Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein OPS.1.2.2 Archivierung

- Einleitung
- Maßnahmen
  - Maßnahmen zum Baustein OPS.1.2.2 Archivierung
- Weiterführende Informationen
  - Wissenswertes
  - Quellenverweise

1. Einleitung

Bei nahezu allen Geschäftsprozessen entstehen Daten, die geeignet archiviert oder über eine lange Zeit gespeichert werden müssen, um sie später wiederfinden und verwenden zu können. Kennzeichnend für die Archivierung (Langzeitspeicherung) ist die dauerhafte und unveränderbare Speicherung von elektronischen Dokumenten und anderen Daten. Die Aufbewahrungsfrist der jeweiligen Daten muss zum Archivierungszeitpunkt festgelegt werden. Eventuell müssen die Daten auch zeitlich unbegrenzt verfügbar sein.

Wenn in diesem Baustein der Begriff "Dokumente" benutzt wird, werden hiermit auch Daten inkludiert.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins OPS.1.2.2 *Archivierung* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein OPS.1.2.2 Archivierung

OPS.1.2.2.M1 Ermittlung von Einflussfaktoren für die elektronische Archivierung (B)

Bevor eine Entscheidung getroffen werden kann, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden sollen, müssen die für den Anwendungsfall relevanten technischen,

rechtlichen und organisatorischen Einflussfaktoren ermittelt und ins Archivierungskonzept übernommen werden.

Ermittlung der technischen Einflussfaktoren

Um die technischen Einflussfaktoren zu ermitteln, sollten die Eigentümer der zu archivierenden Dokumente befragt werden, also beispielsweise die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen und die Systemadministratoren. Die Ergebnisse sind nachvollziehbar im Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) zu dokumentieren.

Maßgebliche technische Einflussfaktoren für die elektronische Archivierung sind unter anderem:

- das zu erwartende Datenaufkommen,
- die Dateiformate der zu archivierenden Inhaltsdaten, Metadaten sowie Beweisdaten (z. B. beweisrelevante Daten, z. B. Signaturen, Siegel, Zeitstempel bzw. technische Beweisdaten (Evidence Records)),
- das Änderungsvolumen und die Versionierung,
- die Aufbewahrungsdauer und Löschvorgaben der Dokumente,
- die Zahl und Art der Zugriffe,
- die vorhandene IT-Einsatzumgebung sowie
- zu beachtende Normen und Standards.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt:

Zu erwartendes Datenaufkommen

Ein wesentliches Auswahlkriterium für elektronische Archivsysteme ist die Größe der zu archivierenden Dateien und das in Zukunft zu erwartende Datenaufkommen. Dies kann typischerweise nur großzügig abgeschätzt werden. Die Dateigröße von Dokumenten hängt dabei auch sehr stark vom Dateiformat und dem Umfang der Rendition (siehe weiter unten) ab.

Dateiformate der zu speichernden Dokumente

Je nach Wahl des Archivsystems könnten in diesem grundsätzlich alle verwendeten Dateiformate abgelegt werden, z. B. die in Büroumgebungen üblichen Formate (DOCX, PDF, RTF, ASCII, ZIP, ODT etc.) oder auch Bild- und Tondateien (JPG, GIF, WAV, MPEG etc).

Um allerdings den Aufwand bei der Erhaltung der langzeitgespeicherten Dokumente wirtschaftlich sinnvoll zu gestalten, sollten die in die Langzeitspeicherung zu übernehmenden Dokumente in ein geeignetes Format überführt werden.

Für herkömmliche Textdokumente empfiehlt es sich, diese in den jeweils aktuellen und anforderungsgerechten Standard von PDF/A umzuwandeln. Für spezifische Formate, für die das nicht möglich oder sinnvoll ist, sollte geprüft werden, welche alternativen langzeitspeicherfähigen Formate infrage kommen. Um diese Dokumente zu erhalten, muss jedoch regelmäßig geprüft werden, ob sie noch lesbar sind. Ist das nicht der Fall bzw. zeichnet sich das ab, müssen sie in neuere Formate konvertiert werden.

Weitere langzeiterhaltende Maßnahmen sind in OPS.1.2.2.M9 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* detailliert beschrieben.

Bei der elektronischen Archivierung haben sich in der Vergangenheit mehrere Dateiformate etabliert, die unterschiedlich für künftige Verwendungszwecke der Dokumente geeignet sind. Häufig kann oder soll jedoch der spätere Verwendungszweck nicht festgelegt werden. In so einem Fall ist aber nicht vorhersagbar, welches das beste Datenformat für die spätere Verwendung ist. Ebenso häufig bestehen bereits zum Zeitpunkt der Datenspeicherung konkurrierende Anforderungen an die Wahl des Dateiformates, die sich aus den unterschiedlichen Verwendungszwecken ergeben. Deshalb hat es sich, vor allem bei der Langzeitspeicherung, als vorteilhaft erwiesen, Dokumente in mehreren Dateiformaten gleichzeitig zu archivieren. Die Dokumente müssen dazu vorher konvertiert werden. Dieser Vorgang wird als Rendition bezeichnet. Bei der Rendition ist jedoch auf eine genaue Dokumentation der Verfahrensweise zu achten.

Informationen über das Originalformat müssen mit archiviert werden. Außer den Inhaltsdaten müssen meistens begleitende Beschreibungs- und Beweisdaten mitgespeichert werden.

Das hierfür notwendige Archivinformationspaket (engl. Archival Information Packet - AIP) soll in einer selbsttragenden Form alle zur Erfüllung des Aufbewahrungszwecks notwendigen Informationen bis zum Ablauf der geltenden Aufbewahrungsfristen in einer möglichst hard- und softwareneutralen Form beinhalten. Dabei geht es primär um die Inhaltsdaten (die aufzubewahrenden Daten [1-n] selbst), beschrieben durch die notwendigen Metadaten (sowohl fachliche als auch technische Metadaten) und die zum Nachweis der Authentizität, Integrität sowie Vertraulichkeit notwendigen Daten. Es ist dabei entscheidend eine ausreichende Menge der Metadaten zu erfassen (Kontextsicherung), um den aufbewahrten Vorgang auch in der Zukunft vollständig rekonstruieren zu können.

Für die Meta- und Protokollinformationen hat sich XML als Format und z. B. XDOMEA als Standard für elektronische Akten und Vorgänge etabliert. Beispielsweise kann als XML-Schema für die Meta- und Protokolldaten dabei die jeweils aktuelle Spezifikation von XDOMEA verwendet werden. Als XML-Schema für das AIP zur Aufnahme der beschreibenden Informationen der aufzubewahrenden Dokumente selbst sowie der beweisrelevanten Daten und technischen Beweisdaten empfiehlt es sich die Vorgaben des BSI gemäß BSI TR-03125, siehe [TR-ESOR-F] zu verwenden. Damit ist ein Informationspaket für den Zeitraum der Langzeitspeicherung verfügbar, das alle notwendigen Informationen (Meta- und Primärinformationen) umfasst.

So wird beispielsweise eine Integration von XDOMEA in die Datenpaketstruktur XAIP als selbsttragendes Archivinformationspaket gemäß BSI TR-03125, siehe [TR-ESOR-F] und [TR-ESOR-XB] beschrieben.

Die Rendition von Dokumenten und anschließende Speicherung in mehreren Dateiformaten wirkt sich unmittelbar auf die für die Archivierung notwendige Speicherkapazität aus.

Änderungsvolumen und Versionstiefe

Bei der Archivierung von Daten und Dokumenten ist zu überlegen, welche Änderungen an den Daten im Lauf der Zeit auftreten werden, wie häufig das zu erwarten ist und wie damit zu verfahren ist. Wenn archivierte Daten geändert werden sollen, soll folgendermaßen vorgegangen werden:

- Die neue Version der Daten wird zusätzlich zur ursprünglichen Version archiviert (Versionierung), wobei unter Umständen nur eine maximale Anzahl von Versionen derselben Daten archiviert bleibt. Die Versionstiefe muss eventuell gegen Anforderungen an die Nachvollziehbarkeit geprüft werden.

Institutionsintern oder rechtlich kann eine Versionierung der Daten gefordert werden. Sofern eine Versionierung von Daten vorgenommen wird, muss das sowohl bei der Berechnung der notwendigen Speicherkapazität des Archivsystems als auch bei Aufbau und Struktur des Archivinformationspakets berücksichtigt werden.

Aufbewahrungsdauer der Daten und Dokumente

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist es unerlässlich, abzuschätzen, wie lang die Aufbewahrungsdauer der archivierten Dokumente sein wird. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder institutionsinterner Vorgaben minimale, jedoch teilweise auch maximale Fristen, die zu beachten sind.

Die Aufbewahrungsdauer beeinflusst jedoch nicht nur die Speicherkapazität des Archivsystems, sondern auch die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer. Weiterhin wirkt sich die Aufbewahrungsdauer auch auf die Maßnahmen für die digitale Bestandserhaltung aus.

Zahl und Art der Zugriffe

Zugriffszahlen sowie die Art der Zugriffe auf das Archivsystem wirken sich auf die Konfiguration des Archivservers und die Auswahl der Speicherkomponenten aus. Als Einflussfaktoren sind daher zu ermitteln:

- Wie viele Zugriffe werden innerhalb eines vorgegebenen Zeitraums auf das Archivsystem erfolgen?
- Wie hoch ist der Anteil von Schreibzugriffen gegenüber Lesezugriffen?

- Welche Antwortzeiten werden verlangt?
- Erfolgen die Zugriffe direkt von Benutzer- bzw. Clientsystemen auf das Archivsystem?
- Muss das Archivsystem zwischen Zugriffen verschiedener Benutzer unterscheiden oder erfolgt dies durch übergeordnete Komponenten?
- Muss das Archivsystem mehrere, logisch oder physisch voneinander getrennte Archive verwalten (Mandantenfähigkeit)?

IT-Einsatzumgebung

Archivsysteme sind typischerweise in komplexere IT-Landschaften eingebettet. Hierdurch ergeben sich technische Anforderungen, z. B. hinsichtlich

- der Netzanbindung,
- der verwendbaren Netzprotokolle (deren Definition z. B. bekannt sein muss, wenn die Kommunikationsverbindung über Firewalls geführt wird),
- Kompatibilität zu anderen Programmen oder IT-Systemen,
- der Einbindung in Systemmanagement-Umgebungen sowohl zur Administration als auch zur Überwachung des Archivsystems,
- der Administrations- und Nutzungsschnittstellen sowie
- der Antwortzeiten des Archivsystems.

Zu beachtende Normen und Standards

Die im Bereich der Archivierung bestehenden Standards konzentrieren sich auf die Bereiche

- Datenformate und Kompressionsverfahren,
- Architektur,
- Funktionen und Prozesse,
- Schnittstellen zwischen dem Fachverfahren und dem Langzeitspeichersystem, z. B. Schnittstelle S.4 in BSI TR-03125 TR-ESOR, siehe [TR-ESOR-E]
- Speichermedien und deren Aufzeichnungsverfahren sowie
- einzubindende Fachverfahren.

Systemhersteller erhalten durch die Offenlegung von Schnittstellen, die im Rahmen der Standardisierung erfolgt, die Möglichkeit, eine Kompatibilität von Systemkomponenten, Schnittstellen und Datenformaten herzustellen. Deshalb kann durch die Berücksichtigung von Standards bei der Auswahl von Archivsystemen eine längerfristige Planungs- und Investitionssicherheit gewährleistet werden.

Für den Anwender verringern Standards die Abhängigkeit von einzelnen Herstellern, Systemlieferanten und Dienstleistern. Bei den langen Zeiträumen, über die Archivsysteme typischerweise eingesetzt werden, ist dies besonders wichtig, da nicht absehbar ist, wie sich Produktlinien langfristig entwickeln. So könnte sich z. B. bei Insolvenz eines Herstellers proprietärer Speicherkomponenten das Problem ergeben, dass das Archivierungssystem nicht mehr in der bisherigen Art durch Zukauf neuer Speichermedien und -komponenten erweitert werden kann. Behörden und Unternehmen mit hohem Archivierungsbedarf müssen dann typischerweise kurzfristig die Archivdaten migrieren. Bei Einsatz standardisierter Komponenten kann dagegen einfach ein anderer Lieferant für die betroffene Teilkomponente gewählt werden.

Hinsichtlich Standards ist allerdings zu beachten, dass auch diese mit der Zeit aufgrund neuer technologischer Entwicklungen an Relevanz verlieren und eventuell durch neue Standards ersetzt werden. Zudem besteht auch ein Wettbewerb zwischen unterschiedlichen Standardisierungsgremien und Herstellern, wodurch es auch konkurrierende Standards gibt. Insofern empfiehlt es sich auf anerkannte Standards unabhängiger Standardisierungsgremien wie z.B. ISO, ETSI/CEN, DIN oder BSI zu setzen.

Prinzipiell ist die Archivierung jedoch auch ohne Standards und mit proprietären Datei- und Speicherformaten möglich, sofern über den Archivierungszeitraum eine ausreichende Wartung und Systembetreuung durch Hersteller und eine Anpassung der Schnittstellen an sich verändernde Anforderungen sichergestellt wird. Es wird jedoch empfohlen, sich bei der Planung von Archivsystemen eng an geltenden Standards für Dateiformate und Schnittstellen zu orientieren.

Bereits bei der Planung eines Archivsystems sollte eine spätere Migration berücksichtigt werden, da sich bei der langfristigen Speicherung von Daten typischerweise zwischendurch die Technik oder die Anforderungen ändern. Daher sollten Schnittstellen, Dateiformate und Index-Datenbank besonders sorgfältig ausgewählt werden. Auch sollten alle Entscheidungen nachvollziehbar dokumentiert werden.

Weitere Empfehlungen enthält die BSI TR-03125 (siehe [TR-ESOR]) hinsichtlich des Einsatzes offener, interoperabler und standardisierter Datenformate BSI TR-03125 (siehe [TR-ESOR-F], insbesondere Kap. 3) und herstellerunabhängiger interoperabler Schnittstellen (siehe [TR-ESOR-E], insbesondere Kap. 3] entsprechend nationaler und internationaler Standards, insbesondere für die Schnittstellen zwischen dem Fachverfahren und dem Langzeitspeichersystem sowie weitere Harmonisierungen in Form einer Profilierung für Bundesbehörden (siehe BSI TR-03125 [TR-ESOR-B] und [TR-ESOR-XB]).

Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

Für die Aufbewahrung bestimmter Informationen bestehen verschiedene rechtliche Vorgaben. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben. Daher sollten sich die Zuständigen informieren, welche rechtlichen Vorgaben zu beachten sind. Hieraus ergeben sich Anforderungen, die im Archivierungskonzept berücksichtigt werden müssen. Das betrifft unter anderem

- die Mindestaufbewahrung aus rechtlichen Gründen,
- Höchstaufbewahrungsdauer aus Datenschutzgründen,
- Zugriffsrechte für Externe, z. B. Steuerbehörden oder Gerichte,
- Beweiswerterhaltung elektronischer Dokumente,Umgang mit ersetzend gescannten oder signierten Eingängen,
- Vorlage von Daten bei Prüfbehörden, Gerichten, Dritten,
- Auswertbarkeit oder Reproduzierbarkeit von Daten, z. B. im Forschungsumfeld,
- Anbietungspflicht gemäß Archivrecht gegenüber öffentlichen Archiven sowie
- Qualität von eingesetzten elektronischen Signatur- oder Siegel- oder Zeitstempel-Algorithmen bzw. Verfahren für technische Beweisdaten (engl. Evidence Records).

Die anzuwendenden rechtlichen Grundlagen sind im Einzelfall zu klären.

Im Folgenden werden einige Quellen genannt, die in Deutschland typischerweise zu berücksichtigen sind:

- Bürgerliches Gesetzbuch (BGB)
  Hier werden insbesondere Anforderungen an die Rechtsgültigkeit von Dokumenten im Zivilrecht gestellt. Das BGB definiert auch Verjährungsfristen, z. B. für Schadenersatz aus unerlaubter Handlung.
- Zivilprozessordnung (ZPO)
  Analog zum BGB wird durch die ZPO geregelt, welche Dokumente als Urkunde anerkannt werden müssen, beispielsweise aufgrund einer eigenhändigen Unterschrift oder einer qualifizierten elektronischen Signatur.
- Handelsgesetzbuch (HGB)
  Hier werden Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit gestellt. Dies umfasst auch bestimmte Aufbewahrungsfristen für Geschäftsdokumente.
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).
- Fachvorschriften, z. B. Luftfahrt, Gesundheitswesen, Zulassungsrecht, Forschung, Atomrecht.

- Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz), siehe [EIDAS-DG].
- Vertrauensdienstegesetz (siehe [VDG]) als Artikel 1 des eIDAS-Durchführungsgesetzes (siehe [EIDAS-DG]).
- Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktion im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, siehe [EIDAS-VO].
- eIDAS-Durchführungsbeschlusses (EU) 2015/1506
- Verordnung (EU) 2016/679 des europäischen Parlaments und des vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Weiterhin gibt es Gesetze und Vorschriften, die speziell für Behörden und in der Verwaltung zu beachten sind, beispielsweise:

- Verwaltungsverfahrengesetz (VwVfG)
  Definiert grundsätzliche Zulässigkeit der Übermittlung elektronischer Dokumente sowie den Einsatz von QES des Personalausweises/elektronischen Aufenthaltstitels bzw. De-Mail mit Absenderbestätigung als Ersatz der angeordneten Schriftform.
- Verwaltungsgerichtsordnung (VwGO)
  Grundsätzliche Zulässigkeit der Verwendung einer elektronischen Akte sowie die Übertragung der Dokumente in einer elektronischen Form im Bereich der Prozessakten.
- Bundesarchivgesetz und die entsprechen Landesarchivgesetze,
  Aussonderung digitaler Unterlagen und deren Archivierung im Bundesarchiv. Ein Leitfaden. Version 1.2. Bundesarchiv 2010
- E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749)
  §§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen und Langzeitaufbewahrung nach dem "Stand der Technik", mit Verweis auf TR-ESOR und TR RESISCAN, Landesgesetze folgen.

Darüber hinaus gibt es weitere zahlreiche gesetzliche und institutionsinterne Regelungen (z. B. Vorschriften für Sozialversicherungsträger, Krankenhäuser, Pharmaindustrie, Militär oder Kreditwesen), die ermittelt werden müssen. Wesentliche Regelungskriterien sind üblicherweise die Aufbewahrungsdauer sowie der Vertraulichkeits- und Integritätsbedarf.

Für die öffentliche Verwaltung besteht darüber hinaus die gesetzliche Verpflichtung, auch in digitaler Form vorliegende Dokumente nach Ablauf der geltenden Aufbewahrungsfristen den zuständigen Archiven zur Übernahme anzubieten (Anbietungspflicht, siehe Archivgesetz Bund für Bundesbehörden sowie entsprechende Landesarchivgesetze).

Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

Für die elektronische Archivierung gibt es eine Reihe von organisatorischen Einflussfaktoren, die bei der Konzeption des Archivsystems berücksichtigt werden müssen. Dazu gehören unter anderem

- der Zeitraum des Einsatzes des Archivsystems,
- die Aufbewahrungsfristen,
- der Vertraulichkeitsbedarf der Dokumente,
- der Verfügbarkeitsbedarf der Dokumente
- der Integritätsbedarf der Dokumente
- der Authentizitätsbedarf der Dokumente
- die Verkehrsfähigkeit der Dokumente

- die Festlegung akzeptabler Antwortzeiten,
- der Personalaufwand,
- die Kenntnisse und IT-spezifischen Qualifikationen der Benutzer,
- die Ergonomie und Bedienfreundlichkeit des Archivsystems und
- die finanziellen Randbedingungen.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt.

Um entsprechend lange Aufbewahrungsfristen abdecken zu können, wird empfohlen, das elektronische Archiv nach dem geltenden Stand der Technik und basierend auf den aktuellen Standards und Normen aufzusetzen. Die Implementierung der einzelnen Prozesse des OAIS-Modells (Übernahme, Datenmanagement, Speicherung, Zugriff, Planung der digitalen Bestandserhaltung und Administration), sowie Aufbewahrung der archivierten Daten in Form von selbsttragenden Archivinformationspakete (X)AIP (mit Inhaltsdaten, Metadaten sowie Beweisdaten) und Anwendung der Maßnahmen für die Beweiswert-Erhaltung garantieren einen beweissicheren Umgang mit gespeicherten Daten.

Einsatzzeitraum des Archivsystems

Die Einsatzdauer eines Archivsystems ist getrennt von der Zeitdauer der Archivierung zu kalkulieren. Es ist abzuschätzen, über welchen Zeitraum das konkret auszuwählende System betriebsbereit sein soll. Dies wirkt sich auf die Auswahl der Komponenten und speziell auf die geforderte Lebensdauer der Komponenten aus. Ein langer Zeitraum impliziert die Auswahl langlebiger IT-Komponenten sowie die Gestaltung entsprechender Service- und Lieferverträge, die typischerweise mit höheren Kosten verbunden sind. Ein kurzer Zeitraum impliziert eine frühere Migration des Archivs auf ein neues Archivsystem.

Vertraulichkeitsbedarf der Dokumente

Bei der Bestimmung des Vertraulichkeitsbedarfs ist vor allem zu beachten, dass er sich während der Archivierungsfrist ändern kann. Hierbei können wirtschaftliche und juristische Einflussfaktoren eine Rolle spielen. Typischerweise ist davon auszugehen, dass der Vertraulichkeitsbedarf im Lauf der Zeit abnimmt (insbesondere im Falle einer Aussonderung der Daten in ein historisches Archiv).

Wenn ein langfristiger Schutz der Vertraulichkeit gefordert wird, so hat das Einfluss auf die organisatorische Gestaltung des Archivierungskonzepts (siehe OPS.1.2.2.M15 *Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung*) und die Auswahl technischer Komponenten.

Verfügbarkeitsbedarf der Dokumente

Die elektronische Archivierung wird typischerweise zur langfristigen Aufbewahrung von Daten und Dokumenten eingesetzt. Hierbei ist als wesentliche Anforderung in einem der vorigen Punkte bereits festgelegt worden, für welchen Zeitraum die betreffenden Daten zu archivieren sind.

Daneben ist festzulegen, welche weitergehenden Anforderungen an die Verfügbarkeit zu stellen sind, z. B. die Ausfallsicherheit des Archivsystems, die Stabilität der verwendeten Speichermedien oder die Informationserhaltung der Daten.

Integritätsbedarf der Dokumente

Die Integrität elektronisch archivierter Daten und Dokumente muss typischerweise auch nach einer langen Aufbewahrungsdauer noch sichergestellt und prüfbar sein (z. B. bis zum Ablauf der Aufbewahrungsfristen). Hierbei ist insbesondere davon auszugehen, dass bei langen Aufbewahrungsfristen die Ursprungsverfahren und -daten und weitere Kontextinformationen zwischenzeitlich nicht mehr existieren, so dass die Integritätsprüfung sowohl durch die Aufbewahrung von Kontextinformationen im Archivinformationspaket als auch durch Maßnahmen zur Informations- und Beweiswerterhaltung im Zusammenspiel mit dem Archivsystem bereitgestellt werden muss.

Es muss neben der Klassifizierung des Integritätsbedarfs (z. B. niedrig bis mittel, hoch oder sehr hoch) festgelegt werden, über welchen Zeitraum dies prüfbar sein soll.

Die Integrität der aufbewahrten Daten kann durch selbsttragende Archivinformationspakete (AIP) in Verbindung mit der Umsetzung der Anforderungen der Beweiswerterhaltung (siehe z. B. BSI TR-03125 [TR-ESOR]) dauerhaft gesichert werden.

Authentizitätsbedarf der Dokumente

Analog zur Integrität muss auch der Authentizitätsbedarf und der Zeitraum (gemäß der Aufbewahrungsfrist) festgelegt werden, innerhalb dessen die Authentizität von Daten prüfbar sein muss. Auch hier ist davon auszugehen, dass typischerweise nach einer längeren Archivierungsdauer die Ursprungsverfahren bzw. -daten und Kontextinformationen zwischenzeitlich nicht mehr existieren. Die Authentizitätsprüfung muss also ebenso vor allem durch die Umsetzung der Maßnahmen zur Beweiswerterhaltung (siehe z. B. BSI TR-03125 [TR-ESOR]) dauerhaft gesichert werden.

Verkehrsfähigkeit der Dokumente

Bei einer gerichtlichen Auseinandersetzung müssen die aufbewahrten Daten eventuell dem Gericht vorgelegt werden. Es müssen dabei nicht nur Inhaltsdaten, sondern auch Begleitdaten, z. B. Beweisrelevante Daten und technische Beweisdaten, sowie Metadaten in einer für das Gericht "verkehrsfähigen" Form vorgelegt werden, die die Anwendung der notwendigen Informations- und Beweiswert-Erhaltungsmaßnahmen während der Aufbewahrungszeit belegen. Hierzu wird die Verwendung selbsttragender AIPs sowie die Anwendung der Beweiswerterhaltung nach BSI TR-3125 [TR-ESOR] empfohlen.

Bestimmung akzeptabler Antwortzeiten

Zwischen der Anfrage an ein Archivsystem und der Antwort ergibt sich eine Verzögerung (Antwortzeit). Die Anforderungen an diese Verzögerung werden typischerweise durch eine zu erzielende mittlere und eine maximal akzeptable Antwortzeit definiert.

Die Antwortzeit ist nach unterschiedlichen Faktoren zu charakterisieren, z. B.

- die Zeitdauer bis zur Reaktion des Archivsystems bei einer Anfrage,
- die Zeitdauer bis zur Speicherbestätigung des Archivsystems und
- die Zeitdauer bis zur vollständigen Übertragung der gewünschten Daten an das Clientsystem.

Die geforderte Antwortzeit hängt dabei sehr stark vom Einsatzszenario ab. So können z. B. bei einer Recherche in Altdatenbeständen eines Enterprise Resource Planning (ERP)-Verfahrens durchaus Reaktionszeiten im Stundenbereich innerhalb der Regelarbeitszeit akzeptabel sein.

Typischerweise ergeben sich auch subjektive Anforderungen an die Antwortzeiten. So kann z. B. eine hohe Reaktionszeit auf Suchanfragen oder beim Öffnen archivierter Dokumente als störender empfunden werden als eine gleich lange Zeitdauer bis zur Speicherbestätigung bei der Ablage von Daten im Archiv.

Die Anforderungen an die Antwortzeit sind zu ermitteln und zu dokumentieren.

Personalaufwand

Der Personalaufwand für den Betrieb des Archivsystems beeinflusst wesentlich die Auswahl des Systems. Es ist zu ermitteln, welcher zusätzliche Personalaufwand und welche zusätzliche individuelle Belastung des Personals durch die Archivierung als tragbar angesehen werden.

Dies wirkt sich auf die künftige Personalplanung aus, da eventuell zusätzliches Personal erforderlich ist. Die Rollen Archivverwalter, Archivadministrator und (technischer) Benutzer sind mindestens zu besetzen. Wenn im laufenden Betrieb zu wenig Personal verfügbar ist, muss die fehlende Personalkapazität durch externe Wartungs- und Serviceverträge kompensiert werden.

Kenntnisse und IT-spezifische Qualifikationen der Benutzer

Die Auswahl geeigneter Bedienschnittstellen des Archivsystems wird unter anderem von den Vorkenntnissen der vorgesehenen Benutzer beeinflusst. Hier sollte ermittelt werden, welche IT-spezifischen Fachkenntnisse vorliegen.

Dies hat auch Einfluss auf Dienstleistungen im Umfeld der Archivierung, etwa die Organisation einer Benutzerunterstützung (Helpdesk) oder die Erweiterung des Helpdesks zur Unterstützung des Archivsystems.

Alle Benutzer müssen im Umgang mit dem Archivsystem geschult werden. Die erforderliche Schulung muss in den Gesamtkosten berücksichtigt werden.

Ergonomie und Bedienfreundlichkeit des Archivsystems

Je einfacher ein Archivsystem zu bedienen ist, desto besser akzeptieren es die Benutzer. Auch gehen sie dann eher ordnungsgemäß mit dem System um.

Neben gesetzlichen Anforderungen zur Ergonomie an Arbeitsplätzen ist hierbei auch der subjektive Eindruck von Benutzern zu berücksichtigen. Um die entsprechenden Anforderungen zu ermitteln, können die zukünftigen Benutzer z. B. befragt werden. Es sollten jedoch auch Erfahrungen aus Pilot- und Testinstallationen der vorgesehenen Archivsystem-Komponenten einfließen.

Im Falle eines Langzeitspeichers handelt sich gewöhnlich um einen nachgeordneten Dienst, der durch eine Geschäftsanwendung angesteuert wird. Deshalb ist diese Anforderung zweitrangig.

Finanzielle Randbedingungen

Die Einführung von Archivsystemen und die Gestaltung eines entsprechenden organisatorischen Rahmens werden typischerweise von den anfallenden Kosten beeinflusst:

- einmalige Investitionen,
- laufende Kosten, inklusive Personalkosten sowie
- Lizenzgebühren.

Die technische Planung von Archivsystemen wird daher typischerweise von einer Finanzplanung begleitet. Hierbei sind die institutionsinternen Regelungen (Budgetplanung, Verteilung von Kostenstellen etc.) zu berücksichtigen. Die notwendigen Schulungen für Benutzer und Administratoren müssen in die Kalkulation der Gesamtkosten einbezogen werden.

OPS.1.2.2.M2 Entwicklung eines Archivierungskonzepts (B)

Um eine elektronische Archivierung in einer Institution einzuführen, sind die Ziele festzulegen, die damit erreicht werden sollen. Dabei muss das Management der betreffenden Institution einbezogen werden. Eventuell müssen die Ziele auch mit übergeordneten Organisationseinheiten koordiniert werden. Insbesondere ist festzulegen,

- welche Regularien (Compliance) einzuhalten sind (rechtlich-organisatorischer Rahmen),
- in welchen Bereichen bzw. für welche Prozesse welche Daten in welcher Form archiviert werden sollen,
- welches Sicherheitsniveau es zu erreichen gilt,
- welcher Funktions- und Leistungsumfang angestrebt ist und
- wer die Verantwortung hierfür trägt.

Die Ergebnisse sind im Archivierungskonzept zu fixieren.

Welche Regularien (Compliance) sind bei der Archivierung zu berücksichtigen?

Welche Informationen archiviert werden, ist auch von den gesetzlichen und vertraglichen Rahmenbedingungen der Institution abhängig. Dabei spielen vorgeschriebene Speicher- und Löschfristen für Daten eine entscheidende Rolle, die sich aus verschiedenen Gesetzen und Regelungen ergeben können (siehe hierzu auch OPS.1.2.2.M1 *Ermittlung von Einflussfaktoren für die elektronische Archivierung*). Ziel der Archivierung ist es unter anderem Nachweispflichten zu erfüllen, die sich aus Compliance-Vorgaben ergeben. Die Informationserhaltung gilt beispielsweise sowohl für die Langzeitspeicherung als auch für die historische Archivierung, wobei die Beweiswerterhaltung insbesondere im Falle eines Langzeitspeichers zu berücksichtigen ist.

Welche Daten sind zu archivieren?

Von den zu archivierenden Daten hängt ab, welche technischen Anforderungen das zukünftige Archivsystem erfüllen muss. Die Eingrenzung sollte aber so allgemein erfolgen, dass ausreichend Spielraum für die technische Ausgestaltung bleibt. Dabei ist aber zu beachten, dass sich Anforderungen im Laufe der Zeit auch ändern können, z. B. im Rahmen des OAIS-Referenzmodells: Planung der digitalen Bestandserhaltung (engl. Preservation Planning). Besonders auf Managementebene sind allgemeine Charakterisierungen sinnvoll wie:

- Daten/Dokumente der Abteilung,
- Daten/Dokumente der Geschäftsprozesse,
- Geschäftsdaten,
- Buchhaltungsdaten,
- Kundendaten sowie
- Daten der Klassifikationsstufe.

Wenn Daten mit unterschiedlichem Schutzbedarf archiviert werden sollen, wird empfohlen, die Ziele und Anforderungen an die Archivierung anhand der jeweiligen Schutzbedarfskategorie zu definieren. Ein Beispiel hierfür ist die Archivierung von Daten, die als offen, intern, vertraulich etc. klassifiziert worden sind.

Welches Sicherheitsniveau soll erreicht werden?

Das zu erreichende Sicherheitsniveau bei der Archivierung lässt sich auf Managementebene typischerweise wie folgt charakterisieren:

- Erfüllung gesetzlicher sowie institutionsinterner Anforderungen an den Schutz der Daten bei der Archivierung sowie darüber hinaus (z. B. nach Entsorgung der Datenträger),
- Widerstandsfähigkeit des Archivierungsprozesses gegen Manipulation,
- Informations- und Beweiswerterhaltung der archivierten Daten,
- Widerstandsfähigkeit des verwendeten Archivsystems gegen interne und externe Angriffe auf die gespeicherten Daten sowie das IT-System selbst.

Wenn Daten und Dokumente klassifiziert werden, kann das Sicherheitsniveau auch anhand dieser Klassifikation detaillierter differenziert werden.

Welcher Funktions- und Leistungsumfang soll erreicht werden?

Der angestrebte Funktions- und Leistungsumfang elektronischer Archivierung kann je nach Institution unterschiedlich ausfallen. Üblicherweise werden auf Managementebene die folgenden Anforderungen definiert:

- Integrationsfähigkeit in die bestehende IT-Systemlandschaft,
- Integrationsfähigkeit in bestehende Prozesse,
- Einhaltung (gesetzlich sowie intern) vorgeschriebener Aufbewahrungs- und Löschfristen für Daten,
- Erfüllung der Informations- und Beweiswert-Erhaltungsaufgaben,
- Aussonderungsmodalitäten und Beachtung der Anbietungspflicht.

Dies betrifft vor allem die öffentliche Verwaltung, da öffentliche Stellen dazu verpflichtet sind, alle Unterlagen, die sie für die laufende Aufgabenerfüllung nicht mehr benötigen (i. d. R. nach Ablauf der geltenden Aufbewahrungsfrist) einem dafür zuständigen Archiv anzubieten (z. B. Übergang aus einem Langzeitspeicher, in ein historisches Archiv). Erst wenn das zuständige Archiv entscheidet, dass die entsprechenden Daten nicht archivwürdig sind oder deren Übernahme durch das zuständige Archiv erfolgt ist, dürfen diese endgültig gelöscht werden. Über die Archivwürdigkeit von Daten kann in vielen Fällen erst nach Ablauf der Aufbewahrungsfrist entschieden werden, sodass die Daten am Ende der Aufbewahrungsfrist nicht immer automatisch gelöscht werden können.

- Einhaltung des angestrebten Sicherheitsniveaus der Daten sowie
- Migrationsfähigkeit des Archivsystems sowie der archivierten Daten, wenn sich Anforderungen und Einflussfaktoren ändern, z. B. im Rahmen der OAIS: Planung der digitalen Bestandserhaltung (engl. Preservation Planning).

Wer trägt die Verantwortung?

Es müssen Mitarbeiter benannt werden, die dafür verantwortlich sind, die elektronische Archivierung aufzubauen und zu betreiben. Üblicherweise beauftragt das Management eine Fachabteilung bzw. deren Leiter mit der Umsetzung der Archivierung. Hiermit müssen auch Zielvorgaben, Befugnisse, personelle und finanzielle Ressourcen verknüpft werden. Die Delegation der Umsetzung ist entsprechend den institutionsinternen Richtlinien durchzuführen und im Archivierungskonzept zu fixieren. Es ist zu beachten, dass im Falle der Archivierung bis zum Ablauf der Aufbewahrungsfristen die zuständige Fachabteilung die Datenhoheit und damit die fachliche Verantwortung für die Archivierung besitzt.

Entwicklung des Archivierungskonzepts

Der Aufbau eines Archivsystems sollte sorgfältig konzipiert werden. Dabei sind einerseits zahlreiche Einflussfaktoren (z. B. institutionsinterne oder rechtliche Vorgaben, technische und organisatorische Umgebungsbedingungen) zu beachten, andererseits bestehen vielfältige technische Möglichkeiten, um ein elektronisches Archiv aufzubauen. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten Archivierungssystems und der entsprechenden Produkte berücksichtigt werden.

Im Archivierungskonzept ist der technische bzw. organisatorische Einsatz des Archivsystems festzulegen, also z. B.

- Zuständigkeiten und Verantwortlichkeiten,
- Definition von Benutzerrollen (z. B. Archivverwalter, Administratoren, Benutzer, technische Benutzer),
- Definition von Zugriffsrechten und Modalitäten zur Rechtevergabe,
- die notwendigen Prozesse und Funktionen,
- Auswahl der zu archivierenden Daten,
- Form und Struktur der im Archiv abzulegenden Daten,
- Schutz der archivierten Daten, z. B. indem sie verschlüsselt bzw. signiert bzw. gesiegelt bzw. zeitgestempelt werden,
- angestrebte Systemanbindung bzw. die Einsatzbedingungen für Archivierungskomponenten,
- technische Ausgestaltung des Archivsystems,
- Integration des Archivsystems in die bestehende IT-Infrastruktur sowie
- Betrieb des Archivsystems, z. B. Beschreibung von Service Level Agreements.

Die Ergebnisse sollen aktualisierbar und erweiterbar schriftlich dokumentiert werden. Das Archivierungskonzept selbst sollte in allen umgesetzten Fassungen aufbewahrt werden. Die Mitarbeiter sind über den sie betreffenden Teil des Konzepts zu unterrichten. Dies sollte nachprüfbar dokumentiert werden.

Wie sich ein Archivierungskonzept aufbauen lässt, zeigt beispielhaft das nachfolgende Inhaltsverzeichnis:

Inhaltsverzeichnis Archivierungskonzept

- **Dokumentkontext**
- Regelungsgegenstand
- Regelmäßige Anpassung
- Anordnung der Umsetzung

- **Definitionen**
- Archivierung, Dokumentenbegriff
- Langzeitspeicherung, digitales Langzeitarchiv (dLZA)
- Archivierung zu Revisionszwecken
- Beschreibung der Einsatzart und des Archivsystems
- **Gefährdungslage zur Motivation**
- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie Datenverlust, Rekonstruktionsfehler ...
- Institutionsrelevante Schadensursachen
- Beispiele zu Schadensfällen im eigenen Haus
- **Festlegung einer institutionsinternen Sicherheitsleitlinie**
- Festlegung von Verantwortlichkeiten
- Zielsetzung, Sicherheitsniveau
- **Beschreibung der Einflussfaktoren**
- Identifikation der zu archivierenden Daten
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Authentizitätsbedarf der Daten
- Verfügbarkeitsanforderungen an die Daten
- Rechtliche, fachliche und organisatorische Rahmenbedingungen
- Archivierungsfristen (minimale, bei Bedarf auch maximale Speicherdauer)
- Anforderungen an die Performance beim Einlesen bzw. Auslesen von Daten, Rekonstruktionsaufwand
- Datenvolumen sowie Änderungsvolumen
- Art der Daten (Formate)
- Art der Zugriffe auf die archivierten Daten (z. B. lokal oder verteilt im LAN bzw. WAN, SAN)
- Zu beachtende Normen und Standards
- Erforderliche Funktionalität
- Personalaufwand
- Kosten inklusive Folgekosten (Wartung, Administration, Updates etc.)
- Kenntnisse und IT-spezifische Qualifikationen der Benutzer
- **Festlegung des Einsatzes**
- Art des Archivsystems
- Einsatzbedingungen für das Archivsystem
- Zeitraum des Einsatzes (starke Abhängigkeit von rechtlich geregelten Aufbewahrungsfristen beachten)
- Definition der vom Archivsystem abzubildenden Prozesse (Ablage, Erweiterung, Abruf, Löschen etc.)
- Benennung der Verantwortlichen
- Festlegung von Service Level Agreements

- Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
- Dokumentation der Einsatzbedingungen und der Konfiguration
- Interoperabilität, Standardkonformität, Investitionsschutz
- Regelmäßige Datensicherung
- Virenschutz
- Einsatz kryptografischer Verfahren (insbesondere für die Umsetzung der Beweiswert-Erhaltung relevant, siehe [TR-ESOR])
- Definition der Form der archivierten Daten (Struktur, Format etc.)
- **Randbedingungen für die Archivierung**
- Vertragsgestaltung
- Maßnahmen der Bestandserhaltung (z. B. Refresh-Zyklen für die Speichermedien, Beobachtung der technischen Entwicklung der eingesetzten Datenformate, Produkte und Techniken)
- Bestandsverzeichnis
- Löschen von Daten
- Vernichtung von unbrauchbaren Datenträgern
- Vorhalten von arbeitsfähigen Lesegeräten

Bei der elektronischen Archivierung handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Archivierungskonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden, z. B. Planung der digitalen Bestandserhaltung (engl. Preservation Planning) gemäß dem OAIS-Modell.

OPS.1.2.2.M3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (B)

Da in Archivsystemen wichtige Behörden- bzw. Unternehmensdaten konzentriert aufbewahrt werden, müssen deren IT-Komponenten in gesicherten Räumen aufgestellt werden, die nur berechtigte Personen betreten dürfen. Dies betrifft neben den eingesetzten Servern und Netzkomponenten insbesondere die Speichereinheiten (Plattenarrays, Bandlaufwerke etc.).

Für die geeignete Aufstellung dieser IT-Komponenten sind alle relevanten Maßnahmen, die im IT-Grundschutz-Kompendium zur Infrastruktur-Sicherheit beschrieben sind, umzusetzen. Je nach Art und Größe des Speicher- oder Archivsystems sind die Bausteine INF.1 *Allgemeines Gebäude*, INF.2 *Rechenzentrum*, INF.5 *Serverraum* bzw. INF.6 *Schutzschrank* heranzuziehen. Hierbei sollte besonders darauf geachtet werden, dass die infrastrukturellen Komponenten (Stromzufuhr etc.) ausreichend zuverlässig sind. Wenn Speichersysteme eingesetzt werden, sind zudem angemessene Redundanzen in der technischen Infrastruktur zu schaffen, um die Verfügbarkeit dieser zentralen Ressourcen so gut wie möglich zu unterstützen.

Für die langfristige Aufbewahrung der verwendeten Archiv-Speichermedien sind die unten genannten Lagerbedingungen einzuhalten (siehe Abschnitt Geeignete Lagerung von Archivmedien). Vor allem die zweckmäßige Klimatisierung von Speichermedien, aber auch der Archivsysteme selbst, sind hier zu beachten.

Häufig werden elektronische Archive so realisiert, dass auf Archivmedien dauerhaft durch die Speichereinheit zugegriffen werden kann. Hierfür werden vielfach dedizierte Speichereinheiten eingesetzt, die selbsttätig Wechselmedien verwalten und einlegen können, beispielsweise Roboter für Bandlaufwerke oder Jukeboxen für Disc-Medien. Wenn ein Archivsystem solche Komponenten beinhaltet, werden meistens die Archivmedien während ihrer gesamten Lebensdauer nicht mehr aus der Speichereinheit ausgelagert. Das bedeutet, dass die an Archivmedien zu stellenden Lagerbedingungen (bezüglich Klimatisierung, Zugriffsschutz etc.) bereits in der Speicherkomponente erfüllt und überwacht werden müssen.

Wenn das Archivsystem ausgewählt wird, ist daher als Kriterium zu berücksichtigen, dass die erforderlichen Lagerbedingungen für Archivmedien in Speicherkomponenten eingehalten werden können bzw. welcher Zusatzaufwand hierfür entsteht.

Geeignete Lagerung von Archivmedien

Für den Langzeiteinsatz von Archivmedien sind besonders der Zugriffsschutz sowie klimatische Lagerbedingungen zu beachten und deren Einhaltung zu überwachen.

Sofern Archivmedien im Online-Zugriff, also im Archivsystem bzw. in Speicherlaufwerken gehalten werden, kann das Archivsystem nicht vom Archivmedium getrennt werden.

Wenn Archivmedien außerhalb des Archivsystems "offline" gelagert werden, so sind die im Baustein INF.7 *Datenträgerarchiv* beschriebenen Anforderungen unter besonderer Berücksichtigung der Anforderungen an die Klimatisierung anzuwenden.

Klimatisierung

Welche klimatischen Anforderungen erfüllt sein müssen, damit Archivmedien länger halten, hängt von den jeweils eingesetzten Archivmedien selbst ab. Hersteller geben hierzu vereinzelt unverbindliche Hinweise zu den Lagerbedingungen (z. B. hinsichtlich der Temperatur und Luftfeuchte) und zur Haltbarkeit der Medien.

Für den langfristigen Einsatz elektronischer Archivsysteme müssen die konkreten Lagerbedingungen jedoch von den Herstellern der eingesetzten Archivmedien verbindlich erfragt werden. Es sollten folgende Punkte vor der Auswahl der verwendeten Archivmedien geklärt werden (siehe auch OPS.1.2.2.M18 *Verwendung geeigneter Archivmedien*):

- Die klimatischen und physischen Lagerbedingungen für die betrachteten Archivmedien sollten seitens des Herstellers ausreichend detailliert beschrieben sein (inklusive der Auswirkungen auf die maximale Lebensdauer). Diese Angabe sollte verbindlich sein, möglichst mit einer Garantieerklärung des Herstellers bei Einhaltung der Lagerbedingungen.
- Die geeignete Lagerung technisch umzusetzen, kann unter Umständen sehr komplex sein. Je nach den vorhandenen technischen und infrastrukturellen Vorgaben können bestimmte Archivmedien auch gänzlich ungeeignet sein. Daher muss im Vorfeld geprüft werden, ob eine geeignete Lagerung mit vertretbarem Aufwand technisch überhaupt realisierbar ist.

Die Lagerbedingungen sollten im Betriebshandbuch des Archivsystems dokumentiert werden. Zusätzlich muss sichergestellt werden, dass die Lagerbedingungen kontinuierlich eingehalten und überwacht werden.

Physische Schutzmaßnahmen

Über die klimatischen Bedingungen hinaus müssen die verwendeten Archivmedien vor unautorisiertem Zugriff und mechanischer Beschädigung oder Veränderung geschützt werden. Hierzu wird insbesondere auf die im Baustein INF.7 *Datenträgerarchiv* genannten Anforderungen verwiesen.

Neben Zutrittskontrolle zum Datenträgerraum, Brandschutz und Schutz vor Wassereinwirkung sind je nach Art der verwendeten Archivmedien weitere Maßnahmen zu realisieren, z. B. zum Schutz vor Magnetfeldern. Hierfür sind verbindliche Empfehlungen von Herstellern zu mechanischen Lagerbedingungen einzuholen und zu beachten.

Wenn die Lagerbedingungen nicht eingehalten werden, ist der verantwortliche Mitarbeiter zu alarmieren. Hierzu sind Eskalationsprozeduren und -wege zu definieren.

OPS.1.2.2.M4 Konsistente Indizierung von Daten bei der Archivierung (B)

Beim Betrieb eines Archivs ist es wichtig, alle abgelegten Daten, Dokumente und Datensätze bzw. ArchivInformationsPaket (AIP) eindeutig zu referenzieren, um sie bei späteren Archivanfragen korrekt wiederfinden zu können. Zusätzlich können Archivsysteme die Suchanfragen anbieten. Da eine Volltextsuche abhängig von Art und Umfang der archivierten Daten sehr lange dauern kann, können Archivsysteme zu jedem selbsttragenden AIP einen separaten Datensatz mit Indexangaben in einer eigenen Suchdatenbank (Metadaten, vgl. auch Datenmanagement im OAIS-Modell) speichern. Struktur und Umfang der Indexangaben sind in der Regel konfigurierbar und sollten die folgenden Eigenschaften aufweisen:

- Eindeutigkeit: Die Dokumenten-/Datensatzbezeichner müssen eindeutig sein.
- Unterstützung zu erwartender Suchanfragen: Durch die Kontextangaben sollen spätere Suchanfragen beschleunigt werden. Da der spätere Suchkontext nicht feststeht, kann im Vorfeld nur eine Abschätzung späterer Suchanfragen vorgenommen und versucht werden, die Kontextangaben so aussagekräftig wie möglich zu gestalten.
- Geringer Umfang: Ein geringer Umfang an Indexdaten beschleunigt spätere Suchanfragen, jedoch kann ein zu geringer Umfang der Indexdaten Suchanfragen behindern bzw. das Auffinden von Daten erschweren. Der Umfang der Kontextangaben ist letztlich in Abhängigkeit vom erwarteten Datenvolumen festzulegen.

Diese Parameter müssen grundsätzlich vor der Inbetriebnahme des Archivs festgelegt werden. Trotzdem kann es im Laufe der Zeit notwendig werden, die Eigenschaften zu ändern. Je nach Umfang und Art der Änderung der Indexdaten kann dies eine sehr aufwändige Neuindizierung der Archivdatenbestände erforderlich machen.

Der konkrete Kontext für einzelne zu archivierende Dokument kann auf unterschiedliche Art und Weise erzeugt werden. Drei Verfahren werden dabei unterschieden:

- manuelle Erstellung: Über Eingabemasken können Indexangaben zu jedem Dokument manuell erzeugt werden. Hierdurch besteht besonders bei großen Datenmengen die Gefahr, dass inkonsistente Indexangaben erfasst werden.
- halbautomatische Erzeugung: Diese Verfahren automatisieren die Vergabe von Indexdaten, gestatten jedoch eine manuelle Kontrolle und Korrektur.
- vollautomatische Erzeugung: Hierbei werden Indizes vollautomatisch ohne manuelle Eingriffsmöglichkeit vergeben.

Die Wahl des Verfahrens ist abhängig vom erwarteten Datenvolumen. Werden in unregelmäßigen Abständen Informationen archiviert, ist ein manuelles Verfahren auf der Grundlage konkreter Vorgaben zur Erstellung eines Kontextes ausreichend.

Werden regelmäßig große Datenvolumen archiviert, sollte ein halbautomatisches Verfahren zur Erzeugung der Indexdaten gewählt werden. Hier besteht die Möglichkeit, diese Informationen manuell zu kontrollieren und zu korrigieren, bevor die Informationen und die zugehörigen Indexdaten archiviert werden und dann gegebenenfalls nicht mehr nachträglich geändert werden können.

Bei der vollautomatischen Erzeugung der Indexdaten können Fehler nicht erkannt bzw. korrigiert werden. Eine eventuelle Fehlzuordnung von zu archivierenden Daten, z. B. zu Geschäftsprozessen, kann dann nicht erkannt oder ausgeschlossen werden. Dieses Verfahren sollte deshalb nur dann angewandt werden, wenn alle Daten so strukturiert sind, dass alle Indexdaten in jedem Fall zweifelsfrei und zuverlässig extrahiert werden können.

OPS.1.2.2.M5 Regelmäßige Aufbereitung von archivierten Datenbeständen (B)

Für eine ordnungsgemäße Archivierung muss über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das benutzte Datenformat dem Stand der Technik entspricht und von den benutzten Anwendungen derzeit und zukünftig verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar sind und unter Beibehaltung der Semantik und des Beweiswerts reproduziert werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können,

- die verwendeten kryptografischen Verfahren zur Bewahrung des Beweiswertes kryptografisch signierter Dokumente und/oder der Vertraulichkeit verschlüsselter Dokumente dem Stand der Technik entsprechen und
- für alle Komponenten der Speichereinheit (Speichermedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

Ist abzusehen, dass eine der geforderten Eigenschaften in naher Zukunft nicht mehr gegeben ist, müssen die betroffenen Systeme ausgetauscht werden. Dabei ist zu berücksichtigen, dass unter Umständen eine erhebliche Menge an archivierten Daten migriert werden muss.

Die Transformation auf aktuelle Datenformate und die Migration auf neuere Speichermedien, IT-Hardware oder IT-Software wird in OPS.1.2.2.M16 *Regelmäßige Erneuerung technischer Archivsystem-Komponenten* beschrieben.

Wie sich verschlüsselte oder signierte Dokumente aufbereiten lassen, wird in OPS.1.2.2.M15 *Regelmäßige Aufbereitung von kryptographisch gesicherten Daten bei der Archivierung* und OPS.1.2.2.M20 *Geeigneter Einsatz kryptographischer Verfahren bei der Archivierung* erläutert.

OPS.1.2.2.M6 Schutz der Integrität der Indexdatenbank von Archivsystemen (B)

Die Indexdatenbank ist besonders wichtig, damit ein Archivsystem korrekt funktioniert. In ihr sind die Verweise auf sämtliche archivierten Dokumente bzw. ArchivInformationsPakete (AIP) abgelegt. Fehlende oder beschädigte Einträge in der Indexdatenbank können dazu führen, dass archivierte Dokumente nicht oder nur sehr schwer wiedergefunden und Geschäftsvorgängen zugeordnet werden können. Daher muss für einen ordnungsgemäßen Archivbetrieb die Integrität der Indexdatenbank sichergestellt werden und überprüfbar sein. Zur Integritätssicherung sind folgende Empfehlungen zu berücksichtigen:

Redundante Ablage der Indexeinträge

Abhängig von der Archivgröße sind folgende Abstufungen vorzusehen:

- Bei kleinen Archiven mit geringem Datenaufkommen und geringen Anforderungen an die Antwortzeiten ist es ausreichend, eine tägliche Datensicherung der Indexdatenbank vorzunehmen. Die Datensicherung sollte gemäß Baustein OPS.1.1.6 *Datensicherung* vorgenommen werden.
- Bei Archiven mit hohem Datenaufkommen sowie hohen Anforderungen an die Antwortzeit sollte die Indexdatenbank selbst redundant ausgelegt, d. h. gespiegelt sein. Auch hier ist zusätzlich eine tägliche Datensicherung durchzuführen. Die gespiegelten Teil-Datenbanken sollten in unterschiedlichen Brandabschnitten aufgestellt sein.

Regelmäßige Integritätsprüfung

Die Indexdatenbank sollte regelmäßig (mindestens wöchentlich, bei großen Archiven täglich) geprüft werden, ob sie konsistent und integer ist, z. B. indem Prüfsummen benutzt werden. Alle in der Indexdatenbank referenzierten Dokumente bzw. ArchivInformationsPaket (AIP) müssen auf den Archivmedien auffindbar sein. Integritätsverletzungen müssen dokumentiert und zeitnah behoben werden.

In regelmäßigen Abständen (z. B. monatlich) sollte zudem geprüft werden, ob die Datensicherungen der Indexdatenbank lesbar und wiederverwendbar sind. Bei redundant ausgelegten Datenbanken sollte getestet werden, ob die Funktionsübergabe noch ordnungsgemäß funktioniert, wenn ein Teil ausfällt.

Alle Ergebnisse der regelmäßigen Integritätsprüfung sollten ebenfalls archiviert werden, damit Datenänderungen später nachvollzogen werden können.

OPS.1.2.2.M7 Regelmäßige Datensicherung der System- und Archivdaten (B)

Elektronische Archivsysteme unterliegen denselben Risiken hinsichtlich eines Datenverlustes wie andere IT-Systeme auch. Die Auswahl geeigneter Datenträger allein bietet keinen ausreichenden Schutz vor Verlust, beispielsweise bei Zerstörung oder Diebstahl des Archivmediums selbst.

Eine redundante Speicherung der Archivdaten, der zugehörigen Indexdatenbank und der Systemdaten ist daher unerlässlich. Für die Datensicherung ist grundsätzlich die im Baustein OPS.1.1.6 *Datensicherung* beschrieben Vorgehensweise zu verwenden.

Alternativ zu einer Datensicherung der Archivdaten können diese auch redundant auf physisch getrennten und in unterschiedlichen Brandabschnitten aufgestellten Archivsystemen gespeichert werden. Einige Hersteller von Archivsystemen bieten hierzu Hochverfügbarkeitslösungen an. Trotzdem muss auch in diesem Fall die Daten des Archivsystems selbst sowie die Indexdatenbank gesichert werden.

Wenn Datensicherungen wieder in das Archivsystem eingespielt werden, ist zu überprüfen, ob dadurch Datenverluste aufgetreten sind, also ob zu archivierende Daten erneut erfasst werden müssen. Außerdem muss kontrolliert werden, ob für die wieder eingespielten Daten Löschvermerke vorliegen, die berücksichtigt werden müssen.

OPS.1.2.2.M8 Protokollierung der Archivzugriffe (B)

Die Zugriffe auf elektronische Archive sind zu protokollieren. Hierdurch soll ermöglicht werden, alle Aktivitäten nachvollziehen und eventuelle Fehler korrigieren zu können. Die folgende Aufzählung gibt einen Überblick darüber, welche Arten von Ereignissen mithilfe der Protokollierung erkannt werden können:

- Vertraulichkeits- bzw. Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ausschalten des Servers im laufenden Betrieb,
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen,
- defekte Datenträger,
- Verlust gespeicherter Daten,
- Datenverlust bei erschöpftem Speichermedium,
- Manipulation an Daten oder Software,
- unberechtigtes Kopieren der Datenträger,
- Manipulation eines Kryptomoduls,
- Kompromittierung kryptografischer Schlüssel und
- unberechtigtes Überschreiben oder Löschen von Archivmedien.

Der Umfang der Protokollierung richtet sich einerseits nach den Anforderungen an die Nachvollziehbarkeit und Authentizität der in Archiven gespeicherten Daten. Andererseits müssen auch die institutionsintern abgestimmten Regelungen beachtet werden, z. B. zum Datenschutz.

Sofern möglich, sollten mindestens folgende Daten protokolliert werden:

- Datum und Uhrzeit des Zugriffs,
- Clientsystem, von dem aus zugegriffen wurde,
- Archivbenutzer und ausgeübte Benutzerrolle,
- ausgeführte Aktionen sowie
- eventuelle Fehlermeldungen und -codes.

Im Archivierungskonzept ist festzulegen, wie lange die Protokolldaten aufbewahrt werden sollen. Eventuell können die Protokolldaten mit archiviert werden.

Die Protokolldaten müssen unter Beachtung interner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist. Solche Vorfälle sollten umgehend signalisiert werden, z. B. indem

vorhandene Systemmanagement-Umgebungen genutzt werden. Außerdem ist es wichtig, dass die Benachrichtigung rollenbezogen und nicht personenbezogen erfolgt. Wird beispielsweise eine E-Mail an eine konkrete Person geschickt, bleibt die Nachricht eventuell unbeachtet, wenn diese Person nicht anwesend ist.

Folgende Ereignisse weisen bei der Archivierung typischerweise eine hohe Kritikalität auf und sollten daher permanent protokolliert, überwacht und umgehend signalisiert werden:

- Kopieren von Archivmedien,
- Kopieren von Archivsystem-Datenträgern,
- Löschen oder Löschmarkierung von Datensätzen,
- Offline-Schaltung von Archivmedien in Archivsystemen,
- Entnahme von Archivmedien aus dem Archivsystem,
- Einlegen von Archivmedien,
- Online-Schalten von Archivmedien,
- Fehler oder Probleme beim Zugriff auf das Archiv,
- Systemfehler und Timeouts,
- Katastrophenszenarien (Brand, unzulässige Temperatur, Wasser etc.), die in der Regel durch externe Sensorik gemeldet werden.

Nachdem ein Ereignis signalisiert wurde, sollte es sofort geprüft und gegebenenfalls weiter eskaliert werden. Typischerweise erfolgt eine erste Eskalation an den Leiter IT. Es können aber auch andere Eskalationsprozesse vorgesehen werden.

OPS.1.2.2.M9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (B)

Grundsätzlich können in den Archiven Dokumente jeglicher Art abgelegt werden, z. B. DOCX, RTF, XLSX, ZIP. Um allerdings langzeitgespeicherte Dokumente wirtschaftlich sinnvoll erhalten zu können, sollten sie in ein geeignetes Format (siehe z. B. [TR-ESOR-F]) überführt werden.

Für herkömmliche Textdokumente empfiehlt es sich, diese in einen passenden Standard der PDF/A-Formatfamilie umzuwandeln. Für spezifische Formate, für die das nicht möglich oder sinnvoll ist, sollte geprüft werden, welche alternativen langzeitspeicherfähigen Formate infrage kommen. Um diese Dokumente zu erhalten, muss jedoch regelmäßig geprüft werden, ob sie noch lesbar sind. Ist das nicht der Fall bzw. zeichnet sich das ab, müssen sie in neuere Formate konvertiert werden.

Für die langfristige Archivierung elektronischer Dokumente (nachhaltige Verfügbarkeit, maschinelle Lesbarkeit und Verfügbarkeit) müssen geeignete Datenformate gewählt werden. Das Datenformat sollte langfristig eine originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums (z. B. Papierformat, Farben, Logos, Seitenzahl, Wasserzeichen, Unterschrift) ermöglichen. Die derzeit verwendeten Datenformate sind hierfür unterschiedlich geeignet, ihre Eignung hängt sehr stark vom Einsatzzweck der archivierten Daten und ihren Ursprungsmedien ab. Bei einem Wechsel des Medien- und Datenformats können jedoch in der Regel nicht alle Strukturmerkmale des Ursprungsmediums gleichzeitig abgebildet werden.

Da im Vorfeld meist nicht absehbar ist, welche Merkmale des Originaldokuments bei einer späteren Reproduktion nachgewiesen werden sollen und mit welchem Beweiswert dies erfolgen soll, werden Dokumente typischerweise in mehreren elektronischen Datenformaten gleichzeitig archiviert. Dadurch soll eine möglichst hohe Überdeckung der Merkmale des Originaldokuments erreicht werden.

Für die Wahl geeigneter Datenformate sind folgende Kriterien maßgeblich:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- die Dokumentstruktur sollte eindeutig interpretiert werden können,

- der Dokumentinhalt sollte elektronisch weiterverarbeitet werden können,
- die gesetzlichen Vorschriften sollten beachtet werden,
- die Grammatik und Semantik des Datenformates muss ausführlich dokumentiert sein, sodass später problemlos migriert werden kann,
- Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Typischerweise wird neben einer strukturellen Repräsentation (in einer Strukturbeschreibungssprache) bei Papierdokumenten auch eine grafische Repräsentation des Dokuments (Digitalisierung) archiviert. Hinzu kommen unter Umständen elektronische Signaturen Wahrung von Authentizität und Integrität

In den folgenden Abschnitten werden typische Datenformate beschrieben und diskutiert, ob sie sich für die elektronische Archivierung eignen. Die Liste der Formate ist nicht als abgeschlossen zu betrachten. Entsprechend der Anforderungen eines einzelnen Archivs kann die Liste erweitert werden.

A. Metadaten

XML

Die Extensible Markup Language (XML) wurde als Nachfolger des Standards SGML (Standard Generalized Markup Language) entwickelt und enthielt ursprünglich eine Teilmenge des Sprachumfangs von SGML. Wichtige Merkmale von XML sind:

- In XML können Tags und Attribute neu definiert werden. Hierdurch können Anpassungen an der Syntax und Semantik der Beschreibungselemente vorgenommen werden.
- Analog zu HTML können Links in die Dokumentenstruktur integriert werden. Somit können auf einfache Art und Weise bestehende Dokumente referenziert und z. B. Bilder in Dokumente eingebunden werden.
- XML kann direkt in Webbrowsern angezeigt werden. Zur Darstellung wird eine separate Definition des Layouts in Form der Beschreibungssprache XSL (Extensible Stylesheet Language) benötigt.

XML kann in manchen Fällen als Format für die Langzeitspeicherung von elektronischen Dokumenten genutzt werden (z. B. SIARD-Format für die Aufbewahrung von relationalen Datenbanken). Bei der Archivierung sind jedoch unbedingt auch die Semantikspezifikation (DTD, Document Type Definition) bzw. das XML-Schema und eventuell auch die Layout-Informationen (in XSL beschrieben) zu archivieren.

XML wird häufig benutzt, um Metadaten (z. B. die Formate PREMIS oder Dublin Core) aufzubewahren und um einzelne (selbsttragende) Informationspakete (z. B. in Anlage TR -ESOR-F spezifizierte XAIP für ein selbsttragendes XML-basierten Archivinformationspaket) aufzubauen.

XML-Schema (XSD)

Mithilfe von XML-Schema kann die Struktur von XML-Dokumenten definiert werden. Hierfür werden formelle Regeln und Beschränkungen vorgegeben, die auf beliebige XML-Dokumente (Instanzen) angewandt werden, deren Zugehörigkeit zu einer bestimmten Klasse der XML-Dokumente geprüft werden kann. Diese Prüfung wird Validierung genannt und im Erfolgsfall bestätigt sie, ob ein XML-Dokument gegenüber einem vorgegebenen XML-Schema syntaktisch korrekt ist.

Im Umfeld der Archivierung werden entsprechende Schemata beispielsweise in folgenden Anwendungsbereichen benutzt:

- Definition der Struktur Archivinformationspakete, z. B. XAIP (vgl. Anhang [TR-ESOR-F]),
- Definition der Struktur der Metadaten, z. B. xDomea, SIARD, xBarch (vgl. hierzu auch [TR-ESOR-F]),
- Definition der bestimmten Formate für elektronische Signaturen, z. B. XAdES,
- Definition der beliebigen zu archivierenden Inhalte.

B. Inhaltsdaten – Dokumente

Text (ASCII)

Ein Textdokument, das ausschließlich mithilfe des ASCII-Zeichensatzes kodiert wurde, kann nur rudimentäre Layoutinformationen beinhalten. Solche Dokumente sind somit nur für einfache Information oder Metadaten geeignet. Der 7-Bit-ASCII-Code wurde 1972 von ISO unter 646 spezifiziert und bietet eine solide Grundlage für eine langfristige Verkehrsfähigkeit der Daten.

Eine Weiterentwicklung des ASCII-Codes war der 8-Bit-ASCII-Code, der zusätzlich zu den 7-Bit-ASCII-Zeichen einige Sonderzeichen enthält, z. B. Umlaute für die deutsche Sprache. Eine weitere Stufe ist der Unicode-Standard, der entsprechend auf 8-Bit (UTF-8), 16-Bit (UTF-16) oder 32-Bit (UTF-32) pro Zeichencode basiert, nun aber stets 7-Bit-ASCII-Code als erste 128-Zeichen beinhaltet.

PDF und PDF/A

Das Portable Document Format (PDF) ist ein Dokumentformat, bei dem neben der Strukturinformation von elektronischen Dokumenten auch wesentliche Layoutinformationen mitgespeichert werden. PDF wurde von der Firma Adobe auf Basis des Datenformats PostScript entwickelt.

Das Erscheinungsbild wird dabei durch einen Datenstrom beschrieben, der eine Reihe von grafischen Objekten enthält. Durch diese Beschreibung ist ein Dokument vollkommen festgelegt. Die Entscheidung über das Erscheinungsbild wird dabei zum Zeitpunkt der Erstellung des Dokuments getroffen und ist dann fixiert. Gegenüber einer rein bildlichen Darstellung (Pixeldarstellung) benötigen PDF-Dokumente meist deutlich weniger Speicherplatz.

Zielsetzung beim Einsatz von PDF ist es, das Erscheinungsbild eines elektronischen Dokuments unabhängig von der zur Erstellung benutzten Software, der Hardware-Plattform oder dem Betriebssystem zu bewahren. PDF eignet sich daher primär für die Archivierung von Dokumenten, bei denen eine Abbildung in Papierform vorgesehen ist bzw. die den Charakter von Briefen und Geschäftsdokumenten haben.

Speziell für die Anforderungen der Langzeitspeicherung wurde mit PDF/A eine Version von PDF als ISO 19005-1:2005 genormt. PDF/A (A steht hier für Archivierung) definiert eine stabile Untermenge von PDF, mit der zu archivierende Dokumente so beschrieben werden können, dass alle erforderlichen Informationen in der Datei selber enthalten sind und zwar vollständig, eindeutig, zugänglich und erschließbar.

PDF/A kann als Format für die Langzeitspeicherung von elektronischen Dokumenten genutzt werden. Hierbei ist die Konformität der Dokumente zur PDF/A-Spezifikation zu überprüfen.

Mithilfe von PDF/A-3-Container lassen sich beliebige binäre Daten in einem Zusammenhang aufbewahren. Dadurch ist dieses Format eventuell eine Alternative für die Implementierung von Archivdatenpaketen.

ODF

Die Organization for the Advancement of Structured Information Standards (OASIS) hatte das Open Document Format (ODF) als ein XML-basiertes Dokumentenformat für die Verwendung in Büroanwendungen zur Abbildung von Texten (mit Layout), Tabellenkalkulationen, Präsentationen und weiteren Dokumenten standardisiert. Der Inhalt und das Layout der Dokumente sind dabei strikt voneinander getrennt.

ODF eignet sich relativ gut, um komplexe Dokumente auszutauschen, die weiterbearbeitet werden sollen. Für eine langfristige Aufbewahrung von finalen Dokumentenbeständen wird jedoch eher PDF/A-Format empfohlen.

Office Open XML Formats (OO-XML)

Die Office Open XML File Formats beschreibt eine Sammlung von Office-Formaten, die analoge Anwendungsbereiche, wie das oben genannte ODF, abdecken. Ursprünglich wurden die XML-basierten Formate durch die Firma Microsoft entwickelt und im Rahmen einer ECMA- sowie ISO-Standardisierung offen gelegt.

Das OO-XML wird insbesondere durch die einzelnen Produkte der Office-Suite von Microsoft als Ablageformat für Daten verwendet. Ähnlich wie bei ODF eignet sich OO-XML dafür, Dokumente

auszutauschen, die weiterbearbeitet werden sollen. Für die langfristige Aufbewahrung der finalen Dokumente wird jedoch eher PDF/A empfohlen.

TIFF

Das Format TIFF (Tagged Image File Format) wird zur Speicherung gerasterter Bilder verwendet. Eine TIFF-Datei besteht aus einem Datei-Header und der Bildinformation. Der Header enthält sogenannte Tags, in denen Eigenschaften des aufgezeichneten Bildes gespeichert sind, z. B. Auflösung oder verwendete Kompressionsverfahren. Wichtige Merkmale von TIFF sind:

- Bildinformationen können sowohl in Schwarz/Weiß als auch in Grauabstufungen verlustfrei gespeichert werden, jedoch nur dann, wenn eine Farbtiefe von 24-Bit (Truecolor) gewählt wird. Nur in dieser Stufe können alle Graustufen wiedergegeben werden. Um Farbinformationen originalgetreu aufzunehmen und zu speichern, ist jedoch eine regelmäßige Feineinstellung der optischen Sensoren notwendig, damit die Farbinformation nicht durch Farbverschiebungen verfälscht werden. Dies kann z. B. durch einen Farbabgleich mit Weiß als Referenzfarbe erfolgen.
- Alle gängigen Grafik- und Präsentationsprogramme unterstützen das TIFF-Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Faxgeräte benutzen TIFF als gängiges Datenformat.
- Die Bilddaten können komprimiert abgespeichert werden. TIFF ist mit den meisten Kompressionsverfahren kompatibel. Zwei der wichtigsten Kompressionsverfahren werden hier kurz angesprochen:
- ITU/CCITT - Gruppe 4: Die ITU-Kompression benutzt TIFF als Eingangsformat. Dabei wird bei normalen Textdokumenten ein Kompressionsfaktor von etwa 1:40 erreicht. Es ist damit ideal geeignet für Schwarz/Weiß-Dokumente. Die Kompression ist verlustfrei. Die ITU-Kompression ist im Bereich der Archivierung weltweit standardisiert.

TIFF ist sowohl in komprimierter als auch in unkomprimierter Form als Format für die Langzeitspeicherung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Es wird empfohlen, ein verlustfreies Kompressionsverfahren zu verwenden, z. B. ITU/CCITT-Gruppe 4, um den benötigten Speicherbedarf zu minimieren.

JPEG

JPEG wurde von der Joint Photographic Experts Group entwickelt und eignet sich besonders für Farb- und Grauwertbilder. In diesem Bereich ist die JPEG-Kompression auch effektiver als die ITU-Gruppe-4-Kompression.

JPEG kann anhand einiger Parameter unterschiedlich konfiguriert werden. Je nach Einstellung werden dann unterschiedliche Kompressionsraten erreicht. Allerdings können auch Verluste auftreten. Wichtige Merkmale von JPEG sind:

- Alle gängigen Grafik- und Präsentationsprogramme unterstützen das Format JPEG.
- Die Konvertierung in JPEG ist in einigen Kompressionsstufen verlustbehaftet, es können dann zugunsten einer geringen Dateigröße wesentliche Bildinformationen verloren gehen.

JPEG ist als Format für die Langzeitspeicherung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Für eine revisionssichere Archivierung wird empfohlen, bei der Auswahl der Kompressionsstufe eine verlustfreie Kompression zu wählen, z. B. JPEG 2000 Part 6.

PNG

Das Portable Network Graphics Format (PNG) eignet sich aufgrund der Möglichkeiten der verlustfreien Kompression und inkrementellen Anzeige der Grafiken insbesondere für die Anwendung im Internet. Das PNG-Format wurde offen gelegt und ist durch ISO standardisiert (vgl. ISO/IEC 15948).

Da sogenannte Kalibrierungsinformationen innerhalb der PNG codierten Bilder untergebracht werden können und das Format standardmäßig von allen gängigen Bildverarbeitungsprogrammen unterstützt wird, ist PNG für die Archivierung geeignet.

C. Audio- und Video-Formate

Bei der digitalen Verarbeitung von Audio- und Videodaten entstehen schon bei zeitlich kurzen Aufzeichnungen sehr große Datenmengen. Daher ist eine effektive Kompression wichtig.

Verlustfreie Kompressionsverfahren für Audio- und Videodaten erreichen derzeit jedoch nur Kompressionsraten von etwa 2:1. Gebräuchlicher sind Verfahren, die eine Kompressionsrate bis zu 200:1 erreichen, jedoch nicht verlustfrei arbeiten. Der durch die Kompression entstehende, teilweise erhebliche Datenverlust wird typischerweise akzeptiert, solange er mit dem menschlichen Auge bzw. Ohr nicht wahrnehmbar ist bzw. nicht als störend empfunden wird.

Die Eignung verlustbehafteter Kompressionsverfahren für die Archivierung von Video- und Tonmaterial ist anwendungsspezifisch zu prüfen.

Im Folgenden werden einige typische Formate vorgestellt:

MPEG, insbesondere MPEG-4 Part 14

Innerhalb der ISO ist die Motion Pictures Expert Group (MPEG) für die Bearbeitung weltweiter Standards zur Kompression digitalisierter Bewegtbilder verantwortlich. Derzeit sind drei verschiedene Verfahren bekannt:

- MPEG1: Dieses Format gibt es in drei verschiedenen Layern. Layer 3 ist in der Kurzform MP3 bekannt und als Kompression für Audiodaten verbreitet.
- MPEG2: Dieses Format ist derzeit für die Speicherung von Videodaten auf DVD in Gebrauch und als Standard akzeptiert.
- MPEG4 (MP4): Dieses Format definiert ein Containerformat für die Ablage von Multimedia-Dateien.
- MPEG-7 (ISO/IEC 15938): Dieses Format dient nicht zur Kompression von Audio- und Videodateien, sondern zur Organisation multimedialer Daten.

Insbesondere das MP4-Format in den standardisierten Teilen 12 und 14 (vgl. ISO/IEC 14496-12 und -14) bietet sich als ein für die Archivierung geeignetes Audio- bzw. Videoformat an.

OGG Encapsulation Format

Das in RFC3533 spezifizierte Containerformat für die Multimedia-Dateien OGG ist eine bekannte und verbreitete Methode, Audio- und Video-Informationen zu speichern. Es handelt sich hier um ein von Softwarepatenten freies und unbeschränktes Format, das zusammen mit einem zur Verfügung stehenden Codecs (z. B. Vorbis, FLAC oder Theora) sehr gut für die Archivierung geeignet ist.

AAC

Eine weitere Alternative für die Langzeitspeicherung von Audio-Dateien bietet Advanced Audio Coding (AAC). AAC ist durch die ISO standardisiert worden (vgl. ISO/IEC 13818-7) und ist auch Teil der MPEG-2- und MPEG-4-Spezifikation. Das Format selbst ist frei von Patenten, jedoch müssen Lizenzgebühren durch die Hersteller eines AAC-Codecs entrichtet werden. AAC kann als eine durchaus geeignete Alternative für die Archivierung betrachtet werden.

WAVE

Audiodaten werden üblicherweise mit Hilfe der Linear Pulse Code Modulation (LPCM) codiert. In diesem Fall werden die einzelnen Sequenzen jeweils separat in Intervallen gespeichert. LPCM wird sinnvollerweise im Waveform Audio File Format (WAVE) gespeichert. Die WAVE-Spezifikation beschreibt eine unbegrenzte Anzahl an Datenblöcken, die sowohl den Content selbst als auch die Metadaten beinhalten. WAVE ermöglicht die unkomprimierte Speicherung von Audiodaten und sollte für die Aufbewahrung digitalen Master von Audioaufzeichnungen verwendet werden. Daneben ist das Format WAVE frei verfügbar.

AVI

Um digitale Videodaten abzulegen sind verschiedene Elemente zu betrachten: visuelle Daten, Audiodaten, Untertitel oder Verweise auf externe Untertitel sowie Metadaten die für die korrekte Wiedergabe des Videos erforderlich sind. Konsequenterweise muss das Archivsystem Funktionen beinhalten, die nicht nur das Containerformat selbst erkennen, sondern auch alle Format der enthaltenen Dateien selbst. AVI ist ein

solches Format. Es wurde von Microsoft und IBM entwickelt, die Dokumentation ist jedoch vollständig offen und nutzbar.

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Archivierung.

OPS.1.2.2.M10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen (S)

Durch eine Richtlinie mit entsprechenden Regelungen ist sicherzustellen, dass das Archivsystem so benutzt wird, wie es im Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) vorgesehenen ist. Hierzu sollten Richtlinien für die Benutzung und die Administration des Archivsystems erstellt werden. Die Richtlinien sind entsprechend den institutionsinternen Gepflogenheiten zu verankern und bekanntzugeben. Wenn externe Personen das Archivsystem benutzen sollen, müssen sie dazu verpflichtet werden, die Richtlinien zu beachten.

Die Administrationsrichtlinien sollten mindestens die folgenden Punkte umfassen:

- Festlegung der Rollen und Verantwortlichkeiten für Betrieb und Administration des Archivsystems,
- Vereinbarungen über Leistungsparameter (Service Level Agreements) beim Betrieb des Archivsystems, insbesondere wenn die Administration oder der Betrieb durch Externe erfolgen soll,
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten zu den Komponenten des Archivsystems und den Archivmedien,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen für das Archivsystem und die verwendeten Archivmedien,
- Regelung zur Datensicherung der Software-Komponenten des Archivsystems selbst,
- Protokollierung der Aktivitäten am Archivsystem.

Die Benutzerrichtlinien sollten mindestens umfassen:

- Erläuterung der Zielsetzung der elektronischen Archivierung und der Aufbewahrungsfristen für Daten,
- Festlegung der Rollen und Verantwortlichkeiten für Arbeiten mit dem Archivsystem,
- Festlegung, in welchem Umfang die Nutzung des Archivsystems verpflichtend ist,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Schulungsanforderungen an Benutzer, damit sie zur Nutzung des Archivsystems freigeschaltet werden dürfen,
- Regelung der Vergabe von Kontextinformationen zu den archivierten Daten (siehe auch OPS.1.2.2.M4 *Konsistente Indizierung von Daten bei der Archivierung)*,
- Verpflichtung zum sorgfältigen Umgang mit recherchierten Daten unter Beachtung der eventuellen Zweckbindung der Informationen,
- Regelung zum Umgang mit Daten nach Ablauf der festgelegten Archivierungsdauer,
- Regelung, dass Daten, deren Löschung nach einem festgelegten Zeitraum vorgesehen ist, nicht mehr verwendet werden dürfen, obwohl sie unter Umständen aus technischen Gründen noch vorhanden sind,
- Regelung zum Umgang mit personenbezogenen Daten,
- Nutzung der vom Archivsystem bereitgestellten Schutzmechanismen, um eine spätere Prüfung der Integrität und Authentizität der archivierten Daten zu ermöglichen, sowie zur Gewährleistung der erforderlichen Vertraulichkeit,
- Gewährleistung der Verkehrsfähigkeit der archivierten Daten,

- Verpflichtung zur Überprüfung der Integrität und Authentizität recherchierter Daten vor der Weiterverwendung,
- Umgang mit Daten, deren Integrität oder Authentizität sich nicht nachweisen lässt, z. B. bei fehlgeschlagener Signaturprüfung,
- Protokollierung der Benutzeraktivitäten am Archivsystem,
- Abrechnungsmodalitäten bei Nutzung des Archivsystems durch mehrere Organisationseinheiten.

Die Regelungen sowie deren Kenntnisnahme durch die Administratoren und Benutzer des Archivsystems sind zu dokumentieren.

OPS.1.2.2.M11 Einweisung in die Administration und Bedienung des Archivsystems (S)

Um ein Archivsystem korrekt und sicher administrieren zu können, müssen sich die Verantwortlichen und hier vor allem die Administratoren und Archivverwalter mit den eingesetzten Systemen auskennen. Hierfür ist eine Schulung der verantwortlichen Archivverwalter und Administratoren notwendig. Dadurch sollen Konfigurationsfehler und Fehlverhalten vermieden werden. Die Schulung sollte mindestens folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems, Handhabung der verwendeten Archivmedien und Kennzeichnung der Archivmedien,
- Einsatzbedingungen des Archivsystems und der Archivmedien (Klimatisierung etc.),
- Dokumentation der Administrationstätigkeiten,
- Protokollierung der Systemereignisse am Archivsystem,
- Vorgehensweise bei der Definition von Regeln/Prozeduren für die Prozesse des Archivsystems
- Vorgehensweise zur Konfiguration des Archivsystems (soweit dies nicht der Hersteller vornimmt)
- Vorgehensweise bei der Auffrischung von Datenbeständen (siehe OPS.1.2.2.M5 *Regelmäßige Aufbereitung von archivierten Datenbeständen* und OPS.1.2.2.M15 *Regelmäßige Aufbereitung kryptographisch gesicherter Daten bei der Archivierung*),
- Grundbegriffe von Verschlüsselung und digitaler Signatur, wenn kryptografische Verfahren verwendet werden,
- Vorgehensweise bei der Vernichtung ausgesonderter Archivmedien,
- Systemüberwachung und Wartung des Archivsystems,
- Eskalationsprozeduren, z. B. bei Nichteinhaltung von Reaktionszeiten, Unterschreiten der Rest-Speicherkapazität der Archivmedien, Manipulation oder Sabotage des Archivsystems oder Ereignissen höherer Gewalt sowie unberechtigten Zugriffen.

Die Schulung der Administratoren und Archivverwalter ist zu dokumentieren. Bei Systemänderungen sollten sie entsprechend weitergebildet werden.

Einweisung der Benutzer in die Bedienung des Archivsystems

Die Archivierung ist eine besonders verantwortungsvolle Aufgabe und stellt hohe Anforderungen an die Bedienung. Die dafür vorgesehenen Mitarbeiter sind auf diese Verantwortung besonders hinzuweisen und vorzubereiten. Hierzu müssen die Benutzer entsprechend geschult werden. Eine derartige Schulung sollte unter anderem folgende Themen umfassen:

- Vorgehensweise bei der Umwandlung analoger Daten: Die korrekte Vorgehensweise bei der Erfassung der Dokumente, der Umwandlung in die elektronische Form sowie der elektronischen Archivierung sind zu erläutern und anhand von praktischen Beispielen zu üben.
- Korrekte Nutzung der Prozesse des Archivsystems (Ablage, Änderung, Abruf, Löschen etc.)
- Vorgehensweise zur digitalen Bestandserhaltung
- Rechtliche Rahmenbedingungen der Archivierung: Bei der Archivierung sind rechtliche Anforderungen einzuhalten (siehe OPS.1.2.2.M1 *Ermittlung von Einflussfaktoren für die elektronische Archivierung)*. Diese Anforderungen und die Folgen, wenn sie nicht eingehalten werden, müssen den Benutzern deutlich gemacht werden.
- Schutz der Vertraulichkeit und Integrität der Dokumente: Die korrekte Vorgehensweise bei der Behandlung vertraulicher Informationen sowie bei der Integritätssicherung und -prüfung archivierter Daten ist zu demonstrieren. Auf mögliche Folgen bei fehlerhafter Bedienung ist hinzuweisen.
- Institutionsspezifische Sicherheitsrichtlinien und ihre Anwendung bei der elektronischen Archivierung: Bei der Konzeption des Archivsystems sind üblicherweise diverse Sicherheitsmaßnahmen vorgesehen worden, die von den einzelnen Benutzern des Archivsystems umgesetzt werden müssen. Dies kann z. B. die Art der Kennzeichnung der Archivmedien oder auch den Umgang mit als vertraulich oder anderweitig klassifizierten Informationen betreffen. Alle Benutzer müssen auf diese Sicherheitsrichtlinien hingewiesen werden.

Die Schulung der Mitarbeiter ist zu dokumentieren. Bei Systemänderungen sollten sie entsprechend weitergebildet werden.

OPS.1.2.2.M12 Überwachung der Speicherressourcen von Archivmedien (S)

Die auf den Archivmedien vorhandene, freie Speicherkapazität ist kontinuierlich zu überwachen. Wenn die freie Speicherkapazität unter einen festzulegenden Schwellwert sinkt, sollte der Administrator benachrichtigt werden. Gegebenenfalls sollte an die Systemmanagement-Umgebung signalisiert werden, dass der Schwellenwert erreicht wurde. Sinkt die freie Speicherkapazität weiter unter einen kritischen Grenzwert, sollte alarmiert werden. Dabei ist besonders darauf zu achten, dass sie rollenbezogen erfolgt, das heißt unabhängig von konkreten Personen. Damit ist sichergestellt, dass sie auch im Krankheitsfall oder bei Urlaub wahrgenommen wird.

Der Schwellwert, der kritische Grenzwert sowie die Eskalationsprozeduren und -wege sind institutionsspezifisch festzulegen.

Die Grenzwerte müssen anhand der verwendeten Archivmedien und des durchschnittlichen Volumens der zu archivierenden Daten bestimmt werden. Nachdem der kritische Alarm ausgelöst wurde, sollte gewährleistet sein, dass für eine hinreichende Zeit weiterhin das durchschnittliche Datenaufkommen archiviert werden kann. Typischerweise wird für den Schwellwert eine Restkapazität von 15 % der Gesamtkapazität des Speichermediums und für den kritischen Grenzwert eine Restkapazität von 10 % zugrunde gelegt.

Um etwaige Lieferengpässe bei Speichermedien zu überbrücken, sollte eine ausreichende Zahl leerer Archivmedien an einem bekannten Ort gelagert werden. Dabei müssen die klimatischen und physischen Lagerbedingungen eingehalten werden (siehe OPS.1.2.2.M3 *Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien*).

Für den Fall der Alarmierung ist zu dokumentieren, in welcher Weise und in welchem Zeitraum auf die Alarme reagiert werden soll. Das ist z. B. in Service Level Agreements (SLAs) festzulegen, falls der Betrieb des Archivsystems durch Dritte erfolgt.

Neben dem Speicherplatz müssen eventuell noch betriebssystem- oder anwendungsspezifische Restriktionen überwacht werden. Die entsprechenden Programmdokumentationen müssen daraufhin geprüft werden. In Zweifelsfällen oder bei fehlenden Angaben in der Dokumentation sollte der jeweilige Hersteller befragt werden. Beispielsweise können die Anzahl der maximal zugelassenen Dateien pro

Verzeichnis oder die maximal erlaubten Datenbankeinträge überschritten werden, sodass keine weiteren Dateien auf dem Speichermedium angelegt werden können.

OPS.1.2.2.M13 Regelmäßige Revision der Archivierungsprozesse (S)

Die Archivierungsprozesse (vgl. OAIS-Modell bzw. BSI TR-03125 [TR-ESOR]) sind regelmäßig einer Revision zu unterziehen, um zu überprüfen, ob sie noch korrekt sind und ordnungsgemäß ablaufen. Daraus lässt sich dann ableiten, ob die im Archiv abgelegten Daten korrekt und authentisch sind.

Für die Revision ist eine geeignete Vorgehensweise entsprechend OPS.1.2.2.*M2 Entwicklung eines Archivierungskonzepts* beschriebenen Konzept zu entwickeln und in Form einer Checkliste zu dokumentieren. Diese sollte mindestens die folgenden Punkte umfassen:

Fragen zu Verantwortlichkeiten

- Sind die verantwortlichen Personen benannt und in ihre Aufgaben eingewiesen worden? Ist das dokumentiert?
- Bestehen Vertretungsregelungen für alle verantwortlichen Personen?

Fragen zum Organisationsprozess

- Bestehen institutionsweite Regelungen zum Einsatz elektronischer Archivierung?
- Ist institutionsweit geregelt und dokumentiert, welche Dokumente/Daten zu archivieren sind? Ist diese Regelung umfassend und vollständig?
- Sind die Sicherheitsanforderungen an die Daten und Dokumente ausreichend dokumentiert?
- Werden die institutionsweiten Regelungen regelmäßig an aktuelle Entwicklungen angepasst?
- Werden alle Anpassungen der Regelungen ordnungsgemäß dokumentiert und archiviert?
- Werden die relevanten Standards ordnungsgemäß eingehalten?

Fragen zum Einsatz der Archivierung

- Bestehen eindeutige Regelungen, welche Daten und Dokumente zu archivieren sind?
- Bestehen dokumentierte Regelungen, welche Kontextangaben an zu archivierende Daten vergeben werden, etwa die Angabe von Dokumentkategorien?
- Werden die zu archivierenden Daten vollständig und reproduzierbar archiviert?
- Werden die Anforderungen an die Vertraulichkeit der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Authentizität der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Integrität der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Verfügbarkeit der zu archivierenden Daten eingehalten?
- Werden die Anforderungen an die Verkehrsfähigkeit der zu archivierenden Daten eingehalten?
- Werden die rechtlichen Vorgaben an die Archivierung eingehalten?
- Sind alle Benutzer und Administratoren entsprechend ihrer Rollen und ihrer Aufgaben geschult und eingewiesen? Ist dies dokumentiert?

Fragen zur Redundanz der Archivdaten

- Werden Archivdaten ausreichend redundant gespeichert und aufbewahrt, z. B. mithilfe redundanter Archivsysteme oder alternativer Backup-Medien?
- Erfolgt eine regelmäßige Datensicherung der Archivsysteme sowie gegebenenfalls der Archivdaten?
- Sind die Datensicherungen den Vorgaben entsprechend durchgeführt worden?
- Sind die Datensicherungen der Archivdaten vollständig und lesbar?

- Gab es seit der letzten Revision Datenverluste? Wenn ja, wie häufig und wie schwer waren diese Vorfälle?
- Traten Fehler bei der Rekonstruktion archivierter Daten auf? Wenn ja, wie häufig waren diese Vorfälle und waren die Fehler behebbar?

Fragen zur Administration

- Wird der geforderte Refresh-Zyklus der Archivmedien eingehalten?
- Werden die notwendigen Maßnahmen für die Bewahrung des Beweiswerterhaltes der kryptografisch signierten Daten und Dokumente (z. B. Bewahrung der Gültigkeit der dazu gehörenden Signaturen, Siegel, Zeitstempel, technischen Beweisdaten (Evidence Records) etc.) durchgeführt?
- Werden die notwendigen Maßnahmen durchgeführt, um die Vertraulichkeit der Daten zu bewahren?
- Werden die Maßnahmen zur Informationserhaltung der Daten durchgeführt.
- Werden nicht mehr benötigte, beschriebene Archivmedien ordnungsgemäß vernichtet und entsorgt?
- Werden Lesegeräte und Speichermedien im geforderten Maße vorgehalten?

Technische Beurteilung des Archivsystems

Die Revision sollte jeweils die Archivsystem-Komponenten und die verwendeten Datenformate technisch bewerten, um Weiterentwicklungen und geplante Änderungen des Herstellers frühzeitig zu erkennen.

Bei dieser Prüfung kann sich herausstellen, dass technische Komponenten des Archivsystems geändert werden müssen. Dann muss sichergestellt werden, dass ausgetauschte Komponenten, z. B. Laufwerke, Speichermedien, Betriebssoftware, einwandfrei mit allen anderen Komponenten zusammenarbeiten.

Die Prüfergebnisse der Revisionen sind ebenfalls gemäß den Anforderungen an den Archivierungsprozess zu archivieren.

OPS.1.2.2.M14 Regelmäßige Beobachtung des Marktes für Archivsysteme (S)

Die geforderten Aufbewahrungszeiten für Archivdaten liegen normalerweise um ein Vielfaches höher als die durchschnittliche Lebenserwartung einzelner Bestandteile eines elektronischen Archivs. Dies betrifft sowohl Hardware- als auch Software-Komponenten sowie die verwendeten Datenformate und kryptografischen Verfahren.

Um den vollen Funktionsumfang über den gesamten Zeitraum der Archivierung dennoch sicherzustellen, ist davon auszugehen, dass einzelne Hardware-Komponenten, ganze Baugruppen oder auch Software-Komponenten eventuell mehrfach ausgetauscht werden müssen.

Eine wichtige Voraussetzung dafür ist eine regelmäßige Marktbeobachtung, mit der sich abzeichnende Veränderungen rechtzeitig registriert werden können. Solche Veränderungen sind beispielsweise:

- Änderung eines alten Standards oder Verabschiedung eines neuen Standards bei Funktionen und Prozessen, Architektur, Datenformaten, beweisrelevanten Daten oder technischen Beweisdaten, Schnittstellen, Speichermedien oder anzubindenden Fachverfahren
- Veränderungen beim Hersteller des genutzten Archivsystems oder seiner Speicherkomponenten (Wechsel auf neue Systemplattformen, Beendigung einer Produktreihe und Einstellung des Supports, Einstellung der Produktion von Speichermedien, Insolvenz eines Herstellers),
- Bekanntwerden von Sicherheitslücken oder Schwachstellen, z. B. bei eingesetzten Verschlüsselungsalgorithmen,
- Drohender Verlust der Sicherheitseignung bei kryptografischen Algorithmen,
- Änderung eines vorhandenen oder Verabschiedung eines neuen Datenformats, das für die Kodierung der AIP-Container-, Inhalts-, Meta-, Beweis- oder weiterer aufbewahrter Daten verwendet wird.

Es wird empfohlen, einen regelmäßigen Kontakt zu allen beteiligten Herstellern aufzubauen, beispielsweise durch die Teilnahme an Informationsforen, Fachkonferenzen, z. B. Newsgroups und Mailinglisten, in denen aktuelle Informationen über das eingesetzte Archivsystem versandt werden.

Es sollte mindestens ein Mitarbeiter dafür verantwortlich sein, die oben beschriebenen Informationen regelmäßig aufzunehmen, hinsichtlich ihrer Bedeutung für das verwendete Archivsystem auszuwerten und gegebenenfalls notwendige Aktivitäten zu empfehlen. Hierzu muss festgelegt werden, wie eine eventuell erforderliche Migration des Systems eingeleitet wird. Die hier gewonnenen Informationen fließen in die regelmäßige Revision des Archivierungsprozesses ein.

Es ist dabei zu beachten, dass die Langzeitspeicherung die aufbewahrten Informationen erhalten soll und nicht das Archivsystem selbst. Somit sind eine konsequente Verwendung von selbsttragenden verkehrsfähigen Archivinformationspaketen (AIP) sowie die Wahrnehmung der Aufgaben der Langzeiterhaltung (Preservation Planning) gemäß OAIS-Modell zu empfehlen.

OPS.1.2.2.M15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (S)

Kryptografische Verfahren unterliegen einem Alterungsprozess, da im Laufe der Zeit durch mathematische oder technische Weiterentwicklungen Schwächen aufgezeigt werden können, die bei der Auswahl noch nicht bekannt oder relevant waren.

Bei Aufbewahrungsfristen von zehn Jahren und länger ist davon auszugehen, dass verschlüsselte oder signierte Daten wiederholt mit neuen Schlüsseln und gegebenenfalls auf Basis neuer Algorithmen verschlüsselt werden müssen, um die Vertraulichkeit bzw. Integrität/Authentizität der Daten weiterhin zu schützen.

Um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist, sollten die Entwicklungen auf dem Gebiet der Kryptografie kontinuierlich beobachtet werden, beispielsweise anhand der Technischen Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (siehe [TR-02102]) und der ETSI- Spezifikation (siehe [TS 119 312] und [SOG-IS]). Darüber hinaus sind einschlägige Informationsquellen laufend dahingehend auszuwerten, ob Möglichkeiten bekannt werden, bestehende Verfahren zu kompromittieren.

Für die **Verschlüsselung** gelten die folgenden Maßnahmen:

Bevor die verwendeten Kryptoverfahren nicht mehr zeitgemäß sind und daher die Vertraulichkeitder archivierten Daten nicht mehr sichergestellt werden kann, müssen die verschlüsselten Daten mithilfe von sicheren digitalen Verfahren neu verschlüsselt werden.

Folgende Aspekte sind bei den Maßnahmen zur **Bewahrung der Vertraulichkeit** zu beachten (siehe auch Baustein CON.1 *Kryptokonzept*):

- Es muss ein nach aktuellen Maßstäben sicherer Kryptoalgorithmus verwendet werden, von dem angenommen werden kann, dass er für einen langen Zeitraum sicher ist (siehe die Empfehlungen oben).
- Es muss ein sicheres Verfahren zur Verschlüsselung und zur Schlüsselverteilung gewählt werden, das den Anforderungen der Archivierungsanwendung gerecht wird und den Empfehlungen der Technischen Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (siehe [TR-02102]) und der ETSI- Spezifikation (siehe [TS 119 312] und [SOG-IS]) genügt.
- Die neu erzeugten Schlüssel müssen entweder zentral erzeugt werden und auf sicherem Weg an die Benutzer des Kryptoverfahrens verteilt werden oder jeder Benutzer erzeugt seine Schlüssel (sicher) selbst.
- Eine Authentisierung der Kryptoschlüssel ist vorzusehen, z. B. durch ein elektronisches Zertifikat.

Die Verteilung der Schlüssel kann auf zwei unterschiedlichen Wegen erfolgen: Falls die Schlüsselerzeugung durch eine unabhängige, vertrauenswürdige Instanz erfolgen soll, ist sicherzustellen, dass die neuen Schlüssel vertraulich und unverfälscht an den ursprünglichen Eigentümer der Daten übertragen werden.

Bei der Nutzung asymmetrischer Verfahren zur Verschlüsselung kann der Dokumenteneigentümer alternativ selbst ein neues Schlüsselpaar erzeugen und den öffentlichen Schlüssel der archivierenden Instanz mitteilen.

In jedem Fall ist zu berücksichtigen, dass eine derartige Neuverschlüsselung einen gewissen Vorlauf braucht: Die Eigentümer der Daten bzw. der Schlüssel müssen benachrichtigt, die notwendigen Schlüssel generiert

und verteilt werden. Bei einer großen Anzahl verschiedener Eigentümer und großen Datenmengen ist ein entsprechender Aufwand einzukalkulieren.

Die Maßnahmen zur **Bewahrung des Beweiswertes** sind der Technischen Richtlinie BSI TR 03125 (siehe [TR-ESOR]) zu entnehmen. Dabei gilt:

Um entsprechend lange Aufbewahrungsfristen abdecken zu können, wird empfohlen, das neue elektronische Beweismittel zum Nachweis der Integrität und/oder Authentizität und/oder des Beweiswertes kryptografisch signierter Dokumente im elektronischen Archiv gemäß dem geltenden Stand der Technik und basierend auf den aktuellen Standards und Normen zu erzeugen.

Insbesondere die BSI-Technische Richtlinie TR-03125 TR-ESOR (siehe [TR-ESOR]) auf Basis der DIN 31647 stellen aktuell den maßgeblichen Stand der Technik für den Zweck der Bewahrung des Beweiswertes zum Nachweis der Integrität und/oder Authentizität von kryptografisch signierten Dokumenten dar. Dabei wird die Bewahrung mittels sicherer digitaler Signaturtechniken sichergestellt. Details dazu befinden sich in BSI TR-03125 (siehe [TR-ESOR]).

Dabei ist zu beachten: Geeignete kryptografische Verfahren zur Bewahrung des Beweiswertes kryptografisch signierter Dokumente/Daten oder zum Schutz der Vertraulichkeit der aufbewahrten Daten bei der Archivierung sind elektronische Signaturen, Siegel, Zeitstempel und technische Beweisdaten (Evidence Records) bzw. Verschlüsselung. Das ist für die elektronische Archivierung eine Herausforderung, da die Verfahren technisch bedingt nur eine begrenzte Lebensdauer haben, die jedoch vorher nicht immer bekannt ist. Andererseits sind sie aber auch erforderlich, wenn elektronische Dokumente beweissicher beziehungsweise vertraulich archiviert werden müssen. Die Aussagekraft elektronischer Signaturen, Siegel, Zeitstempel oder technischer Beweisdaten (Evidence Records) hängt sehr stark von deren Interpretation zum Zeitpunkt der Prüfung und damit vom so genannten Gültigkeitsmodell ab.

Gültigkeit

Die Gültigkeit einer elektronischen Signatur, eines Siegels oder eines Zeitstempels wird üblicherweise wie folgt definiert: Eine elektronische Signatur ist genau dann gültig,

- wenn sie mathematisch richtig ist und
- wenn zum Zeitpunkt der Signaturprüfung der zugehörige Signaturschlüssel und alle Zertifikate bis hin zum Wurzelzertifikat gültig sind (Schalenmodell).
- wenn zum Zeitpunkt der Signaturausübung der zugehörige Signaturschlüssel und alle Zertifikate bis hin zum Wurzelzertifikat gültig waren (Kettenmodell).

Die Prüfung technischer Beweisdaten (Evidence Record) kann gemäß TR 03125 TR-ESOR (siehe [TR-ESOR]) auf Basis von RFC 4998 und RFC 6283 erfolgen.

Aussagekraft

Elektronische Signaturen und Siegel können zu unterschiedlichen Zwecken eingesetzt werden, unter anderem

- zum Nachweis der Integrität von Dateien,
- zur Beglaubigung der Authentizität von kryptografischen Schlüsseln oder elektronischen Daten

Ein elektronischer Zeitstempel und technische Beweisdaten (Evidence Records) bestätigen die Integrität der gestempelten Daten sowie deren Existenz zu einem gegebenen Zeitpunkt.

Der Einsatz und die Aussagekraft elektronischer Signaturen, Siegeln,Z eitstempeln oder von technischen Beweisdaten können anwendungsspezifisch in einer Sicherheitsrichtlinie (Policy) vorgegeben werden. Darin sollte unter anderem festgelegt werden,

- unter welchen Voraussetzungen elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten erzeugt werden,
- von welcher Stelle elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten erzeugt werden (bei Zertifikats-Signaturen z. B. in einem neutralen Trust Center),

- welches Gültigkeitsmodell für die Anwendung herangezogen wird,
- ob und wie elektronische Signaturen, Siegel, Zeitstempel sowie technische Beweisdaten gegebenenfalls widerrufen werden können,
- wie die Bewahrung der Integrität, Authentizität sowie des Beweiswertes kryptografisch signierter Dokumente mittels sicherer digitaler Signaturtechniken (z. B. neue Signaturen, (Archiv-)Zeitstempel, Hashbäume oder Evidence Records etc.) sichergestellt werden kann sowie
- welche Aussage damit verbunden sein soll, d. h. was damit beglaubigt wird. Bei einem Zeitstempel beispielsweise, ob ein Dokument zu einem bestimmten Zeitpunkt vorliegt.

Die Sicherheitsrichtlinie muss schriftlich dokumentiert und archiviert werden, damit bei einer späteren Prüfung der elektronischen Signatur, Siegel, Zeitstempel sowie technischen Beweisdaten klar ist, was diese aussagt bzw. beweisen soll und was nicht. Außerdem sollte sie auch in geeigneter Form veröffentlicht werden, damit alle, die auf die Signaturen vertrauen müssen bzw. wollen, sich darauf beziehen können.

Sicherheitseignung

Die Sicherheitseignung elektronischer Signaturen, Siegel, Zeitstempel sowie technischer Beweisdaten wird durch die technische Entwicklung von Hard- und Software sowie Fortschritte in der Kryptografie beschränkt. Daher müssen sie regelmäßig nach dem Stand der Technik aktualisiert werden. Zusätzlich ist in bestimmten Zeitabständen eine "Re-Signing" oder "Re-Hashing" für technische Beweisdaten (Evidence Records) erforderlich, beispielsweise gemäß RFC 4998, RFC 6283 bzw. TR-ESOR-M.3 (siehe [TR-ESOR-M3]).

Empfehlung

Archivierte Daten müssen neu verschlüsselt und die elektronischen Beweismittel neu erzeugt werden, bevor ein kryptografisches Verfahren nicht mehr sicher ist. Um lange Aufbewahrungsfristen abdecken zu können, sollten für Archivdaten nur kryptografische Verfahren auf Basis aktueller Standards und Normen verwendet werden.

OPS.1.2.2.M16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten (S)

Archivsysteme müssen über lange Zeiträume auf einem aktuellen technischen Stand gehalten werden. In der Informationstechnik haben Standards für Hard- und Software sowie Datenformate zur digitalen Speicherung bisher jedoch nur kurzzeitig Bestand gehabt. Es ist davon auszugehen, dass dies auch künftig so bleibt, da die Standards in hohem Maße vom technischen Fortschritt geprägt werden. (vgl. Bestandserhaltung gemäß OAIS-Modell).

Hardware-Komponenten unterliegen zudem Verschleißerscheinungen und müssen daher regelmäßig gewartet sowie gegebenenfalls ausgetauscht werden. Zusätzlich ist damit zu rechnen, dass Hersteller unvorhergesehen die Unterstützung bestehender Systeme einstellen oder, z. B. aufgrund von Insolvenz, nicht mehr in der Lage sind, langfristige Unterstützung zu gewährleisten.

Es ist daher damit zu rechnen, dass die Komponenten des Archivs regelmäßig erneuert werden müssen und eventuell der komplette Datenbestand auf ein neues Archivsystem migriert werden muss. Dieser Prozess ist eng mit OPS.1.2.2.M14 *Regelmäßige Beobachtung des Marktes für Archivsysteme* verknüpft.

Vor der Installation neuer Hard- und Software in ein laufendes Archivsystem ist diese ausführlich zu testen, um die Stabilität des bestehenden Systems nicht zu gefährden. Bei der Installation z. B. neuer Datenträger und Laufwerke muss darauf geachtet werden, dass sie mit den bestehenden Systemen und Datenträgern kompatibel sind.

Vor der Inbetriebnahme neuer Komponenten oder der Einführung neuer Datenformate ist ein Migrationskonzept zu erstellen, in dem alle Änderungen und Tests beschrieben werden. Die Konvertierung der einzelnen Daten ist immer zu dokumentieren. Diese Dokumentation ist zusammen mit den konvertierten Daten aufzubewahren (Transfervermerk). Das Archivierungskonzept (siehe OPS.1.2.2.M2 *Entwicklung eines Archivierungskonzepts*) ist unter Umständen anzupassen. Bei größeren Änderungen muss die in der Bausteinbeschreibung beschriebene Planungsphase erneut durchlaufen werden.

Bei der Änderung von Formaten muss geprüft werden, ob bei der Konvertierung von Altdaten in die neuen Formate aufgrund rechtlicher Anforderungen zusätzlich die Daten in ihren ursprünglichen Formaten archiviert werden müssen.

OPS.1.2.2.M17 Auswahl eines geeigneten Archivsystems (S)

Die Auswahl eines Archivsystems erfolgt auf der Grundlage der im Archivierungskonzept (siehe *OPS.1.2.2.M2 Entwicklung eines Archivierungskonzepts*) festgeschriebenen Vorgaben. Typischerweise werden folgende Mindestanforderungen an das einzusetzende Archivsystem gestellt, wobei institutionsspezifische Anforderungen zu ergänzen sind:

- Versionierung von Dokumenten/Datensätzen: Das Archivsystem sollte die mehrfache Speicherung von Dokumenten/Datensätzen in unterschiedlichen Fassungen unterstützen (Versionierung).
- Funktionen und Prozesse angelehnt an das OAIS-Modell sowie [TR-ESOR]
- Zugriffsschutz auf die archivierten Daten: Durch das Archivsystem sollte ein Zugriffsschutz auf die archivierten Daten und die Funktionen des Archivsystems umgesetzt werden können. Dies sollte auf der Grundlage eines vorgegebenen Berechtigungskonzepts erfolgen.
- Mehrstufiges, rollenbasiertes Berechtigungskonzept: Bei einer rollenbasierten Rechtevergabe werden Zugriffsrechte nicht an konkrete Benutzer vergeben, sondern an definierte Benutzergruppen (Rollen). Im Gegensatz zu normalen Berechtigungsgruppen werden in einem rollenbasierten Zugriffsmodell auch Rollenkonflikte berücksichtigt. Dies bedeutet zum Beispiel, dass eine Person nicht gleichzeitig die Rolle des Administrators und des Revisors einnehmen kann.
- Protokollierung: Das Archivsystem sollte es ermöglichen, alle Vorgänge rund um die Archivierung zu protokollieren und nachvollziehbar zu machen (siehe auch OPS.1.2.2.M8 *Protokollierung der Archivzugriffe*). Dabei sollte es auch möglich sein, kritische Ereignisse zu definieren und einen Administrator zu benachrichtigen, wenn solche auftreten.
- Einrichtung eines Benutzerkontos für die Revision: Für Zugriffe während der regelmäßigen Revision des Archivsystems sollte ein entsprechendes Benutzerkonto mit den dafür notwendigen Rechten eingerichtet werden. Die konkrete Rechtevergabe ist institutionsintern festzulegen. Im Rahmen der Revision werden typischerweise Leserechte (read-only) auf Konfigurationsdaten und Protokolldaten eingerichtet.
- Erweiterbarkeit des Archivsystems: Das Archivsystem sollte erweiterbar sein, damit es bei Änderungen der Anforderungen angepasst werden kann. Die Erweiterbarkeit betrifft vor allem die eingesetzten Speicherkomponenten und Speichermedien, aber auch sonstige Hardware-Änderungen sowie die Archivsystem-Software und Nutzungslizenzen.
- Geringe Zugriffszeit: Für das Archivsystem wird typischerweise eine geringe Zugriffsverzögerung und gleichzeitig eine hohe Bandbreite bei der Übertragung und Bereitstellung der angeforderten Dokumente verlangt. Die Anforderungen sind institutionsspezifisch zu ermitteln. Hierbei ist neben der Einbindung in die vorhandene Systemumgebung auch das abzusehende Benutzerverhalten zu berücksichtigen. Die festgelegten Anforderungen wirken sich auf die Auswahl der Archivmedien und der Speicherlaufwerke aus. Ebenso können die Anforderungen die Auswahl und Dimensionierung von Cache-Komponenten beeinflussen.
- Ausreichende Kapazität der Archivmedien: Die Archivmedien sollten eine ausreichende Kapazität aufweisen. Sowohl die mehrfache Speicherung von Dokumenten zur Versionierung als auch die zu erwartende Datenmenge sollten bei der Kapazitätsplanung berücksichtigt werden.
- Systemgesteuertes Einlegen oder Entnehmen von Archivmedien: Das Archivsystem sollte unterstützen, dass Archivmedien nur systemgestützt aus den Laufwerken entnommen werden können. Hierdurch soll gewährleistet werden, dass Archivmedien nur nach kontrollierter Offline-Schaltung (unmount) sowie unter Beachtung entsprechender Zugriffsrechte entnommen werden und die Entnahme protokolliert werden kann. Gleiches gilt für die Online-Schaltung (mount) von Archivmedien. Dies ist erforderlich, damit eine konsistente Verwendung der Archivmedien sichergestellt ist. Für Notfälle sehen in der Regel alle Archivsysteme und Laufwerke manuelle Möglichkeiten vor, Archivmedien zu entnehmen.

- Kapazitätsüberwachung der Archivmedien: Die Restkapazität der in Benutzung befindlichen Archivmedien muss laufend überwacht werden. Wird eine Restkapazitätsgrenze unterschritten, muss eine Signalisierung bzw. Alarmierung erfolgen.
- Alarmierung und Signalisierung: Das Archivsystem muss die Signalisierung von Systemmeldungen an übergreifende Systemmanagement-Umgebungen gestatten. Wenn keine Anbindung an eine Systemmanagement-Umgebung vorgesehen ist, so sollte über E-Mail, SMS oder SNMP individuell alarmiert werden können.
- Einhaltung von Standards: Die Einhaltung von Standards erleichtert die Interoperabilität zwischen einzelnen Komponenten. Dies ist erforderlich, weil damit gerechnet werden muss, dass im Betriebszeitraum einzelne Komponenten ausgetauscht werden müssen oder das System erweitert werden soll. Standards sind insbesondere in folgenden Bereichen relevant:
- Archivmedien und Aufzeichnungsverfahren (siehe OPS.1.2.2.M18 *Verwendung geeigneter Archivmedien*),
- Dateiformate und Komprimierungsverfahren (siehe OPS.1.2.2.M9 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*).
- Komponenten, Prozesse, Organisation des Archivsystems
- Beweiswerterhaltung der elektronischen Daten,
- Anbindung an die vorhandene IT-Umgebung (Schnittstellen).

Es sollte überlegt werden, die Daten durch Verschlüsselung und sichere elektronische Signaturtechniken zu schützen. Weiterhin kann die Grundverschlüsselung von Archivmedien durch das Archivsystem implementiert werden. Hierdurch soll ein Missbrauch des Archivmediums außerhalb des Archivsystems verhindert werden.

OPS.1.2.2.M18 Verwendung geeigneter Archivmedien (S)

Die dauerhafte elektronische Archivierung von Daten erfordert den Einsatz geeigneter Datenträger (Archivmedien). Für die Wahl der Archivmedien sollten folgende Fragen berücksichtigt werden:

- Welches Datenvolumen soll archiviert werden?
- Welche Zugriffszeiten sind im Mittel zu erbringen?
- Wie hoch ist die Zahl gleichzeitiger Zugriffe im Mittel?
- Welche Aufbewahrungsfristen sollen durch das Archivmedium abgedeckt werden?

In den folgenden Abschnitten werden typische Archivmedien und deren Einsatzbereiche beschrieben. Für die Datenträger werden üblicherweise magnetische, magnetooptische oder optische Speichertechniken verwendet. Die Vor- und Nachteile der Techniken sind in den jeweiligen Abschnitten beschrieben.

Sämtliche beschriebenen Archivmedien sind anfällig gegenüber physischen Beschädigungen, etwa durch

- Wasser,
- Feuer bzw. Hitzeentwicklung,
- Verkratzen des Mediums,
- Zerknittern und Aufreißen des Mediums im Bandlaufwerk sowie
- Sabotage und Diebstahl.

Archivmedien müssen daher sorgsam aufbewahrt und geschützt werden. Außerdem muss der unbefugte Zugriff auf die Datenträger verhindert werden. Hierzu wird, abhängig vom konkreten Einsatzszenario des elektronischen Archivs, die Anwendung der im Baustein INF.7 *Datenträgerarchiv* bzw. INF.6 *Schutzschrank* beschriebenen Maßnahmen zum Schutz der Datenträger empfohlen.

Digitale magnetische Speichermedien

Bei magnetischen Speichersystemen wird durch gezielte lokale Veränderung eines magnetisierten Grundmediums ein Speichereffekt erzielt. Die Magnetisierung kann durch ein Lesegerät erfasst, die gespeicherten Daten können dadurch gelesen werden. Durch erneutes Einwirken eines Magnetfeldes können die gespeicherten Daten verändert werden. Dies erfolgt gezielt durch Verwendung eines Schreib-/Lesegerätes oder ungezielt durch starke externe Magnetfelder (z. B. elektromagnetische Felder in der Nähe von Transformatoren oder großen Spulen).

Magnetische Datenträger sind anfällig gegenüber Angriffen mit starken Magnetfeldern, die auf das Speichermedium einwirken. Da das magnetisierte Grundmedium typischerweise als Verbundwerkstoff aus Kunststoffen sowie einer metallischen (magnetisierbaren) Beschichtung hergestellt wird, ist außerdem auch bei sorgsamer Behandlung mit langfristigen Veränderungen zu rechnen. Diese können z. B. durch Zersetzung (durch Weichmacher in Kunststoffen), Aufquellen (Ablösung von Kunststoff- und Metallschichten) oder Oxydation (der Metallschicht) bedingt sein.

Aufgrund der verwendeten Techniken sind magnetische Speicher zudem stets wiederbeschreibbar bzw. löschbar. Sie müssen daher im Rahmen der Archivierung stets mit zusätzlichen Sicherungsverfahren eingesetzt werden, um zu verhindern, dass Dokumente verändert werden. Typische magnetische Speicher sind Festplatten und (Magnet-)Bandmedien.

- Festplatten: In Festplatten sind typischerweise das Speichermedium und das Schreib-/Lese-Laufwerk zusammen in einer Einheit untergebracht. Sie sind daher fehleranfällig gegen mechanische Ausfälle. Durch die physische Kapselung wird eine dichtere Anordnung der Magnetmedien bei gleichzeitigem Schutz vor Staubpartikeln ermöglicht, sodass Festplatten meist über mehrere Schreib-Lese-Einheiten verfügen. Festplatten weisen typischerweise eine hohe Kapazität und eine geringe Zugriffszeit bei hoher Übertragungsrate auf.
- Magnetbänder: Magnetbänder bestehen aus einem aufgewickelten Magnetstreifen, der in der Regel an einem Schreib-Lesekopf sequenziell vorbeigeführt wird. Magnetband und Schreib-Lese-Einheit sind typischerweise nicht miteinander verbunden. Magnetbänder weisen technisch bedingt eine sehr lange Zugriffszeit und eine sehr geringe Übertragungsrate auf. Ihre Speicherdichte und ihr Platzverbrauch sind jedoch vergleichbar mit Festplatten. Magnetbänder eignen sich für die Speicherung großer Datenmengen, auf die nur selten und sequenziell zugegriffen werden muss. Sie sind daher geeignet für Backups, bei denen eine mittelfristige, jedoch nicht langfristige Stabilität erwartet wird.

Digitale magneto-optische Speichermedien

Bei der magneto-optischen (MO) Speichertechnologie werden gespeicherte Daten, ähnlich wie bei optischen Speichern, durch Abtasten eines Speichermediums mit einem Laserstrahl gelesen. Der optische Effekt wird dabei durch eine Magnetschicht verursacht, deren Partikel beim Durchlaufen und Reflexion des Laserstrahls als Polarisationsfilter wirken. Die Polarisation der Oberfläche lässt sich punktuell beeinflussen, indem ein Magnetfeld angelegt wird, das nur an einer (wiederum durch einen Laser) speziell aufgeheizten Region des Speichermediums wirkt. In einem Schreibprozess werden die Regionen der Medienoberfläche gezielt unterschiedlich polarisiert.

Auch bei magneto-optischen WORM-Medien kann technisch bedingt ein nachträgliches unbefugtes Überschreiben (Brennen) bislang ungenutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um echte Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Magneto-optische Systeme weisen eine hohe Langzeitstabilität (nach Herstellerangaben mehr als 30 Jahre) und eine Speicherkapazität von bis zu 9,1 GB je Medium auf.

Netzbasierte Speichermedien

Netzbasierte Speichermedien sind für die Langzeitspeicherung und Archivierung immer wichtiger. Sie lassen sich einfach als Dienst integrieren und sind hervorragend skalierbar sowie verfügbar. Insbesondere folgende zwei Vertreter können empfohlen werden:

- Storage-Area-Network (SAN): SANs wurden für serielle, kontinuierliche und mit großer Geschwindigkeit erfolgende Übertragung von großen Datenmengen konzipiert. Ein SAN kann mehrere im Netz

vorhandene Festplattensysteme, Tape-Libraries etc. den Servern für eine sehr schnelle Speicherung der Daten zur Verfügung stellen. Gängige unterstütze Übertragungsraten liegen im Bereich von 16 GBit/s.

- cloudbasierte Speichersysteme: Infrastruktur-Cloud-Dienste erlauben eine einfache Implementierung von hoch skalierbaren und hoch verfügbaren Speichermedien, die der Langzeitspeicherung bzw. Archivierung zur Verfügung gestellt werden können (siehe hierzu auch Baustein OPS.2.2 *Cloud-Nutzung)*.

Hierarchisches Speichermanagement

Mithilfe eines gemäß den Prinzipien des hierarchischen Speichermanagements (HSM) umgesetzten Langzeitspeichers lassen sich die Zugriffszeiten auf die mit großer Häufigkeit benötigten Objekte deutlich verkürzen. Dafür werden die Speichermedien stufenförmig aufgebaut, sortiert nach der steigenden Zugriffszeit. Die am häufigsten benötigten Daten werden im schnellen Medium vorgehalten und können nach und nach auf den nachgeordneten langsameren (und billigeren) Speicher ausgelagert werden, wenn diese später nicht mehr so oft benötigt werden.

Insgesamt ist auf Basis der im Archivierungskonzept definierten technischen, rechtlichen und organisatorischen Anforderungen zu entscheiden, welches Speichermedium eingesetzt werden soll.

OPS.1.2.2.M19 Regelmäßige Funktions- und Recoverytests bei der Archivierung (S)

Durch verschiedene Ursachen in den Bereichen Datenträger, Hardware und beim Programmablauf kann es bei der Archivierung zu Datenverlusten kommen. Regelmäßige Funktions- und Recoverytests sind daher unumgänglich.

Datenträger unterliegen ebenso wie alle anderen Archivierungskomponenten Verschleißerscheinungen und sollten daher mindestens einmal jährlich geprüft werden, ob sie noch lesbar und integer sind.

Werden Fehler auf einem Archivmedium festgestellt, so ist unverzüglich sicherzustellen, dass die betroffenen Dateien aus dem Backup-Bestand wieder hergestellt werden. Wenn fehlerhafte Archivdatenträger ausgetauscht werden müssen, so sind diese nach der Kopie der darauf enthaltenen Daten sicher zu löschen bzw. zu vernichten. Der gesamte Vorgang ist zu dokumentieren.

Alle Hardwarekomponenten, insbesondere die mechanischen Teile des Archivs, müssen regelmäßig auf einwandfreie Funktion geprüft werden. Nur so kann gewährleistet werden, dass archivierte Datenbestände den geforderten Verfügbarkeitsanforderungen entsprechen und beim Schreiben und Lesen der Daten die Datenintegrität gegeben ist.

Der Archivierungsvorgang selbst kann fehlerhaft verlaufen. Mögliche Ursachen dafür können sein: Konfigurationsfehler, Softwarefehlfunktionen, Probleme mit den Speichermedien oder Änderungen und Fehler in der Ablaufsteuerung. Einmal pro Tag ist daher zu überprüfen, ob alle Archivierungsprozesse fehlerfrei abgelaufen sind. Das kann geschehen, indem Logdateien ausgewertet werden sowie durch eine stichprobenartige Ansicht der erstellten Archivmedien durch den Administrator.

Die notwendigen Integritätsprüfungen der Indexdatenbank sind in Maßnahme OPS.1.2.2.M6 *Schutz der Integrität der Indexdatenbank von Archivsystemen* beschrieben.

OPS.1.2.2.M20 Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (H)

Archivierte Daten sollten parallel mit mindestens zwei verschiedenen kryptografischen Verfahren verarbeitet werden und die elektronischen Beweismittel auf dieselbe Art und Weise neu erzeugt werden, bevor ein kryptografisches Verfahren nicht mehr sicher ist. Um lange Aufbewahrungsfristen abdecken zu können, sollten für Archivdaten nur kryptografische Verfahren auf Basis aktueller Standards und Normen verwendet werden.

OPS.1.2.2.M21 Übertragung von Papierdaten in elektronische Archive (H)

Für die Übertragung von Papierdaten in elektronische Archive wird die Anwendung der [TR-03138 RESISCAN] empfohlen.

3. Weiterführende Informationen

3.1. Wissenswertes

Damit sich Geschäftsprozesse und -unterlagen in elektronischen Geschäftsanwendungen abbilden lassen, müssen die entstehenden Dokumente geeignete archiviert werden. So können sie später wieder verwendet, wieder gefunden sowie noch einmal aufbereitet werden. Das betrifft sowohl Datensätze als auch elektronische Repräsentationen eingescannter Geschäftsdokumente. Der Lebenszyklus elektronischer Dokumente kann grundsätzlich in drei Phasen unterteilt werden:

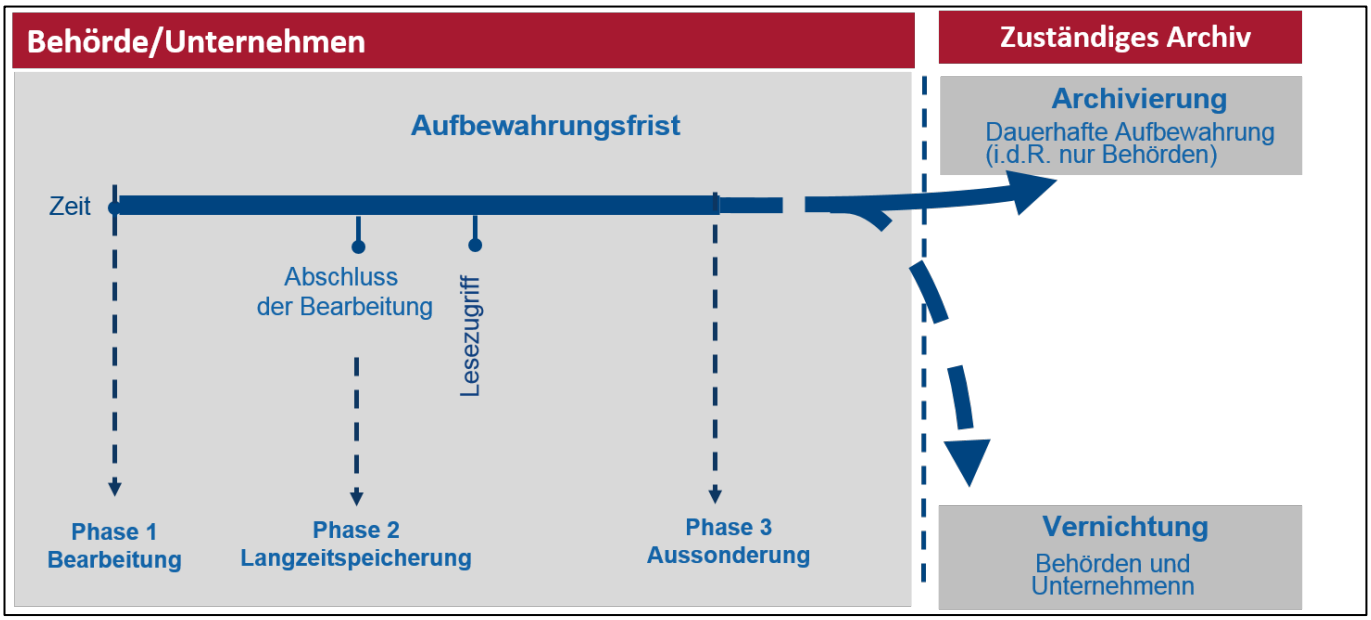


Abbildung 1 Lebenszyklus elektronischer Daten

- Phase 1 – Bearbeitung der Dokumente: In dieser Phase werden normalerweise die Dokumente innerhalb einer Geschäftsanwendung gehalten und öfter angepasst. Die Datenhoheit liegt bei der zuständigen Instanz, z. B. einer Behörde oder einem Unternehmen.
- Phase 2 – Langzeitspeicherung (LZSP) der Dokumente: Die Dokumente erreichen einen stabilen (finalen) Stand und werden bis zum Ablauf einer festgelegten Frist aufbewahrt, z. B. nachdem ein Vorgang abgeschlossen wurde. Die Datenhoheit liegt bei der zuständigen Instanz.
- Phase 3 – Aussonderung und dauerhafte Aufbewahrung der Dokumente: Nach dem Ablauf der Aufbewahrungsfrist müssen die aufbewahrten Dokumente vernichtet werden. Im Fall von Behörden müssen die zu vernichtenden Dokumente dem zuständigen Archiv zwecks dauerhafte Aufbewahrung angeboten werden. Die Datenhoheit geht somit auf das Archiv über.

Davon abgeleitet werden die Langzeitspeicherung, (dauerhafte) Archivierung und Datensicherung (Backup) für die weitere Verwendung in diesem Baustein voneinander abgegrenzt.

- Aufbewahrung und Erhaltung (Information und Beweiswert) von elektronischen Dokumenten **für den Zeitraum der geltenden Aufbewahrungsfristen** wird **Langzeitspeicherung** (LZSP) genannt.
- Die dauerhafte und unveränderbare Aufbewahrung und Erhaltung von elektronischen Dokumenten, mit dem Ziel der **Sicherstellung der historischen Überlieferung** insbesondere in staatlichen und kommunalen Archiven (z. B. Bundesarchiv), wird als (dauerhafte) **Archivierung** bezeichnet.
- Eine vom IT-System physisch getrennte und vor Gefahren geschützte Aufbewahrung einer Kopie von System- und Nutzdaten, die in regelmäßigen Abständen erneuert wird, wird als **Datensicherung** (Backup) bezeichnet.

ISO 14721 - Open Archival Information System

Die ISO 14721 (auch OAIS-Referenzmodell (Referenz Model for an Open Archival Information System) genannt) 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 und wurde als ISO-Standard im Jahr 2003 veröffentlicht und 2012 aktualisiert.

Das OAIS-Referenzmodell beschreibt die notwendigen Komponenten (Prozesse und Informationspakete) zur langfristigen oder dauerhaften Aufbewahrung von elektronischen Dokumenten.

Ein System, das nach OAIS aufgebaut ist, besteht aus mehreren Prozessen, die einzelne Funktionen übernehmen und miteinander kommunizieren.

Eine zentrale Rolle im OAIS-Referenzmodell spielt das darin definierte Archivinformationspaket (Archival Information Package, AIP). Es enthält neben den Primärdaten alle zur Interpretation, Lesbarkeit, Nutzbarkeit, Verständlichkeit und Recherche notwendigen Informationen, beweisrelevante Nachweise der Integrität und Authentizität der aufzubewahrenden Unterlagen sowie auch die Primärdaten in standardisierter und herstellerunabhängiger Form in einem Paket. Ein AIP besteht demnach aus:

- Metainformationen,
- Inhalts-/Primärinformationen,
- beweisrelevanten Daten und
- technischen Beweisdaten.

Das OAIS-Referenzmodell wurde für End-Archive konzipiert, die ihr Archivgut dauerhaft aufbewahren. So hat auch das Bundesarchiv sein elektronisches Archivsystem entsprechend den Vorgaben und Empfehlungen des OAIS- Referenzmodells entwickelt.

Der modulare Aufbau des OAIS-Referenzmodells ermöglicht eine authentische Wahrung und Reproduzierbarkeit des Archivguts. Für den Bereich der Langzeitspeicherung sind die Ausführungen zur Erhaltung des Beweiswerts, der Lesbarkeit sowie der Verfügbarkeit der elektronischen Objekte wesentlich.

Das OAIS-Referenzmodell kann, insbesondere das Modul Bestanderhaltung, als organisatorische Hilfe im Rahmen der Langzeitspeicherung dienen.

Dieses Modul hat zur Aufgabe, die

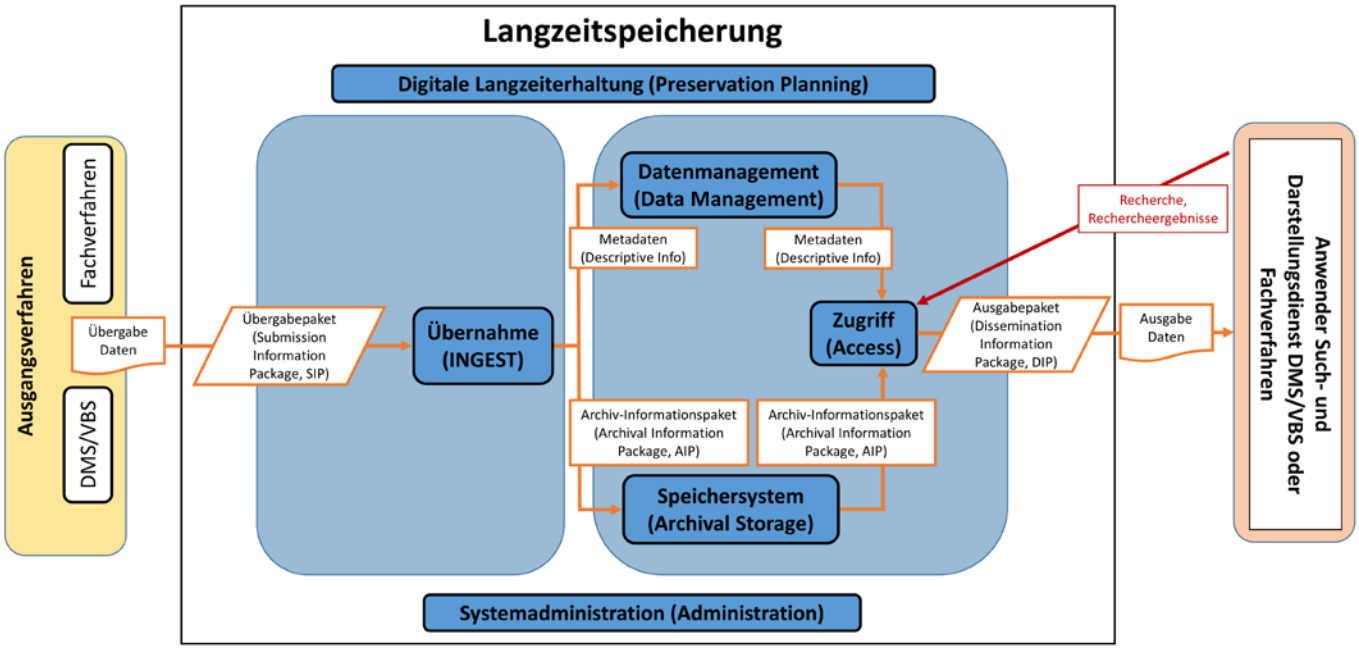
- Les- und Nutzbarkeit,
- Unverfälschbarkeit,
- Vollständigkeit sowie
- die Sicherheit vor Verlust

des Archivguts zu gewährleisten.

In der praktischen Arbeit umfasst dies die Überwachung der Lesbarkeit von Formaten, deren Konvertierung oder auch die Migration auf andere Speichermedien. Um dabei alle wichtigen Einflussfaktoren zu berücksichtigen und die Bestandserhaltung sicherzustellen, ist eine entsprechende Konzeption zu entwickeln und umzusetzen.

Das in ISO 14721:2012 genormte OAIS gilt aus oben genannten Gründen als zentrale Norm zur Langzeitspeicherung und Archivierung elektronischer Unterlagen und sollte z.B. insbesondere auch für Stellen und Einrichtungen des Bundes als Basis für die Umsetzung ihrer Langzeitspeicherungs- und Archivsysteme dienen.

Die ISO 14721 definiert die für Langzeitspeicherung und Archivierung notwendigen Prozesse Übernahme, Datenmanagement, Speichersystem, Zugriff, digitale Langzeiterhaltung und Systemadministration sowie die Informationspakete Übergabeinformationspaket (SIP), Archivinformationspaket (AIP) und Ausgabeinformationspaket (DIP).



Das Archivinformationspaket (engl. Archival Information Packet, AIP) soll in einer selbsttragenden Form alle zur Erfüllung des Aufbewahrungszwecks notwendigen Informationen bis zum Ablauf der geltenden Aufbewahrungsfristen in einer möglichst hard- und softwareneutralen Form beinhalten. Dabei geht es primär um die Inhaltsdaten (die aufzubewahrenden Daten selbst), beschrieben durch die notwendigen Metadaten (sowohl fachliche als auch technische Metadaten) und die zum Nachweis der Authentizität und Integrität notwendigen Daten. Es ist dabei entscheidend, eine ausreichende Menge der Metadaten zu erfassen (Kontextsicherung), um den aufbewahrten Vorgang auch in der Zukunft vollständig rekonstruieren zu können.

Der Übernahme-Prozess (engl. Ingest) beinhaltet die notwendigen Funktionen zur Übernahme der Dokumente in das digitale Archiv, indem das aus der Geschäftsanwendung übergebene SIP in ein korrespondierendes AIP überführt wird. Es werden dabei die Dokumente in langfristig lesbare Dateiformate überführt, die Inhalte geeignet indexiert, Metadaten erhoben bzw. generiert sowie die AIP-Struktur erzeugt.

Der Speicher-Prozess (engl. Archival Storage) ist für die physische Ablage und Bereitstellung der aus dem Übernahme-Prozess hervorgegangenen AIP-Strukturen notwendig. Dieses kann durch Einsatz von unterschiedlichen Speichertechniken aus dem Speicher-Segment umgesetzt werden, z. B. Plattenspeicher, SAN.

Der Datenmanagement-Prozess (engl. Data Management) verwaltet und stellt die gesammelten Beschreibungsdaten (engl. Metadata) zu Verfügung. Die Metadaten werden durch den Übernahme-Prozess abgelegt und können durch den Zugriff-Prozess verwendet werden. Dabei kann es sich auch um die Geschäftsanwendung selbst handeln, deren Daten aufbewahrt werden sollen.

Der Zugriff-Prozess (engl. Access) bietet eine Möglichkeit, die gewünschten Daten mithilfe von Metadaten aus dem Datenmanagement zu finden sowie diese auch abzurufen. Die Daten werden dem Speicher in Form eines AIP entnommen und dem Konsumenten in Form eines Ausgabepakets (DIP) zur Verfügung gestellt.

Der Planung und Steuerung der Maßnahmen zur digitalen Bestandserhaltung dienen der Langzeiterhaltung der Dokumente (engl. Preservation Planning). Basierend auf den Metadaten können Maßnahmen umgesetzt werden, welche die Informations- (z. B. Migration der Formate der gespeicherten Inhaltsdaten etc.) und die Beweiswerterhaltung (z. B. Signatur-/Hasherneuerung etc.) gewährleisten.

Mithilfe des Systemadministration-Prozesses (engl. Systemadministration) werden die Aufgaben zum Aufbau und Betrieb, zur Weiterentwicklung, Überwachung und Kontrolle des Langzeitarchivs umgesetzt.

Die Spannweite der Realisierungsmöglichkeiten eines solchen Archivsystems umfasst

- kleine Archivsysteme, z. B. bestehend aus einem Archivserver mit angeschlossenem Massenspeicher als Teil der Geschäftsanwendung, bis hin zu
- komplexen, gegebenenfalls weltweit verteilten Archivsystemen zur institutionsweiten Archivierung von relevanten Geschäftsdaten als verfahrensübergreifende IT-Dienste.

DIN 31644

Das allgemeingültige OAIS-Modell wird in Deutschland durch die DIN 31644 "Kriterien für vertrauenswürdige digitale Langzeitarchive" mit organisatorischen und funktionalen Anforderungen an ein vertrauenswürdiges Langzeitarchiv untermauert. Der Fokus der Norm liegt dabei auf der Informationserhaltung.

DIN 31647

Die DIN 31647 "Beweiswerterhaltung kryptographisch signierter Dokumente" enthält fachliche und funktionale Anforderungen an ein generisches System zur Beweiswerterhaltung kryptografisch signierter Unterlagen unter Wahrung der Authentizität und Integrität (indirekt auch Verfügbarkeit, Nachvollziehbarkeit sowie Verkehrs- und Austauschfähigkeit) innerhalb eines Archivsystems. Die Norm ergänzt somit die DIN 31644.

Eine Referenzarchitektur zur Umsetzung der DIN 31647 und des OAIS-Referenzmodells ist durch die technische Richtlinie BSI TR-03125 (siehe [TR-ESOR]) gegeben.

TR-03125 des BSI

Die Technische Richtlinie TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR) (siehe [TR-ESOR]) auf Basis der Standards [RFC4998] und [RFC6283] wurde vom BSI mit dem Ziel bereitgestellt, die Integrität und Authentizität archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht unter Wahrung des rechtswirksamen Beweiswertes zu erhalten.

Auch kann die TR-03125 (siehe [TR-ESOR]) Abhilfe leisten, wenn nicht signierte Dokumente integritätsgesichert werden sollen.

Die Richtlinie enthält konkrete technische Vorgehensweisen und behandelt dabei die Themen:

- Daten- und Dokumentenformate,
- Empfehlungen zu einer Referenzarchitektur, zu ihren Prozessen, Modulen und Schnittstellen als Konzept einer Middleware,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Austauschformate für Schnittstellenspezifikationen
- Konformitätsregeln für die Konformitätsstufe 1 "logisch-funktional" und die Konformitätsstufe 2 "technisch-interoperabel" sowie für die Konformitätsstufe 3 "Bundesbehördenprofil".

Eine Infrastruktur, die TR-03125 (siehe [TR-ESOR]) entspricht, besteht aus mehreren Modulen, die Funktionen zur Beweiswerterhaltung bereitstellen.

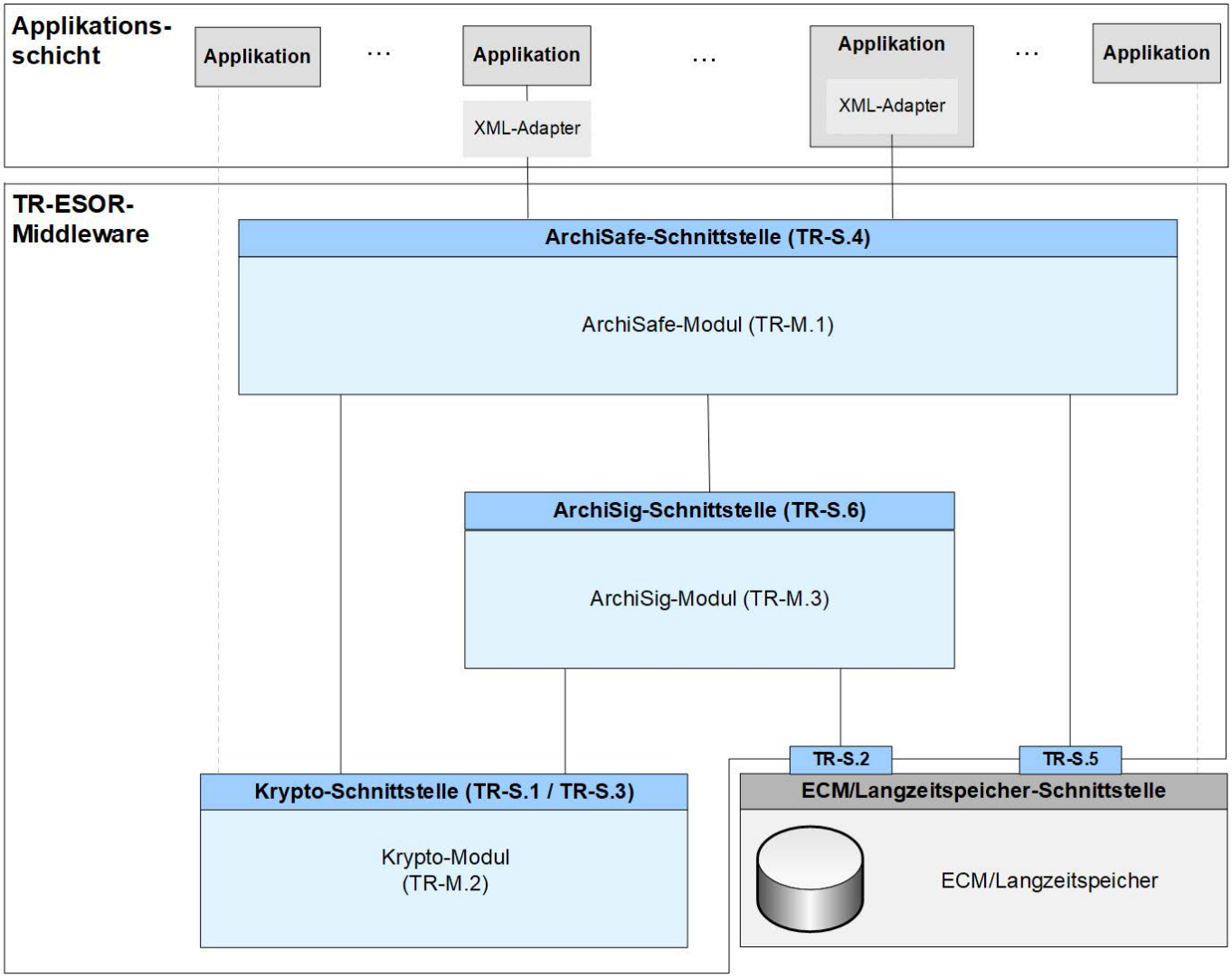


Abbildung 2 Referenzarchitektur der TR-03125

Der Einsatz einer TR-03125-Middleware zwischen der IT-Applikation und dem Langzeitspeichersystem empfiehlt sich somit insbesondere

- für kryptografisch signierte Dokumente, die langfristig in dieser Form benötigt werden oder
- falls der Schutzbedarf von Dokumenten sehr hoch ist oder
- wenn ein besonders verkehrsfähiger Integritätsnachweis für Dokumente angestrebt wird.

Die Referenzarchitektur ermöglicht es Softwareherstellern und Benutzern, TR-03125-konforme Systeme aufzubauen und zertifizieren zu lassen.

Die Richtlinie empfiehlt darüber hinaus den Einsatz offener, interoperabler und standardisierter Datenformate und herstellerunabhängiger Schnittstellen entsprechend nationaler und internationaler Standards.

3.2. Quellenverweise

[DIN31644] DIN 31644:2012-04: Information und Dokumntation - Kriterien für vertrauenswürdige digitale Langzeitarchive, April 2012

[DIN31647] DIN 31647:2015-05: Information und Dokumentation - Beweiswerterhaltung kryptograhisch signierter Dokumente, Mai 2015

[EIDAS-DG] EIDAS-DG: Gesetzt zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaents und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für

elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz), Bundesblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017

[EIDAS-VO] EIDAS-VO: Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG vom 23. Juli 2014

[ISO14721] ISO 14721:2012: International Organization for Standardization (Hrsg.), Space data and information transfer system - Open archival information system (OAIS) - Reference model, September 2012

[RESISCAN] BSI TR-03138 RESISCAN: Ersetzendes Scannen, April 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf?__blob=publicationFile&v=4 , zuletzt abgerufen am 06.04.2021

[RFC4998] Evidence Record Syntax (ERS): RFC4998, August 2007, https://tools.ietf.org/html/rfc4998, zuletzt abgerufen am 26.07.2018

[RFC6283] Extensible Markup Language Evidence Record Syntax (XMLERS): RFC 6283, Juli 2011, https://www.ietf.org/rfc/rfc6283.txt , zuletzt abgerufen am 26.07.2018

[SOG-IS] SOG-IS Crypto Working Group: SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, 2016, https://www.sogis.org/uk/supporting_doc_en.html , zuletzt abgerufen am 26.07.2018

[TR02102] Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2021, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html , zuletzt abgerufen am 06.04.2021

[TR-ESOR] BSI TR- 03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente, Hauptdokument, 2014, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html , zuletzt abgerufen am 26.07.2018

[TR-ESOR-B] BSI TR-03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-B: Profilierung für Bundesbehörden, Januar 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_B_V1_2_1.pdf?__blob=publicationFile&v=2 , zuletzt abgerufen am 26.07.2018

[TR-ESOR-E] BSI TR-03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks des eCard-API-Frameworks, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf?__blob=publicationFile&v=2 , zuletzt abgerufen am 26.07.2018

[TR-ESOR-F] BSI TR-03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-F: Formate, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_F_V1_2_1.pdf?__blob=publicationFile&v=2 , zuletzt abgerufen am 26.07.2018

[TR-ESOR-M3] BSI-TR-03125 TR-ESOR: Beweiswerterhaltung kryptographischer signierter Dokumente, Anlage TR-ESOR-M.3, ArchiSig Modul, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_M3_V1_2_1.pdf?__blob=publicationFile&v=2 , zuletzt abgerufen am 26.07.2018

[TR-ESOR-XB] BSI TR-03125 TR_ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-XBDP, Profilierung des XAIP mit XBARCH, XDOMEA und PREMIS, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_XBDP_V1_2_1.pdf?__blob=publicationFile&v=2 , zuletzt abgerufen am 26.07.2018

[TS119132] ETSI: Electronic Signatures and Infrastructures (ESI): Cryptographic Suites, Version 1.2.1, Mai 2015

[VDG] Vertrauensdienstgesetz - VDG: Artikel 1 des Gesetzes zur Durchführung der Verordnung (EU) NR. 910/2014 des Europäischen Parlaments und des Rates vom 23.Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1993/93/EG (eIDAS-Durchführungsgesetz), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 52, ausgegeben zu Bonn am 28. Juli 2017