Anwendung der TR-RESISCAN und TR-ESOR im Gesundheitswesen

Detlef Hühnlein[1] · Silke Jandt[2] · Ulrike Korte[3] · Maxi Nebel[2] · Astrid Schumacher[3]

[1] ecsec GmbH, Sudetenstraße 16, 96247 Michelau, detlef.huehnlein@ecsec.de

[2] Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Pfannkuchstr. 1, 34109 Kassel, {s.jandt,m.nebel}@uni-kassel.de

[3] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, {ulrike.korte,astrid.schumacher}@bsi.bund.de

Abstract: Im Gesundheitswesen besteht eine hohe Notwendigkeit, Geschäftsprozesse zu digitalisieren. Hierfür müssen Papierdokumente gescannt und originär elektronische Daten und Dokumente oft auf Grund von Formvorschriften oder aus Sicherheitsgründen mit elektronischen Signaturen versehen werden. Besondere Herausforderungen existieren in diesem Umfeld bei der rechtssicheren Gestaltung des Scanvorganges sowie beim dauerhaften Erhalt der Beweiskraft der elektronisch signierten Dokumente. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt zur Unterstützung der Anwender entsprechende Technische Richtlinien mit Lösungsansätzen und Empfehlungen für diese beiden Problembereiche, die insbesondere auch im Gesundheitswesen eingesetzt werden können. Dieser Beitrag stellt die wesentlichen Inhalte und das mögliche Zusammenspiel der beiden Richtlinien TR-RESISCAN [BSI-TR-RESISCAN] und TR-ESOR [BSI-TR-03125] vor und geht auf besondere Aspekte des Gesundheitswesens ein.

1 Einleitung

Durch die elektronische und weitgehend automatisierte Abwicklung von Geschäftsprozessen im Gesundheitswesen lassen sich Kosten senken sowie Fehlerquoten und Prozesslaufzeiten reduzieren. Gleichzeitig geht die Nutzung elektronischer Dokumente mit zusätzlichen Herausforderungen einher: Elektronische Dokumente können ohne Hilfsmittel weder wahrgenommen noch gelesen werden. Sie liefern aus sich heraus keine Anhaltspunkte für ihre Integrität und Authentizität, garantieren also weder eine inhaltliche Echtheit noch ermöglichen sie die Identifikation ihres Ausstellers. Ihre Eignung für den elektronischen Rechts- und Geschäftsverkehr ist daher stark eingeschränkt. Diese Eigenschaften, die den Papierdokumenten immanent sind, müssen bei der Transformation von Papierdokumenten in elektronische Dokumente und bei der längerfristigen Aufbewahrung elektronischer Dokumente durch organisatorische und

technische Maßnahmen hergestellt und dauerhaft erhalten werden. Vor diesem Hintergrund entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) entsprechende Technische Richtlinien mit Lösungsansätzen und Empfehlungen für diese beiden Problembereiche. Diese werden voraussichtlich zunächst in § 6 EGovG (Elektronische Aktenführung) und § 7 EGovG (Übertragen und Vernichten des Papieroriginals) ihren Niederschlag finden (siehe [EGovG-RE]), aber in ähnlicher Weise auch in anderen Anwendungsbereichen, wie z.B. dem Gesundheitswesen, eingesetzt werden können.

Dieser Beitrag stellt in Abschnitt 2 die wesentlichen rechtlichen Rahmenbedingungen für das ersetzende Scannen und die ordnungsgemäße Aufbewahrung im Gesundheitswesen dar. Abschnitt 3 beleuchtet den Regelungsgegenstand und Anwendungsbereich der beiden BSI-Richtlinien TR-RESISCAN und TR-ESOR. Abschnitt 4 bietet einen Überblick über die in TR-RESISCAN spezifizierten Anforderungen für das ordnungsgemäße ersetzende Scannen. Abschnitt 5 greift ausgewählte Aspekte der TR-ESOR auf, die auf der Grundlage bestehender rechtlicher Normen sowie nationaler und internationaler technischer Standards ein modular aufgebautes Gesamtkonzept für die beweiswerterhaltende Langzeitspeicherung bereitstellt. Abschnitt 6 fasst die wesentlichen Ergebnisse des Beitrags kurz zusammen und liefert einen Ausblick auf zukünftige Entwicklungen.

2 Rechtliche Rahmenbedingungen im Gesundheitswesen

Die Aufbewahrung medizinischer Dokumentation ist umfangreich geregelt. Jedoch werden hinsichtlich der Zulässigkeit ersetzenden Scannens meist keine Aussagen getroffen. Allgemeingültige Vorschriften bestehen nicht. In der Regel ist ersetzendes Scannen nur gestattet, wenn keine gesetzlichen Aufbewahrungs-, Dokumentations- oder Aktenführungspflichten entgegenstehen [RoWi06, S. 2146].

Im Gesundheitswesen ist dies jedoch kaum denkbar. Dokumentationspflichten erfüllen multiple Zwecke. Sie dienen gem. § 10 Abs. 1 Satz 2 der Musterberufsordnung der Ärzte 1997 (MBO-Ä) sowohl der Gedächtnisstütze des Arztes als auch dem Interesse der Patienten an einer ordnungsgemäßen Dokumentation. Die ausführliche, sorgfältige und vollständige Aufzeichnung der Behandlung ist eine vertragliche Nebenpflicht aus dem Behandlungsvertrag [Wilk11, S. 103] und ermöglicht es dem Patienten, Kenntnis über seine Behandlung zu erlangen. Damit wird eine wesentliche Voraussetzung für ihn geschaffen, seine Rechte auszuüben, zum Beispiel die Einholung anderweitiger sachkundiger Auskünfte über Gesundheitszustand und Behandlungsbedarf. Anerkannt sind außerdem die Zwecke der Therapiesicherung und der Erfüllung der Rechenschaftspflicht der Ärzte [Wilk11, S. 102]. Ob die Dokumentation darüber hinaus der gerichtlichen oder außergerichtlichen Beweissicherung dient, ist umstritten [Wilk11, S. 102 mit weiteren Nachweisen]. In Anbetracht des potentiell hohen Risikos eines gesundheitlichen wie finanziellen Schadens des Patienten erscheint dies aber sachgerecht. Außerdem wäre eine Beweisführung für beide Parteien eines Arzthaftungsprozesses ohne eine ärztliche Dokumentation nahezu ausgeschlossen [Wilk11, S. 102].

Folgende Vorschriften treffen Aussagen über die Art und Weise der Aufbewahrung medizinischer Dokumentation:

§ 10 Abs. 1 MBO-Ä verpflichtet Ärzte zur Dokumentation und Aufzeichnung der von ihnen getroffenen Feststellungen. Die Dokumentation ist bis zehn Jahre nach Abschluss der Behandlung aufzubewahren. Gemäß § 10 Abs. 5 MBO-Ä ist die Dokumentation auf elektronischen Speichermedien zulässig, sofern sichergestellt ist, dass durch besondere Sicherheits- und Schutzmaßnahmen eine Veränderung, Vernichtung oder unrechtmäßige Verwendung verhindert werden kann. Die Archivierung muss jedenfalls so erfolgen, dass über den Verbleib der Behandlungsunterlagen zu jeder Zeit Klarheit besteht [BGH, NJW 1996, 779, 780]. Gemäß § 57 Bundesmantelvertrag–Ärzte (BMV-Ä) sowie § 13 Bundesmantelvertrag-Ärzte/Ersatzkassen (EKV) hat der Vertragsarzt Zeit und Umfang der Leistung in geeigneter Weise zu dokumentieren. Auch hier beträgt die Aufbewahrungsfrist zehn Jahre. Gemäß § 57 Abs. 2 BMV-Ä sowie § 13 Abs. 11 EKV ist die Aufbewahrung in elektronischer Form möglich. Hierin liegt aber keine Erlaubnis zur ersetzenden Transformation, also zur Vernichtung der Originalunterlagen [RoWi06, S. 2147], [Wilk11, S. 103].

Einzig § 28 Abs. 4 RöV enthält eine klare Regelung zur Zulässigkeit des ersetzenden Scannens. Demnach dürfen Röntgenbilder und sonstige damit in Zusammenhang stehende Aufzeichnungen auf einem Bildträger wiedergegeben oder auf einem anderen Datenträger aufbewahrt werden, wenn sichergestellt ist, dass die Wiedergaben oder die Daten mit den Bildern oder Aufzeichnungen bildlich und inhaltlich übereinstimmen. Die elektronischen Dokumente müssen während der Dauer der Aufbewahrungsfrist verfügbar sein und jederzeit innerhalb angemessener Zeit lesbar gemacht werden können. Weiterhin muss sichergestellt sein, dass während der Aufbewahrungszeit keine Informationsänderungen oder -verluste eintreten. Die Aufbewahrungsfrist beträgt gemäß § 28 Abs. 3 RöV bei Röntgenaufnahmen zehn Jahre und bei sonstigen Aufzeichnungen über die Behandlung 30 Jahre.

Eine allgemeine Zulässigkeit ersetzenden Scannens im Gesundheitswesen kann aus dieser Regelung nicht gefolgert werden. Ein Vergleich der Vorschriften zeigt, dass lediglich § 28 RöV die Übertragung eines Papierdokuments auf einen elektronischen Datenträger voraussetzt (Abs. 4 Nr. 1: „bildlich oder inhaltlich übereinstimmen“), § 10 Abs. 5 MBO-Ä 1997 hingegen nur originär elektronische Dokumente berücksichtigt. Da in § 28 Abs. 4 RöV die Zulässigkeitsvoraussetzungen für eine ersetzende Transformation konkret normiert werden, vergleichbare Vorschriften für andere Arten der medizinischen Dokumentation jedoch nicht existieren, muss davon ausgegangen werden, dass der Gesetzgeber dies bewusst nicht regeln wollte. Somit ist nach derzeitiger Rechtslage das ersetzende Scannen für andere Arten der medizinischen Dokumentation nicht zulässig. Die hier bestehende Regelungslücke ist weder gerechtfertigt noch sachdienlich. Es kann hier nur wiederholt an den Gesetzgeber appelliert werden, eine verbindliche und eindeutige Regelung zu erlassen, da in der Praxis ein dringender Bedarf des ersetzenden Scannens medizinischer Dokumente besteht.

Ferner stellt sich die Frage, welchen Beweiswert gescannte Dokumente haben und ob nicht schon aus diesen Gründen die Originaldokumente aufzubewahren sind.

Elektronische Dokumente stellen keine Urkunden dar, sondern lediglich Augenscheinobjekte. Beweiserleichterungen schafft § 371a ZPO für solche elektronischen Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind. § 371a ZPO gilt allerdings nur für Willens- und Wissenserklärungen [BT-Drs. 15/4067, S. 34]. Vielfach ist der Inhalt des Originaldokuments eine Erklärung. Das Scanprodukt ist jedoch nur ein technisches Abbild, dem selbst kein eigener Erklärungsgehalt zukommt [SCATE, S. 91]. Wird eine elektronische Signatur in einem automatischen Scanprozess an das elektronische Scanprodukt angefügt, wird keine Erklärung signiert. Die Signatur ist in diesem Fall kein Unterschriftenersatz, sondern nur ein Sicherungsmittel, das später belegen kann, dass das Scanprodukt nach der Signierung nicht mehr verändert wurde. Es sichert so die Integrität – nicht aber die Authentizität – des elektronischen Dokuments ([SCATE, S. 90], [RoWi06, S. 2148]). Daher können in der Regel nur originär elektronische Dokumente § 371a ZPO in Anspruch nehmen. Eine qualifiziert signierte Erklärung der scannenden Stelle kann aber 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 ([SCATE, S. 90f.], [RoWi06, S. 2148]).

Lagert ein Unternehmen das Scannen seiner medizinischen Unterlagen an externe Dienstleister aus, stellen sich darüber hinaus Fragen hinsichtlich des Daten- und Geheimnisschutzes, welche nicht nur das ersetzende Scannen, sondern unabhängig vom Verwendungszweck alle externen Dienstleistungen berühren. Das Verhältnis zwischen Arzt und Patient ist geprägt durch den Schutz des Patientengeheimnisses, dass dem behandelnden Arzt die ärztliche Schweigepflicht auferlegt. Zusätzlich wird der Umgang mit personenbezogenen Patientendaten durch das Recht des Patienten auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG begrenzt (näher hierzu [JaRoWi11, 641]).

Der Patient muss eine Erklärung über die Entbindung von der ärztlichen Schweigepflicht abgeben. Andernfalls würde sich der Arzt gemäß § 203 StGB wegen Offenbarung von Patientengeheimnissen strafbar machen. Das Krankenhaus ist hierdurch mittelbar verpflichtet, den Arzt bei der Einhaltung der Schweigepflicht zu unterstützen und die Datenverarbeitung so zu gestalten, dass vom Arzt kein rechtswidriges Verhalten verlangt wird [JaRoWi11, S. 645].

Eine Datenverarbeitung ist gem. § 4 Abs. 1 BDSG nur zulässig, wenn eine gesetzliche Erlaubnisvorschrift diese vorsieht oder eine Einwilligung des Betroffenen vorliegt. Verantwortliche Stelle ist gem. § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich erhebt, verarbeitet oder nutzt oder durch andere im Auftrag vornehmen lässt. Diese hat für die Einhaltung aller datenschutzrechtlichen Vorschriften Sorge zu tragen.

Wird das Scannen durch externe Dienstleister vollzogen, stellt sich die Frage, wer verantwortliche Stelle ist. Handelt es sich um eine Auftragsdatenverarbeitung, ist gemäß § 11 BDSG das Krankenhaus verantwortliche Stelle. Kennzeichnend ist hierbei, dass der Datenumgang der externen Stelle durch Weisungen oder überlassene Arbeitsmittel sehr genau bestimmt ist, ihr kein Gestaltungsspielraum überlassen bleibt und sie keine

rechtliche Verfügungsbefugnis über die Daten hat [JaRoWi11, S. 644]. Juristisch gesehen liegt damit in der Weitergabe der Daten keine Datenübermittlung vor, sie bedarf also nicht einer gesetzlichen Erlaubnisnorm oder Einwilligung. Hier ist dann nur die Zulässigkeit der weiteren Datenverarbeitung (zum Beispiel das Scannen) anhand der gesetzlichen Vorschriften zu prüfen.

Erfolgt der Datenumgang der externen Stelle zum Beispiel auf eigene Rechnung oder fehlt es dem Auftraggeber an Einflussmöglichkeiten, so spricht viel für eine Funktionsübertragung [JaRoWi11, S. 645]. Verantwortliche Stelle ist dann das externe Dienstleistungsunternehmen und die Weitergabe der Daten von Krankenhaus an die externe Stelle bedarf einer gesetzlichen Erlaubnisvorschrift oder der Einwilligung des Betroffenen. Ist schon die Datenübermittlung mangels Erlaubnisvorschrift oder Einwilligung rechtswidrig, kann eine weitere Datenverarbeitung (zum Zwecke des Scannens) nicht mehr rechtmäßig erfolgen [JaRoWi11, S. 645].

3 Zusammenwirken der beiden Richtlinien

Während die TR-RESISCAN Anforderungen für eine ordnungsgemäße und Risiko-minimierende Gestaltung des Scanprozesses für die Transformation eines papiergebundenen Originals in ein elektronisches Abbild definiert, adressiert die TR-ESOR insbesondere den Beweiswerterhalt kryptographisch signierter Dokumente unter Verwendung von qualifizierten Zeitstempeln, wie dies in § 17 SigV für die langfristige Aufbewahrung von qualifiziert signierten Daten gefordert ist.

Wie in Abb. 1 dargestellt, kann mit einem Aufbewahrungssystem gemäß [BSI-TR-03125] insbesondere auch die in [BSI-TR-RESISCAN] geforderte Integritätssicherung der Scanprodukte erfolgen.

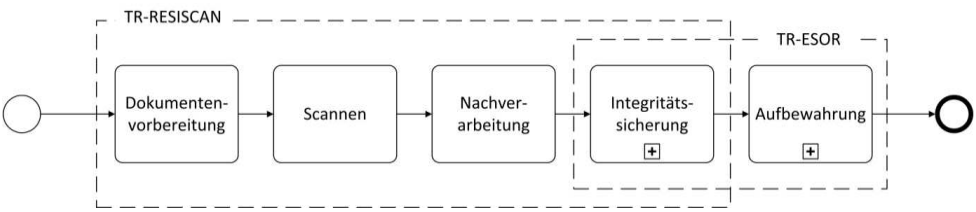

Abbildung 1: Zusammenwirken der TR-RESISCAN und TR-ESOR

Auf der anderen Seite ist die Anwendung der in [BSI-TR-03125] spezifizierten Mechanismen für die ordnungsgemäße Integritätssicherung von Dokumenten gemäß [BSI-TR-RESISCAN] nicht in jedem Fall notwendig und wirtschaftlich sinnvoll. Wie im beispielhaften Entscheidungsprozess in Abb. 2 erkennbar, können im Kontext des ersetzenden Scannens gemäß TR-RESISCAN auch alternative Mechanismen zur Integritätssicherung und Aufbewahrung eingesetzt werden. Ist der Schutzbedarf hinsichtlich der Integrität nicht sehr hoch und wird kein verkehrsfähiger Integritätsnachweis benötigt, müssen die aufzubewahrenden Dokumente nicht mit einer qualifizierten elektronischen Signatur versehen werden.

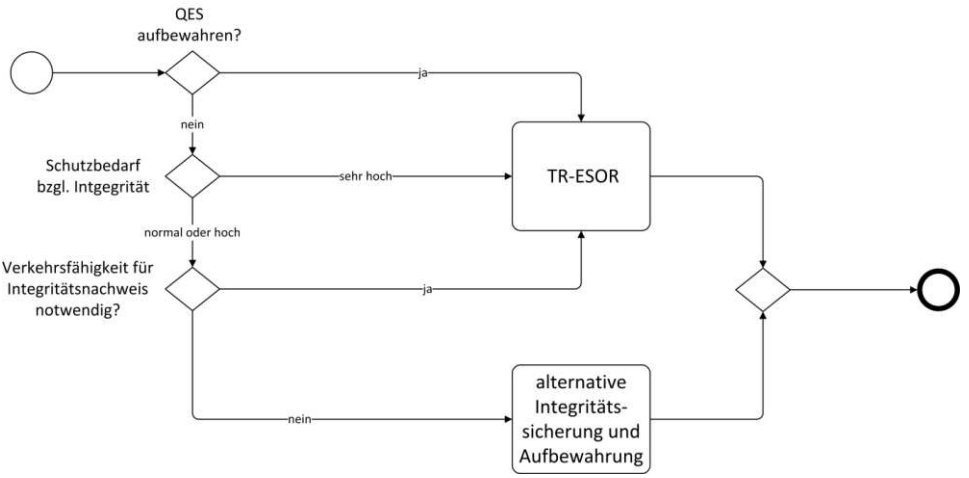

Abbildung 2: Möglicher Entscheidungsprozess für die Anwendung von TR-ESOR

4 Technische Richtlinie TR-RESISCAN

Für die Entwicklung der TR-RESISCAN wurde eine Markt-, Struktur-, Schutzbedarfs- und Bedrohungsanalyse für ein „typisches Scansystem“ und für den „generischen Scanprozess“ durchgeführt, der die Schritte Dokumentenvorbereitung, das Scannen, die Nachverarbeitung und schließlich die Integritätssicherung umfasst (vgl. Abb. 1 und Abschnitt 4.1).

Hieraus wurde ein modularer Anforderungs- und Maßnahmenkatalog (vgl. Abb. 3 und Abschnitt 4.2) entwickelt. Die Einhaltung der dort formulierten Anforderungen kann durch eine neutrale Stelle geprüft und objektiv bestätigt werden (Zertifizierung).

4.1 Struktur-, Schutzbedarfs- und Bedrohungsanalyse

Die bei der Entwicklung der TR-RESISCAN genutzte Methodik ist in informeller Weise an die internationalen Standards [ISO27001], [ISO27005], das IT-Sicherheitshandbuch [BSI-IT-SiHB] und die IT-Grundschutz-Vorgehensweise (siehe [BSI-100-2], [BSI-100-3]) des BSI angelehnt und umfasst die im Folgenden kurz erläuterten Aufgaben.

Auf Basis des durch Abstraktion aus der Praxis abgeleiteten „generischen Scanprozesses“ (siehe Abb. 1) und des „typischen Scansystems“ wurden die im weiteren Verlauf zu betrachtenden Objekte identifiziert. Hierbei wurden insbesondere die relevanten Datenobjekte (Schriftgut, Scanprodukt, Sicherungsmittel, Protokolle etc.), IT-Systeme, Netze und Anwendungen betrachtet. Für diese identifizierten Objekte wurde in zwei Schritten eine detaillierte fachliche und technische Schutzbedarfsanalyse durchgeführt. Im Rahmen der fachlichen Schutzbedarfsanalyse (siehe z.B. [SGHJ12] für Gerichtsakten) wurde zunächst ausgehend von den rechtlichen Anforderungen der

Schutzbedarf der Datenobjekte ermittelt, wobei die differenzierten Sicherheitsziele „Integrität“, „Authentizität“, „Vollständigkeit“, „Nachvollziehbarkeit“, „Verfügbarkeit“, „Lesbarkeit“, „Verkehrsfähigkeit“, „Vertraulichkeit“ und „Löschbarkeit“ betrachtet wurden. Durch die technische Schutzbedarfsanalyse wurde der Schutzbedarf der IT-Systeme, Anwendungen und Kommunikationsbeziehungen hinsichtlich der Grundwerte „Integrität“, „Verfügbarkeit“ und „Vertraulichkeit“ bestimmt.

Um die einfache Wiederverwendbarkeit der Ergebnisse im IT-Grundschutz-Kontext [BSI-100-2] zu gewährleisten, wurde der jeweilige Schutzbedarf in Abhängigkeit des Schutzbedarfs des ursprünglichen Papierdokumentes ausgedrückt und die differenzierten Sicherheitsziele wurden den oben genannten Grundwerten zugeordnet.

Bei der Bedrohungsanalyse wurden für die einzelnen Datenobjekte, IT-Systeme, Anwendungen und Kommunikationsverbindungen entsprechende Gefährdungen und Schwachstellen ermittelt. Hierbei wurden entlang des „generischen Scanprozesses“ etwaige Bedrohungen ermittelt und geeignete Gegenmaßnahmen vorgeschlagen, die den identifizierten Gefährdungen entgegenwirken können. Dabei wurde auf anwendbare IT-Grundschutz-Bausteine [BSI-GSKat] aufgebaut und bei Bedarf eine entsprechende Präzisierung und Ergänzung vorgenommen. Im Ergebnis ist ein für das ersetzende Scannen spezifischer Maßnahmenkatalog entstanden, der neben den generischen Gefährdungen und Maßnahmen aus dem IT-Grundschutzhandbuch auch eine Vielzahl von zusätzlichen anwendungsspezifischen Bedrohungen und Maßnahmen enthält.

Unter den spezifischen Bedrohungen in der Dokumentenvorbereitung finden sich beispielsweise die Manipulation oder die Vernichtung des Originals sowie das versehentliche Umdrehen einzelner Blätter in einem Scan-Stapel. Beim Scannen könnten Fehler bei der Erfassung des Scangutes zum Beispiel durch einen Doppeleinzug oder gezielte Manipulationen der Scan-Workstation oder des Scanners auftreten. Bei der Nachverarbeitung könnte beispielsweise eine falsche Zuordnung der Index- und Metadaten erfolgen, wodurch das zukünftige Auffinden der Scanprodukte erschwert oder gar unmöglich gemacht werden würde. Außerdem sind entsprechende Maßnahmen zur Qualitätssicherung notwendig, um die gute Lesbarkeit und Vollständigkeit des Scanproduktes sicher zu stellen. Ohne geeignete Maßnahmen für den Integritätsschutz könnte das Scanprodukt unbemerkt manipuliert werden und hierfür eingesetzte kryptographische Mechanismen könnten im Laufe der Zeit ihre Sicherheitseignung verlieren. Aus all diesen Gefährdungen ergibt sich ein mehr oder weniger großes Risiko, das von den Gerichten bei der beweisrechtlichen Bewertung des Scanprodukts berücksichtigt werden und im Ergebnis den Beweiswert mindern kann.

4.2 Modularer Anforderungs- und Maßnahmenkatalog

Um diese Risiken zu minimieren, wurden entsprechende technische und organisatorische Sicherheitsmaßnahmen festgelegt, die den identifizierten Gefährdungen entgegenwirken. Aus diesen Sicherheitsmaßnahmen wurden Anforderungen abgeleitet, die gemäß der TR-RESISCAN zu beachten sind. Hierbei wurde – angelehnt an [RFC2119] – zwischen zwingend notwendigen Anforderungen (MUSS) und Empfehlungen (SOLL) differenziert. Die Umsetzung der aus den Anforderungen resultierenden

Sicherheitsmaßnahmen ist im Rahmen einer Konformitätsprüfung nachzuweisen. Um ein für den jeweiligen Anwendungsfall und damit für das konkrete Fachverfahren angemessenes Sicherheitsniveau erreichen zu können, wurde der Maßnahmenkatalog in einer modularen Weise aufgebaut. Bei der Entwicklung der TR-RESISCAN wurde bewusst dieser Weg gewählt, damit der Anwender die für seinen konkreten Einsatzbereich angemessene Sicherheitsstufe wählen und dadurch die in betriebswirtschaftlicher Hinsicht effizienteste Lösung realisieren kann.

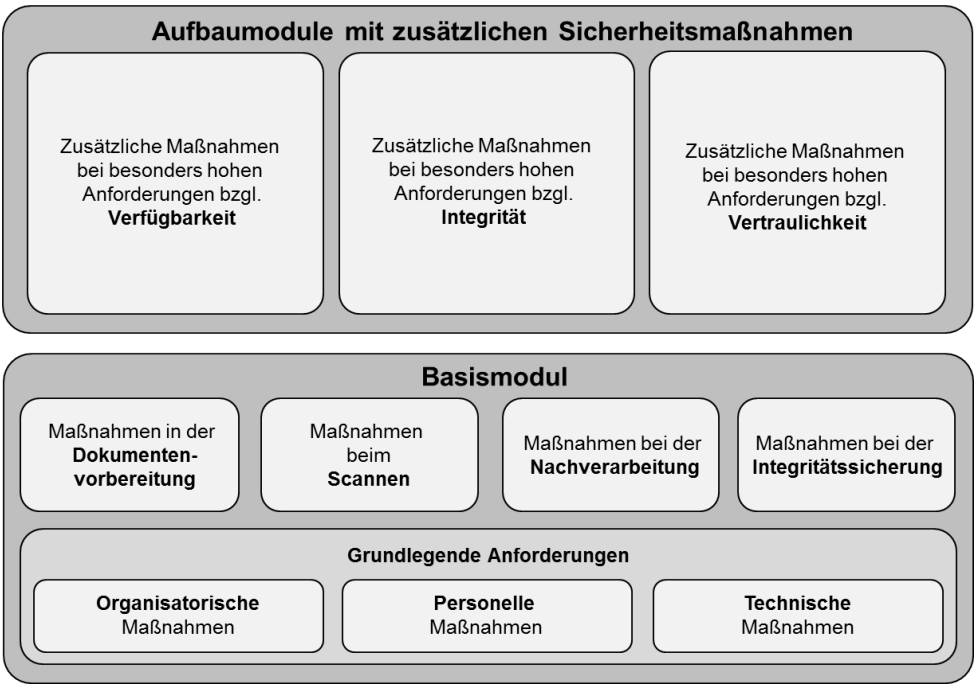

Abbildung 3: Der modulare Maßnahmenkatalog der TR-RESISCAN im Überblick

Der in Abb. 3 im Überblick dargestellte Maßnahmenkatalog sieht zunächst grundlegende Anforderungen vor, die für eine ordnungsgemäße Ausgestaltung des Scanprozesses gemäß der TR-RESISCAN umzusetzen sind. Diese umfassen übergreifende und somit in allen Phasen des Scanprozesses wirksame organisatorische Maßnahmen, wie z.B. Festlegung von Verantwortlichkeiten und Funktionstrennung, sowie personelle Maßnahmen, wie z.B. Verpflichtung zur Einhaltung von Gesetzen, Sensibilisierung und Schulung der Mitarbeiter, und technische Maßnahmen, wie z.B. die geeignete Netztrennung bei Einsatz von netzwerkfähigen Scannern.

Darüber hinaus sieht die Richtlinie spezifische Maßnahmen in den verschiedenen Phasen des Scanprozesses vor. Diese umfassen beispielsweise:

- Sicherheitsmaßnahmen in der Dokumentenvorbereitung, wie die sorgfältige Vorbereitung der Papierdokumente, die Kennzeichnung der Dokumente bzgl. Sensitivität oder die Beschränkung des Zugriffs auf sensible Papierdokumente;
- Sicherheitsmaßnahmen beim Scannen, wie das sorgfältige Scannen[1], die Verwendung geeigneter Scan-Einstellungen, die Nutzung von Metainformationen aus der Dokumentenvorbereitung sowie verschiedene Maßnahmen für Drucker, Kopierer, Scanner und Multifunktionsgeräte.
- Sicherheitsmaßnahmen bei der Nachbereitung, wie die Durchführung von geeigneten Maßnahmen zur Qualitätssicherung und Nachbearbeitung und schließlich
- Sicherheitsmaßnahmen zur Integritätssicherung, wie die Nutzung geeigneter Dienste und Systeme für den Integritätsschutz. Während die oben erläuterten Maßnahmen für ein grundlegendes Schutzniveau sorgen, können in bestimmten Anwendungsszenarien zusätzliche Sicherheitsmaßnahmen zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit empfehlenswert oder unmittelbar notwendig sein.

Beispielsweise empfiehlt sich der Einsatz fortgeschrittener elektronischer Signaturen oder Zeitstempel für die Integritätssicherung. In entsprechender Weise kann ein besonders hohes Maß an Vertraulichkeit durch Einsatz von geeigneten Verschlüsselungsmechanismen erreicht werden. In den beiden genannten Fällen sind darüber hinaus zusätzliche Maßnahmen für das Schlüsselmanagement, die Auswahl geeigneter kryptographischer Produkte und nicht zuletzt Aspekte der Nachsignatur oder der Umschlüsselung zu beachten.

5 Technische Richtlinie TR-ESOR (TR 03125)

Die Übertragung von Papierdokumenten in die elektronische Form induziert zusätzliche Risiken bezüglich der Authentizität und Integrität der Daten, denen oft durch Einsatz elektronischer Signaturen begegnet wird. Auf der anderen Seite ist die Sicherheitseignung der eingesetzten kryptographischen Algorithmen selbst eine Funktion der Zeit, so dass bei der langfristigen Aufbewahrung signierter Dokumente zusätzliche Maßnahmen für den Erhalt der Beweiskraft notwendig sind.

Für diesen Zweck hat das BSI die Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) auf Basis des Evidence Record Syntax (ERS) Standards (vgl. [RFC4998] und [RFC6283]) und der Ergebnisse der vorausgegangenen Projekte ArchiSig [RoSc06] und ArchiSafe [ArchiSafe] entwickelt. Hierdurch kann insbesondere die Integrität und Authentizität archivierter Daten und Dokumente bis zum Ende der gesetzlich vorgeschriebenen Aufbewahrungspflicht unter Wahrung des rechtswirksamen Beweiswertes erhalten werden. Die Einhaltung der Anforderungen an die ordnungsgemäße Aufbewahrung wird dabei vorausgesetzt.

[1] Beispielsweise ist bei mehrseitigen Dokumenten auf eine einheitliche Orientierung und die korrekte Reihenfolge der Seiten sowie die korrekte Trennung und Indizierung der Dokumente zu achten.

Thematisch behandelt die Technische Richtlinie dabei:

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

Aus den für den Erhalt des Beweiswerts notwendigen funktionalen Anforderungen wurde eine modulare Referenzarchitektur abgeleitet, die in Abschnitt 5.1 kurz vorgestellt wird. Die Erfüllung dieser Anforderungen kann im Rahmen eines TR-spezifischen Zertifizierungsverfahrens nachgewiesen werden. Abschnitt 5.2 stellt den aktuellen Stand zur Konformitätsprüfung gemäß TR-ESOR vor.

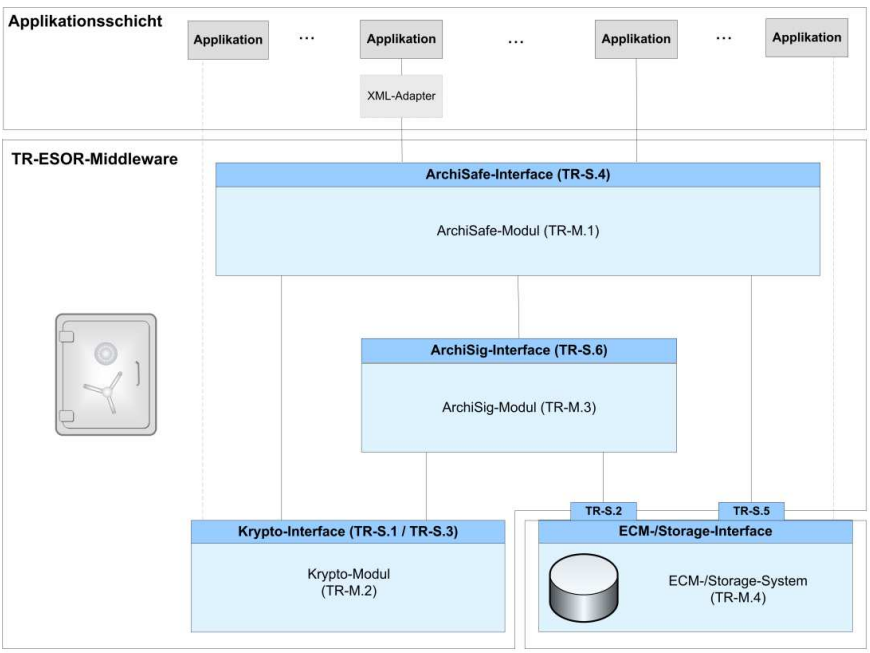

Abbildung 4: TR-ESOR Referenzarchitektur

5.1 TR-ESOR Referenzarchitektur

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (siehe Abb. 4) 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.
- 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)“ [BSI-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 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. [BSI-TR-03112], [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 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. 4 dargestellte IT-Referenzarchitektur orientiert sich an der ArchiSafe-Referenzarchitektur [ArchiSafe] und 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.

5.2 Konformität und Interoperabilität

Für die Technische Richtlinie 03125 TR-ESOR sind drei Stufen für die Konformitätsprüfung von Produkten und Systemen vorgesehen:

- Konformitätsstufe 1 – Funktionale Konformität gemäß [BSI-TR-03125-C.1]
- Konformitätsstufe 2 – Technische Konformität gemäß [BSI-TR-03125-C.2]
- Konformitätsstufe 3 – Technische Konformität gemäß der Profilierung für Bundesbehörden [BSI-TR-03125-B])

Diese drei Konformitätsstufen unterscheiden sich in technischen Detailspezifikationen der Schnittstellen und Formate.

Produkte und Systeme, die gemäß der Technischen Richtlinie 03125 TR-ESOR zertifiziert werden möchten, haben ihre Konformität zu den vorliegenden Spezifikationen nachzuweisen.

Die drei Konformitätsstufen bauen aufeinander auf. Um entsprechend der angestrebten Konformitätsstufe zertifiziert zu werden, muss ein Produkt oder System alle Konformitätskriterien (Testfälle) für diese Konformitätsstufe und für alle tieferen Konformitätsstufen erfüllen.

5.2.1 Funktionale Konformität

Ein System oder eine Komponente ist „funktional konform“ zu [BSI-TR-03125], wenn das System oder die Komponente funktional auf die in dieser Richtlinie beschriebene Systemkomposition oder auf einzelne (auch mehrere) Module dieser Systemkomposition abgebildet werden kann und die Übereinstimmung zu den Anforderungen an das Gesamtsystem oder an einzelne Module festgestellt wird.

Funktional konform im Sinne der [BSI-TR-03125] bedeutet, dass die Komponenten die in dieser TR definierten funktionalen und sicherheitstechnischen Anforderungen erfüllen, die logische Abbildung der funktionalen Anforderungen nachvollziehbar dargestellt wird und die Komponenten zweckmäßig auf der Basis der in dieser TR aufgeführten Ziele und Standards miteinander arbeiten können.

Funktional konform im Sinne dieser TR bedeutet nicht, dass die Schnittstellen der Komponente bzw. des Systems den ASN.1- oder XML- Spezifikationen exakt entsprechen müssen.

Wesentliches Ziel dieser Konformitätsprüfung ist der Nachweis, dass das Modul bzw. das Gesamtsystem den entsprechenden Anteil für die Beweiswerterhaltung funktional umsetzt.

Aktuell wird der Anhang [BSI-TR-03125-C.1] erstellt, der im Herbst 2012 fertiggestellt sein soll.

Dieses Dokument spezifiziert die funktionalen Konformitätskriterien (Testfälle), die aus den bereits veröffentlichten Anforderungen in [BSI-TR-03125] abgeleitet wurden. Zusätzlich werden die vorliegenden Anforderungen und die daraus resultierenden Testfälle der entsprechenden Konformitätsstufe zugeordnet.

Die Testfall-Spezifikation wird so erstellt, dass dieses Dokument als Muster für die Dokumentation der Testdurchführung und Testergebnisse dienen kann.

5.2.2 Technische Konformität

Ein System oder eine Komponente ist „technisch konform“ zu [BSI-TR-03125], wenn zusätzlich zum Nachweis der funktionalen Konformität auch alle bzw. die betreffenden Schnittstellen auf Basis der eCard-API [BSI-TR-03112], wie in [BSI-TR-03125-E] beschrieben, umgesetzt sind und ein definiertes XML-Datenformat (z.B. für selbsterklärende Archivdatenobjekte „XML Archiving Information Package“ (XAIP) gemäß [BSI-TR-03125-F]) für die Kommunikation und das Speichern verwendet wird.

Außerdem wird in der Technischen Richtlinie TR-ESOR festgelegt, dass ein Richtlinienkonformes ArchiSig-Modul auf Anforderung Evidence Records gemäß [RFC4998] bzw. [RFC6283] erzeugen können muss.

Die Prüfung der technischen Konformität umfasst dabei insbesondere:

1. die Prüfung der in [BSI-TR-03125-E] spezifizierten Webservice-Schnittstellen (vgl. Abb. 4),
2. die Prüfung der syntaktischen und semantischen Korrektheit der Evidence Records gemäß [RFC4998] bzw. [RFC6283] und
3. die Prüfung der syntaktischen und semantischen Korrektheit der XAIP-Container.

Als XML-Datenformat soll XAIP aus [BSI-TR-03125-F] verwendet werden. Abweichungen im verwendeten XML-Datenformat sind zulässig, allerdings muss dann erläutert werden, dass gleichwertige Funktionalität unterstützt wird. Insbesondere ist zu erläutern, wie eine Transformation in das XAIP Format aus [BSI-TR-03125-F] erfolgen kann.

Außerdem wird derzeit für die automatisierte Durchführung von technischen Konformitätsprüfungen eine erweiterbare Testumgebung geschaffen, die möglichst auf bereits beim BSI existierende Testumgebungen aufbaut, so dass Webservice-Schnittstellen und Signatur-spezifische Funktionen und Datenobjekte in einer einheitlichen Umgebung getestet werden können.

6 Zusammenfassung

Auch im Gesundheitswesen werden Geschäftsprozesse zunehmend digitalisiert, wodurch meist die Effizienz gesteigert wird aber oft auch zusätzliche Risiken entstehen. Sofern die Dokumente originär in Papierform vorliegen, müssen diese außerdem zunächst in die elektronische Welt übertragen werden. Damit der mit diesem Schritt verbundene Beweiswertverlust so gering wie möglich ist, müssen die in der TR-RESISCAN aufgeführten Maßnahmen bei der Dokumentenvorbereitung, beim Scannen, der Nachverarbeitung und schließlich bei der Integritätssicherung umgesetzt werden. Bei sehr hohem Schutzbedarf bzgl. der Integrität müssen geeignete kryptographische Mechanismen zur Integritätssicherung eingesetzt werden. Um in diesem Fall die Beweiskraft langfristig zu erhalten, müssen die Vorgaben der TR-ESOR berücksichtigt werden. Entsprechendes gilt, sofern originär elektronische und mit einer qualifizierten elektronischen Signatur versehene Dokumente aufbewahrt werden müssen.

Vor der Vernichtung des papiergebundenen Originals ist die Zulässigkeit des ersetzenden Scannens genau zu prüfen. Wie in Abschnitt 2 ausführlich erläutert, ist die Zulässigkeit des ersetzenden Scannens im Gesundheitswesen zwar bei Unterlagen gemäß § 28 RöV gegeben, aber ansonsten nicht geregelt und somit vor dem Hintergrund einer systematischen Betrachtung der rechtlichen Rahmenbedingungen nicht erlaubt. Hier ist der Gesetzgeber gefragt, eine verbindliche und eindeutige Regelung zu erlassen, da in der Praxis ein dringender Bedarf des ersetzenden Scannens medizinischer Dokumente besteht.

Literaturverzeichnis

[ArchiSafe] Physikalisch-Technische Bundesanstalt: ArchiSafe-Webseite, siehe unter http://www.archisafe.de.

[BGH] Bundesgerichtshof, Urteil vom Urteil vom 21.11.1995 - VI ZR 341/94, NJW 1996, 779.

[BSI-100-2] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.

[BSI-100-3] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz.

[BSI-GSKat] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, 2011.

[BSI-IT-SiHB] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, 1992.

[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, http://docs.ecsec.de/BSI-PP-0049, 2008.

[BSI-TR-03112] Bundesamt für Sicherheit in der Informationstechnik (BSI): eCard-API-Framework, Version 1.1.2, TR-03112, http://docs.ecsec.de/BSI-TR-03112, 2012.

[BSI-TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, Version 1.1, http://docs.ecsec.de/BSI-TR-03125, 2011.

[BSI-TR-03125-B] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage B zu *[BSI-TR-03125]*, Profilierung für Bundesbehörden, http://docs.ecsec.de/BSI-TR-03125-B, 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), geplant für 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 2012.

[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: http://docs.ecsec.de/BSI-TR-03125-E, 2011.

[BSI-TR-03125-F] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage F zu *[BSI-TR-03125]*, Formate und Protokolle, http://docs.ecsec.de/BSI-TR-03125-F, 2011.

[BSI-TR-RESISCAN] Bundesamt für Sicherheit in der Informationstechnik (BSI): Rechtssicheres ersetzendes Scannen (TR-RESISCAN), Version 1.0 geplant für Oktober 2012.

[BT-Drs.] Bundestagsdrucksachen, abrufbar unter http://www.bundestag.de/dokumente/drucksachen/index.html.

[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.

[ISO27001] ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements, International Standard, 2005.

[ISO27005] ISO/IEC 27005: Information technology – Security techniques – Information security risk management, International Standard, 2008.

[JaRoWi11] Jandt, S., Roßnagel, A., Wilke, D.: Outsourcing der Verarbeitung von Patientendaten – Fragen des Daten- und Geheimnisschutzes, Neue Zeitschrift für Sozialrecht (NZS) 2011, 641-646.

[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.

[RFC2119] S. Bradner: Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119, via http://www.ietf.org/rfc/rfc2119.txt.

[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.

[RoWi06] A. Roßnagel, D. Wilke: Die rechtliche Bedeutung gescannter Dokumente, Neue Juristische Wochenschrift (NJW) 2006, 2145-2150.

[SCATE] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, D. Wilke: Scannen von Papierdokumenten – Anforderungen, Trends und Empfehlungen, Band 18 der Reihe „Der elektronische Rechtsverkehr“, Nomos, 2008.

[SGHJ12] A. Schumacher, O. Grigorjew, D. Hühnlein, S. Jandt: Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen, in Tagungsband FTVI 2012, GI, LNI, 2012, http://www.ftvi.de/.

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