Vertrauenswürdige und beweiswerterhaltende elektronische Langzeitspeicherung auf Basis von DIN 31647 und BSI-TR-03125

Steffen Schwalm[1] · Ulrike Korte[2] · Detlef Hühnlein[3]

[1] BearingPoint GmbH, Kurfürstendamm 207-208, 10719 Berlin, steffen.schwalm@bearingpoint.com
[2] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, ulrike.korte@bsi.bund.de
[3] ecsec GmbH, Sudetenstraße 16, 96247 Michelau, detlef.huehnlein@ecsec.de

Abstract: Es besteht eine hohe Notwendigkeit, nicht nur in der öffentlichen Verwaltung, sondern auch in Unternehmen, Geschäftsprozesse zu digitalisieren und für die elektronischen Dokumente und Daten auch in ferner Zukunft die Lesbarkeit, Verfügbarkeit sowie die Integrität, Authentizität und Verkehrsfähigkeit gewährleisten zu müssen. Besondere Herausforderungen existieren in diesem Umfeld beim dauerhaften Erhalt der Beweiskraft der elektronisch signierten Dokumente. Vor diesem Hintergrund entwickelt der DIN-Arbeitskreis NA 009-00-15-06 AK „Arbeitskreis Beweiswerterhaltung kryptographisch signierter Dokumente“ den DIN-Standard 31647, der auf der Technischen Richtlinie TR 03215 „Beweiswerterhaltung kryptographisch signierter Dokumente“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufsetzt. Dieser Beitrag stellt die wesentlichen Inhalte und das mögliche Zusammenspiel des DIN-Standards und der BSI-TR-03125 (TR-ESOR) vor.

1 Einleitung

Die Nutzung der Informationstechnologie für Abwicklungen von Geschäftsprozessen ist allgemein etabliert. Geschäftsrelevante Unterlagen liegen zunehmend ausschließlich elektronisch vor. Elektronische Dokumente können jedoch aus sich heraus weder wahrgenommen noch gelesen werden. Sie liefern aus sich heraus auch keine Hinweise für ihre Integrität und Authentizität sowie die Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Gleichzeitig bestehen jedoch umfassende Dokumentations- und Aufbewahrungspflichten, deren Dauer zwischen zwei und 110 Jahre oder dauernd umfasst, die einen langfristigen Nachweis von Authentizität, Integrität und Nachvollziehbarkeit elektronischer Unterlagen erfordern. Während dieser Fristen muss es zudem möglich sein, die Dokumente Prüfbehörden oder Gerichten vorzulegen und anhand der Daten die genannten Nachweise zu führen. Dies erfordert eine langfristige Verkehrsfähigkeit der Unterlagen. Die Nutzung kryptographischer Mittel, wie fortgeschrittene oder qualifizierte elektronischer Signaturen und qualifizierte

Zeitstempel, ermöglicht nach geltendem Recht die Erhaltung des für die Nachweisführung notwendigen Beweiswerts, ohne die Verkehrsfähigkeit einzuschränken (siehe [F 06], [Ro07], [BMWi 07]).

Besondere Herausforderungen existieren in diesem Umfeld bei der Beweiswerterhaltung der elektronisch signierten Dokumente, da die Sicherheitseignungen der eingesetzten kryptographischen Algorithmen mit der Zeit abnehmen können, so dass im Rahmen der langfristigen Aufbewahrungsdauer signierter Dokumente zusätzliche Maßnahmen für den Erhalt der Beweiskraft notwendig sind. Die BSI-TR-03125, die auch Eingang in den ersten Kommentar zu § 6 EGovG (Elektronische Aktenführung) gefunden hat, wurde auf der Grundlage bestehender rechtlicher Normen sowie nationaler und internationaler technischer Standards entwickelt und liefert eine modular aufgebaute, logische Gesamtkonzeption und technische Spezifikation für die beweiswerterhaltende Langzeitspeicherung kryptographisch signierter Daten und Dokumente im Rahmen der gesetzlichen Aufbewahrungsfristen. Die DIN-Norm 31647 (Entwurf) beschreibt, basierend u.a. auf der Technischen Richtlinie BSI-TR-03215 „Beweiswerterhaltung kryptographisch signierter Dokumente“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie in Anlehnung an das OAIS-Modell [OAIS] und die DIN 31644, grundsätzliche fachliche und funktionale Anforderungen an ein generisches System zur Beweiswerterhaltung kryptographisch signierter Dokumente unter Wahrung der Authentizität, Integrität, Verlässlichkeit, Verkehrs- und Migrationsfähigkeit der Dokumente bis zum Ablauf der geltenden Aufbewahrungsfristen.

Der vorliegende Beitrag stellt den aktuellen Arbeitsstand hinsichtlich der Entwicklung der DIN 31647 und das mögliche Zusammenspiel mit der existierenden BSI-TR-03125 vor und ist folgendermaßen gegliedert: Abschnitt 2 erläutert die grundsätzlichen Anforderungen an die Aufbewahrung elektronischer Unterlagen. Der Abschnitt 3 enthält einen Überblick über die DIN-Norm 31647. Abschnitt 4 greift ausgewählte Aspekte der BSI-TR-03125 (TR-ESOR) auf. In Abschnitt 5 werden die wesentlichen Ergebnisse des Beitrags kurz zusammengefasst und um einen Ausblick auf zukünftige Entwicklungen ergänzt.

2 Grundsätzliche Anforderungen an die Aufbewahrung elektronischer Unterlagen

2.1 Grundsatz

Um insbesondere im Bereich der öffentlichen Behörden eine Abgrenzung zum normativ definierten Begriff der Archivierung, die die dauerhafte Aufbewahrung archivwürdiger Unterlagen im zuständigen öffentlichen Archiv umfasst, hat sich für die Aufbewahrung im Rahmen geltender Aufbewahrungsfristen der Terminus „Langzeitspeicherung“ gemäß ([BMI 12], [BSI-TR-03125], [BarchG]) bzw. gemäß äquivalenten Gesetzen der Länder und Archivsatzungen der Kommunen etabliert und wird dementsprechend auch im Text verwendet. Ein System, dass die Langzeitspeicherung umsetzt, wird dementsprechend als elektronischer „Langzeitspeicher“ bezeichnet.

Während dieser Aufbewahrungsfristen muss die Authentizität, Integrität und Nachvollziehbarkeit (siehe auch [BSI-TR-RESISCAN], Tabelle 6) gegenüber Prüfbehörden, Gerichten, etc. nachgewiesen werden können, was neben der Erhaltung der Unterlagen selbst vor allem die Erhaltung des Beweiswerts dieser Unterlagen erfordert (siehe [F 06], [Ro07]). Durch die Verwendung geeigneter kryptographischer Mittel, wie sie bei der qualifizierten elektronischen Signatur und bei qualifizierten Zeitstempeln zum Einsatz kommen, kann ein hoher Beweiswert erzielt und langfristig erhalten werden.

So ermöglichen fortgeschrittene oder qualifizierte elektronische Signaturen und qualifizierte Zeitstempel nach geltendem Recht die zur eindeutigen Nachweisführung notwendige Beweiswerterhaltung direkt am eigentlichen Dokument, da Signaturen und Zeitstempel direkt am Dokument oder der digitalen Akte bzw. dem Vorgang, in der sich das Dokument befindet, angebracht werden.

Der Beweiswert ist also eine inhärente Eigenschaft der jeweiligen elektronischen Unterlagen. Dementsprechend müssen Maßnahmen zur Beweiswerterhaltung auch direkt an den elektronischen Unterlagen ansetzen. Dies bedingt quasi die Langzeitspeicherung selbsttragender Archivpakete im Sinne geltender Standards und Normen (z.B. OAIS-Modell, [BSI-TR-03125]).Dabei ergibt sich der folgende Lebenszyklus elektronischer Unterlagen.

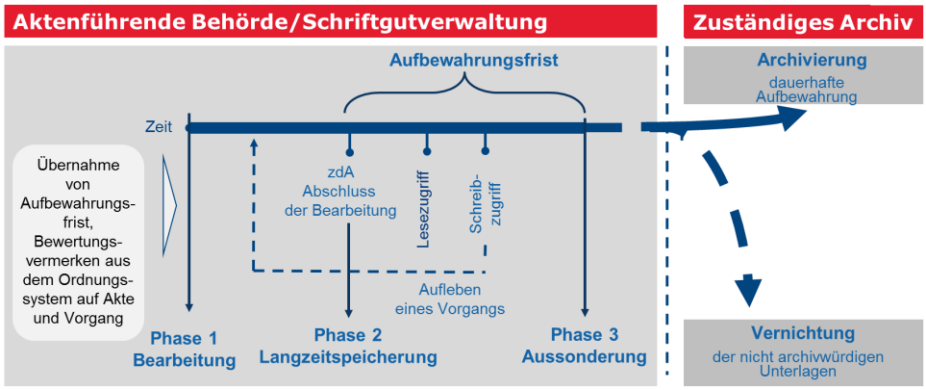

Abbildung 1: Lebenszyklus elektronischer Unterlagen

Da die Sicherheitseignung der den kryptographischen Mitteln zugrundeliegenden Algorithmen im Kontext der technischen Entwicklung abnehmen kann, ist es insbesondere bei qualifizierten elektronischen Signaturen notwendig, diese vor Ablauf der Sicherheitseignung zu erneuern. Dies erfolgt durch eine Nachsignatur (§ 17 SigV), also der Anbringung einer neuen qualifizierten elektronischen Signatur sowie eines qualifizierten Zeitstempels. Hierbei genügt die Erstellung von qualifizierten Zeitstempeln, sofern diese mittels einer qualifizierten elektronischen Signatur erzeugt wurden. Außerdem kann ein solcher Zeitstempel mehrere Dokumente, ihre Hashwerte oder einen aus solchen Hashwerten gebildeten Merkle-Hashbaum gemäß RFC 4998 bzw. RFC 6283 umfassen, was eine sehr wirtschaftliche Nachsignatur einer Vielzahl von

Dokumenten ermöglicht[1]. Die Nachsignatur muss dabei jeweils alle vorhergehenden Signaturen und Zeitstempel einschließen. Sofern auch die Sicherheitseignung der der Signatur zugrundeliegenden Hashalgorithmen ausläuft, sind zunächst neue Hashwerte mit einem geeigneten Algorithmus zu berechnen, bevor die Nachsignatur unter Verwendung qualifiziert signierter qualifizierter Zeitstempel erfolgt.

Hinzu kommt eine sichere Speicherung und Datenhaltung, um den Anforderungen hinsichtlich Datensicherheit und Datenschutz gerecht zu werden. Dabei ist es z.B. für die öffentliche Verwaltung nicht ausreichend, einzelne Dokumente oder Daten aufzubewahren. Vielmehr muss die Langzeitspeicherung den Entstehungskontext bzw. den Aktenzusammenhang wahren. Es gilt, Verwaltungsentscheidungen für die gesamte Dauer der Aufbewahrungsfristen nachvollziehbar und beweissicher zu halten. Nur so kann der bestehende Beweiswert erhalten und Kosten für die aufwändige Rekonstruktion der Unterlagen vermieden werden. Der Beweiswert und damit die Behandlung elektronischer Unterlagen vor Gericht wird in §§ 371a ff. ZPO geregelt. Diese Regelungen gelten gem. u.a. § 98 VwGO auch für die öffentliche Verwaltung. Für die öffentliche Verwaltung ist darüber hinaus zu beachten, dass der Beweis anhand von Akten und in der Folge den Dokumenten geführt wird (§ 99 VwGO). Hierfür ist es also notwendig, erst einmal Akten zu bilden und im Aktenzusammenhang aufzubewahren.

Diese Anforderungen und Rahmenbedingungen gelten für alle elektronischen Unterlagen, unabhängig davon, in welchen Verfahren oder Ablage diese gehalten werden. Um die geltenden Anforderungen an die Aufbewahrung elektronischer Unterlagen zu erfüllen, gilt es, aktuelle nationale sowie internationale Standards und Normen zu berücksichtigen. Hierzu zählt z.B. das in ISO 14721 definierte Open Archival Information System (OAIS) - Modell als zentrale Norm, an das sich auch die DIN 31647 (Entwurf) anlehnt sowie die in RFC 4998 und RFC 6283 standardisierte Evidence Record Syntax, die im Regelfall Zeitstempeln gemäß RFC 3161 umfasst.

2.2 Beweiswerterhaltende Langzeitspeicherung und OAIS-Modell

Das in ISO-14721:2012 genormte OAIS kann als zentrale Norm zur Langzeitspeicherung und Archivierung elektronischer Unterlagen betrachtet werden. Es beschreibt die grundsätzlichen Prozesse und Informationspakete zur langfristigen oder dauerhaften Aufbewahrung digitaler Daten[2]. Ursprünglich entwickelt wurde es für die Aufbewahrung von Forschungsdaten in der Raumfahrt, aber inzwischen hat es sich weltweit zur Langzeitspeicherung und Archivierung durchgesetzt.

Die nachstehende Grafik zeigt das OAIS-Modell im Überblick:

---

[1] Umgekehrt würde bei Einsatz der von ETSI für die langfristige Archivierung von Signaturen standardisierten {C,X,P}AdES-A – Formate für jede zu konservierende Signatur ein eigener Zeitstempel benötigt werden.

[2] Das OAIS-Modell gibt dabei keinerlei Vorgaben zur Implementierung oder Umsetzung. [OAIS].

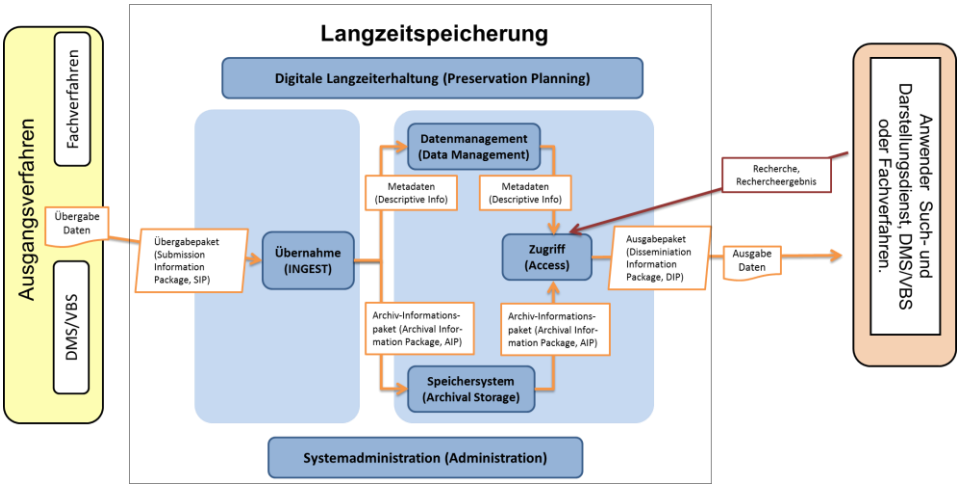

Abbildung 2: Open Archival Information System

Eine an ISO-14721-2012 angelehnte Langzeitspeicherung ist vollständig *hersteller- und systemneutral*. Das OAIS-Modell bezieht sich ausschließlich auf die Aufbewahrung und langfristige Erhaltung der elektronischen Unterlagen selbst, denn Hard- und Software unterliegen regelmäßigen Veränderungen aufgrund der IT- und wirtschaftlichen Entwicklung. Die Aufbewahrungspflichten beziehen sich zudem ausschließlich auf die Unterlagen selbst, nicht auf die Verfahren und die Hardware. Insofern gilt es, die Unterlagen selbst aufzubewahren in Form selbsttragender Archivinformationspakete. Eine solche hersteller- und systemneutrale Langzeitspeicherung umfasst für alle aufzubewahrenden Unterlagen die folgenden Prozesse mit den jeweils angegebenen grundlegenden Eigenschaften.

- Prozesse
    - Ingest (Übernahme),
    - Archival Storage (Speicher/elektronisches Magazin),
    - Daten Management (Metadatenverwaltung),
    - Access (Nutzung),
    - Preservation Planning (digitale Bestandserhaltung),
    - Systemadministration,
- Informationspakete
    - Submission Information Package – SIP (Übergabepaket): aufzubewahrende Daten aus dem laufenden Verfahren,

- Archival Information Package – AIP (Archivinformationspaket): Form, in der die Daten aufbewahrt werden,

- Dissemination Information Package – DIP (Ausgabepaket): Form, in der die Daten beim Zugriff abhängig von den Zugriffsrechten ausgegeben werden.

Das OAIS-Modell geht dabei grundsätzlich davon aus, dass selbsttragende Informationspakete, die sog. Archivinformationspakete (AIP), im Archivspeicher abgelegt werden.

3 Rahmen und mögliche Inhalte der DIN 31647 (Entwurf)

3.1 Fachliche Einführung

Die DIN 31647 formuliert fachliche und funktionale Anforderungen an ein generisches System zur Beweiswerterhaltung kryptographisch signierter Dokumente unter Wahrung der Authentizität[3], Integrität[4], Nachvollziehbarkeit, Verfügbarkeit, Verkehrs- und Austauschfähigkeit der Dokumente bis zum Ablauf der geltenden Aufbewahrungsfristen. Die Archivierung in Gedächtnisorganisationen ist kein Anwendungsfeld der DIN 31647.

Die in der Norm 31647 beschriebenen Funktionen zur Beweiswerterhaltung kryptographisch signierter Dokumente stellen dabei kein eigenes System dar. Sie ergänzen vielmehr einen in Anlehnung an das OAIS-Modell aufgebauten „Langzeitspeicher“, z.B. ein vertrauenswürdiges digitales Langzeitarchiv (dLZA) im Sinne der DIN 31644, um die notwendigen Funktionen zur Beweiswerterhaltung kryptographisch signierter Dokumente. Die DIN 31647 (Entwurf) lehnt sich insbesondere hinsichtlich der Informationspakete an das OAIS-Modell an.

Das bedeutet in der Folge, dass ein „Langzeitspeicher“, in dem die Beweiswerterhaltung kryptographisch signierter Dokumente erfolgen und der die in Kap. 2 beschriebenen Anforderungen an eine elektronische Langzeitspeicherung vollständig erfüllen soll, sowohl

- Beweiswerterhaltung[5]

als auch

[3] Unter Authentizität wird hier Übereinstimmung des kryptographisch signierten Dokuments mit den Ursprungsdaten (Echtheit der Dokumente) und deren eindeutige Zurechenbarkeit zu einem Aussteller (Verfassers, Erstellers und/oder Absenders) verstanden.

[4] Integrität bedeutet im Kontext der Beweiswerterhaltung, dass die betreffenden Daten vollständig sind und bezüglich ihrer signifikanten Eigenschaften nachweislich keine Veränderungen oder Manipulationen an den Daten festgestellt werden können

[5] Beweiswerterhaltung im Sinne der DIN 31647 bedeutet, die Gewährleistung der mit der Aufbewahrung bezweckten Rechtsfolgen elektronischer Unterlagen bis zum Ablauf der vorgeschriebenen Aufbewahrungszeiträume. Technisch wird dies durch Beweisdaten und beweisrelevante Daten realisiert also kryptographische Sicherungsmittel und deren Erhaltung realisiert.

- Informationserhaltung

ermöglicht und so eine bedarfsorientierte Verbindung der etablierten Standards und Normen zu einer Gesamtlösung umfasst, die beide Teile adressiert. Das heißt auch, dass Fragen nach der Informationserhaltung kryptographisch signierter Dokumente keine Bestandteile der DIN 31647 darstellen, sondern für diese Aspekte vielmehr im Rahmen Preservation Planning eigenständig entsprechende Maßnahmen, z.B. unter Aufgreifen des Migrations- oder Emulationsverfahrens, zu treffen sind[6].

Unter kryptographisch signierten Dokumenten werden alle elektronischen Datenobjekte verstanden, deren Integrität und ggf. Authentizität durch die Verwendung kryptographischer Sicherungsmittel (z.B. Signaturen, Zeitstempel) nachgewiesen werden und damit deren Beweiswert erhalten werden soll. Hintergrund ist, dass diese Sicherungsmittel einen langfristigen, mathematisch eindeutigen Integritäts- und ggf. Authentizitätsnachweis und die vollständige Beweiswerterhaltung ermöglichen.

Ein selbsttragendes Informationspaket in einem solchen „Langzeitspeicher“, der auch die Beweiswerterhaltung kryptographisch signierter elektronischen Unterlagen ermöglicht würde faktisch bedeuten, dass insbesondere das AIP selbst alle Informationen zur Interpretation, Lesbarkeit, Nutzbarkeit, Verständlichkeit, Recherche und zu den beweisrelevanten Nachweisen der Integrität und Authentizität der aufzubewahrenden Unterlagen in standardisierter und herstellerneutraler Form (i.d.R. in einem XML-basierten Paket) enthalten. Dies würde:

- Metadaten,
- Inhalts-/Primärdaten sowie die
- zum langfristigen Nachweis von Authentizität und Integrität notwendige Daten

umfassen.

3.4 Mögliche Anforderungen und Funktionen eines generischen Systems zur Beweiswerterhaltung im Sinne der DIN 31647 (Entwurf)

Aufbauend auf einem allgemeingültigen Vokabular beschreibt die DIN 31647 (Entwurf) Anforderungen und Funktionen an ein generisches System zur Beweiswerterhaltung. Die Darstellung basiert auf der TR-03125, ermöglicht in der Umsetzung jedoch explizit auch eine die TR-03125 ergänzende oder über diese hinausgehende Realisierung. Die DIN-Norm ist hier technik- und anwendungsneutral.

Dieses erfüllt z.B. die folgenden Anforderungen:

---

[6] Das Projekt TransiDoc hat z.B. eine Lösung zur Nutzung des Migrationsverfahrens als Methode zur Informationserhaltung kryptographisch signierter Dokumente erarbeitet (Vgl. http://www.transidoc.de).

- Hashen von AIP:
  - Erzeugung kryptographischer, sicherheitsgeeigneter Hashwerte[7],
  - Vermeidung von Mehrdeutigkeiten bei signierten XML-Daten,
  - Möglichst frühzeitiges Hashen der AIP zur Integritäts-/Authentizitätssicherung, Aufbau eines Hashbaums (RFC 4998 bzw. RFC 6283) und Versiegelung des Baums mit einem Archivzeitstempel (RFC 3161 und RFC 5652),
  - Sortierung, Konkatenation und Kanonisierung von Daten,
  - Nachvollziehbarkeit der Beweiswerterhaltung einschl. Wahrung von Hard- und Softwareneutralität sowie Interoperabilität,
  - Fähigkeit zum Datenaustausch zwischen IT-Verfahren bzw. Speichersystemen durch selbsttragende AIP.

Ein generisches System zur Beweiswerterhaltung beinhaltet daneben z.B. folgenden Funktionen:

- Einholung und Prüfung der beweisrelevanten Daten des SIP:
  - Signaturprüfung, Einholung beweisrelevanter Daten (z.B. Zertifikatsinformationen, Sperrdaten) und Einlagerung im AIP
- Erzeugen von technischen Beweisdaten des AIP:
  - Evidence Record gem. RFC 4998 bzw. RFC 6283 einschl. Archivzeitstempel und Nachweis über Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung / Hasherneuerung,
- Abruf der technischen Beweisdaten und beweisrelevanten Daten des AIP,
- Prüfung der technischen Beweisdaten,
- Erhaltung durch Erneuerung der technischen Beweisdaten des AIP,
- Nachsignatur und Hasherneuerung.

Im Ergebnis entsteht so die branchen- und anwendungsfallübergreifende Darstellung eines generischen Systems zur Beweiswerterhaltung kryptographisch signierter Unterlagen anhand standardisierter kryptographischer Funktionen insbesondere auf Basis von Hashwerten und qualifizierten Zeitstempel.

---

[7] Die Sicherheitseignung wird aktuell durch das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur festgestellt und veröffentlicht.

3.3 Mögliche Konkretisierung der Informationspakete orientiert am OAIS-Modell im Kontext der Beweiswerterhaltung

Zur fachlichen Einordnung und Verständnis der Norm bestehen Planungen, ggf. einen Vorschlag zur Konkretisierung der Informationspakete des OAIS-Modell im Hinblick auf die Beweiswerterhaltung z.B. in einem möglichen Anhang aufzunehmen. Nachstehend wird ein Auszug der Überlegungen hierzu gegeben.

Im Kontext der Beweiswerterhaltung kryptographisch signierter Dokumente sind grundsätzlich alle Informationspakete, SIP, AIP und DIP, relevant. Einzig das AIP enthält jedoch einen vollständigen Satz der Preservation Description Information (PDI bzw. Erhaltungsmetadaten), welche die zu bewahrenden Eigenschaften der Datenobjekte beinhalten. Der Konkretisierungsvorschlag fokussiert auf die PDI.

Innerhalb der Provenance Information (Herkunftsinformation) der PDI beschreibt die Information Property Description, welche Eigenschaften der Inhaltsdatenobjekte zu den signifikanten Eigenschaften gehören. Für den Beweiswerterhalt ist es notwendig, dass der Anwender / Produzent die kryptographisch zu schützenden Datenobjekte kennzeichnet und ihre zu erhaltenen Eigenschaften durch spezielle Erhaltungsmetadaten, die sog. Beweisdatenbeschreibung, innerhalb der Information Property Description aufführen. Diese Beschreibung muss nach den derzeitigen Überlegungen dabei mindestens die folgenden Informationen enthalten:

- auf welche Datenobjekte sich kryptographische Sicherungsmittel beziehen,
- welche Eigenschaften (Integrität und/oder Authentizität) der Datenobjekte geschützt werden sollen und
- welche Anforderungen an die Prüfung der Sicherungsmittel und ihre Ergänzung um Validierungsdaten gestellt werden.

Die Beweisdatenbeschreibung dokumentiert faktisch, wie Integrität und Authentizität nachgewiesen werden.

Für die Beweiswerterhaltung sind Beweisdaten und beweisrelevante Daten notwendig. Beweisdaten dienen dem Nachweis der Unversehrtheit der Integrität und Authentizität. Ein Beweisdatensatz (sog. Technische Beweisdaten) auf Basis von RFC4998 bzw. RFC6283 enthält u.a. Archivzeitstempel über die gespeicherten Archivdatenobjekte sowie weitere Informationen, die die Richtigkeit und die Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung nachweisen. Beweisrelevante Daten sind Signaturen bzw. Zeitstempel zu genau einem Datenobjekt inklusive der für die Prüfung der Signatur bzw.- Zeitstempel notwendigen Prüfdaten. Diese ermöglichen es, die Eigenschaften Integrität und / oder Authentizität von digitalen Objekten nachzuweisen und damit die Basis zur Beweiswerterhaltung kryptographisch signierter Dokumente zu bilden. Vor diesem Hintergrund wären Beweisdaten und beweisrelevante Daten in den Fixity Information der Erhaltungsmetadaten eines Informationspakets abzulegen. Das Archivinformationspaket

muss dabei einen vollständigen Satz der Beweisdaten und beweisrelevanten Daten innerhalb der Fixity Information der Erhaltungsmetadaten umfassen.

Sofern kryptographisch signierte Dokumente z.B. in ein dLZA übernommen werden, muss bereits das Übernahmeinformationspaket (SIP) die Signaturen als Beweisdaten in den Erhaltungsmetadaten umfassen. Der Schutz des Beweiswertes kann sich dabei sowohl auf in Transferpaketen (SIP) enthaltene Beweisdaten als auch auf dort ungeschützte Inhaltsdaten beziehen. Für ursprünglich ungeschützte, also nicht kryptographisch signierte Datenobjekte können zum Zeitpunkt der Einlagerung Integritätsnachweise erzeugt und nachweisbar erhalten werden. In Transferpaketen enthaltene kryptographische Authentizitätsnachweise (elektronische Signaturen) sind explizit auszuweisen.

Beweisdaten und beweisrelevante Daten sind grundsätzlich einem digitalen Objekt zugeordnet. Sie bilden mit dem AIP eine logische Einheit und stehen mit diesem für die vollständige Aufbewahrungsdauer in einem untrennbaren Zusammenhang.

Zusammenfassend würde dies bedeuten, dass die Provenance Information den Aussteller eines Dokuments sowie die in den Fixity Information enthaltenen beweisrelevanten Daten und Beweisdaten beschreiben und auf diese verweisen. Die kryptographischen Daten für den Authentizitäts- und Integritätsnachweis im Kontext der Beweiswerterhaltung selbst würden letztlich in den Fixity Information nachgewiesen. Die nachstehende Grafik verdeutlicht diese Überlegungen:

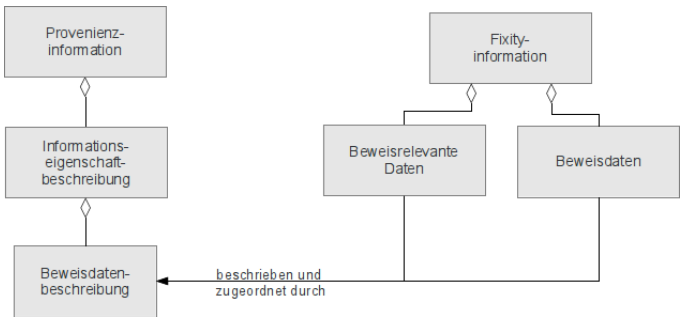

Abbildung 3: Einordnung der Metadaten für den Beweiswerterhalt

4 Technische Richtlinie TR-ESOR (TR 03125)

Das BSI hat die Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) ebenfalls auf Basis der Standards RFC 4998 und RFC6283 und der Ergebnisse der vorausgegangenen Projekte ArchiSig und ArchiSafe 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.

Thematisch behandelt die Technische Richtlinie dabei:

- Daten- und Dokumentenformate,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Empfehlungen zu einer Referenzarchitektur, zu ihren Prozessen, Modulen und Schnittstellen als Konzept einer Middleware,
- zusätzliche Anforderungen für Bundesbehörden sowie
- Konformitätsregeln für die Konformitätsstufe 1 „logisch-funktional“ und die Konformitätsstufe 2 „technisch-interoperabel“.

Auf der Basis des vorliegenden Anforderungskatalogs können Anbieter und Produkthersteller zu dieser Richtlinie 03125 konforme Lösungsangebote entwickeln, die auf Basis der Konformitätsstufe 1 „logisch-funktional“ bzw. der Konformitätsstufe 2 „technisch-interoperabel“ zertifiziert werden können.

4.1 TR 03125 Referenzarchitektur

Aus den funktionalen Anforderungen für den Erhalt des Beweiswerts wurde in der TR 03125 eine modulare Referenzarchitektur abgeleitet, die nachfolgend erklärt wird.

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (siehe Abb. 5) besteht aus den folgenden funktionalen und logischen Einheiten:

- Das „ArchiSafe-Interface“ (TR-S. 4) bildet die Eingangs-Schnittstelle zur TR-ESOR-Middleware und bettet diese in die bestehende IT- und Infrastrukturlandschaft ein.

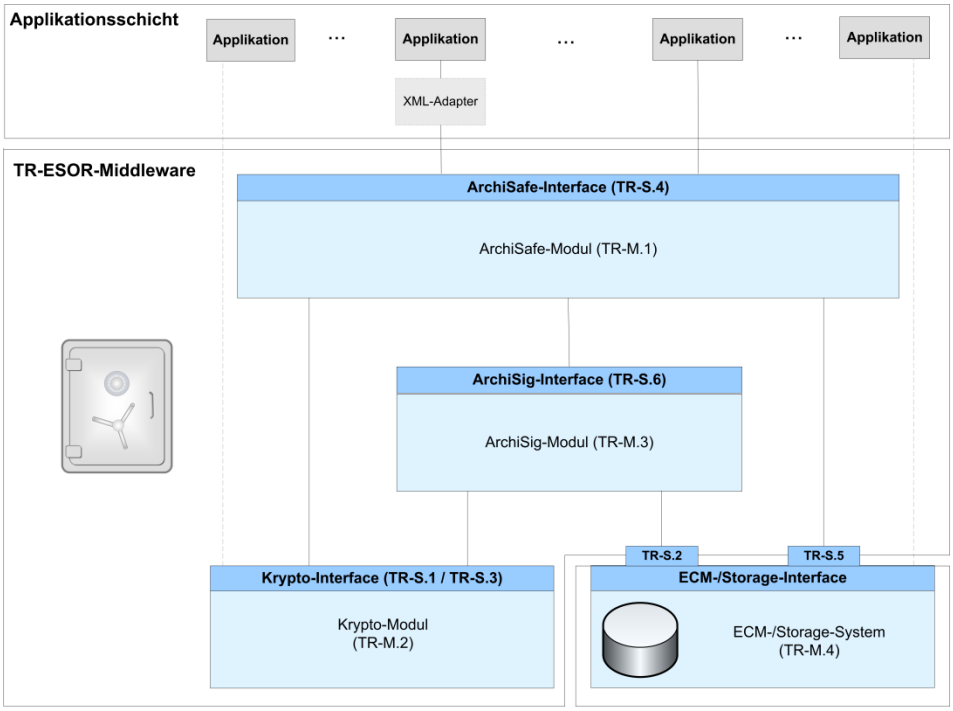

Abbildung 4: TR 03125 Referenzarchitektur

- Das „ArchiSafe-Modul“ (TR-M.1) regelt den Informationsfluss in der Middleware, sorgt dafür, dass die Sicherheitsanforderungen an die Schnittstellen zu den IT-Anwendungen umgesetzt werden und gewährleistet eine Entkopplung von Anwendungssystemen und Enterprise Content Management (ECM)/Langzeitspeicher. Die Sicherheitsanforderungen dieses Moduls sind im „Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Legally compliant Long-Term Preservation of Electronic Documents (ACM_PP)“ **Fehler! Verweisquelle konnte nicht gefunden werden.** definiert.

- Das „Krypto-Modul“ (TR-M.2) mit den Eingangsschnittstellen TR-S.1 und TR-S.3 stellt die kryptographischen Funktionen bereit, welche für den Beweiswerterhalt kryptographisch signierter Dokumente wesentlich sind. Das Krypto-Modul stellt Funktionen zur Erstellung (optional) und Prüfung elektronischer Signaturen, zur Nachprüfung elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel sowie weiterer beweisrelevanter Daten für die Middleware zur Verfügung. Das Krypto-Modul muss die Anforderungen des Gesetzes über Rahmenbedingungen für elektronische Signaturen (SigG) und der Verordnung zur elektronischen Signatur (SigV) erfüllen. Die Aufrufschnittstellen des Krypto-Moduls sollen nach dem eCard-API-Framework (vgl. **Fehler! Verweisquelle konnte nicht gefunden werden.**, [OASIS-DSS] und [BSI-TR-03125-E]) gestaltet sein, um die Integration und Austauschbarkeit kryptographischer Funktionen zu erleichtern.

- Das „ArchiSig-Modul“ (TR-M.3) mit der Schnittstelle TR-S. 6 stellt die erforderlichen Funktionen für die Beweiswerterhaltung der digital signierten Unterlagen gemäß [RoSc06] zur Verfügung. Auf diese Weise wird gewährleistet, dass die in § 17 SigV geforderte Signaturerneuerung einerseits gesetzeskonform und anderseits performant und wirtschaftlich durchgeführt werden kann und somit dauerhafte Beweissicherheit gegeben ist. Das ArchiSig-Modul bildet in der Middleware faktisch das zentrale Modul zur technischen Beweiswerterhaltung und wird daher im Folgenden näher beschrieben:

    - Um den Nachweis der Integrität und damit auch der Authentizität eines Archivdatenobjekts (AIP) auch noch nach langer Zeit führen zu können, werden Hashwerte der jeweiligen Archivdatenobjekte zusätzlich in einem Merkle-Hashbaum gespeichert. Die Hashwerte werden mit einem qualifizierten Zeitstempel mit qualifizierter elektronischer Signatur geschützt. Der Zeitstempel zusammen mit der Liste der Hashwerte wird als Archivzeitstempel (engl. Archive-Time Stamp) bezeichnet. Archivbetreiber sind gehalten, die Sicherheitseignung der eingesetzten kryptographischen Algorithmen regelmäßig zu überprüfen.

    - Wenn nur der eingesetzte Signaturalgorithmus absehbar seine Sicherheitseignung verliert, aber der eingesetzte Hashalgorithmus beibehalten werden kann, ist es ausreichend, eine Zeitstempelerneuerung durchzuführen. Für diesen Zweck wird vor Eintritt dieses Zustandes ein neuer Zeitstempel über dem zuletzt erzeugten Zeitstempel erzeugt. Auf Basis dieses Prozesses entsteht mit der Zeit eine Folge von Archivzeitstempel, die in einer „ArchiveTimeStampChain“ enthalten sind

    - Der kryptographisch geschützte Hashbaum ermöglicht so ein wirtschaftliches Verfahren zur Erneuerung elektronischer Signaturen, da nur ein zusätzlicher Zeitstempel pro Hashbaum benötigt wird.

    - Falls der eingesetzte Hash-Algorithmus in absehbarer Zeit seine Sicherheitseigenschaften verliert, muss eine Hashbaum-Erneuerung durchgeführt werden. Hierzu werden für alle Archivdatenobjekte neue Hashwerte berechnet und mit einem neu erzeugten Archivzeitstempel versehen. Das Ergebnis wird in einen neuen „ArchiveTimeStampChain“ eingefügt, so dass eine Sequenz von „ArchivTimeStampChains“, eine sogenannte „ArchiveTimeStampSequence“, entsteht.

    - Darüber hinaus unterstützt das ArchiSig-Modul u.a. auch den Abruf und Prüfung technischer Beweisdaten für den Nachweis der Integrität und Authentizität eines gespeicherten elektronischen Dokumentes und dessen Existenz zu einer bestimmten Zeit mittels der im RFC 4998 und im RFC 6283 standardisierten Beweisdaten (engl. Evidence Record). Bei der Erzeugung eines Evidence Records wird aus dem gesamten Hashbaum der reduzierter Hashbaum (siehe [RFC4998], [RFC6283]) für das entsprechende Archivdatenobjekt oder die entsprechende Archivdatenobjekt-Gruppe gewonnen und in eine

ArchivTimeStampChain eingefügt, die wiederum in einer ArchivTimeStampSequence eingebettet wird (siehe auch [DIN 31647], Kap. 3.3.2).

- Das ECM- bzw. das Langzeitspeicher-System mit den Schnittstellen TR-S. 2 und TR-S. 5, das nicht mehr Teil der Technischen Richtlinie 03125 TR-ESOR ist, sorgt für die physische Archivierung/Aufbewahrung.

Die in Abb. 5 dargestellte IT-Referenzarchitektur soll die logische (funktionale) Interoperabilität künftiger Produkte mit den Zielen und Anforderungen der Technischen Richtlinie ermöglichen und unterstützen (siehe auch [BSI-TR-03125-C.1] und [BSI-TR-03125-C.2]).

Diese strikt plattform-, produkt-, und herstellerunabhängige Technische Richtlinie [BSI-TR-03125] hat einen modularen Aufbau und besteht aus einem Hauptdokument und Anlagen, die die funktionalen und sicherheitstechnischen Anforderungen an die einzelnen Module, Schnittstellen und Formate der TR-ESOR-Middleware beschreiben.

5 Mögliche Beziehungen zwischen DIN 31647 (Entwurf) sowie der TR-03125

Die DIN 31647 (Entwurf) soll grundlegende Anforderungen und Funktionen eines generischen Systems zur Beweiswerterhaltung kryptographisch signierter Dokumente beinhalten. Der Normungsentwurf lehnt sich z.B. hinsichtlich der Informationspakete an das OAIS-Modell an. Die konkrete Umsetzung einer Lösung zur Beweiswerterhaltung kryptographisch signierter Dokumente nach DIN 31647 wäre abhängig von den fachlichen wie technischen Anforderungen der jeweiligen Institution.

Die TR-03125 des BSI beschreibt anhand dedizierter Komponenten, Prozesse sowie Anforderungen an Informationspakete aus Sicht der Beweiswerterhaltung eine mögliche und die derzeit wohl bekannteste Umsetzungsvariante der DIN 31647 (Entwurf). Mit der Empfehlung einer Referenzarchitektur unterstützt die Technische Richtlinie gezielt die Realisierung einer Beweiswerterhaltung kryptographisch signierter Dokumente im Sinne der DIN 31647 (Entwurf). Daneben konkretisiert die TR-03125 die Norm hinsichtlich Formaten, Schnittstellen und damit Interoperabilität und bietet mit den Konformitätsregeln die Option eine Zertifizierung technischer Lösungen gemäß dieser Umsetzungsvariante der DIN 31647 (Entwurf). Die Technische Richtlinie detailliert insofern die Anforderungen an die Beweiswerterhaltung digitaler Unterlagen unter Verwendung kryptographischer Methoden und lässt dabei die Anwendung der definierten Komponenten und Prozesse sowohl für vor der Langzeitspeicherung, signierte als auch unsignierte Unterlagen zu.
Neben der TR-03125 sind jedoch noch weitere Umsetzungsformen der DIN 31647 denkbar. Deren Ausprägung ist letztlich abhängig vom konkreten Bedarf und Anforderung der betreffenden Institution. Im kunden- bzw. projektspezifischen Customizing entsteht so eine bedarfs-wie anforderungsgerechte Lösung zur Beweiswerterhaltung kryptographisch signierter Dokumente.

6 Zusammenfassung

Es besteht eine hohe Notwendigkeit, nicht nur in der öffentlichen Verwaltung (E-Government) sondern auch in Unternehmen, Geschäftsprozesse zu digitalisieren und für die elektronischen Dokumente und Daten auch in ferner Zukunft die Lesbarkeit, Verfügbarkeit sowie die Integrität, Authentizität und Verkehrsfähigkeit gewährleisten zu können. Besondere Herausforderungen existieren in diesem Umfeld beim dauerhaften Erhalt des Beweiswerts kryptographisch signierter Dokumente. Vor diesem Hintergrund entwickelt der DIN-Arbeitskreis NA 009-00-15-06 „Beweiswerterhaltung kryptographisch signierter Dokumente“ mit der DIN 31647 eine verbindliche DIN-Norm. Diese setzt auf der Technischen Richtlinie TR 03215 „Beweiswerterhaltung kryptographisch signierter Dokumente“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf. Darüber hinaus lehnt sich der Normungsentwurf an weitere maßgebliche Standards und Normen explizit an. Hierzu zählen insbesondere die DIN 31644 sowie das in ISO-14721:2012 genormte OAIS-Modell. Die DIN 31647 kann diese etablierten Standards um die notwendigen Anforderungen und Funktionen an die Beweiswerterhaltung kryptographisch signierter Dokumente ergänzen.

Im Rahmen der Umsetzung einer elektronischen Langzeitspeicherung in den jeweiligen Institutionen ist letztendlich anhand des konkreten Bedarfs sowie der entsprechenden Anforderungen zu entscheiden, wie und in welchem Umfang die einschlägigen Standards und Normen angewendet werden. So könnte beispielsweise in einem bedarfs- und anforderungsgerechten Zusammenspiel von Beweiswerterhaltung und Informationserhaltung der Aufbau ganzheitlicher wie wirtschaftlicher und langfristiger Lösungen zur Langzeitspeicherung aller elektronischen Unterlagen realisiert werden, wie dies z.B. bei der Bundesagentur für Arbeit, dem Bundesministerium für Gesundheit einschl. Geschäftsbereich oder dem DVZ Mecklenburg-Vorpommern bereits umgesetzt wird bzw. in Planung ist

Literaturverzeichnis

[BArchG] Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz - BArchG) vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch § 13 Abs. 2 des Informationsfreiheitsgesetzes vom 5. September 2005 (BGBl. I S. 2722).

[BMI 12] Organisationskonzept elektronische Verwaltungsarbeit. Baustein E-Akte. Bundesministerium des Innern (Hrsg), Berlin 2012.

[BMWi 07] Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente. Bundesministerium für Wirtschaft und Technologie (Hrsg.), Berlin 2007.

[BSI-PP-0049] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents (ACM_PP)*, Version 1.0, 2008.

[BSI-TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR)*, TR 03125, Version 1.1, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2011.

[BSI-TR-03125-B] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage B zu [BSI-TR-03125], Profilierung für Bundesbehörden*, Ver. 1.1, 2011.

[BSI-TR-03125-C.1] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage C.1 zu [BSI-TR-03125], Conformity Test Specification (Level 1 – Functional Conformity)*, Ver. 1.1, 2012.

[BSI-TR-03125-C.2] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage C.2 zu [BSI-TR-03125], Conformity Test Specification (Level 2 – Technical Conformity)*, geplant für 2013.

[BSI-TR-03125-E] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage E zu [BSI-TR-03125]: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks*, TR 03125 Version 1.1, 2011.

[BSI-TR-03125-F] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Anlage F zu [BSI-TR-03125], Formate und Protokolle*, Version 1.1, 2011.

[BSI-TR-RESISCAN] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Rechtssicheres ersetzendes Scannen (TR-RESISCAN)*, Version 1.0 2013.

[DIN 31644:2012-04] Information und Dokumentation — Kriterien für vertrauenswürdige digitale Langzeitarchive.

[DIN 31645:2011-11] Information und Dokumentation — Leitfaden zur Informationsübernahme in digitale Langzeitarchive.

[DIN 31646:2013-01] Information und Dokumentation— Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier).

[DIN-31647] DIN 31645:2013-Entwurf: Beweiswerterhalt kryptografisch signierter Dokumente.

[EGovG-RE] Referentenentwurf der Bundesregierung: *Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften*, Bearbeitungsstand 16.03.2012, über http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_EGov.html.

[F 06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung. Baden-Baden 2006.

[OAIS] ISO 14721:2012, Space data and information transfer systems — Open archival information system — Reference model. 2nd Edition vom 01.09.2012

[OASIS-DSS] OASIS: *Digital Signature Service Core, Protocols, Elements, and Bindings*, Version 1.0, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html, 2007.

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP)*, IETF RFC 3161, http://www.ietf.org/rfc/rfc3161.txt, 2001.

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: *Evidence Record Syntax (ERS)*, IETF RFC 4998, http://www.ietf.org/rfc/rfc4998.txt, August 2007.

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt, Juli 2011.

[RoSc06] A. Rossnagel, P. Schmücker (Hrsg.): *Beweiskräftige elektronische Archivierung. Ergebnisse des Forschungsprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“*, Economica Verlag, 2006.

[Ro07] A. Rossnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007.