Ersetzendes Scannen und Beweiswerterhaltung für SAP

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

[1]BearingPoint
steffen.schwalm@bearingpoint.com

[2]Bundesamt für Sicherheit in Informationstechnik (BSI)
ulrike.korte@bsi.bund.de

[3]ecsec GmbH
detlef.huehnlein@ecsec.de

Zusammenfassung

In der öffentlichen Verwaltung und in privaten Unternehmen besteht zunehmend eine hohe Notwendigkeit, Geschäftsprozesse zu digitalisieren. Dabei entstehen besondere Herausforderungen in dem Umfeld der rechtssicheren Gestaltung der Scanvorgänge sowie beim dauerhaften Erhalt der Beweiskraft der elektronisch signierten Dokumente im Rahmen der gesetzlichen Aufbewahrungspflicht. Dieser Beitrag stellt zunächst die grundsätzlichen Anforderungen an die Aktenführungspflicht sowie an das ersetzende Scannen und an die vertrauenswürdige Langzeitspeicherung elektronischer Unterlagen im Allgemeinen und auf Basis der beiden Richtlinien TR-RESISCAN und TR-ESOR [TR-03138, TR-03125] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor. Danach wird eine kostensparende und effiziente Integration dieser spezifischen Verfahren gemäß TR-RESISCAN und TR-ESOR in ein SAP-System präsentiert und auf den Aspekt eines verfahrensunabhängigen weiteren Ausbaus dieser Lösungen eingegangen.

1 Einleitung

Die Nutzung der Informationstechnologie zur Abbildung der Geschäftsprozesse ist in der öffentlichen Verwaltung und privaten Unternehmen allgemein etabliert. Wesentliche Lücken oder Unsicherheiten bestehen vielfach in den Fragen:

- Können Unterlagen ausschließlich elektronisch geführt werden? Und hiermit unmittelbar im Zusammenhang stellt sich die Frage:
- Können gescannte Dokumente nach der Digitalisierung vernichtet werden?
- Wie können elektronische Unterlagen beweissicher aufbewahrt werden?

Vor dem Hintergrund sinkender Personal- und Finanzressourcen auf der einen Seite und bestehenden Dokumentations-, Nachweis- und Aufbewahrungspflichten auf der anderen Seite stellt eine nachhaltige Lösung der o.g. Fragen einen zentralen Erfolgsfaktor zur Umsetzung durchgängig elektronischer wie beweissicherer Geschäftsprozesse in Verwaltung und Unternehmen

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 72-85.

dar. Insbesondere an die öffentliche Verwaltung werden hohe Anforderungen an den gerichtsfesten Nachweis behördlicher Entscheidungen gestellt. Tragfähige wie wirtschaftliche Lösungen berücksichtigen diese Rahmenbedingung unmittelbar durch die Möglichkeit des ersetzenden Scannens, also die zeitnahe Vernichtung der digitalisierten Papierunterlagen.

Mit Blick darauf, dass Verwaltungsakten erfahrungsgemäß schnell einen Umfang von mehreren Regalkilometern, insbesondere bei Massenakten (z.B. Bußgeld, Justizakten, Antragsunterlagen etc.) annehmen, ist die Papierlagerung allein aus Kostensicht kritisch zu betrachten. Hinzu kommt, dass der Ausdruck eines elektronischen Dokuments nach geltender Rechtsmeinung eine Kopie darstellt. Ohne die Anbringung eines amtlichen Beglaubigungsvermerks auf der papiernen Kopie ist das Ausdrucken insofern hinsichtlich dessen Gerichtsfestigkeit ein durchaus heikler Punkt ([Roßn08]).

Die Problematik des ersetzenden Scannens besteht für die öffentliche Verwaltung derzeit zum einen in der notwendigen rechtlichen Ermächtigung, zum anderen im Verlust des Originalcharakters durch das Scannen. Die mit der Digitalisierung erzeugte Kopie besitzt nicht denselben Rechtscharakter als Original wie die papierne Vorlage. Der Beweiswert geht nicht auf die digitale Kopie über, da wesentliche Eigenschaften wie z.B. Unterschrift, Schriftbild, Beschaffenheit der papierbasierten Vorlage etc. aus dem Digitalisat weder erkennbar noch an diesem prüfbar sind. Mit einem ersetzenden Scannen stellt sich die anwendende Behörde damit zunächst einmal beweisrechtlich schlechter als bei einer Aufbewahrung des papiernen Originals ([Roßn07], [TR-03138]). Die besondere Herausforderung des ersetzenden Scannens besteht dementsprechend darin, den Beweiswertverlust zu minimieren und höchstmögliche Beweissicherheit zu gewährleisten.

Die Nutzung kryptographischer Mittel, wie fortgeschrittene oder qualifizierte elektronische Signaturen und qualifizierte Zeitstempel, ermöglicht nach geltendem Recht zum einen ein ersetzendes Scannen mit höchstmöglicher Beweissicherung und zum anderen die Erhaltung des für die Nachweisführung notwendigen Beweiswerts im Rahmen einer elektronischen Langzeitspeicherung, ohne die Verkehrsfähigkeit einzuschränken ([Fisc06, TR-03138, BMWi07]). Auf dieser Basis entwickelte das BSI die Technischen Richtlinien [TR-03138] und [TR-03125] mit Lösungsansätzen und Empfehlungen für Hersteller und Anwender. Sowohl die [TR-03138] als auch die [TR-03125] wurden auf Basis nationaler und internationaler Standards erstellt. Beide Technischen Richtlinien fanden Eingang in das E-Government-Gesetz des Bundes [EGovG], welches die Basis einer nachhaltigen wie beweissicheren elektronischen Verwaltungsarbeit für die öffentliche Verwaltung bildet. Auf Landesebene werden aktuell korrespondierende Gesetze erarbeitet. Im Verbund mit diesen Technischen Richtlinien, Gesetzen und Standards wie z.B. dem OAIS-Modell ([OAIS]) lassen sich ganzheitliche elektronische Prozesse abbilden, die die Beweissicherheit der Unterlagen bis zum Ablauf der geltenden Aufbewahrungsfristen gewährleisten.

Der vorliegende Beitrag stellt basierend auf konkreten Projekterfahrungen in der öffentlichen Verwaltung, bei der Bundesanstalt für Immobilienaufgaben (BImA) eine Lösungsmöglichkeit zum ersetzenden Scannen sowie der beweiswerterhaltenden Langzeitspeicherung elektronischer Unterlagen unter Einbindung von SAP auf Basis der [TR-03138] und der [TR-03125] vor. Abschnitt 2 beschreibt grundlegend die maßgeblichen rechtlichen und fachlichen Rahmenbedingungen zum ersetzenden Scannen sowie zur beweissicheren Langzeitspeicherung. Hierauf aufbauend stellt Abschnitt 3 Rahmenbedingungen und Vorgehen des Projekts sowie die gewählte Lösung vor. In Abschnitt 4 wird ein Überblick über die weiteren Ausbaustufen des

Verfahrens sowie dessen Übertragbarkeit auf vergleichbare Anwendungsfälle und Behörden oder Unternehmen gegeben.

2 Ersetzendes Scannen und Beweiswerterhaltung

2.1 Grundsätze Aktenführungspflicht und des Beweiswerts

Die öffentliche Verwaltung unterliegt als Teil der Exekutive gem. Art. 20 Abs.3 Grundgesetz dem Rechtsstaatsprinzip. Aus dem Rechtsstaatsprinzip folgen die Grundprinzipien des Verwaltungshandelns. Im Kontext des ersetzenden Scannens sowie der Langzeitspeicherung sind dabei besonders hervorzuheben:

- das Prinzip der Regelgebundenheit des Verwaltungshandelns sowie
- das Prinzip der Aktenmäßigkeit

Demgemäß ist die öffentliche Verwaltung in ihrem Handeln an Recht und Gesetz gebunden (Regelgebundenheit) und zur Nachvollziehbarkeit und Transparenz des Verwaltungshandelns – also der behördlichen Prozesse und Entscheidungen gezwungen. Dies erfordert, dass der Stand einer Sache jederzeit aus den Akten erkennbar sein muss, was erfordert, dass die Akten entweder:

- vollständig in Papierform oder
- vollständig elektronisch

zu führen sind. Das Prinzip der Aktenmäßigkeit ist für die gesamte Dauer, in der die Unterlagen für die behördliche Aufgabenerfüllung benötigt werden, sicherzustellen. Dies ist die elementare Grundlage zur Prüfbarkeit und Kontrolle behördlicher Entscheidungen durch Prüfbehörden, Gerichte, Dritte und so auch zur Rechtssicherheit für die Verwaltung selbst. Dementsprechend muss eine ordnungsgemäße Schriftgutverwaltung, die dies sicherstellt, die

- Authentizität und Integrität,
- Verfügbarkeit,
- Nachvollziehbarkeit,
- Verkehrsfähigkeit,

und damit Vertrauenswürdigkeit des Schriftguts im Aktenzusammenhang bis zum Ablauf der geltenden Aufbewahrungsfrist gewährleisten ([TR-03138, BMI12, Roßn07, Lutz12]). Dies umfasst regelmäßig neben der Erhaltung des Beweiswerts (vgl. [Fisc06, Roßn07, BMWi07]) die Aufbewahrung der Dokumente eines Vorgangs bzw. einer Akte in einem untrennbaren Zusammenhang. Die verteilte Aufbewahrung, z.B. Laufwerk, Mailpostfach und DMS/VBS resp. eine Verknüpfung loser und verteilt aufbewahrter Dokumente via Links, ist damit nicht möglich (siehe [Lutz12, Koop09, RFJK07]). Dementsprechend muss für den kompletten Lebenszyklus behördlichen Schriftguts der Entstehungskontext bzw. der Aktenzusammenhang gewahrt bleiben. Es gilt, Verwaltungsentscheidungen für die gesamte Dauer der Aufbewahrungsfristen nachvollziehbar und beweissicher zu halten.

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) [OVG

Greifswald]. Für gescannte Unterlagen ist zu beachten, dass der Beweiswert des papiernen Originals, also auch mögliche Beweiserleichterungen aufgrund technischer Vorkehrung wie Nutzung der qualifizierten elektronischen Signatur (z.B. Anscheinsbeweis etc.), nicht auf die digitale Kopie übergeht [RFJW07], da in der Regel nur originär elektronische Dokumente § 371a ZPO in Anspruch nehmen können. Die Scan-Stelle kann aber mittels einer qualifiziert signierten Erklärung die Übereinstimmung von Ausgangs- und Zieldokument bestätigen. Die Beweiserleichterung des § 371a ZPO gilt in diesem Fall nur für die Übereinstimmungserklärung und nicht auch für den Inhalt des Zieldokuments ([Wilk11, Roßn14]).

Fortgeschrittene oder qualifizierte elektronische Signaturen und qualifizierte Zeitstempel bewirken 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 denen 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, [TR-03125]). Um neben dem Beweiswerterhalt auch die Daten selbst langfristig nutzen zu können, müssen für diese, im Kontext der technischen Entwicklung Maßnahmen zur Informationserhaltung (z.B. periodische Migration) greifen. Eine nachhaltige Langzeitspeicherung umfasst also Beweiswerterhaltung und Informationserhaltung [KoSH13].

2.2 Vorgaben zur E-Akte und ersetzendes Scannen

Für die elektronische Aktenführung bestehen grundsätzlich keine besonderen Anforderungen. Zu beachten sind neben Fragen der Beweis- und Nachweisführung vor allem Formerfordernisse, wie dies auch für papierbasierte Prozesse gilt. Unterschiede liegen lediglich in der Umsetzung vor. So dürfen Dokumente, die bestimmten Formerfordernissen unterliegen (z.B. öffentliche Beglaubigung, notarielle Beurkundung), nicht ausschließlich elektronisch geführt werden, bei anderen ist dies aus praktischen Gründen (z.B. gebundene Eingänge) nicht zielführend. Diese werden bei elektronischer Verwaltungsarbeit soweit wie möglich gescannt, parallel jedoch im Original, in der sog. Papierrestakt, korrespondierend zur zugehörigen vollständigen elektronischen Akte vorgehalten, mit beiderseitigem Verweis. Die Schriftform (eigenhändige Unterschrift) kann elektronisch durch die qualifizierte elektronische Signatur, De-Mail mit Absendebestätigung oder Authentifizierung mit neuem Personalausweis erfüllt werden.

Nach geltender Rechtsmeinung bedarf die öffentliche Verwaltung eine gesetzliche Ermächtigung zum ersetzenden Scannen [RFJW07]. Diese wurde mit § 7 E-Government Gesetz des Bundes [EGovG] geschaffen. Demgemäß ist das ersetzende Scannen möglich, sofern das gewählte Scanverfahren dem Stand der Technik entspricht mit der Maßgabe der inhaltlichen wie bildlichen Übereinstimmung der digitalen Kopie.

2.3 Ersetzendes Scannen nach TR-RESISCAN

Das BSI hat mit der TR-RESISCAN [TR-03138] eine Technische Richtlinie (TR) zum ersetzenden Scannen entwickelt, die derzeit als maßgeblicher Standard zur Umsetzung entsprechend dem Stand der Technik gem. § 7 EGovG gilt. Die TR regelt Vorgehen und Maßnahmen zum dokumentenersetzenden Scannen entlang des „generischen Scanprozesses“, wie ihn die nachfolgende Grafik zeigt:

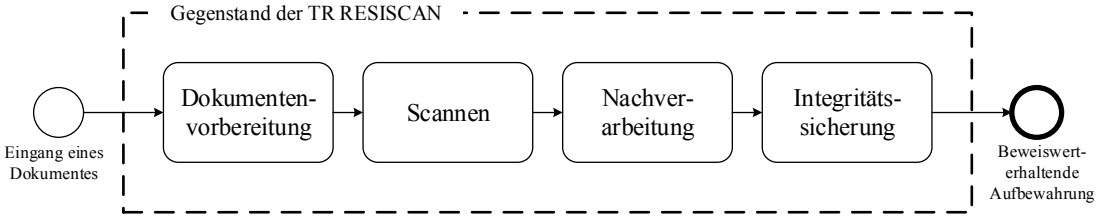

Abb. 1: Der „generische Scanprozess“ nach BSI-TR-03138

Die TR gilt dabei insbesondere für die öffentliche Verwaltung, kann jedoch auch von Unternehmen angewandt werden. Ausgangspunkt für die im Zuge der Erstellung der TR durchgeführte Risikoanalyse war ein abstraktes Modell für ein „typisches Scansystem“ [TR-03138], Anhang A 1.3. Voraussetzung für das ersetzende Scannen ist gem. [TR-03138] eine Verfahrensdokumentation, in der die Art der zu scannenden Dokumente, die notwendigen Verantwortlichkeiten Aufgaben, Abläufe, Anforderungen an die scannenden Personen, genutzte Räume, IT-Systeme, Anwendungen und Sicherungsmittel sowie Regelungen zur Systemadministration und Wartung und Maßnahmen zur IT-Sicherheit beschrieben sind. Außerdem wird eine Schutzbedarfsanalyse der zu scannenden Dokumente entsprechend der relevanten Sicherheitsziele (Authentizität, Integrität, Vollständigkeit, Nachvollziehbarkeit, Verfügbarkeit, Lesbarkeit, Verkehrsfähigkeit, Vertraulichkeit und Löschbarkeit) erwartet. Hierbei stützt sich die [TR-03138] auf das IT-Grundschutzhandbuch des BSI und korrespondierende internationale Standards, wie z.B. ISO/IEC 27001 und ISO/IEC 27005. Basierend auf der Schutzbedarfsanalyse werden die notwendigen organisatorischen, personellen und technischen Maßnahmen für das Scannen festgelegt. So ist neben organisatorischen Aspekten (z.B. Festlegung von Verantwortlichkeiten, Abläufen etc.) u.a. die Bestätigung der ordnungsgemäßen, also manipulationsfreien Transformation von Papier zum digitalen Dokument mit Hilfe eines Transfervermerks vorgesehen. Bei der technischen Ausgestaltung des Transfervermerks lässt die TR großen Gestaltungsspielraum und fordert lediglich, dass der Transfervermerk in das Scanprodukt integriert oder logisch mit diesem verknüpft wird wichtige Informationen dokumentiert (z.B. den Ersteller des Scanproduktes, das technische und organisatorische Umfeld des Erfassungsvorganges, etwaige Auffälligkeiten während des Scanprozesses, den Zeitpunkt der Erfassung und das Ergebnis der Qualitätssicherung).

Sofern Dokumente mit einem Schutzbedarf von „hoch“ für die Integrität ersetzend gescannt werden sollen, empfiehlt die TR den Einsatz kryptographischer Mittel wie z.B. fortgeschrittener oder qualifizierter elektronischer Signaturen. Werden diese nicht genutzt, ist nachzuweisen, dass die verwendeten Mittel den gleichen Schutz gewährleisten. Sofern das Scanprodukt einen sehr hohen Schutzbedarf aufweist oder als Beweismittel verwendet werden soll, was sich bei aktenrelevanten Dokumenten faktisch aus dem Prinzip der Aktenmäßigkeit ergibt, so sollen zur Integritätssicherung des Scanprodukts sowie des Transfervermerks qualifizierte elektronische Signaturen und zur Sicherung der Integrität des Scanzeitpunkts qualifizierte Zeitstempel verwendet werden. Diese Empfehlung wird insbesondere auch durch aktuelle Rechtsprechung unterstützt (vgl. [VGWiesb14]). Für den Erhalt der Beweiskraft kryptographisch signierter Daten wird in Maßnahme A.AM.IN.H.5 der [TR-03138] der Einsatz der in [TR-03125] spezifizierten Verfahren und Formate empfohlen.

2.4 Langzeitspeicherung gem. TR-ESOR

Das BSI hat die Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) auf Basis der Standards RFC4998 und RFC6283 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,
- Konformitätsregeln für die Konformitätsstufe 1 „logisch-funktional“ und die Konformitätsstufe 2 „technisch-interoperabel“ sowie für die Konformitätsstufe 3 „Bundesbehördenprofil“.

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“ bzw. der Konformitätsstufe 3 zertifiziert werden können.

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (siehe Abbildung2) besteht aus den folgenden funktionalen und logischen Einheiten:

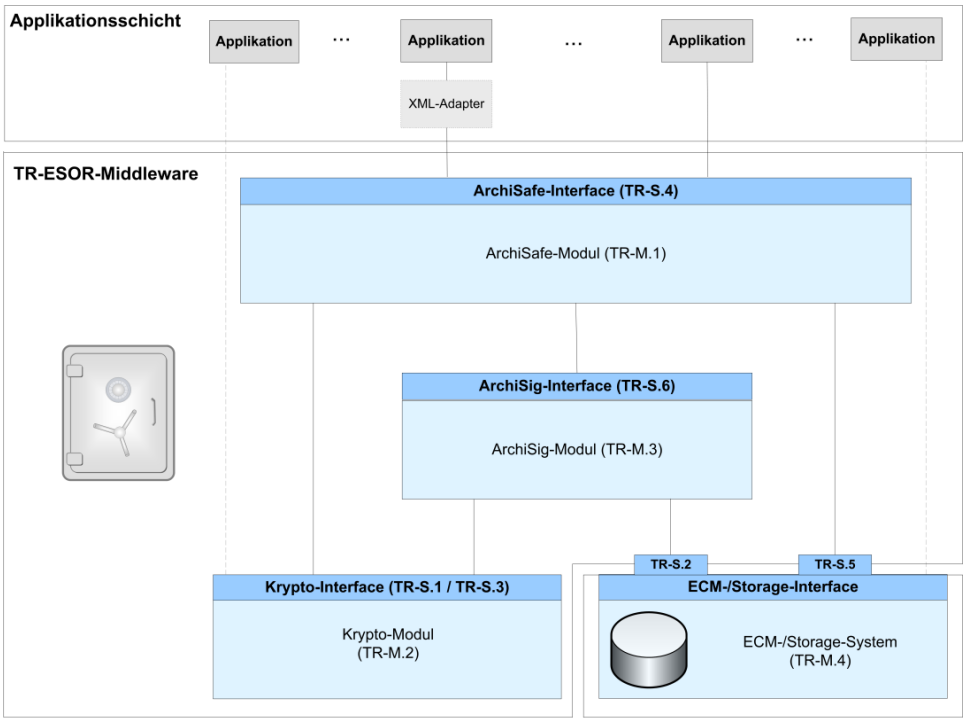

Abb. 2: Die BSI-TR-TR 03125 Referenzarchitektur

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

- 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 [PP-0049] 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. [TR-03112]) 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 elektronisch signierten Unterlagen gemäß [RFC4998]/[RFC6283][1] 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 dauerhaften technischen Beweiswerterhaltung. So werden, 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. Archivbetreiber sind gehalten, die Sicherheitseignung der eingesetzten kryptographischen Algorithmen regelmäßig zu überprüfen. Durch iterative Erneuerung des Archivzeitstempels bzw. des Hashbaums vor Ablauf der Eignung der benutzten kryptographischen Algorithmen wird sichergestellt, dass die in § 17 SigV geforderte Signaturerneuerung einerseits gesetzeskonform und anderseits performant und wirtschaftlich durchgeführt werden kann und somit Rechtssicherheit und dauerhafte Beweissicherheit gegeben sind. Um die Existenz eines speziellen Datenobjekts oder einer speziellen Datengruppe zu einem bestimmten Zeitpunkt zu beweisen, kann der Hashbaum auf eine kleine Menge von Hashwerten reduziert werden, die auch als reduzierter Hashbaum oder technische Beweisdaten (engl.: Evidence Record) bezeichnet werden. Dieser Evidence Record reicht aus, die Existenz sowie Integrität und Authentizität eines Datenobjektes oder einer Datengruppe zu einem bestimmten Zeitpunkt zu beweisen.
- Das ECM- bzw. das Langzeitspeicher-System wird über die Schnittstellen TR-S.2 und TR-S.5 angesprochen und sorgt für die physische Aufbewahrung.
- Hinsichtlich des Formats eines Archivdatenobjektes AIP wird in TR-ESOR mit dem XAIP eine XML-Struktur empfohlen, welche die Erzeugung selbsttragender AIP gem. OAIS-Modell ermöglich, ergänzt um eine Sektion für die beweisrelevanten Daten und technischen Beweisdaten – also die zur Beweiswerterhaltung notwendigen Credentials.

[1] [RFC4998] muss, [RFC6283] kann zusätzlich unterstützt werden.

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

Im Zusammenspiel von TR-RESISCAN und TR-ESOR kann so ein ganzheitliches, beweissicheres ersetzendes Scannen realisiert werden, das die Einhaltung der Anforderungen an eine ordnungsgemäße Schriftgutverwaltung bis zum Ablauf der geltenden Aufbewahrungsfristen gewährleistet.

3 TR-RESISCAN und Beweiswerterhaltung mit SAP

3.1 Einführung und Herausforderungen

Im konkreten Anwendungsfall der Bundesanstalt für Immobilienaufgaben war es das Ziel, in mehreren Stufen eine vollständig elektronische Rechnungsbearbeitung einzuführen. Die jährliche Dokumentenmenge umfasst insgesamt ca. 500.000 Dokumente. Eine Grundlage, um die Kosten einer parallelen Papieraufbewahrung zu begrenzen, ist wie beschrieben das ersetzende Scannen papierbasiert eingehender Unterlagen. Hinzu kommt die wesentliche Frage, ob die Digitalisierung intern oder extern vorgenommen wird. Mit Blick auf die erfahrungsgemäß begrenzten Personalressourcen öffentlicher Institutionen sowie den hohen finanziellen Aufwand zur Beschaffung der notwendigen Scantechnik und Schulung der Mitarbeiter der Scanstelle ist die Wahrnehmung der Aufgabe durch einen externen Dienstleister eine wirtschaftliche Alternative. Gleichzeitig zieht dies eine effiziente Qualitätssicherung und Kommunikation auf Seiten der Behörden nach sich, um eine erfolgreiche Umsetzung sicherzustellen. Der Posteingang der betreffenden Unterlagen ist dementsprechend beim Dienstleister lokalisiert.

Aus rechtlich-organisatorischer Sicht besteht im konkreten Anwendungsfall aufgrund des Dokumentinhalts (z.B. Bauwesen, Instandhaltung etc.), der zugrundeliegenden Geschäftsprozesse und bestehender Sicherheitsanforderungen aus der Immobilienverwaltung (die BImA verwaltet auch sicherheitsrelevante Gebäude) für die gescannten wie die elektronisch eingehenden Dokumente erfahrungsgemäß ein hohes Klagerisiko. Die Gewährleistung der Authentizität, Integrität, Nachvollziehbarkeit und Verkehrsfähigkeit der digitalen Unterlagen ist damit, neben der Optimierung der Prozesse sowie einer nachhaltigen wie wirtschaftlichen Lösung, ein zentraler Erfolgsfaktor.

Neben der sicheren Übergabe der gescannten Dokumente vom Scandienstleister an den SAP-Workflow ist es im konkreten Anwendungsfall dementsprechend erforderlich, die Integritätssicherung der Dokumente durch den Einsatz der qualifizierten elektronischen Signatur (Stapelsignatur je Dokument) sicherzustellen und die Unterlagen selbst beweissicher in einem geeigneten Verfahren gem. TR-ESOR aufzubewahren.

Vor dem Hintergrund der Maßgabe, dass die Verwaltung jederzeit in der Lage sein muss, die eigenen Dokumente im Aktenzusammenhang als Beweismittel vor Gericht verwenden zu können ([Koop09], [Fisc06]), können diese Maßgaben grundsätzlich auf alle Behörden übertragen werden.

3.2 Vorgehen und gewählte Lösung

3.2.1 Scanverfahren

Aufgrund der gegebenen Rahmenbedingungen in der BImA erfolgt die Digitalisierung papierner Eingänge, deren Indexierung sowie die automatisierte Verschlagwortung elektronischer Eingänge bei einem externen Dienstleister. Das Scannen erfolgt vor Beginn der Bearbeitung. Um das ersetzende Scannen gem. § 7 EGovG entsprechend dem Stand der Technik umzusetzen, war der Dienstleister verpflichtet, eine Zertifizierung des eingesetzten Scanverfahrens nach TR-RESISCAN nachzuweisen

Da die digitalisierten Dokumente künftig potenziell als Beweismittel vor Gericht dienen können, wird zur Integritätssicherung eine qualifizierte elektronische Signatur am Scanstapel angebracht. Technisch wird eine Stapelsignatur für jedes Einzeldokument des Stapels verwendet. Die Trennung der Dokumente erfolgt durch Trennblätter. Geeignete Transfervermerke gemäß der Anforderung A.NB.4 sollen künftig auf Basis der im Scanprozess entstehenden Protokolldaten erzeugt werden. Auch hier wird zur Integritätssicherung eine qualifizierte elektronische Signatur eingesetzt.

Technisch erfolgt nach der Dokumentvorbereitung ein Scannen der Dokumente nach PDF/A 1b. Ziel ist es, von Anfang an ein Dateiformat zu verwenden, das auf geltenden Standards zur langfristigen Informationserhaltung (vgl. [ISO-19005]) beruht. Entsprechend den fachlichen Notwendigkeiten werden nach dem Scannen und einer OCR-Verarbeitung Metadaten aus den Digitalisaten indexiert. Jeder Datei werden Metadaten in einer XML-Datei zugeordnet. Jede XML-Datei enthält eine eindeutige DocID für das gescannte Dokument. Dies ist eine Basis zur späteren Übergabe der Dokumente an SAP.

Der Scanstapel wird in einer ZIP-Datei, welche die XML-Dateien sowie die PDF/A-Dateien als Windows-Ordnerstruktur enthält, in einer den Maßgaben des IT-Grundschutzkataloge des BSI genügenden sicheren Verbindung vom Dienstleister in eine geschützte Datenablage der Behörde übergeben.

Die Unterlagen werden nach dem Scannen und der erfolgreichen Qualitätssicherung vernichtet. Eine wesentliche Bedingung ist die erfolgreiche Ablage im beweissicheren Langzeitspeicher gem. Kap. 3.2.2.

3.2.2 Langzeitspeicherung und Einbindung SAP

3.2.2.1 Grundsatz

Erste Planungen sahen vor, die gescannten Daten direkt an SAP zu übergeben und erst nach Beendigung des Workflows in einem SAP-Archiv abzulegen. Für ersetzend gescannte Dokumente oder sonstige Eingänge (z.B. De-Mail), die als Beweismittel dienen sollen, wird nach geltender Rechts-/Fachmeinung allerdings empfohlen, diese frühzeitig in einem geeigneten Verfahren abzulegen (vgl. [TR-03138], [RFJK07], [Roßn08]). Hintergrund dieser Empfehlung ist es, ungewollte, technische Manipulationen durch eine weitere Verarbeitung (z.B. in einem Mailserver, Workflows etc.) zu vermeiden und die Nachweiskette bis zur Ablage in einem geeigneten System möglichst gering zu halten, um so größtmögliche Sicherheit für die Behörde zu schaffen. Im Falle einer direkten Ablage im SAP ohne Prüfung der qualifizierten elektronischen Signatur der Scanprodukte und einer fehlgeschlagenen Signaturprüfung bei dem Versuch

der Archivierung am Workflow-Ende würde sich eine kaum nachvollziehbare Fehlersuche ergeben, zumal ohne gültige Signatur der Beweiswert des nach Abschluss des Scannens signierten Scanprodukts dann auch stark beeinträchtigt wäre.

Demgegenüber ermöglicht die frühzeitige Ablage des im Entstehungs-/Aktenzusammenhang unveränderten Scanprodukts oder elektronisch eingehenden Originals in einem Langzeitspeicher gem. [TR-03125] es, ab Anbringung des Archivzeitstempels, die Integrität und (implizit) Authentizität zweifelsfrei am Dokument nachzuweisen und den Beweiswert über lange Zeiträume zu erhalten. Nach aktuellem technischem Stand ist dies nur mit solchen kryptographischen Sicherungsmitteln möglich (vgl. [Fisc06], [RFJW07]).

Da es sich bei der BImA zum einen mehrheitlich um ersetzend gescannte Dokumente handelt, die, wie auch die elektronisch eingehenden Dokumente zum anderen als Beweismittel dienen sollen, wurde demgemäß entschieden, diese unter Vermeidung einer Zwischenspeicherung auf direktem Weg in einem sicheren Langzeitspeicher aufzubewahren. Die Kette möglicher Fehlerquellen sollte auf ein Minimum beschränkt werden

3.2.2.2 Lösungsfindung

Die zunächst im Fokus der Betrachtungen stehenden gescannten oder originär elektronisch vorliegenden Rechnungsunterlagen stellen nur einen kleinen Ausschnitt der aufbewahrungspflichtigen Unterlagen der BImA dar. Hinzu kommen weitere heterogene Datenbestände, die bis zum Ablauf der geltenden Aufbewahrungsfristen unter Erhaltung des Beweiswertes sowie der Daten selbst aufzubewahren sind. Die Anforderungen an eine solche Langzeitspeicherung sind für alle elektronischen Unterlagen grundsätzlich gleich und umfassen die Sicherung von deren Authentizität, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Verkehrsfähigkeit. Langzeitspeicherung ist ein Teil der Schriftgutverwaltung, insofern gelten die gleichen Vorgaben ([KoSH13]). Um den Aufbau paralleler Infrastrukturen zu vermeiden und die Option zu wahren, das einzusetzende Langzeitspeichersystem auch für weitere Unterlagen, außer den zunächst im Vordergrund stehenden Rechnungsunterlagen nutzen zu können und um auch langfristig Kostenvorteile (z.B. hinsichtlich Informations- und Beweiswerterhaltung) nutzen zu können, fiel die Entscheidung, ein an den maßgeblichen Standards zur beweissicheren Langzeitspeicherung orientiertes System gemäß [TR-03125] zu nutzen und an SAP anzubinden. Die fachliche Basis der Entscheidung war insbesondere:

- OAIS-Modell, ISO 14721:2012 [OAIS],
- Nutzung definierter Prozesse und Funktionen
- Nutzung selbsttragender Archivinformationspakete, die alle zur Interpretation, Lesbarkeit, Nutzbarkeit, Verständlichkeit, Recherche, beweisrelevanten Nachweisen der Integrität und Authentizität der aufzubewahrenden Unterlagen und damit auch für die Nachvollziehbarkeit notwendigen Daten in standardisierter und herstellerneutraler Form in einem Datenobjekt enthält
- Informationserhaltung
- DIN 31644:2012 [DIN 31644]
- Aufbau vertrauenswürdiger Aufbewahrung
- BSI TR-03125
- Beweiswerterhaltung

Mit dieser Entscheidung wurde Neuland betreten, da ein Langzeitspeicher entsprechend den o.g. Standards mit Anbindung an SAP zum Projektzeitpunkt nach allgemeiner Marktübersicht so bislang in keiner Behörde umgesetzt wurde.

Als erster Anwendungsfall dieses Langzeitspeichers wurde die Aufnahme der ersetzend gescannten Rechnungsdokumente vom Scandienstleister und deren Übergabe an den Langzeitspeicher sowie im Anschluss den SAP-Workflow umgesetzt. Als wichtigste Anforderungen an Prozesse und Datenpakete sind dabei zu nennen:

- Ablage und Speicherung der Dokumente und Metadaten in selbsttragenden XAIP-Container gem. [TR-03125-F]
- Abbildung der folgenden Prozesse gem. TR-ESOR bzw. der rechtlichen Rahmenbedingungen unter Verwendung der Schnittstellen und Protokolle gem. [TR-03125-E]
- Ablage aufzubewahrender Unterlagen und Übergabe der SAP-Doc ID an den SAP-Workflow
- Änderung (Erweiterung) der AIP und für SAP auch Ausleitung der relevanten Metadaten (z.B. finaler Beginn der Aufbewahrungsfrist) zu einem definierten Zeitpunkt am Ende des Bearbeitungsprozesses aus SAP an den Langzeitspeicher über einen ABAP-Export
- Abruf der AIP bzw. Abruf einzelner Datenobjekte (z.B. PDF/A-Dateien der Dokumente)
- Abruf technischer Beweisdaten je AIP bzw. Version
- Löschen von AIP
- Aussonderung (Kombination aus Abruf von AIP und Löschen) um die Anbietungspflicht gegenüber dem Bundesarchiv gem. § 2 BArchG zu erfüllen
- Anbindung SAP über eine SAP-ArchiveLink-zertifizierte Schnittstelle
- Erweiterung der Prozesse um notwendige Funktionen zur Erzeugung von XAIP-Containern, Verfahrensanbindung, Konvertierung etc.

Im Ergebnis entstand eine standardisierte Langzeitspeicherlösung, die die Beweiswerterhaltung und die Informationserhaltung sowohl für den ersten Anwendungsfall der Rechnungsunterlagen ermöglicht als auch ohne Weiteres zur Langzeitspeicherung anderer Daten in der BImA z.B. SAP-Datenarchivierung, Aufbewahrung digitaler Karten und Pläne, Akten, CAFM-Daten verwendet werden kann.

Sie umfasst die folgenden Komponenten:

- Upload
- Aufnahme der Dokument aus der Ablage bei der BImA
- Prüfung der erwarteten XML-Struktur
- Adapterschicht
- SAP-Anbindung durch eine SAP-ArchiveLink-zertifizierte Schnittstelle
- ID-Mapping (DocID SAP zur Archivobjekt-ID „AOID“ des Langzeitspeichers und vice verca)
- Konvertierung und Validierung (z.B. Prüfung PDF/A-Konformität)
- Erzeugung XAIP-Container für die jeweiligen Datentypen

- Management der o.g. Prozesse des Langzeitspeichers gem. TR-ESOR im Zusammenspiel mit den Geschäftsanwendungen (z.B. SAP), z.B. im Falle des Abrufs die Rückgabe der Daten in verfahrensgerechter Form
- Such- und Darstellungsdienst
- Berechtigter Zugriff auf aufbewahrte Daten
- Abbildung der Funktionen, die vom Ausgangsverfahren aus technischen Gründen nur mit unverhältnismäßigem Aufwand realisierbar sind (z.B. Abruf technischer Beweisdaten, Aussonderung)
- TR-ESOR-konforme Middleware mit folgendem Spezifikum
- Ablage der Evidence Records in den nicht gehashten Teilen des XAIP gem. [TR-ESOR-F] im Rahmen des Ablageprozesses um ein vollständig selbsttragendes AIP zu erzeugen neben der Nutzung der Hashdatenbank des ArchiSig-Moduls als Fallback.

Die folgende Abbildung 3 zeigt die Architektur im Überblick.

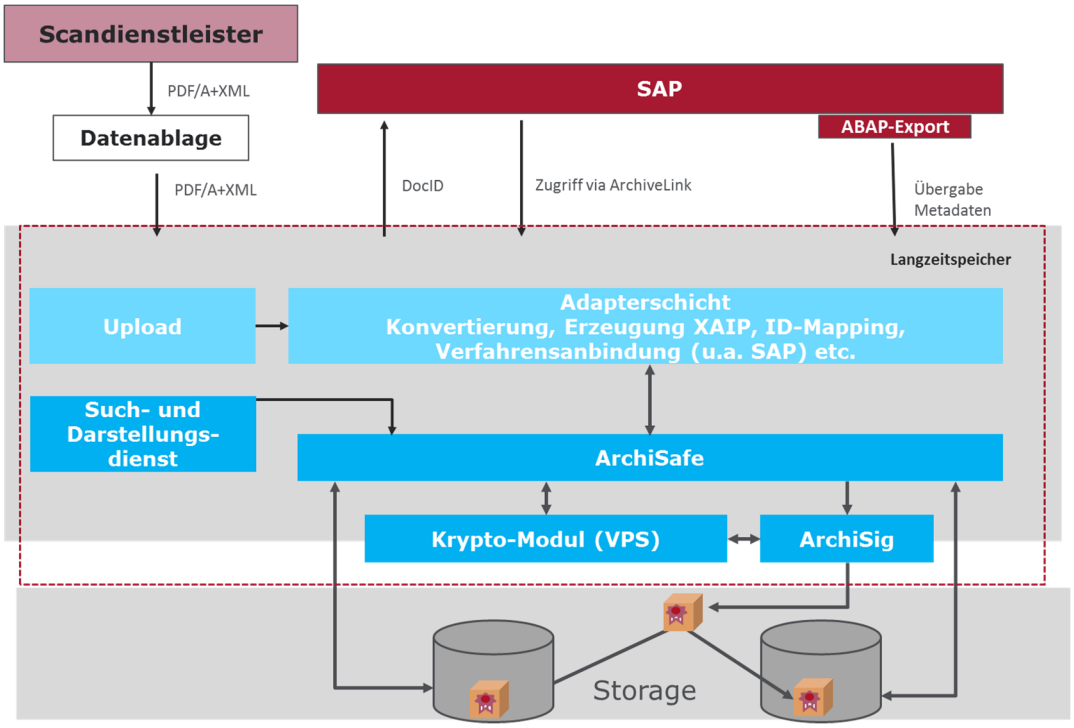

Abb. 3: Systemarchitektur im Überblick

In künftigen Anwendungsfällen, in denen das ersetzende Scannen keine Rolle spielt, würde der Scandienstleister entfallen.

Ein wesentlicher Erfolgsfaktor für diese Lösung waren wirtschaftliche Gesichtspunkte. Eine marktübliche SAP-Archivlösung hätte sich hinsichtlich der Kosten im größeren sechsstelligen Bereich bewegt und wäre einzig und allein für ein Verfahren, nämlich SAP nutzbar gewesen. Die schlussendlich beschaffte und eingeführte Variante eines nationalen wie internationalen Standards genügenden verfahrensunabhängigen Langzeitspeichers gemäß [TR-03125] senkte im Endergebnis die erforderlichen Kosten um mehr als ein Drittel.

4 Zusammenfassung und Ausblick

Die beschaffte Lösung ist für den ersten Anwendungsfall, das ersetzende Scannen sowie die beweissichere Langzeitspeicherung von Rechnungsunterlagen, seit Mai 2014 produktiv im Einsatz. Sie wird bei einem externen Dienstleister betrieben. Damit wurde der Nachweis erbracht, dass eine beweissichere Langzeitspeicherung, die sowohl die Informations- als auch die Beweiswerterhaltung in selbsttragenden und damit langfristig nutzbaren AIP ermöglicht, auch mit spezifischen Verfahren wie SAP nicht nur technisch möglich ist. Vielmehr werden mit diesem Vorgehen explizite Kostenvorteile gegenüber bisherigen, verfahrensgebundenen Lösungen erzielt.

Aufgrund des verfahrensunabhängigen Charakters des Systems ist eine Übertragbarkeit auf andere Daten erfahrungsgemäß problemlos möglich. Dies wird aktuell in der BImA konzipiert und in 2015 umgesetzt. Aufgrund der konsequenten Aufbewahrung der Unterlagen in selbsttragenden AIP in standardisierter Form wird darüber hinaus der Datenaustausch z.B. zu einem geltenden Standards genügenden Langzeitspeicher mit vereinfacht. So werden vergleichbare Lösungen zur verfahrensunabhängigen beweissicheren Langzeitspeicherung u .a. bei der Bundesagentur für Arbeit (digitales Zwischenarchiv), der Bundesministerium für Gesundheit oder auch auf Landes- und kommunaler Ebene bereits eingesetzt. Im Ergebnis besteht für die einsetzende Institution langfristige Investitionssicherheit und Flexibilität hinsichtlich der Langzeitspeicherung.

Literatur

[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).

[BMI12] Bundesministerium des Innern (Hrsg): *Organisationskonzept elektronische Verwaltungsarbeit. Baustein E-Akte.,* Berlin 2012.

[BMWi07] Bundesministerium für Wirtschaft und Technologie (Hrsg.): *Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente*, Berlin 2007.

[DIN31644] DIN 31644:2012 *Information und Dokumentation — Kriterien für vertrauenswürdige digitale Langzeitarchive*, 2012.

[DIN31647] DIN 31647:2015 *Beweiswerterhalt kryptografisch signierter Dokumente*, 2015.

[EGovG] *E-Government-Gesetz* vom 25. Juli 2013 (BGBl. I S. 2749)

[Fisc06] S. Fischer-Dieskau: *Das elektronisch signierte Dokument als Mittel zur Beweissicherung*, Baden-Baden, 2006.

[KoopA 09] AG IT-gestützte Verwaltungsarbeit des KoopA-ADV, *Grundsatzpapier „Aktenrelevanz von Dokumenten“*, Version 1.0.0, 2009.

[KoSH13] U. Korte, S. Schwalm, D. Hühnlein: *Vertrauenswürdige und beweiswerterhaltende Langzeitspeicherung auf Basis von DIN 31647 und BSI TR-03125*, Informatik 2013, GI-LNI, P220, ISBN 978-3-88579-614-5, S. 550-566, 2013

[ISO-19005] ISO 19005-1: *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4* (PDF/A-1), 2005.

[Lutz12] *Schriftgutverwaltung nach DIN ISO 15489-1. Ein Leitfaden zur qualitätssicheren Aktenführung*, Hrsg. von Alexandra Lutz c/o Arbeitskreis Schriftgutverwaltung im DIN NABD 15. Berlin 2012.

[OAIS] ISO 14721:2012*, Space data and information transfer systems – Open archival information system – Reference model*, 2nd Edition, 2012

[PP-0049] BSI: *Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents* (ACM_PP), V1.0, 2008.

[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

[Roßn07] A. Roßnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007.

[Roßn08] A. Roßnagel: Scannen von Papierdokumenten. Anforderungen, Trends und Empfehlungen. Baden-Baden 2008

[Roßn14] A. Roßnagel: Roßnagel, Alexander et. al.: Beweisführung mittels ersetzend gescannter Dokumente. In: NJW 2014 S. 886 ff.

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

[TR-03112] BSI: *eCard-API-Framework*, Version 1.1.2, 2012

[TR-03125] BSI: *Beweiswerterhaltung kryptographisch signierter Dokumente* (TR-ESOR), TR 03125, V1.2., 2015.

[TR-03125-E] BSI: *Anlage E zu TR-03125: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks*, TR 03125, V1.2, 2015.

[TR-03125-F] BSI: *Anlage F zu TR-03125, Formate und Protokolle*, TR-03125, V1.2, 2015.

[TR-03138] BSI: *Ersetzendes Scannen*, (RESISCAN), TR 03138, V1.0, 2013.

[VGWiesb14] VG Wiesbaden: Urteil vom 28. Februar 2014, Az. 6 K 152/14.WI.A

[Wilk11] D. Wilke: Die rechtssichere Transformation von Dokumenten. Rechtliche Anforderungen an die Technikgestaltung und rechtlicher Anpassungsbedarf, Baden-Baden, 2011.