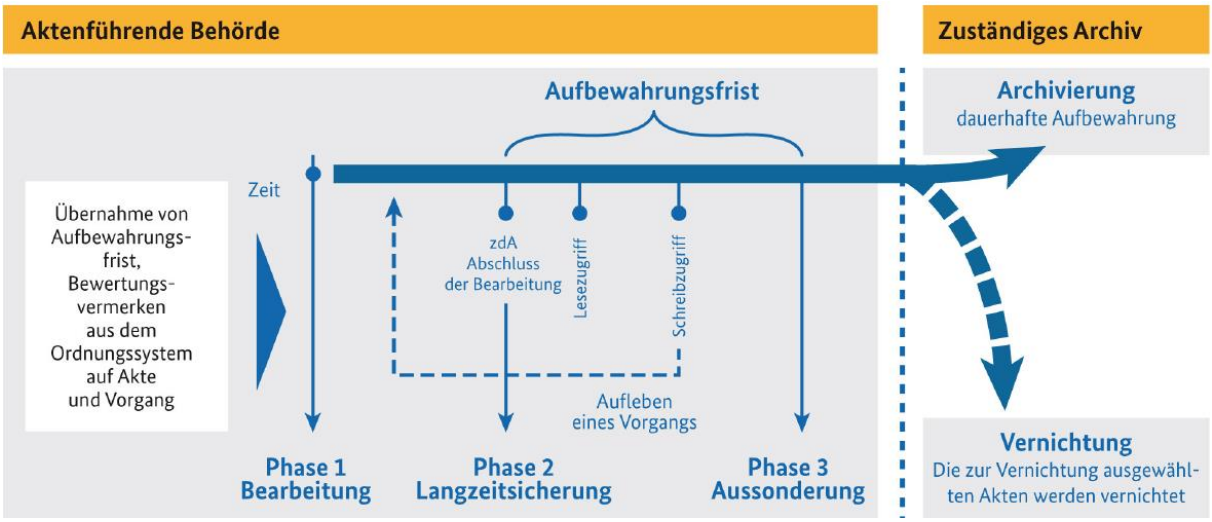


ABBILDUNG 2: LEBENSZYKLUS EINER ELEKTRONISCHEN AKTE NACH[6]

Während der Langzeitspeicherung bleiben die elektronischen Unterlagen in der Verantwortung der Behörde, die die Datenhoheit besitzt. Zur Sicherstellung der Beweissicherheit muss diese sich an Standards und geltenden Normen orientieren. Dazu gehören nach[5] die bereits erwähnten:

- TR-03125 des BSI zur beweiswerterhaltenden Langzeitspeicherung in der jeweils geltenden Fassung
- ArchiSafe, ArchiSig, TransiDoc (rechtssichere Transformation signierter Dokumente)
- Open Archival Information System zum grundlegenden Aufbau eines Langzeitspeichers (ISO-14721)
- ISO-15489 mit Leitlinien zur Verwaltung von Schriftgut von öffentlichen und privaten Organisationen
- ISO-19005 für PDF/A als Standarddateiformat für Dokumentformate

Der Baustein E-Langzeitspeicherung[6] ergänzt diese Liste um

- Prüfkriterien für Dokumentenmanagementlösungen (PK-DML)
- XDOMEA[7]

[7] XDomea - IT-gestützter Austausch und IT-gestützte Aussonderung behördlichen Schriftgutes (KoSIT - Koordinierungsstelle für IT-Standards, 2011)

Die Auswahl langzeitspeicherfähiger Formate wird trotz der Empfehlung von PDF/A nicht explizit eingeschränkt. Es wird geraten, Empfehlungen des zuständigen Archivs und anderer Einrichtungen wie dem BSI zu berücksichtigen. Entsprechend den Festlegungen können die notwendigen technischen Vorkehrungen, wie die Beschaffung und Bereitstellung von Konvertierungssoftware, getroffen werden.

3.2.1 Bewertung

In Bezug auf die Ermittlung von Anforderungen an offene Dokumentenformate ergibt sich aus dem Umfeld der elektronischen Aktenführung die Notwendigkeit, Dokumente qualifiziert elektronisch signieren zu können. Dies ist jedoch eine Anforderung an die, beispielsweise zur Nutzung eines Signatur-Zertifikats auf dem neuen Personalausweis, erforderliche IT-Infrastruktur und keine Frage des Dokumentenstandards.

3.3 Signaturgesetz und Signaturverordnung

Signaturgesetz[8] und Signaturverordnung[9] regeln in ihren Paragraphen § 17 SigV i. V. m. §6 Abs. 1 Satz 2 SigG (vergleiche dazu Kapitel 4.1.2.2) den Beweiswerterhalt von qualifiziert elektronisch signierten Dokumenten. Wenn die Behörde die signierten Dokumente für längere Zeit in signierter Form benötigt, ist sie verpflichtet, neue Signaturen anzubringen (Übersignierung), bevor die aktuell verwendeten Signaturen als kryptografisch nicht mehr sicher gelten. Inwieweit der Erhalt des Beweiswertes von qualifiziert elektronisch signierten Dokumenten auch über eine längere Zeit erforderlich ist, als durch die aktuell verwendete elektronische Signatur gewährleistet, liegt dabei im Entscheidungsermessen der jeweiligen Behörde.

[8] Gesetz über Rahmenbedingungen für elektronische Signaturen (Bundesregierung, 2001)
[9] Verordnung zur elektronischen Signatur (Bundesministeriums der Justiz und für Verbraucherschutz, 2013)

4 Bestandsaufnahme

4.1 Rahmenwerke

4.1.1 OAIS

Das von der ISO als ISO 14721 publizierte „Open Archival Information System-OAIS[10]" gilt als das international anerkannte Rahmenwerk für die Archivierung von Dokumenten. Es entspricht dem vom „Consultative Committee for Space Data Systems-CCSDS" veröffentlichte Dokument „Recommended Practice"[11] und liegt auch in deutscher Übersetzung vor[12]. Das 2003 veröffentlichte und 2012 aktualisierte OAIS-Referenzmodell ISO 14721 stellt eine fachliche Grundlage für die Langzeitspeicherung und Archivierung dar. Es ist ein organisatorisches Modell für den Aufbau von elektronischen Systemen zur Langzeitspeicherung und Archivierung.
Das OAIS-Referenzmodell beschreibt die notwendigen Prozesse und Informationspakete zur langfristigen oder dauerhaften Aufbewahrung von elektronischen Dokumenten. Nach OAIS aufgebaute Systeme bestehen aus kommunizierenden Prozessen. Die Archivinformationspakte (Archival Information Package, AIP) enthalten neben den Primärdaten alle zur Interpretation, Lesbarkeit, Nutzbarkeit, Verständlichkeit und Recherche notwendigen Informationen, beweisrelevante Nachweise der Integrität und Authentizität der aufzubewahrenden Unterlagen in standardisierter und herstellerunabhängiger Form:

- Metainformationen
- Inhalts-/Primärinformationen
- Beweisrelevante Daten
- Technische Beweisdaten

[10] ISO 14721 Open archival information system (OAIS) -- Reference model (ISO, 2012)
[11] Reference Model for an Open Archival Information System (OAIS) - Recommended Practice (CCSDS - Consultative Committee for Space Data Systems, 2012)
[12] Referenzsystem für ein Offenes Archiv-Informationssystem (nestor, 2012)

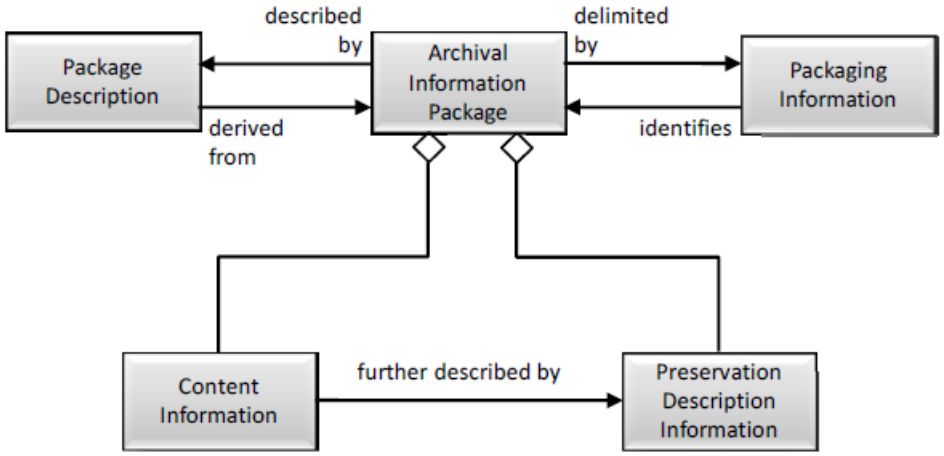


ABBILDUNG 3: ARCHIVAL INFORMATION PACKAGE AIP NACH OAIS[10]

Das OAIS-Referenzmodell wurde grundsätzlich für End-Archive konzipiert, die ihr Archivgut dauerhaft aufbewahren. Sein modularer Aufbau ermöglicht eine authentische Wahrung und Reproduzierbarkeit des Archivguts. Für den Bereich der Langzeitspeicherung sind die Ausführungen zur Erhaltung der Beweiskraft, der Lesbarkeit sowie der Verfügbarkeit der elektronischen Objekte wesentlich. Insbesondere das Modul „Bestanderhaltung" (Preservation) gewährleistet die Les- und Nutzbarkeit, Unverfälschbarkeit, Vollständigkeit sowie die Sicherheit vor Verlust.
OAIS definiert keinen spezifischen Dokumentenbegriff. Vielmehr spricht OAIS von Datenobjekten, wobei digitale Datenobjekte als Bit-Stream definiert sind:

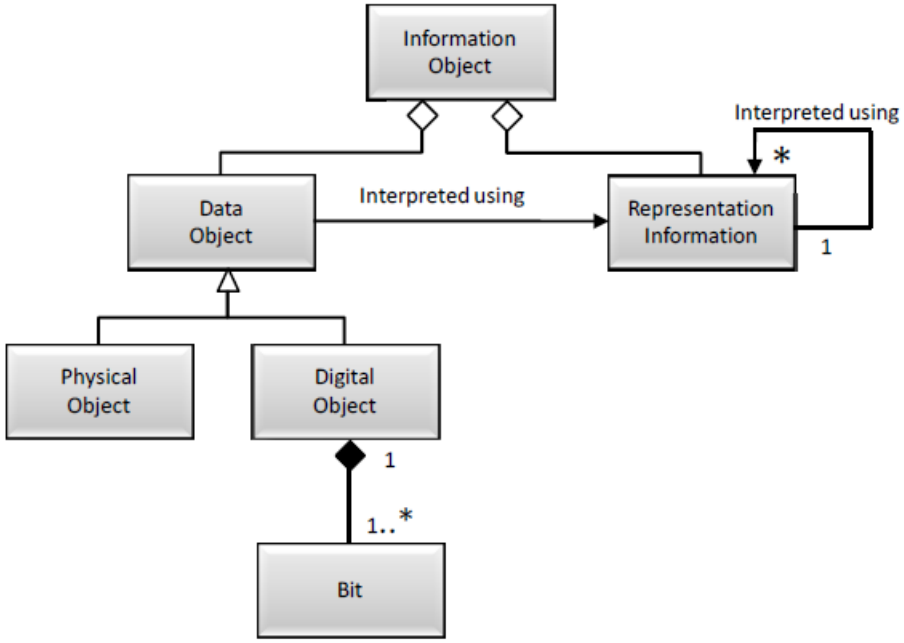


ABBILDUNG 4: INFORMATIONSOBJEKTE NACH OAIS[10]

Datenobjekte selber besitzen eine Repräsentation, d.h. eine in formalisierter Weise rückinterpretierbare Darstellung von Information, die zur Kommunikation, Interpretation oder Verarbeitung geeignet ist. Beispiele für Daten sind eine Bitsequenz, eine Zahlentabelle oder die die Buchstaben auf einer Seite.
Für spezielle Inhalte, sogenannte „Digital Library Collections", wird die „Fixity" (Beständigkeit), d.h. die Sicherstellung des unveränderten Originalzustands des Inhalts, durch digitale Signaturen, Prüfsummen und Authentitätsindikatoren sichergestellt. „Fixity Information" definiert neben Informationen über Referenzen, Kontext, Geschichte/Herkunft und Zugriffsrechte die sogenannte „Preservation Description Information" (Erhaltungsmetadaten).

4.1.1.1 Bewertung

OAIS arbeitet mit unterschiedlichen Informationspaketen, durch die Inhaltsdaten und Metadaten streng separiert werden. Signaturen sind daher kein Bestandteil der Nutzdaten sondern Bestandteil der Metadaten, so dass keine Anforderungen an die Formate der gespeicherten, digitalen Daten ableitbar sind.

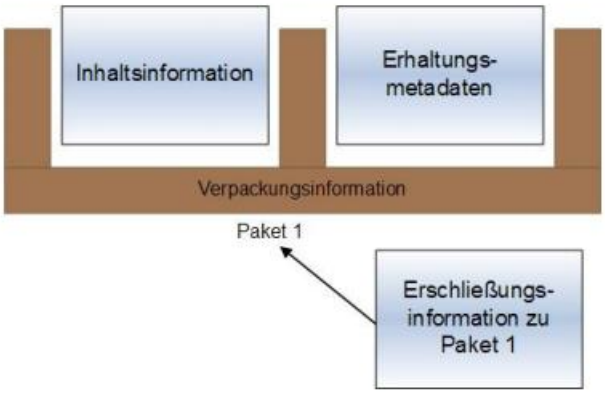


ABBILDUNG 5: INFORMATIONSPAKETE IN OAIS NACH[12]

4.1.2 BSI TR-03125 – TR-ESOR

Die vom BSI herausgegebene Technische Richtlinie BSI-TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente"[13] beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume, d.h. bis zum Ende der Aufbewahrungsfristen, im Sinne eines rechtswirksamen Beweiswerterhalts, d.h. der Wahrung der Authentizität und Integrität kryptografisch signierter Dokumente, vertrauenswürdig gespeichert werden können. Ausgehend von Anforderungen an die ordnungsgemäße Aufbewahrung elektronisch signierter Dokumente definiert die TR-03125 eine Referenz-Architektur für

[13] BSI Technische Richtlinie 03125 - Vertrauenswürdige elektronische Langzeitspeicherung (BSI - Bundesamt für Sicherheit in der Informationstechnik, 2009)

eine Middleware zum rechtswirksamen Beweiswerterhalt kryptographisch signierter Dokumente, während des gesetzlich vorgeschriebenen Aufbewahrungszeitraums, insbesondere für Dokumente mit qualifizierten elektronischen Signaturen nach § 17 SigV[14].

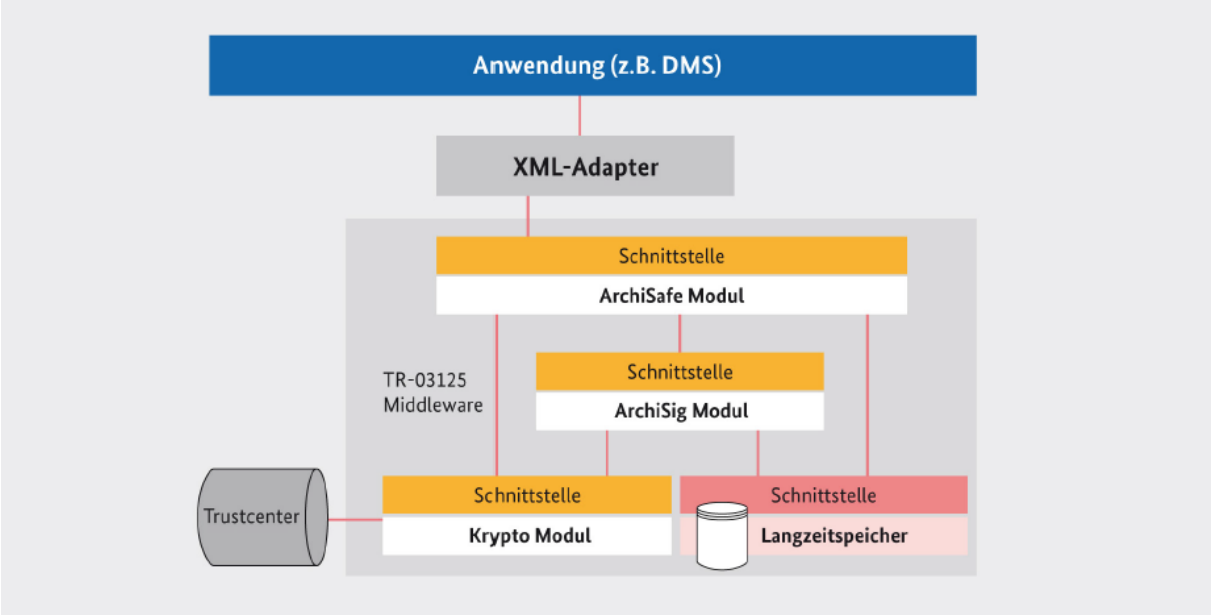


ABBILDUNG 6: REFERENZARCHITEKTUR DER TR-03125 NACH[6]

Die Richtlinie empfiehlt darüber hinaus den Einsatz offener, interoperabler und standardisierter Datenformate und herstellerunabhängiger Schnittstellen, entsprechend nationalen und internationalen Standards: „Im Interesse der dauerhaften Verfügbarkeit und Verkehrsfähigkeit der zu archivierenden Dokumente und Daten sollen ausschließlich Datenformate eingesetzt werden, die eine plattform- und herstellerunabhängige Archivierung in langfristig verkehrsfähiger Form ermöglichen". In der Anlage TR-ESOR B, die die Profilierung für Bundesbehörden regelt, wird mit Hinweis auf § 18 RegR diese Aussage verschärft, indem *sollen* durch *müssen* ersetzt wird.
In der Anlage TR-ESOR F (Formate und Protokolle)[15] werden im Kapitel 4.2.1 „Schriftgut" als im Jahr 2011 unterstützte Formate aufgeführt:

- ASCII Text
    - Einfache, unformatierte Texte mit ausschließlich lateinischen Schriftzeichen sollen den im ISO Standard ISO 646:1991 (ASCII) definierten Zeichensatz verwenden.

[14] Verordnung zur elektronischen Signatur (Bundesministeriums der Justiz und für Verbraucherschutz, 2013)
[15] BSI Technische Richtlinie 03125 Anlage TR-ESOR-F: Formate und Protokolle (BSI - Bundesamt für Sicherheit in der Informationstechnik, 2011)

- Dokumente (Textdateien) mit nicht ausschließlich lateinischen Schriftzeichen sollen die aktuelle Version des Unicode Standards verwenden. Unicode ist funktional äquivalent zum Standard ISO 10646-1:2000. Unicode konforme Texte werden grundsätzlich in UTF-8 oder UTF-16 kodiert.

- PDF/A
  - Für sämtliche, vorwiegend zeichenorientierte, statischen Dokumente soll der Standard ISO 19005-1 (PDF/A-1)[16] mit den im Dokument beschriebenen Einschränkungen verwendet werden. Bez. Authentizität und Integrität wird die Verwendung kryptographischer Verfahren zum Nachweis der Authentizität und Integrität einer PDF-Datei empfohlen. Dabei sollen jedoch ausschließlich Signaturanwendungskomponenten zum Einsatz kommen, die durch das BSI als sichere Signaturanwendungskomponenten im Sinne des SigG evaluiert und zertifiziert wurden. Werden Signaturen im Dokument eingebettet, so gilt die mit PDF 1.3 eingeführte und an PKCS#7 angelehnte Containerstruktur.
- ODF
  - Für sämtliche, vorwiegend zeichenorientierte Dokumente soll OpenDocument v1.0, entsprechend ISO/IEC 26300:200617, eingesetzt werden.

An dieser Stelle erkennt man, dass sich die TR auf den Diskussionstand und den Stand der Technik im Jahr 2010 bezieht, wie er sich zu diesem Zeitpunkt auch in SAGA 4.0[18] als Meta-Standard von BMI und BSI widerspiegelt. Zum heutigen Zeitpunkt müsste man zumindest auf die in SAGA 5.0[19] aufgeführten Dokumentenstandards verweisen, selbst wenn diese bereits ebenfalls überholt sind. Man vergleiche dazu die Beschreibung aktueller Dokumentenstandards in Kapitel 4.2.3.

4.1.2.1 ArchiSafe und ArchiSig Module

In der Anlage TR-ESOR-M.1:ArchiSafe werden die Schnittstellen des Archivierungssystems beschrieben. Ziel und Zweck des ArchiSafe-Moduls ist die Realisierung einer einheitlichen Schnittstelle derjenigen Archiv-Funktionen, die für den Beweiswerterhalt eine Rolle spielen. Das Modul entkoppelt logisch und funktional den Datenfluss zwischen den IT-

[16] Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)(ISO/IEC, 2005)
[17] Open Document Format for Office Applications (ISO/IEC JTC 1/SC34, 2006)
[18] Standards und Architekturen für E-Government-Anwendungen SAGA 4.0 (Bundesminister des Inneren, 2008)
[19] SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0 (Beauftragte der Bundesregierung für Informationstechnik, 2011)

Fachanwendungen und dem Langzeitspeicher zur Ablage oder zum Aufruf archivierter Daten und Dokumente. Darüber hinaus bietet das Modul einheitliche Schnittstellen zur Kommunikation mit kryptographischen Komponenten. Bezüglich unterstützter Datenformate referenziert ArchiSafe auf die bereits erwähnte Anlage TR-ESOR F.
In der Anlage TR-ESOR-M.3:ArchiSig werden die Mechanismen zum Erhalt der Authentizität über den Nachweis der Integrität und damit des beweisrechtlichen Werts vor allem elektronisch signierter Daten und Dokumente durch zusätzliche kryptographische Sicherungsmittel beschrieben. Das ArchiSig-Modul implementiert dazu eine kryptographische Lösung nach RFC4998[20], die insbesondere sicherstellt, dass das durch § 17 SigV skizzierte Verfahren zur Aufrechterhaltung der Sicherheit und Vertrauenswürdigkeit elektronischer Signaturen durch eine erneute Signatur zuverlässig umgesetzt werden kann. Die erneute elektronische Signatur muss dazu die Daten und frühere Signaturen einschließen. Der dabei verwendete, initiale Archivzeitstempel muss, um den Anforderungen des § 17 Satz 3 SigV zu genügen, eine qualifizierte elektronische Signatur enthalten. Da es sich hierbei aber um keine Willenserklärung, sondern nur um ein Sicherungsmittel vorhandener Willenserklärungen handelt, muss die im Zeitstempel enthaltene Signatur auch keine persönliche Signatur, also weder die des ursprünglich Erklärenden noch die eines Archivars) sein. Für eine erneute elektronische Signatur nach § 17 Satz 3 SigV aller durch den initialen Archivzeitstempel geschützten Dokumente und Daten genügt deshalb die alleinige Erneuerung (Übersignatur) des Archivzeitstempels. Eine so definierte Übersignatur impliziert keine Anforderungen an das Datenformat der archivierten Dokumente.
Die ArchiSafe zugrunde gelegte Datenstruktur, das „Submission Data Object", wird im „Common Criteria Protection Profile[2]" beschrieben als schemakonformes XML-Datenpaket, bestehend aus Datenblöcken für Metadaten und Content sowie optionalem Zeitstempel und Signatur. Die Trennung von Inhalt und Signatur macht deutlich, dass sich auch aus der Definition des Profils keine direkten Anforderungen an das Format der Daten ableiten lassen.

[20] RFC 4998 Evidence Record Syntax (IETF, 2007)

ABBILDUNG 7: SUBMISSION DATA OBJECT NACH[2]

4.1.2.2 Bewertung

Die Richtlinie TR-03125 verweist im Wesentlichen auf kryptographisch signierte Dokumente, wobei auf aus heutiger Sicht veraltete Versionen offener Dokumentenstandards referenziert wird. Rein rechtlich wird auf die Bestimmungen des SigV, insbesondere auf §17 verwiesen: „Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes (<<Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird>>) neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen. Anstelle einer neuen qualifizierten elektronischen Signatur nach Satz 2 kann ein qualifizierter Zeitstempel aufgebracht werden, wenn dieser selbst eine qualifizierte elektronische Signatur trägt." Es ist daher nur in Bezug auf die Beibehaltung des erforderlichen Sicherheitswerts zu prüfen, inwieweit aktuelle Dokumentenformate eine Neusignierung entsprechend SigG und SigV erlauben.

4.1.3 NESTOR

Im deutschen Kompetenznetzwerk zur digitalen Langzeitarchivierung nestor arbeiten Bibliotheken, Archive, und Museen zum Thema Langzeitarchivierung und Langzeitverfügbarkeit digitaler Quellen. Aus nestor-Arbeitsgruppen sind drei Normungsprojekte[21] hervorgegangen, die im DIN-Arbeitsausschuss „Schriftgutverwaltung und Langzeitverfügbarkeit digitaler Informationsobjekte (NABD 15)" innerhalb des DIN-

[21] Standards im Bereich digitale Langzeitarchivierung (nestor, 2011-2013)

Normenausschuss „Bibliotheks- und Dokumentationswesen (NABD)" als nationale Normen veröffentlicht sind:

- DIN 31644 (April 2012) basiert auf dem Kriterienkatalog vertrauenswürdiger digitaler Langzeitarchive, Version II[22]
- DIN 31645 (November 2011) basiert auf dem Leitfaden für die Informationsübernahme in das digitale Langzeitarchiv[23]
- DIN 31646 (Januar 2013) basiert auf dem Kriterienkatalog zur Überprüfung der Vertrauenswürdigkeit von Persistent Identifier-Systemen[24]

Das digitale Langzeitarchiv spezifiziert alle objektbezogenen Anforderungen für den Umgang mit digitalen Objekten entsprechend den Hauptphasen des OAIS-Referenzmodells. Für die hier betrachteten Dokumentenformate ergeben sich keine neuen Anforderungen. Durch nestor selber sind die Entwürfe der DIN-Normen sowie die deutsche Übersetzung des OAIS-Referenzmodells publiziert worden.

4.1.4 DIN

Im DIN sind im Zusammenhang mit der Archivierung von Dokumenten die bereits erwähnten Normen DIN 31644/45/46, basierend auf Vorarbeiten aus nestor, veröffentlicht worden.

4.1.4.1 DIN 31644

DIN 31644 beschreibt in allgemeiner Form die notwendigen Rahmenbedingungen für den Aufbau und Betrieb eines vertrauenswürdigen digitalen Langzeitarchivs. Sie legt dazu Kriterien fest, die die Bewertung der Vertrauenswürdigkeit eines digitalen Langzeitarchivs sowohl in organisatorischer als auch in technischer Hinsicht ermöglichen. Begrifflich bezieht sich die Norm auf die in OAIS festgelegten Entitäten wie Archivpaket, digitale Daten, Metadaten oder Repräsentation. Ein digitales Langzeitarchiv spezifiziert Anforderungen für den Umgang mit Informationsobjekten und deren Repräsentationen auf allen Stufen der Verarbeitung im Archiv. Dabei sind Integrität und Authentizität der zu erhaltenden Informationen Kernkonzepte der Vertrauenswürdigkeit. Um aus den Repräsentationen der Datenobjekte nutzbare Information zu rekonstruieren und um die Forderungen nach Integrität, Authentizität und rechtmäßiger Nutzung der Information zu erfüllen, unterstützt das digitale Langzeitarchiv ein auf Metadaten basierendes

[22] DIN 31644: Kriterien für vertrauenswürdige digitale Langzeitarchive (DIN, 2012)
[23] DIN 31645: Leitfaden zur Informationsübernahme in digitale Langzeitarchive (DIN, 2011)
[24] DIN 31646: Anforderungen an die langfristige Handhabung persistenter Identifikatoren (DIN, 2013)

Datenmanagement. Es besitzt nach OAIS eine Schnittstelle für die integritätssichernde Aufnahme der Repräsentationen. Die Schnittstelle beinhaltet all Funktionen und Prozesse, die die Übernahme der Transferpakete, deren Transformation in Archivpakete und die Aufnahme ins digitale Langzeitarchiv gewährleisten.
Die Archivablage beinhaltet diejenigen Funktionen, die für die Überprüfung und den Erhalt der Integrität der Repräsentationen erforderlich sind. Diese umfassen die Abbildung der Archivpakete auf Speichermedien, die langfristige Speicherung, die Wiederherstellung der Archivpakete sowie alle Änderungen an den Archivpaketen. Das digitale Langzeitarchiv unterstützt ferner Verfahren zur Beurteilung der Authentizität der Repräsentationen bei der Aufnahme, zur Beurteilung und Sicherung der Authentizität der Transferpakete, zur Sicherstellung der Authentizität von Objekten bei Langzeiterhaltungsmaßnahmen sowie bei deren Transformation zu Nutzungspaketen.
Das Archiv verwendet intern Kennungen zur Verwaltung der Informationsobjekte und ihrer Repräsentationen sowie gegebenenfalls deren Teile und Beziehungen, insbesondere zur eindeutigen Zuordnung der Inhaltsdaten zu den Metadaten.
Bezüglich unterstützter Datenformate wird im Zusammenhang mit elektronischen Akten darauf hingewiesen, dass entsprechend dem DOMEA-Konzept die einzelnen Dokumente nicht im ursprünglichen Format sondern im PDF/A-Format gespeichert werden. Dadurch bleibt die Möglichkeit einer Volltextrecherche und einer Extraktion der Zeichen erhalten. Für unformatierte Texte werden ASCII/Unicode, für formatierte Texte PDF/A (ISO 19005-1: 2005) als Archivdateiformate empfohlen.

4.1.4.2 DIN 31645

DIN 31645 umfasst Anleitungen und Standards für die Informationsübernahme in digitale Langzeitarchive sowie Anforderungen an den Produzenten bzw. Lieferanten der zu bewahrenden Daten. Der dabei verwendete Datenbegriff leitet sich aus der DIN 31644 ab.
Um Informationsobjekte in digitaler Form über lange Zeiträume verfügbar zu halten, müssen die Repräsentationen in wechselnden technischen Umgebungen dargestellt werden. Sowohl bei einer auf Emulation als auch bei einer auf Migration basierenden Erhaltungsstrategie werden sich die Formate der Daten zwangsläufig ändern. Als signifikante Eigenschaften werden diejenigen Eigenschaften bezeichnet, die zu jeder Zeit in allen aktuellen und zukünftigen Umgebungen bei der Darstellung erhalten bleiben sollen. Dazu müssen Archiv oder Lieferant entscheiden, welche Eigenschaften als signifikant anzusehen sind. Die Norm geht also von der Möglichkeit zur Anpassung des Formats archivierter Daten zur Gewährleistung ihrer Erhaltung aus.
Bei den verwendeten Transferpaketen, d.h. der Zusammenführung von Informationsdaten und Metadaten, kann es sich sowohl um Containerformate wie ZIP oder TAR handeln, als

auch um reine Beschreibungsdateien, die die zu transferierenden Daten und Metadaten nur referenzieren und dadurch für das Archiv verfügbar machen. Bezüglich des Formats der zu archivierenden Daten werden keine expliziten Vorgaben gemacht: „Aus den beim Produzenten vorhandenen Informationen müssen die Informationsobjekte ausgewählt werden, welche als Archivgut dauerhaft, authentisch und sicher übernommen werden sollen. Diese Auswahl erfolgt nach bestimmten Bewertungskriterien, die sich aus dem gesetzlichen oder vertraglich festgelegten Auftrag eines digitalen Langzeitarchivs ergeben."

4.1.4.3 DIN 31646

DIN 31646 beschäftigt sich mit der Prüfung der Vertrauenswürdigkeit von Persistent Identifier-Systemen. „Persistent Identifier" ermöglichen es, über lange Zeiträume und nicht genau vorhersehbare Veränderungen hinweg, digitale Objekte identifizierbar, referenzierbar und verfügbar zu halten. Von Interesse ist der dabei verwendete Begriff der „Identität" von Objekten. Objekte werden als identisch angesehen, wenn sie in ihren wesentlichen Merkmalen übereinstimmen. Welche Merkmale wesentlich sind, hängt vom Zweck bzw. vom Kontext ab. Für die Zwecke der inhaltlichen Informationsarbeit lassen sich beispielsweise die MS-Word-Version und die PDF-Version eines Dokumentes als identisch ansehen. Für den Zweck der Darstellung auf einem Bildschirm sind sie dagegen nicht identisch, da sie in der Regel unterschiedliche Software zu ihrer Interpretation benötigen.
Auch DIN 31646 bezieht sich in ihrer Begrifflichkeit auf OAIS und nimmt somit explizit keinen Bezug auf existierende Dokumentenformate. Die verwendete Definition des Begriffs „Identität" kann sogar bewirken, dass Dokumente nach einer Transformation in ein anderes Datenformat ihre Identität beibehalten.

4.1.4.4 Bewertung

Die betrachteten DIN-Normen verwenden einen sehr allgemeinen, an OAIS angelehnten Dokumentenbegriff. Als einziges für die Archivierung relevantes Dokumentenformat wird PDF/A erwähnt, andere Formate werden jedoch nicht explizit ausgeschlossen. Durch die OAIS-bedingte Trennung von Informationsdaten und Metadaten lassen sich keine expliziten Anforderungen an das Format der Informationsdaten ableiten. Archivierungs- und sicherheitsrelevante Informationen werden auf Paketebene innerhalb der Metadaten behandelt.

4.2 Dokumentenformate und Archivierung

Der in diesem „Dokument" diskutierte Begriff des „Dokuments" ist nicht eindeutig definiert. Im Kontext der im ISO/IEC SC34 definierten Dokumentenstandards werden

Bürodokumente von Typen wie Text, Präsentation oder Tabellenkalkulation betrachtet. Im Vordergrund stehen Erstellung und Speicherung der Bürodokumente. Bei PDF-Dokumenten wird weitestgehend die Speicherung und Darstellung dieser Bürodokumente betrachtet, darüber hinaus werden auch ganz allgemein Veröffentlichungen einbezogen. EBUB konzentriert sich auf die interoperable Darstellung von Veröffentlichungen mittels dedizierter Hardware und Software unter besonderer Berücksichtigung von DRM-Aspekten. Diesen Ansätzen ist gemein, dass Dokumente selbstbeschreibende Entitäten sind. Im Umfeld der E-Akte und OAIS sind Dokumente dagegen eher „Content" oder eine nicht näher betrachtete Menge von Bits. Beschreibende Metadaten und ergänzende Informationen werden zusätzlich in umfassenden Akten oder Containern erfasst und bereitgestellt. Da bei der Archivierung keine starken Annahmen über den betrachteten „Content" gemacht werden, wird von der Selbstbeschreibung innerhalb der betrachteten Dokumente kein Gebrauch gemacht. Vielmehr werden vergleichbare Informationen auf Ebene der umfassenden Objekte auf standardisierte Art und Weise bereitgestellt. Die dabei verwendeten Standards korrespondieren ihrerseits mit den innerhalb der Dokumente verwendeten Standards.

Im Folgenden werden, unabhängig vom betrachteten Dokumentenbegriff, wichtige Faktoren diskutiert, die sich auf die Nachhaltigkeit der Dokumentenarchivierung auswirken und sowohl in Dokumentenstandards als auch in Archivierungsstandards betrachtet werden müssen. Dabei wird die Archivierung digitaler Dokumente nicht primär im rechtlichen Sinne betrachtet sondern im Sinne einer langfristigen Speicherung und Interpretierbarkeit. Die Diskussion orientiert sich weitgehend an Thesen der US-amerikanischen „Library of Congress" zum Thema „Sustainability of Digital Formats"[25]

4.2.1 Faktoren für die Nachhaltigkeit der Dokumentenarchivierung

Mit der nachhaltigen Archivierung von Dokumenten wird die Fähigkeit verbunden, auch nachfolgenden Generationen einen möglichst authentischen Eindruck der archivierten Dokumente vermitteln zu können. Diese Fähigkeit hängt von einer Reihe von Faktoren ab, die im Folgenden beschrieben werden. Die Faktoren sind weitestgehend unabhängig vom Typ des Dokuments bzw. des Dokumenteninhalts. Sie erlauben eine Abschätzung, inwieweit technische Entwicklungen die Interpretation der Dokumente in der Zukunft beeinflussen, welcher Migrationsaufwand für eine sinnerhaltende, technische Migration und Speicherung erforderlich ist bzw. welcher Aufwand für die Beibehaltung oder Emulation heutiger technischer Infrastrukturen notwendig ist.

[25] Sustainability of Digital Formats (Library of Congress)

4.2.1.1 Nachweis der Authentizität - Identität

Die Bewahrung des Inhalts eines Dokuments in einem bestimmten digitalen Format ist auf lange Sicht ist nur möglich, wenn das digitale Speicherformat offengelegt und bekannt ist. Diese Forderung ist bei der Verwendung von offenen Standards, wie sie im vorliegenden Fall betrachtet werden, weitestgehend gegeben. Eine bitweise Identität von Dokumenten ist jedoch nicht erforderlich, um von einer authentischen Interpretation zu sprechen. So können der visuelle Eindruck der pdf und odf-Repräsentationen eines Dokuments durchaus identisch sein, ohne dass die Dokumente auf bitebene gleich sind. Für die Migration zwischen verschiedenen Dokumentenformaten ist in jedem Einzelfall zu definieren, wie der Begriff der Identität kontextspezifisch zu fassen ist und wie identische Abbildungen durchgeführt und dokumentiert werden können.

4.2.1.2 Verbreitungsgrad

Die Speicherung von Dokumenten in verbreiteten, möglichst offenen Formaten erhöht die Wahrscheinlichkeit einer späteren, authentischen Interpretation deutlich. Werkzeuge zur Interpretation, Validierung und Migration der Dokumente haben bei offenen Formaten voraussichtlich eine längere Lebensdauer. Ein hoher Verbreitungsgrad erhöht auch die Wahrscheinlichkeit einer langfristigen Existenz der zu Interpretation erforderlichen Infrastruktur (Werkzeuge, Betriebssystem, Rechnerarchitektur) bzw. einer Existenz abwärts-kompatibler Infrastrukturen.

4.2.1.3 Erkennbarkeit und Transparenz

Textuelle Dokumente besitzen, bei Verwendung standardisierter Kodierungen, eine hohe Lesbarkeit und Wiedererkennbarkeit. Sie können in der Regel mit Texteditoren dargestellt werden. Je komplexer der Inhalt eines Dokuments ist, desto höher werden die Anforderungen an interpretierende Werkzeuge. Es ist daher darauf zu achten, dass auch bei der Archivierung komplexer Inhalte diese entsprechend internationalen Standards kodiert und gespeichert sind.
Die Transparenz eines Dokuments wird erhöht, wenn sein Inhalt einschließlich beschreibender Metadaten strukturiert in Standard-Zeichensatz-Kodierungen wie UNICODE UTF-8 kodiert und gespeichert wird. So ist beispielsweise für die Erhaltung von Software-Programmen Quellcode wesentlich transparenter als kompilierten Code. Andererseits ist die Programmausführung auf Basis von kompiliertem Code leichter als die auf Basis von Quellcode.
Digitale Dokumente werden häufig verschlüsselt oder komprimiert. Verschlüsselung ist nicht kompatibel mit Transparenz, Komprimierung hemmt zumindest Transparenz. Trotzdem werden digitale Audios, Bilder und Videos aus praktischen Gründen selten in nicht-komprimierter Form gespeichert werden. Daher müssen wiederum Werkzeuge zur

Entschlüsselung und Dekomprimierung bereitgehalten werden. In welchem Umfang Authentizität (verlustfreie Wiedergabe) und Komprimierungstechniken zusammenhängen, ist wiederum im Einzelfall zu prüfen.

4.2.1.4 Selbstbeschreibung

Die Anreicherung von Dokumenteninhalten durch Metadaten wird verwendet, um Informationen über Struktur, Inhalte, Erstellungshistorie, eingebettete Inhalte, Berechtigungen, Signaturen usw. bereitzustellen. Metainformationen sind in der Regel ein nicht sichtbarer Bestandteil des Dokuments, können jedoch durch zugehörige Werkzeuge interpretiert und zur Bearbeitung des Dokuments verwendet werden. Je umfangreicher die Beschreibung eines Dokuments durch Metadaten und inkludierte Inhalte ist, desto besser ist seine spätere Interpretierbarkeit. Man denke hier beispielsweise an die Einbettung von Textfonts in Bürodokumente.
Wie bereits erwähnt, verwenden die beschriebenen Archivierungsformate ebenfalls das Konzept selbstbeschreibender Metadaten, um den Lebenszyklus, die Integrität und Zugriffsberechtigungen auf Dokumente nachhaltig zu beschreiben und zu speichern.

4.2.1.5 Abhängigkeiten

Externe Abhängigkeiten zu IT-Infrastrukturen sind bereits im Zusammenhang mit dem Verbreitungsgrad der verwendeten Dokumentenstandards diskutiert worden. Neben diesen offensichtlichen Abhängigkeiten existieren beispielsweise für Bürodokumente noch Abhängigkeiten zu Textfonts, Wörterbüchern, Bibliotheken, zu referenzierten externen Dateien wie lokalen oder entfernten Datenbanken oder zu eingebetteten Dateien. Bei der Archivierung von Dokumenten wird somit in der Regel nicht nur das Dokument selber zu betrachten sein sondern auch der gesamte, für eine spätere Interpretation erforderliche Kontext. Hier bietet sich die Nutzung der Archivierungsstandards an, da diese ein allgemeines, über das eigentliche Dokument hinausgehendes Verständnis von „zu archivierendem Inhalt" besitzen. Für die authentische Interpretation des Dokuments ist es dann jedoch erforderlich, die bei der Erstellung verwendete Umgebungskonfiguration wieder herzustellen. Diese muss dann durch zugehörige Metadaten nachvollziehbar beschrieben worden sein.

4.2.1.6 Patente

Die Verwendung von Patenten zur Kodierung und Speicherung von Dokumenten kann langfristig ein Hindernis für deren nachhaltige Interpretation darstellen. Werden für die Interpretation eines Dokuments kostenpflichtige, zeitlich begrenzte Lizenzen benötigt, so ist eine langfristige Archivierung zwar möglich, nicht jedoch eine authentische

Interpretation. Hier sind bereits bei der Archivierung rechtliche bzw. mittels Umkodierung technische Maßnahmen zu treffen, die die Nachhaltigkeit gewährleisten.

4.2.1.7 Technische Schutzmechanismen

Durch technische Maßnahmen implementierte Abhängigkeiten zu physikalischer Hardware, Zugriffsbeschränkungen durch Kennworte oder Ablauffristen schränken die Nachhaltigkeit von Archivierung und Interpretation ein. Derlei Abhängigkeiten sind im Einzelfall zu vermeiden, werden jedoch durch die betrachteten Dokumenten- und Archivierungsformate auch nicht erwartet.

4.2.2 Ausgewählte Dokumentenformate (Tabelle)

Dokumentenformate

Kurzform	Langform	Standardisierung	XML-basiert?	Container	Archivierungsfunktionen		
					Datenintegrität	Signatur	Verschlüsselung
OOXML	Open Office XML	ISO/IEC FDIS 29500 (Ed 3) Information technology - Document description and pro-cessing languages - Office Open XML File Formats - Part 1-4	✓	✓	✓	✓	✓
ODF	Open Document Format	ISO/IEC 26300:2006 Open Document Format inkl. COR 1, COR 2 und AMD 1	✓	✓	✓	✓	✓
PDF PDF 1.7	Portable Document Format	ISO 32000-1 Document management -- Portable document format -- Part 1: PDF 1.7			✓	✓	✓
PDF/A-2		ISO 19005-2:2011 Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)					
PDF/A-3		ISO 19005-3:2012 Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)					
EPUB_2	Electronic Publication Version 2	ISO/IEC DTS 30135-4, Digital Publishing - EPUB 3 -	✓	✓	✓	✓	✓

		Part 4: Open Container Format, vgl. auch http://idpf.org/EPUB					
EPUB_3	Electronic Publication Version 3	ISO/IEC DTS 30135-4, Digital Publishing - EPUB 3 - Part 4: Open Container Format, vgl. auch http://idpf.org/EPUB	✓	✓	✓	✓	✓
Containerformate							
ZIP	(Document Container File)	ISO/IEC CD 21320-1.2, Document Container File -- Part 1: Core		✓	✓	✓	✓
Meta-Standards							
OAIS	Reference Model	ISO 14721, Reference Model For An Open Archival Information System (OAIS-V2)		✓	✓	✓	✓
eAkte		BMI - Organisationskonzept elektronische Verwaltungsarbeit - Baustein E-Akte		✓	✓	✓	✓

4.2.3 Ausgewählte Dokumentenformate

Die Einführung offener Dokumentenstandards stellt eine Grundvoraussetzung für eine interoperable Bearbeitung von Dokumenten durch unterschiedliche Anwendungen dar. Eine herausragende Bedeutung besitzen dabei die von der "International Standardisation Organisation" (ISO) standardisierten Formate "Portable Document Format" (PDF), "OpenDocument Format" (ODF) und "Office Open XML" (OOXML). Aber auch Formate wie „electronic publication" (EPUB) oder die die "XML Paper Specification" (XPS) werden zunehmend an Bedeutung gewinnen. An dieser Stelle werden die genannten Standards in Bezug auf die angebotene Unterstützung für Signierung und Archivierung untersucht.

4.2.4 OOXML

4.2.4.1 Hintergrund

Microsoft veröffentlichte 2006 die „Open Specification Promise (OSP)" [26] und publizierte im gleichen Jahr das Format der der Microsoft Office Suite (Version 12), für die Microsoft XML als Datenaustausch- und Speicherformat benutzt, als Open Office XML. Der zugehörige Standard ist in vier Teile gegliedert, von denen jeder einzelne normatives sowie informelles Material enthält:

1. **Fundamentals and Markup Language Reference**

   Teil 1 des ISO 29500 Standards[27] enthält die Definitionen für die strikte Konformität (strict conformance) sowie die Definitionen der speziellen Markup-Sprachen WordprocessingML, SpreadsheetML, PresentationML, DrawingML, Shared MLs und Custom XML Schemata. Teil 1 definiert alle Elemente und Attribute, einschließlich der Elementhierarchie (Eltern/Kind Verhältnis). Die strikte Konformität wird von Microsoft erst mit Office 2013 unterstützt, so dass erst vergleichsweise wenige Dokumente existieren.

2. **Open Packaging Conventions**

   Teil 2 des ISO 29500 Standard[28] umfasst die Beschreibung der Paketierung von OOXML-Dokumenten, die sogenannten „Open Packaging Conventions" (package model, physical package) sowie die „Core Properties", „Thumbnails" und digitale Signaturen. Dieser Teil ist insbesondere im Zusammenhang mit der Archivierung von Dokumenten wichtig. Eine Office Open XML Datei ist im Grunde ein

[26] Microsoft Open Specification Promise (Microsoft, 2006)
[27] Office Open XML File Formats - Part 1: Fundamentals and Markup Language Reference (ISO/IEC JTC 1/SC34, 2008)
[28] Office Open XML File Formats - Part 2: Open Packaging Convention (ISO/IEC JTC 1/SC34, 2008)

komprimiertes ZIP Paket, welches hauptsächlich XML-basierte Dateien enthält. Die Struktur des ZIP-Containers wird von der „Open Packaging Convention (OPC)" definiert, die eine Abstraktionsschicht zwischen der physischen Datei/der Verzeichnisstruktur innerhalb der ZIP Datei und der Dokumentenstruktur ist. Im von OPC beschriebenen Konzept beinhalten die „Parts" (Teile) Daten, während die „Relationships" (Beziehungen) die jeweiligen Teile verbinden.
An der Wurzel steht der sogenannte Content Type Stream, welcher sowohl den Typ des Gesamtdokuments als auch den Typ der Inhalte der einzelnen Teile identifiziert. Die Wurzelbeziehung bestimmt den Ort des Hauptdokuments in der ZIP Datei. Je nach Dokumententyp und Inhalt des Dokuments wird der Hauptteil über Beziehungen mit weiteren Teilen und/oder externen Dokumenten verbunden.

3. **Markup Compatibility and Extensibility**

   Teil 3 des ISO29500 Standards[29] definiert, wie Element und Attribute von Folgeversionen oder Erweiterungen von Office Open XML eingebracht werden müssen. Es beschreibt Erweiterungen der Dokumentensyntax mittels eines Konzepts, das die Interoperabilität einer Basis-Version (eine Version ohne Erweiterungen) von OOXML-Dokumenten sicherstellt.

4. **Transitional Migration Features**

   Teil 4 des ISO29500 Standards[30] enthält Definitionen zur Beschreibung des Übergangs existierender Office-Dokumente auf den XML-basierten Standard, die sogenannte „Transitional Conformance". Er definiert Funktionen für die Abwärts-Kompatibilität, die eine nahtlose Migration bestehender binärer Microsoft Office Dokumente ermöglichen. Die meisten derzeit existierenden OOXML-Dokumente genügen dieser Spezifikation.

Der Standard spezifiziert 6 Stufen an Dokumenten- und Anwendungs-Konformität, „strict" und „transitional" für jeweils WordprocessingML, PresentationML und SpreadsheetML, jeweils gemeinsam mit entsprechenden Schema-Definitionen. „Transitional Conformance" ermöglicht die Kompatibilität mit älteren Office Dokumenten. „Strict Conformance" begrenzt die Anzahl an XML Attributen auf den im Teil 1 definierten Kern des Standards. Office 2010 erzeugt „transitional" konforme Dokumente, Office 2013 auch strikt konforme Dokumente.

[29] Office Open XML File Formats - Part 3: Markup Compatibility and Extensibility (ISO/IEC JTC 1/SC34, 2008)
[30] Office Open XML File Formats - Part 4: Transitional Migration Features (ISO/IEC JTC 1/SC34, 2008)

4.2.4.2 Versionsgeschichte

Office Open XML (ISO/IEC 29500:2008/2011) ist ein offenes, XML-basiertes Dokumentenformat zum Speichern und Austauschen von Textdokumenten, Tabellenkalkulationen und Präsentationen.
Office Open XML wurde erstmals im Dezember 2006 von der „ECMA International General Assembly" als ECMA-376 Standard anerkannt. Eine überarbeitete Version wurde im November 2008 von der ISO (ISO/IEC 29500:2008) herausgegeben. Die korrespondierende Version ECMA-376 2nd Edition wurde im Dezember 2008 veröffentlicht. Die Überarbeitungen von OOXML in der ISO wurden im Laufe des Jahres 2011 als ISO/IEC 29500:2011 bzw. von der ECMA als ECMA-376 3rd Edition und mit editoriellen Anpassungen 2012 als ECMA-376 4th Edition verabschiedet. Aktuell arbeitet die ISO an Korrigenden zur 2012-er Version.

4.2.4.3 Signaturen

Die Verwendung von Signaturen in OOXML wird im Teil 2 des Standards (OPC) beschrieben.

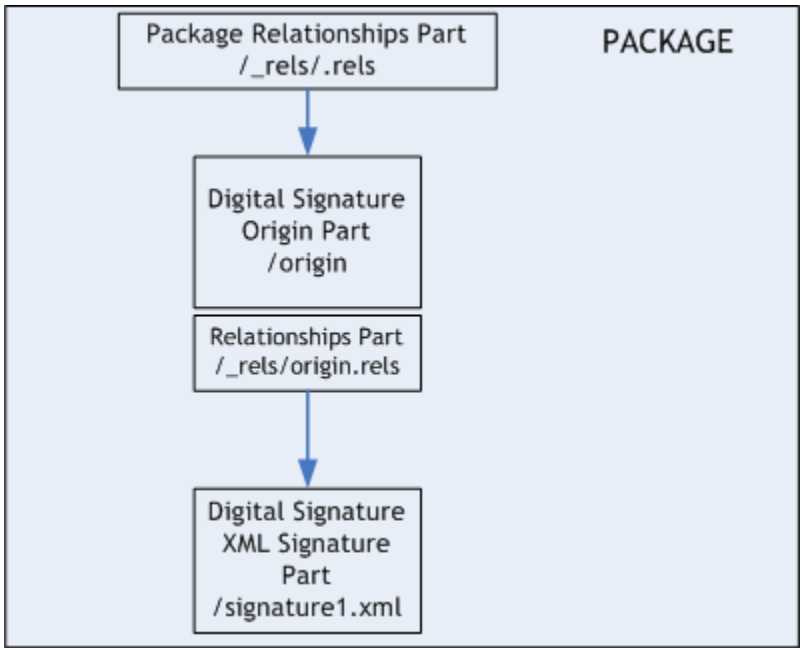
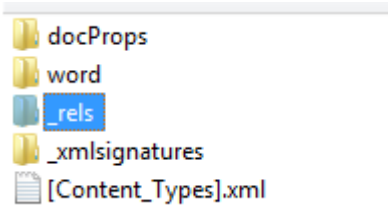


ABBILDUNG 8: DIGITALE SIGNATUREN IN OPC[28]

Über mehrere Indirektionen in dem umfassenden Dokument wird auf die zugehörige Signatur verwiesen:

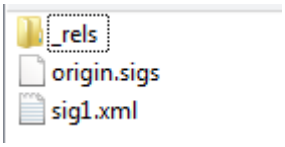
- Dokumentenebene



- Verzeichnis der Relationen im Dokument mit beschreibender XML-Datei

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/core-properties"
Target="docProps/core.xml"/><Relationship Id="rId2"
Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/thumbnail"
Target="docProps/thumbnail.emf"/><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/officeDocument"
Target="word/document.xml"/><Relationship Id="rId5"
Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/origin"
Target="_xmlsignatures/origin.sigs"/><Relationship Id="rId4"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/extended-properties"
Target="docProps/app.xml"/></Relationships>
```

- Verzeichnis der Signaturdateien



- Referenzierte Signaturen

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId1"
        Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/signature"
        Target="sig1.xml"/>
</Relationships>
```

- XML-Datei mit Signatur (auszugsweise)

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Reference URI="#idPackageObject"
Type="http://www.w3.org/2000/09/xmldsig#Object">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>Jh9cOyPkykPhY93gscOVXnmSwg8=</DigestValue>
        </Reference>
        <Reference URI="#idOfficeObject"
Type="http://www.w3.org/2000/09/xmldsig#Object">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
            <DigestValue>5aVJoq6N/a5nSUTd/l4wNm2VyTg=</DigestValue>
        </Reference>
        <Reference URI="#idSignedProperties"
Type="http://uri.etsi.org/01903#SignedProperties">
            <Transforms>
                <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>/SNlIkm+RGH0PYa/Dv7FjBJ8UVk=</DigestValue>
        </Reference>
    </SignedInfo>

<SignatureValue>VPvHqUsnirYm0gSsj9Jo+lyqOStyf1lTNbYdUN7B1uL/yRmCdfemNaJ/NRrE0
BDY9/GbWYxgxw4I
  ...
    </SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509Certificate>...
            </X509Certificate>
        </X509Data>
    </KeyInfo>
    <Object Id="idPackageObject"
        xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature">
        <Manifest>
            <Reference
                URI="/word/styles.xml?ContentType=application/vnd.openxmlformats-
officedocument.wordprocessingml.styles+xml">
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>HayulZ7KakNAr2ploVc9apQLJ+Y=</DigestValue>
            </Reference>
            <Reference
                URI="/word/stylesWithEffects.xml?ContentType=application/vnd.ms-
word.stylesWithEffects+xml">
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>/FWjfWA90br34tLhbVNpCc7JLDA=</DigestValue>
            </Reference>
  ...
        </Manifest>
        <SignatureProperties>
            <SignatureProperty Id="idSignatureTime" Target="#idPackageSignature">
                <mdssi:SignatureTime>
```

```
                <mdssi:Format>YYYY-MM-DDThh:mm:ssTZD</mdssi:Format>
                <mdssi:Value>2011-11-22T11:52:55Z</mdssi:Value>
            </mdssi:SignatureTime>
        </SignatureProperty>
    </SignatureProperties>
</Object>
<Object Id="idOfficeObject">
    <SignatureProperties>
        <SignatureProperty Id="idOfficeV1Details" Target="idPackageSignature">
            <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
                <SetupID/>
                <SignatureText/>
                <SignatureImage/>
                <SignatureComments>Interop-Test</SignatureComments>
                <WindowsVersion>6.0</WindowsVersion>
                <OfficeVersion>14.0</OfficeVersion>
                <ApplicationVersion>14.0</ApplicationVersion>
                <Monitors>1</Monitors>
                <HorizontalResolution>1920</HorizontalResolution>
                <VerticalResolution>1200</VerticalResolution>
                <ColorDepth>16</ColorDepth>
                <SignatureProviderId>{00000000-0000-0000-0000-
000000000000}</SignatureProviderId>
                <SignatureProviderUrl/>
                <SignatureProviderDetails>9</SignatureProviderDetails>

<ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ManifestHashAlgorit
hm>
                <SignatureType>1</SignatureType>
            </SignatureInfoV1>
        </SignatureProperty>
    </SignatureProperties>
</Object>
<Object>
    <xd:QualifyingProperties Target="#idPackageSignature"
        xmlns:xd="http://uri.etsi.org/01903/v1.3.2#">
        <xd:SignedProperties Id="idSignedProperties">
            <xd:SignedSignatureProperties>
                <xd:SigningTime>2011-11-22T11:52:55Z</xd:SigningTime>
                <xd:SigningCertificate>
                    <xd:Cert>
                        <xd:CertDigest>
                            <DigestMethod
```

```
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <DigestValue>UpUYvw6XZ3IivzLhyx1PdTD0KaM=</DigestValue>
                    </xd:CertDigest>
                    <xd:IssuerSerial>
                        <X509IssuerName>CN=Fraunhofer User CA 2007, OU=Fraunhofer
Corporate
                            PKI, O=Fraunhofer, C=DE</X509IssuerName>

<X509SerialNumber>131426527779645332404811</X509SerialNumber>
                    </xd:IssuerSerial>
                </xd:Cert>
            </xd:SigningCertificate>
            <xd:SignaturePolicyIdentifier>
                <xd:SignaturePolicyImplied/>
            </xd:SignaturePolicyIdentifier>
        </xd:SignedSignatureProperties>
    </xd:SignedProperties>
    <xd:UnsignedProperties/>
</xd:QualifyingProperties>
</Object>
</Signature>
```

Das verwendete Verfahren orientiert sich an der W3C Empfehlung zur Signierung von XML-Dateien[31], die den relevanten Rahmen für die Signierung von OOXML-Dokumenten darstellt. Nach OPC können das gesamte Dokument oder aber einzelne Teile des Dokuments signiert werden. Ausgehend vom „Digital Signature Origin Part" werden die mittels Relationen referenzierten und signierten Teile des Dokuments identifiziert. Sofern ein „Digital SignatureCertificate Part" vorhanden ist, enthält dieser ein X.509 Zertifikat zur Verifikation der Signatur.

Ergänzend zur genannten W3C-Spezifikation beschreibt OPC in seinem Kapitel 13.2.4 die Verwendung der XML-Reference-Elemente zur Identifikation der signierten Teile des Dokuments. Die für 2016 geplante Neufassung des OPC ermöglicht die Nutzung von XAdES[32] (W3C: Long term digital signature, entsprechend ETSI: TS 101 903[33]) und soll die Interoperabilität unterschiedlicher OPC-Implementierungen erhöhen.[34] Zudem wird die Verwendbarkeit von OPC in anderen Containerformaten angestrebt.

In dem oben dargestellten Beispiel erkennt man die potentielle Flexibilität des im Standard definierten Verfahrens. In welchem Umfang diese Flexibilität genutzt wird, hängt

[31] XML Signature Syntax and Processing (W3C, 2013)
[32] XML Advanced Electronic Signatures (W3C, 2003)
[33] XML Advanced Electronic Signatures (ETSI - European Telecommunications Standards Institute, 2009)
[34] Die XAdES Spezifikation wird derzeit von ETSI überarbeitet. Mit der Verabschiedung ist im Laufe des Jahres 2015 zu rechnen (ETSI - European Telecommunications Standards Institute, 2015).

jedoch von den verwendeten Werkzeugen zur Erstellung bzw. Interpretation des Dokuments ab.

4.2.5 ODF

4.2.5.1 Hintergrund

OpenDocument wurde ursprünglich ab 2000 von Sun Microsystems als XML-basiertes Speicherformat für StarOffice und OpenOffice entwickelt. Die originale Sun Spezifikation für das „Open Document Format", von OASIS 2005 als OASIS ODF 1.0 Standard übernommen, wurde zwischen 2000 und 2002 mit der folgenden Zielsetzung entwickelt:

> *"Gemeinschaftlich die führende internationale Office Suite für alle wichtigen Umgebungen zu erschaffen, die durch offene Schnittstellen und ein XML Dateiformat den Zugriff auf all seine Funktionen und Daten ermöglicht"* [35]

Die aktuelle Version 1.2 des Standards in drei Teile gegliedert: „Core" (Kern und Schemadefinitionen), „Formulas" (Formeln) und „Packages" (Pakete). Der dritte Teil beschreibt, wir ODF-Dokumente als ZIP-Datei strukturiert werde und ist für die Speicherung von Dokumenten von besonderer Bedeutung. Anders als Office Open XML, enthält ODF keine Abstraktionsschicht oberhalb der physikalischen Dateistruktur innerhalb des ZIP-Archivs; stattdessen werden feststehende Dateinamen für Dokumenteninhalt (content.xml), Stilinformation (styles.xml), Metainformation (meta.xml) und Anwendungseinstellungen (settings.xml) benutzt. Diese Dateien finden sich im Root Directory des Archivs. Das Manifest (manifest.xml) ist in dem Verzeichnis META-INF abgelegt.

4.2.5.2 Versionsgeschichte

Mit der Standardisierung wurde 2002 durch OASIS in der Arbeitsgruppe (Technical Committee TC) „OASIS Open Office XML Format TC" begonnen. Diese Gruppe wurde im Januar 2005 umbenannt in „OASIS Open Document Format for Office Applications TC". Im Mai 2005 wurde der Standard als „OASIS Open Document Format for Office Applications", abgekürzt „OpenDocument" oder ODF[36] veröffentlicht.
OASIS ODF 1.0 wurde von der ISO (ISO/IEC 26300:2006) im Dezember 2006 als internationaler Standard akzeptiert. ODF 1.1 wurde Anfang 2012 als Amendment zu

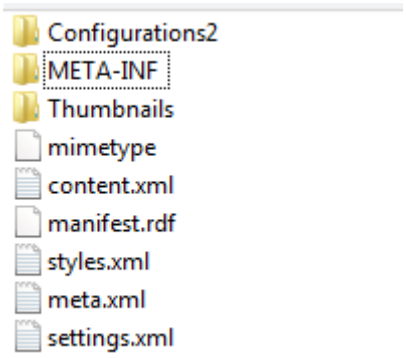
[35] OpenOffice.org announcement (OpenOffice, 2002)
[36] OpenDocument v1.0 Specification (OASIS - Organization for the Advancement of Structured Information Standards, 2005)

ISO/IEC von der ISO 26300:2006[37] verabschiedet. Im Januar 2012 wurde die aktuelle Version ODF 1.2[38] als OASIS Standard veröffentlicht. Im März 2014 wurde ODF1.2 bei der ISO als PAS-Submission eingereicht und wird voraussichtlich im Laufe des Jahres 2015 als dreiteiliger Standard ISO/IEC DIS 26300-1/2/3:2015 verabschiedet.

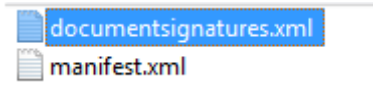
4.2.5.3 Signaturen

Die Verwendung von Signaturen in ODF wird in Teil 3 der ODF 1.2 Spezifikation[39] beschrieben. Sie referenziert, ebenso wie OOXML, auf die W3C Empfehlung zur Signierung von XML-Dateien[40] und verwendet in XAdES[32] spezifizierte Erweiterungen. Aufgrund der eher flachen Struktur der ODF-Pakete wird die die Signatur beinhaltene XML/Datei nicht referenziert sondern befindet sich direkt im Unterverzeichnis META/INF.

- Dokumentenstruktur auf der obersten Ebene. Die Signaturen befinden sich in META-INF



- Verzeichnis META-INF



- XML-Datei mit Signatur (auszugsweise)

```
<?xml version="1.0" encoding="UTF-8"?>
<document-signatures
xmlns="urn:oasis:names:tc:opendocument:xmlns:digitalsignature:1.0">
```

[37] Open Document Format for Office Applications (OpenDocument) v1.0 - Amendment 1 (ODF 1.1) (ISO/IEC JTC 1/SC34, 2012)
[38] Open Document Format for Office Applications: ODF 1.2 (OASIS - Organization for the Advancement of Structured Information Standards, 2012)
[39] Open Document Format for Office Applications (OpenDocument) Version 1.2 Part 3: Packages (OASIS - Organization for the Advancement of Structured Information Standards, 2011)
[40] XML Signature Syntax and Processing Version 2.0 (W3C, 2013)

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
Id="ID_005f0070009d009700f900e30044004600a70054001b00a2007d005600620043">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="Configurations2/accelerator/current.xml">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>2jmj7l5rSw0yVb/vlWAYkK/YBwk=</DigestValue>
      </Reference>
      <Reference URI="mimetype">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>kBA8vElORIEynUWPvr1bzZKG3hw=</DigestValue>
      </Reference><Reference URI="META-INF/manifest.xml">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>zRWyayt1oIkHpx8i5Ng9bm4EufE=</DigestValue>
      </Reference>
      <Reference URI="content.xml">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Rw2ONCNQ+DAffK0aNPvKlirvuRc=</DigestValue>
      </Reference>
      ...
  </SignedInfo>

<SignatureValue>cdrsavQyg4gBxXYqGsNBgFuJrU81J0t8RDElRIcTSqE1E/oJvST/CGzXWYOjzF
XM
  ...
  </SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>
          <X509IssuerName>CN=Fraunhofer User CA 2007, OU=Fraunhofer
Corporate PKI,                O=Fraunhofer, C=DE</X509IssuerName>
          <X509SerialNumber>131426901578414404155981</X509SerialNumber>
        </X509IssuerSerial>
```

```
                <X509Certificate>
                    ...
                </X509Certificate>
            </X509Data>
        </KeyInfo>
        <Object>
            <SignatureProperties>
                <SignatureProperty >
                    <dc:date xmlns:dc="http://purl.org/dc/elements/1.1/">2011-11-
22T12:51:53,71</dc:date>
                </SignatureProperty>
            </SignatureProperties>
        </Object>
    </Signature>
</document-signatures>
```

Erneut erkennt man die potentielle Flexibilität des im Standard definierten Verfahrens. In welchem Umfang diese Flexibilität genutzt wird, hängt jedoch wiederum von den verwendeten Werkzeugen zur Erstellung des Dokuments ab.

4.2.6 PDF

4.2.6.1 Hintergrund

Im Bereich der Langzeitspeicherung und Archivierung von Dokumenten müssen auch übermorgen die Dokumente von gestern bearbeitet oder zumindest gelesen werden können. Dazu bietet sich die Verwendung von PDF, genauer von PDF/A Dokumenten an. Mit dem auf der Version PDF 1.4 basierenden Standard PDF/A1 bzw. ISO/IEC 19005-1:2005[41] werden Anforderungen bezüglich einer nachhaltigen Bildschirm- und Druckausgabe festgelegt. PDF/A-1a wurde entworfen, um die Anforderungen bezüglich Barrierefreiheit zu erfüllen. PDF/A-1b behandelt die eindeutige visuelle Wiedergabe eines Dokuments. Die Standards PDF/A2 und /A3 stellen eine Überarbeitung von PDF/A1 auf Basis von PDF 1.7 (ISO/IEC 32000)[42] dar.

4.2.6.2 Versionsgeschichte

Das „Portable Document Format PDF" wurde 1991 durch Adobe veröffentlicht und bis zum Jahr 2000 zur Version 1.4 weiterentwickelt, die eine 128-bit-Verschlüsselung ermöglicht. Die nachfolgenden Versionen 1.5 bis 1.7 erlauben unter anderen die kennwortgeschützte Vergabe von Zugriffsberechtigungen und stärke

[41] ISO 19005-1:2005 Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)(ISO/IEC, 2005)
[42] ISO 32000-1:2008 Portable document format - Part 1: PDF 1.7 (ISO/IEC, 2008)

Verschlüsselungsmöglichkeiten. Ab der Version 1.3 werden die pdf-Spezifikationen auch als ISO-Standards ISO 15930 bzw. ISO 19005 veröffentlicht. Die angestrebte Version 2.0 oder ISO 32000-2 ist weiterhin in Vorbereitung. Mit PDF/A-1 wurde in 2005 ein Standard für die elektronische Archivierung veröffentlicht. Ziel von PDF/A-1 ist es, alle Informationen in die Datei einzubetten, die zu deren Interpretation erforderlich sind. Mit PDF/A-2 und PDF/A-3 wurden Erweiterungen auf Basis von PDF 1.7 definiert, die unter anderem die Möglichkeit bieten, Container mit Daten in pdf-Dokumente einzubetten. PDF/A-2 erlaubt die Verwendung digitaler Signaturen gemäß PAdES (PDF Advanced Electronic Signatures, ETSI TS 102 778[43])[44].

4.2.6.3 Eigenschaften und Anwendungen

PDF kann als das Standardformat zum Austausch und zur Speicherung von Dokumenten angesehen werden. Insbesondere PDF/A stellt durch die Einbettung von zur Interpretation und Darstellung benötigter Information den De-facto-Standard zur Dokumentenarchivierung dar. Obwohl in PDF/A-3 eingebettete Dateien nicht zwangsläufig „archivierungskonform" sind, stellt der Standard in Deutschland die Grundlage für den Austausch und die Speicherung elektronischer Rechnungen (Zentrale User Guidelines des Forums elektronische Rechnung Deutschland - ZUGFeRD)[45] dar. An diesem Beispiel lässt sich das Prinzip der Verwendung von PDF als Format zur Langzeitarchivierung gut erläutern. Die Rechnung selber wird in einer menschenlesbaren Form als PDF/A-3 Dokument gespeichert und dargestellt. Dieses Dokument beinhaltet eine spezielle XML-Datei eines vorgegebenen Schemas, die die Rechnungsdaten beinhaltet. Das gesamte Konstrukt wird durch geeignete Metadaten derart beschrieben, dass Inhalt und Verwendungszweck aus diesen klar erkennbar sind.

4.2.7 EPUB

EPUB ist ein Austauschformat für digitale Publikationen und Dokumente, das vom International Digital Publishing Forum <ipdf>[46] im Jahr 2007 in der Version 2.0 veröffentlicht wurde. EPUB erlaubt die Speicherung und Verteilung digitaler Dokumente unter Verwendung von Web-Technologien wie XML, CSS oder SVG in einer strukturierten

[43] PDF Advanced Electronic Signatures Profiles (ETSI - European Telecommunications Standards Institute, 2009)
[44] Die PAdES Spezifikation wird derzeit von ETSI überarbeitet. Mit der Verabschiedung ist im Laufe des Jahres 2015 zu rechnen (ETSI - European Telecommunications Standards Institute, 2015)
[45] ZUGFeRD - einheitliches Format für elektronische Rechnungen (Forum elektronische Rechnung Deutschland (FeRD), 2014)
[46] International Digital Publishing Forum (ipdf, 2015)

Datei (Container) und unterstützt die Entwicklung standardisierter Werkzeuge zu deren Darstellung. Die aktuelle Version 3.0.1[47] wurde im Juni 2014 vom <ipdf> verabschiedet. Der zur Version 3.0 korrespondierende ISO-Standard ISO/IEC TS 30135-x:2014 besteht aus sieben Teilen (Overview, Publications, Content Documents, Open Container Format, Media Overlay, Canonical Content Identifier, Fixed-Layout Documents), von denen der vierte Teil[48] für Archivierung und Signaturen relevant ist.
Der logische EPUB-Container wird durch ein Dateisystem repräsentiert, dessen Struktur und Inhalt durch eine Datei META-INF beschrieben werden, die sich direkt unterhalb der Wurzel des Dateisystems befindet. Der Inhalt des Dokuments kann entsprechend den Konventionen der „XML Encryption Syntax"[49] verschlüsselt sein. Signaturen können entsprechend der „XML Signatur Syntax"[50] erzeugt und eingefügt werden. Aus Anwendungssicht dient die Signatur dazu, die Echtheit von E-Books sicherzustellen. Ziel der Verschlüsselung ist es, das unerlaubte Kopieren zu verhindern. Sie wird zur Umsetzung des „Digital Rights Management (DRM)" eingesetzt.
Physikalisch wird das nachfolgend beschriebene zip-Format in der Version 6.3.3 als Container-Format verwendet.
EPUB unterscheidet sich somit in Bezug auf die Archivierung nicht wesentlich von den oben beschriebenen, XML-basierten Dokumentenformaten. Wie bei PDF liegt der Schwerpunkt auf der Speicherung und Darstellung digitaler Dokumente, während bei ODF und OOXML die Bearbeitbarkeit im Vordergrund steht.

4.2.8 ZIP

Die aktuelle Spezifikation des zip-Formats[51] durch die Firma PKWARE, Inc. liegt in der Version 6.3.3 vor. Diese Version wird vom in Abstimmung befindlichen ISO Standard ISO/IEC CD 21320-1[52] referenziert. Die Kapitel über digitale Signaturen sowie über PKWARE spezifische Verschlüsselung sind jedoch kein Bestandteil der ISO-Norm.

[47] EPUB 3.0.1 (ipdf, 2014)
[48] Digital publishing - EPUB3 - Part 4: Open Container Format (ISO/IEC JTC 1/SC34, 2014)
[49] XML Encryption Syntax and Processing Version 1.1 (W3C, 2013)
[50] XML Signature Syntax and Processing Version 2.0 (W3C, 2013)
[51] ZIP File Format Specification Version 6.3.3 (pkware, 2012)
[52] ISO/IEC DIS 21320-1 Document Container File -- Part 1: Core (ISO/IEC, 2014)

5 Ergebnisse

Die Arbeiten haben ergeben, dass eine strikte Trennung zwischen der Analyse offener Dokumentenformate einerseits und technischen bzw. rechtlichen Vorgaben in Bezug auf Signierung, Archivierung und Langzeitarchivierung andererseits erforderlich ist. Insbesondere ist der Unterschied zwischen Speicherung/Archivierung und Langzeitspeicherung/-archivierung im Kontext der deutschen Verwaltung als wichtig anzusehen. Archivierung ist die langzeitige, sichere, unveränderbare, vollständige, nachvollziehbare, authentische, integre, beweisfähige und jederzeit verfügbare Aufbewahrung von Dokumenten. Dies betrifft alle Dokumente, die aufbewahrungspflichtig oder aufbewahrungswürdig sind. In Langzeitarchive der öffentlichen Hand kommen Dokumente aus der öffentlichen Verwaltung erst dann, wenn Bearbeitung und Aufbewahrungspflichten abgeschlossen sind. Der 2009 aufgekommenen Begriff Langzeitarchivierung wird in Initiativen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des DIN verwendet. Danach soll es eine vertrauenswürdige elektronische Langzeitspeicherung nur für elektronisch signierte Dokumente mit Nachsignieren zum Erhalt der Beweisfähigkeit geben. Die Langzeitspeicherung wird mit bis zu 100 Jahren definiert und gilt als Vorstufe zur vertrauenswürdigen elektronischen Langzeitarchivierung.

In Bezug auf die vorliegende Themenstellung wurde daher untersucht, wie weit offene Dokumentenformate und ihre Speicherformate den genannten Anforderungen an Archivierung genügen und ob Unterstützung für Nachsignieren vorhanden ist. Ergänzend wurde geprüft, ob die vorhandenen Konzepte zur Archivierung von „elektronischen, digitalen Unterlagen" so allgemein sind, dass sie die Archivierung offener Dokumentenformate ermöglichen, ohne spezielle Anforderungen an deren Speicherformat zu stellen. Dafür ergibt sich dann jedoch die Notwendigkeit sicherzustellen, dass auch in „bis zu 100 Jahren" Software vorhanden ist, die nachhaltig eine Prüfung und Interpretation/Darstellung der digitalen Dokumente ermöglicht.

6 Schlussfolgerungen und Empfehlungen

Dokumentenstandards werden heute überwiegend technologiegetrieben entwickelt. Die pro-aktive Erfassung und Berücksichtigung von Anforderungen aus strategischen Themenfeldern wie der Einführung von partizipativen Ansätzen im Open Government oder die Verpflichtung zur elektronischen Aktenführung stellt eine neue Vorgehensweise mit hohem Innovationspotential dar. Die Einbeziehung nationaler rechtlicher Rahmenbedingungen auf die Standardisierung, wie sie sich u.a. aus dem eGovernment Gesetz ergeben können, ist bislang noch nicht erfolgt. Die pro-aktive Erfassung von Anforderungen an die Standardisierung bez. Zertifizierung und Archivierung digitaler Dokumente erlaubt der deutschen Wirtschaft und insbesondere KMUs die frühzeitige Entwicklung und Anpassung von interoperablen Softwaresystemen zur Erstellung, Archivierung und Weiterverarbeitung digitaler Dokumente.

Systeme zur Archivierung und Langzeitspeicherung betrachten Dokumente weitestgehend als Spezialfälle digitaler Daten, die für die Archivierung zu beschreiben und zusammen mit den zugehörigen Metadaten in Pakten oder Containern zusammenzufassen und als solche zu signieren sind. Die empfohlenen Dokumentenformate beziehen sich weitestgehend auf die zum Zeitpunkt der Erstellung der Normen oder Richtlinien aktuellen technischen und politischen Stand und sind anschließend nicht mehr aktualisiert worden. PDF/A-1 wird als für die Speicherung bevorzugtes Dokumentenformat genannt.

Dokumentenformate wie OOXML und ODF erlauben prinzipiell die Signierung von Teildokumenten. Diese Möglichkeit wird jedoch von den gängigen Office-Anwendungen nicht genutzt. Hier könnten insbesondere Spezialanwendungen für eingebettete Daten Alternativen bieten, die eine rechtskonforme Signierung derartiger Containerformate ermöglichen. Beide Formate verwenden grundsätzlich W3C-Konzepte aus *XML Signature Syntax and Processing* zur Signierung der XML-Container in Verbindung mit ETSI-Erweiterungen aus XAdES. PDF/A-2 nutzt vergleichbare ETSI PAdES-Erweiterungen und setzt somit ebenfalls auf die Wiederverwendung etablierter Standards. Die Ausweitung der Signatur auf eingebette Daten in PDF/A-3 Dokumenten ist wünschenswert.

Als im Detail zu untersuchen kann die für eine rechtskonforme Langzeitspeicherung erforderliche Übersignierbarkeit von Dokumenten zum Erhalt des Beweiswertes angesehen werden. Da OAIS-konforme Systeme diese Eigenschaft jedoch unabhängig vom Typ der gespeicherten Daten anbieten stellt sich die Frage, ob diese Eigenschaft für die betrachteten Dokumentenformte nativ zwingend erforderlich ist. Interessant ist weiterhin die Fragestellung, ob mehrere Personen ein digitales Dokument signieren können und müssen.

6.1 Bewertung

Betrachtet man die Behandlung von Dokumenten in Verwaltungsabläufen in einem abstrakten Modell, so wird ein Dokument vom Antragsteller/Initiator, das kann ein Bürger oder ein Unternehmen sein, an die Verwaltung gesendet. Entsprechend den rechtlichen Regelungen überprüft der Verwaltungsmitarbeiter die formale Korrektheit des Dokuments. Dazu kann die Überprüfung der Unterschrift gehören, sofern diese erforderlich ist (Schriftformerfordernis). Nach positiver Prüfung wird das Dokument „zu den Akten gelegt". Dieser Vorgang kann darin bestehen, dass das Dokument mit einer Identifikation versehen wird und an einem sicheren Ort abgelegt wird. Ggf. muss der Sachbearbeiter mit seiner Unterschrift bestätigen, dass er das Dokument formal geprüft und unverändert abgelegt hat. In der Bearbeitungsphase des Dokuments werden die Mechanismen der Langzeitspeicherung verwendet. Die das Dokument beinhaltende Akte wird geöffnet, das Dokument wird entnommen und sein Inhalt wird dargestellt, gelesen, verarbeitet. Dabei ist zu prüfen, dass das Dokument seit seiner ersten Ablage unverändert geblieben ist. Weiterhin ist sicher zu stellen, dass der Inhalt des Dokuments so interpretiert bzw. dargestellt wird, wie er sich zum Zeitpunkt der Signatur durch seinen Ersteller präsentiert hat.

Man erkennt an diesem Beispiel, dass sich die eigentliche Herausforderung bei der Interpretation archivierter Dokumente nicht auf die Überprüfung und Erneuerung von Signaturen bezieht sondern auf eine konsistente Darstellung der Inhalte des Dokuments. Diese Forderung mag zwar zunächst trivial klingen, ist es aber in der Praxis keineswegs. Man betrachte dazu beispielsweise die Unterstützung für alternative Darstellungsformen in den betrachteten Dokumentenformaten. Wie kann sichergestellt werden, dass die bei der Signatur vorhandene Darstellung identisch der bei der späteren Interpretation verwendeten Darstellung ist? OOXML-Dokumente erlauben die Verwendung nutzerspezifischer Inhalte, die zwar im Speicherformat vorhanden sind, nicht aber für jeden Betrachter sichtbar. Wie werden Kommentare und Änderungshistorien bei der Signatur betrachtet? Kann und wenn ja, wie, die Konsistenz der angezeigten Informationen mit zugehörigen, eingebetteten Daten, sichergestellt werden? Was besagt eigentlich eine Signatur, wenn sich diese nur auf Teile des Dokuments bezieht? Wie kann sich der Empfänger eines Dokuments über den Geltungsbereich der Signatur informieren? All diese Fragen beziehen sich auf die eingehende Analyse der in den Dokumentenformaten vorhandenen Möglichkeiten zur Signierung und den Grad der Unterstützung durch erzeugende und interpretierende Programme. Selbst in PDF/A-3 gespeicherte Dokumente sind in Bezug auf eine derartige Transparenzanforderung nicht „verwaltungs-/archivierungskonform".

Man kann daher erkennen, dass durch die Untersuchung der Anforderungen an Dokumentenformate in Bezug auf die Unterstützung von rechtskonformer

Langzeitspeicherung und Archivierung im Wesentlichen keine neuen Anforderungen ergeben. Dies ist durch die Tatsache begründet, dass Archivierungsvorschriften von einem sehr einfachen Dokumentenbegriff ausgehen. Vielmehr liegt die eigentliche Herausforderung in der Unterstützung und Transparenz des Signaturvorgangs sowohl bei der Durchführung der Signatur als auch bei der Interpretation des Dokuments unter Berücksichtigung der vorhandenen Signaturen.

Die Auswertung der Analysen von rechtlichen und politischen Aspekten der Dokumentenarchivierung einerseits und der Unterstützung von Signaturen in offenen Dokumentenformaten andererseits führt zu der Erkenntnis, dass die eigentliche Herausforderung an Dokumentenformate nicht in der Unterstützung von Archivierungsanforderungen liegt. Vielmehr ist sicherzustellen, dass die bei der Signatur eines Dokuments bzw. dessen Teilen verwendete Interpretation des Dokuments identisch zur Interpretation durch den Empfänger oder Bearbeiter des Dokuments ist. Dies ist jedoch eine Anforderung an die Werkzeuge zur Erstellung und Interpretation von Dokumenten bzw. deren Interoperabilität und keine Anforderung an die betrachteten Dokumentenformate. Rechtlich betrachtet hängt diese Eigenschaft mit der „Identität" von Dokumenten zusammen, wie sie beispielsweise in DIN 31646 betrachtet wird.

7 Referenzen

Beauftragte der Bundesregierung für Informationstechnik. 2011. SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0. [Online] November 2011. http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/SAGA%205-aktuelle%20Version/saga_5_aktuelle_version_node.html.

BSI - Bundesamt für Sicherheit in der Informationstechnik. 2009. BSI Technische Richtlinie 03125 - Vertrauenswürdige elektronische Langzeitspeicherung. [Online] Juli 2009. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html.

—. 2011. BSI Technische Richtlinie 03125 Anlage TR-ESOR-F: Formate und Protokolle V1.1. [Online] Februar 2011. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html.

—. 2008. Common Criteria Protection Profile for an ArchiSafe Compliant Middleware. *ACM_PP.* [Online] Oktober 2008. http://www.archisafe.de/s/c/EgJsjQEJ/ArchiSafe_Dokumente/ArchiSafe_PP_V10.pdf.

Bundesminister des Inneren. 2008. Standards und Architekturen für E-Government-Anwendungen SAGA 4.0. [Online] März 2008.

Bundesministerium der Justiz und für Verbraucherschutz. 2013. Gesetz über die Sicherung und Nutzung von Archivgut des Bundes. *Bundesarchivgesetz - BArchG.* [Online] August 2013. http://www.gesetze-im-internet.de/barchg/.

Bundesministeriums der Justiz und für Verbraucherschutz. 2013. Verordnung zur elektronischen Signatur (Signaturverordnung - SigV). [Online] August 2013. http://www.gesetze-im-internet.de/bundesrecht/sigv_2001/gesamt.pdf.

Bundesregierung. 2014. Digitale Verwaltung 2020. [Online] September 2014. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/regierungsprogramm-digitale-verwaltung-2020.html.

—. 2013. E-Government Gesetz: Gesetz zur Förderung der elektronischen Verwaltung. *Bundesgesetzblatt .* Jahrgang 2013, Juni 2013, Bd. Teil 1, Nr. 43.

—. 2001. Gesetz über Rahmenbedingungen für elektronische Signaturen. *Bundesgesetzblatt.* 2001, Mai 2001, Bd. Teil 1, Nr. 22.

—. 2013. Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Akte. [Online] Februar 2013. http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_artikel.html.

—. 2014. Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Langzeitspeicherung. [Online] Juni 2014. http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_artikel.html.

CCSDS - Consultative Committee for Space Data Systems. 2012. Reference Model for an Open Archival Information System (OAIS) - Recommended Practice. [Online] June 2012. http://public.ccsds.org/publications/archive/650x0m2.pdf.

DIN. 2012. *DIN 31644: Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive.* 2012.

—. 2011. *DIN 31645: Information und Dokumentation - Leitfaden zur Informationsübernahme in digitale Langzeitarchive.* 2011.

—. 2013. *DIN 31646: Information und Dokumentation - Anforderungen an die langfristige Handhabung persistenter Identifikatoren .* 2013.

ETSI - European Telecommunications Standards Institute. 2015. docbox.etsi.org - /ESI/Open/Latest_Drafts/. [Online] ETSI, 2015. http://docbox.etsi.org/ESI/Open/Latest_Drafts/.

—. 2009. Electronic Signatures and Infrastructures (ESI). *PDF Advanced Electronic Signatures Profiles.* [Online] July 2009. http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf.

—. 2009. XMLAdvanced Electronic Signatures (XAdES). *ETSI TS 101 903 V1.4.1.* [Online] Juni 2009. http://uri.etsi.org/01903/v1.4.1/ts_101903v010401p.pdf.

Forum elektronische Rechnung Deutschland (FeRD). 2014. ZUGFeRD - einheitliches Format für elektronische Rechnungen. [Online] Juni 2014.

IETF. 2007. RFC 4998 Evidence Record Syntax (ERS). [Online] August 2007. http://tools.ietf.org/html/rfc4998.

ipdf. 2014. EPUB 3.0.1. [Online] Juni 2014. http://idpf.org/epub/301.

—. 2015. International Digital Publishing Forum. *Trade and Standards Organization for the Digital Publishing Industry.* [Online] April 2015. http://idpf.org/.

ISO. 2012. ISO 14721:2012 - Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model. [Online] June 2012. https://www.iso.org/obp/ui/#iso:std:iso:14721:ed-2:v1:en.

ISO/IEC. 2005. Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1). [Online] 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57118. ISO 19005-1:2005.

—. 2005. ISO 19005-1:2005 Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1). [Online] 2005. https://www.iso.org/obp/ui/#iso:std:iso:19005:-1:ed-1:v2:en.

—. 2008. ISO 32000-1:2008 Document management -- Portable document format -- Part 1: PDF 1.7. [Online] 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502. ISO 32000-1:2008.

—. 2014. ISO/IEC DIS 21320-1 Information technology -- Document Container File -- Part 1: Core. [Online] September 2014. http://www.iso.org/iso/catalogue_detail.htm?csnumber=60101.

ISO/IEC JTC 1/SC34. 2014. Information technology - Digital publishing - EPUB3 - Part 4: Open Container Format. *ISO/IEC.* [Online] November 2014. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63569&commid=45374.

—. 2008. Office Open XML File Formats - Part 1: Fundamentals and Markup Language Reference. *ISO/IEC 29500-1:2008.* [Online] 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51463. ISO/IEC 29500-1:2008.

—. 2008. Office Open XML File Formats - Part 2: Open Packaging Convention. *ISO/IEC 29500-2:2008.* [Online] 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51459. ISO/IEC 29500-2:2008.

—. 2008. Office Open XML File Formats - Part 3: Markup Compatibility and Extensibility. [Online] 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51461. ISO/IEC 29500-3:2008.

—. 2008. Office Open XML File Formats - Part 4: Transitional Migration Features. *ISO/IEC 29500-4:2008.* [Online] 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51462. ISO/IEC 29500-4:2008.

—. 2006. Open Document Format for Office Applications (OpenDocument) v1.0. *ISO/IEC 26300:2006.* [Online] 30. November 2006. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485. ISO/IEC 26300:2006.

—. 2012. Open Document Format for Office Applications (OpenDocument) v1.0 - Amendment 1 (ODF 1.1). [Online] 2012. http://www.iso.org/iso/iso_catalogue/.

KoSIT - Koordinierungsstelle für IT-Standards. 2011. XDomea - IT-gestützter Austausch und IT-gestützte Aussonderung behördlichen Schriftgutes. [Online] KOSIT, 2011. http://www.xoev.de/detail.php?gsid=bremen83.c.11406.de.

Library of Congress. Sustainability of Digital Formats. *Planning for Library of Congress Collections.* [Online] http://www.digitalpreservation.gov/formats/index.shtml.

Microsoft. 2006. Microsoft Open Specification Promise. [Online] 2006. [Zitat vom: 12. July 2009.] http://www.microsoft.com/interop/osp/default.mspx.

nestor. 2012. Referenzsystem für ein Offenes Archiv-Informationssystem (deutsche Übersetzung). [Online] 2012. http://files.d-nb.de/nestor/materialien/nestor_mat_16.pdf.

—. 2011-2013. Standards im Bereich digitale Langzeitarchivierung. [Online] 2011-2013. https://wiki.dnb.de/display/NESTOR/Standardisierung.

OASIS - Organization for the Advancement of Structured Information Standards. 2011. Open Document Format for Office Applications (OpenDocument) Version 1.2 Part 3: Packages. [Online] September 2011. http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2-part3.html.

—. 2012. Open Document Format for Office Applications: ODF 1.2. [Online] Januar 2012. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office.

—. 2005. *OpenDocument v1.0 Specification.* http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf : s.n., May 2005. ODF 1.0.

OpenOffice. 2002. The OpenOffice.org community announces the availability of OpenOffice.org 1.0. [Online] April 2002. [Zitat vom: 12. July 2009.] http://www.openoffice.org/about_us/ooo_release.html.

pkware. 2012. APPNOTE.TXT - .ZIP File Format Specification Version 6.3.3. [Online] September 2012. http://www.pkware.com/documents/APPNOTE/APPNOTE-6.3.3.TXT.

W3C. 2003. XML Advanced Electronic Signatures (XAdES). [Online] Februar 2003. http://www.w3.org/TR/XAdES/.

—. 2013. XML Encryption Syntax and Processing Version 1.1. *W3C Recommendation 11 April 2013.* [Online] April 2013. http://www.w3.org/TR/xmlenc-core1/.

—. 2013. XML Signature Syntax and Processing Version 2.0. *W3C Working Group Note 11 April 2013.* [Online] April 2013. http://www.w3.org/TR/xmldsig-core2/.

Wir machen
Städte schlau

IMPRESSUM

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kompetenzzentrum ELAN
Kaiserin-Augusta-Allee 31
10589 Berlin

Tel. +49 30 3463-7227
Fax +49 30 3463-99 7227
klaus-peter.eckert@fokus.fraunhofer.de

www.fokus.fraunhofer.de

Projektgruppe
Dr. Klaus-Peter Eckert, Joachim Kaeber, Roman Grahle

Gefördert durch
Bundesministerium für Wirtschaft und Energie

Bildnachweis
DRs Kulturarvsprojekt / flickr