Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen

Astrid Schumacher[1] · Olga Grigorjew[2] · Detlef Hühnlein[3] · Silke Jandt[2]

[1] Bundesamt für Sicherheit in der Informationstechnik,
Godesberger Allee 185-189, 53175 Bonn, astrid.schumacher@bsi.bund.de

[2] Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet),
Wilhelmshöher Allee 64-66, 34109 Kassel, silke.jandt@uni-kassel.de

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

Abstract: Die Notwendigkeit Papierdokumente zu digitalisieren, wird immer drängender. Sowohl im behördlichen als auch privat-wirtschaftlichen Umfeld werden zunehmend Dokumente auch in digitalen Dokumenten- und Vorgangsbearbeitungs- sowie Aufbewahrungssystemen verarbeitet. Gleichzeitig nimmt das Bedürfnis zu, die Papierdokumente anschließend zu vernichten, um kostenintensive Papierarchive auflösen zu können. Während ein Scanprodukt in rechtlicher Hinsicht niemals denselben Beweiswert wie das originäre Papierdokument haben kann, ist eine Annäherung durchaus möglich. Dies setzt voraus, dass das digitale Endprodukt in einem insbesondere für ein Gericht nachvollziehbaren Scanprozess unter gleichbleibenden qualitativ hochwertigen und abgesicherten Bedingungen entstanden ist. Die dafür notwendigen technischen sowie organisatorischen Anforderungen werden in der derzeit projektierten Technischen Richtlinie (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschrieben.

1 Einleitung

In Verwaltung, Justiz und privatwirtschaftlichen Unternehmen (z. B. im Gesundheitswesen, der Versicherungswirtschaft sowie im Steuer- und Buchführungswesen) werden im Zuge der fortschreitenden Digitalisierung zunehmend elektronische Dokumentenmanagement- und Vorgangsbearbeitungssysteme eingesetzt. Zur Umsetzung des elektronischen Rechts- und Geschäftsverkehrs mehren sich Rechtsvorschriften, die die elektronische Aktenführung zulassen oder vorschreiben. Der parallele Umgang mit Papierdokumenten ist aber nach wie vor erforderlich und wird es auch zukünftig sein, da die Digitalisierung von Altbeständen längst noch nicht abgeschlossen ist und weiterhin Neu-Eingänge in Papier erfolgen werden. Die Originale werden bislang in einer Vielzahl von Fällen weiter aufbewahrt, um ggfs. folgenreiche Konflikte mit gesetzlichen Dokumentations- und Aufbewahrungsvorschriften zu vermeiden. Gleichzeitig werden

sie zur Erleichterung der internen Aktenbearbeitung häufig eingescannt. Die Aufbewahrung der Papieroriginale stellt eine hohe finanzielle und organisatorische Belastung der betroffenen Stellen dar. In rechtlicher Hinsicht bestehen – neben der in verschiedenen Rechtsgebieten sehr unterschiedlichen Regelungen zur Zulässigkeit des ersetzenden Scannens – Unsicherheiten aufgrund uneinheitlich ausgestalteter technisch-organisatorischer Anforderungen. Das Recht kann immer allenfalls abstrakte rechtliche Anforderungen stellen. Trotz zahlreicher Bemühungen, z. B. im Bereich der steuerrelevanten und kaufmännischen Unterlagen, bleibt die technische Umsetzung weitestgehend dem Anwender überlassen. Aufgrund vielfältiger Scanlösungen am Markt, die bei der Umsetzung von Sicherheitsvorgaben stark variieren oder aus einer ganzheitlichen informationstechnischen Betrachtung heraus unvollständig sind, führt dies zu Unsicherheit in der praktischen Anwendung.

Die TR hat das Ziel, diese Lücke zwischen abstrakten und uneinheitlichen rechtlichen Anforderungen und der zuverlässigen technischen Realisierung des Scannens zu schließen. Auf Basis der bereits existierenden Empfehlungen[1] führt die TR entlang eines strukturierten Scanprozesses die sicherheitsrelevanten technischen und organisatorischen Maßnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammen. Dabei werden die Ziele der Informationssicherheit und der Rechtssicherheit gleichermaßen berücksichtigt. Die TR dient daher zum einen dem Anwender im behördlichen und privaten Bereich zur Erleichterung der Auswahl von Scan-Lösungen, indem eine Vereinheitlichung der Anforderungen und Sicherheitsmaßnahmen angestrebt wird. Zum anderen werden Herstellern und Dienstleistern notwendige Spezifikationen an die Hand gegeben, mittels derer diese ihre Leistungen TR-konform gestalten und anbieten können.

2 Rechtliche Aspekte des ersetzenden Scannens

Technisch erfolgt beim Scannen von Papierdokumenten eine Umwandlung von analogen in elektronische Daten, und das Medium wechselt von Papier zu elektronischen Datenspeichern. Rechtlich bedeutsam ist dieser Vorgang, weil dadurch die dem Papier immanenten Sicherheitsmerkmale zum Integritäts- und Authentizitätsschutz verloren gehen und das elektronische Dokument neuen Risiken ausgesetzt ist. In diesem Zusammenhang stellen sich für das ersetzende Scannen aus rechtlicher Sicht im Wesentlichen drei Fragen: Erstens ist das ersetzende Scannen im Hinblick auf die gesetzlichen oder vertraglichen Dokumentations-, Aktenführungs- und Aufbewahrungspflichten zulässig und erfüllen die Scanprodukte diese Pflichten, so dass die Papierdokumente vernichtet werden dürfen. Sofern die Zulässigkeit bejaht werden kann, schließt sich zweitens die Frage an, ob bestimmte rechtliche, technische und organisatorische Anforderungen an den Scanprozess und das Scanprodukt zu stellen sind. Schließlich ist drittens zu fragen, welche Beweiswirkung das Scanprodukt hat, wenn es anstelle des Originals in ein Gerichtsverfahren als Beweis eingebracht wird.[2]

---

[1] Wie z.B. [DOMEA], [IDW-FAIT3], [PK-DML], [GoBS], [GdPDU] und weiteren, deren Gültigkeit durch diese TR nicht beeinträchtigt wird.

[2] Siehe [SCATE 2008], S. 63; [BMWi-HL-571], S. 9.

Die rechtliche Zulässigkeit des ersetzenden Scannens ist nicht Gegenstand der Entwicklung der TR, sondern Voraussetzung für ihre Anwendung. In Bezug auf die Beweissicherheit steht nicht die abstrakte rechtliche Bewertung, sondern die konkrete Bewertung der technisch-organisatorischen Umsetzungsalternativen im Fokus der TR.

Rechtliche Anforderungen an das ersetzende Scannen sind entsprechend den Regelungen zur rechtlichen Zulässigkeit anwendungsspezifisch normiert. Der Gesetzgeber hat den Status des Papieroriginals maßgeblich für die Bestimmung der Anforderungen an die Ausgestaltung des ersetzenden Scannens festgelegt.[3] Soweit gesetzliche Vorschriften das ersetzende Scannen von Papierdokumenten – bei gleichzeitig bestehenden Dokumentations- und Aufbewahrungspflichten – erlauben, steht die Erlaubnis unter dem Vorbehalt der Umsetzung fachspezifischer gesetzlicher Anforderungen. Nur wenn diese gesetzlichen Vorschriften eingehalten werden, dürfen die Papieroriginale vernichtet werden.[4]

In folgenden Anwendungsgebieten sind derzeit gesetzliche Regelungen normiert, die ein ersetzendes Scannen ausdrücklich erlauben:

- Gerichtsakten (§ 299a ZPO für Prozessakten; § 298a ZPO für eingereichte Dokumente);
- Verwaltungsunterlagen (§ 6 RegR für Dokumente der Bundesministerien);
- Sozialversicherungsunterlagen (§ 110a Abs. 2 SGB IV; Sondervorschrift § 110d SGB IV für Dokumente, die der öffentlich rechtlichen Verwaltungstätigkeit zugrunde liegen);
- Röntgendokumentation (§ 28 Abs. 4 RöntgenVO);
- Kaufmännische Buchführungsunterlagen (§ 239 Abs. 4 HGB für Handelsbücher; § 257 Abs. 3 HGB für sonstige Unterlagen);
- Besteuerungsunterlagen (§ 147 Abs. 2 AO).

Obwohl sich die rechtlichen Anforderungen an das ersetzende Scannen von Papierdokumenten hinsichtlich Inhalt und Wortlaut unterscheiden, weisen diese eine weitgehende Homogenität hinsichtlich der gesetzlichen Anforderungen an den Scanprozess und das Scanprodukt auf:[5]

- Bildliche und inhaltliche Übereinstimmung zwischen dem Papieroriginal und dem Scanprodukt;
- Übereinstimmungsnachweis;
- Schutz vor Informationsveränderungen und Informationsverlusten;
- Dauerhafte Datenträger.

---

[3] Siehe [SCATE 2008], S. 80.

[4] Siehe [BMWi-HL-571], S. 16.

[5] Eine Ausnahme bildet hier § 110d SGB IV, da hier eine qualifizierte elektronische Signatur für den Übereinstimmungsnachweis gefordert wird. Siehe auch [BMWi-HL-571], S. 17.

3 Entwicklung und erste Ergebnisse der TR

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

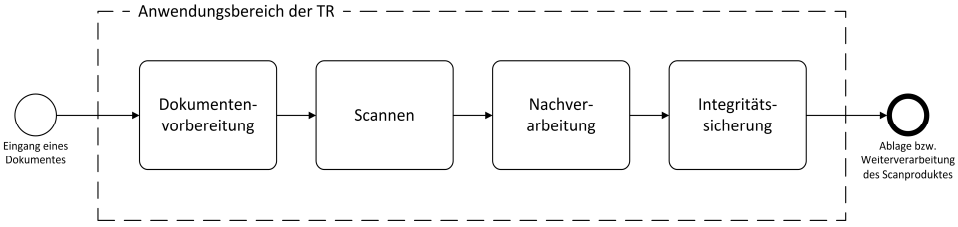

Abbildung 1: Der „generische Scanprozess“

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

Die hierbei 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.

3.1 Struktur-, Schutzbedarfs- und Bedrohungsanalyse

Auf Basis des durch Abstraktion aus der Praxis abgeleiteten „generischen Scanprozesses“ und des „typischen Scansystemes“ wurden die im weiteren Verlauf zu betrachtenden Objekte identifiziert. Hierbei wurden insbesondere die relevanten Datenobjekte (Schriftgut, Scanprodukte, 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* 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.

Die fachliche Schutzbedarfsanalyse für den Dokumententyp „*Gerichtsakten*“ führt zum Beispiel zu dem Ergebnis, dass folgende Kriterien für die Ausgestaltung der Aufbewahrung von Gerichtsakten, die im Scanprozess zu berücksichtigen sind:

- umfassender und effektiver Rechtsschutz,
- funktionsfähige Rechtspflege,
- das Recht auf Akteneinsicht sowie
- die Fortbildung des Rechts.

Darüber hinaus existieren noch weitere Kriterien, die allerdings nur bei einer Einzelfall-bezogenen Schutzbedarfsanalyse herangezogen werden können, wie z. B. das Prozessrisiko. Diese Kriterien wurden aus den Anforderungen abgeleitet, die an einen wirkungsvollen Rechtsschutz, denen die Gerichtsakten letztlich dienen, zu stellen sind. Dieser ergibt sich aus dem Rechtsstaatsprinzip des Art. 20 Abs. 1 GG sowie der Garantie des umfassenden und des effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG durch unabhängige Gerichte.[6] Im Interesse einer funktionsfähigen Rechtspflege bestehen für die Gerichtsbarkeit eine umfassende Aktenführungspflicht sowie die Pflicht zur Aufbewahrung von Akten. Diese Verpflichtungen ergeben sich aus dem Recht der Verfahrensbeteiligten auf Information über den Verfahrensstoff. Dieses Recht lässt sich ausschließlich durch sorgfältige und nachvollziehbare Aktenführung und die Gewährung der Akteneinsicht[7] verwirklichen. Die Aufbewahrung von Gerichtsakten soll darüber hinaus zur Wahrung der Rechtseinheit und zur Fortbildung des Rechts dienen (§ 2 Abs. 2 SchrG).Die Zivilprozessordnung enthält ergänzende Vorschriften zur Führung und Aufbewahrung von Prozessakten. Es wird grundsätzlich zwischen Akten im laufenden Verfahren und Akten von rechtskräftig abgeschlossenen Verfahren differenziert. Gemäß § 298a Abs. 2 ZPO können die in Papierform eingereichten Unterlagen im laufenden Prozess zur Ersetzung der Urschrift in ein elektronisches Dokument umgewandelt werden. Nach § 298a Abs. 3 ZPO ist hierfür Voraussetzung, dass das elektronische Dokument einen Vermerk über die verantwortliche Person und den Zeitpunkt der Übertragung enthält. Darüber hinaus werden keine weiteren Anforderungen an die Ausgestaltung des Vermerks gestellt.[8] Die Originaldokumente sind nach § 298a Abs. 2 S. 2 ZPO mindestens bis zum rechtskräftigen Abschluss des Gerichtsverfahrens aufzu-bewahren, falls sie noch in Papierform benötigt werden.

Nach rechtskräftigem Abschluss eines Verfahrens können Prozessakten gemäß § 299a ZPO zur Ersetzung der Originale nicht nur auf einem Bildträger (Mikrofilm), sondern auch auf anderen Datenträgern wiedergegeben werden, sofern die Übertragung nach ordnungsgemäßen Grundsätzen erfolgt und ein schriftlicher Nachweis darüber vorliegt, dass die Wiedergabe mit der Urschrift übereinstimmt.[9]

Werden diese Voraussetzungen erfüllt, können die Papierakten vernichtet werden.[10] Somit besteht zwar eine grundsätzliche Möglichkeit für das ersetzende Scannen von

---

6 BVErfGE 54, 277, 291; [Wi 2010], S. 54; [SCATE], S. 67.

7 Dieses Recht ergibt sich unmittelbar aus dem Recht auf rechtliches Gehör (Art. 103 Abs. 1 GG) und informationelle Selbstbestimmung.

8 [Wi 2010], S. 54; Greger in [Zö 2007], § 298a Rn.1, 2.

9 In diesem Fall können die Gerichte den Prozessbeteiligten anstelle der Urschriften Ausfertigungen, Auszüge und Abschriften von dem Bild- und Datenträger erteilen.

10 Huber in [Mu2011], § 299a Rn. 1-2.

Gerichtsakten, jedoch ist ihre konkrete Ausgestaltung durch den Gesetzgeber nicht vorgegeben worden.[11]

Danach wurde in der *technischen Schutzbedarfsanalyse* 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[12] aufgebaut und bei Bedarf eine entsprechende Präzisierung und Ergänzung vorgenommen. Hierdurch 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 beispielsweise Fehler bei der Erfassung des Scangutes 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.

Die *Integritätssicherung* könnte schließlich gar nicht oder mit ungeeigneten Sicherungsmitteln erfolgen und die eingesetzten kryptographischen Mechanismen könnten im Laufe der Zeit ihre Sicherheitseignung verlieren. Aus all diesen Gefährdungen ergibt sich ein mehr oder weniger großes Risiko, das den Beweiswert des Scanproduktes schmälern kann.

---

11 [SCATE 2008], S. 67.

12 Dies umfasst insbesondere die Bausteine 1.5 (Datenschutz), 1.6 (Schutz vor Schadprogrammen), 1.11 (Outsourcing), 1.12 (Archivierung), 3.101 (Allgemeiner Server), 3.201 (Allgemeiner Client), 3.406 (Drucker, Kopierer und Multifunktionsgeräte) sowie 5.7 (Datenbanken).

3.2 Modularer Anforderungskatalog

Um diesen Risiken entgegen zu wirken, wurden entsprechende technische und organisatorische Sicherheitsmaßnahmen festgelegt, die den identifizierten Gefährdungen entgegenwirken. Aus diesen Sicherheitsmaßnahmen wurden Anforderungen abgeleitet, die bei der richtlinienkonformen Ausgestaltung des Scanprozesses berücksichtigt werden müssen, sollen oder können. 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 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.

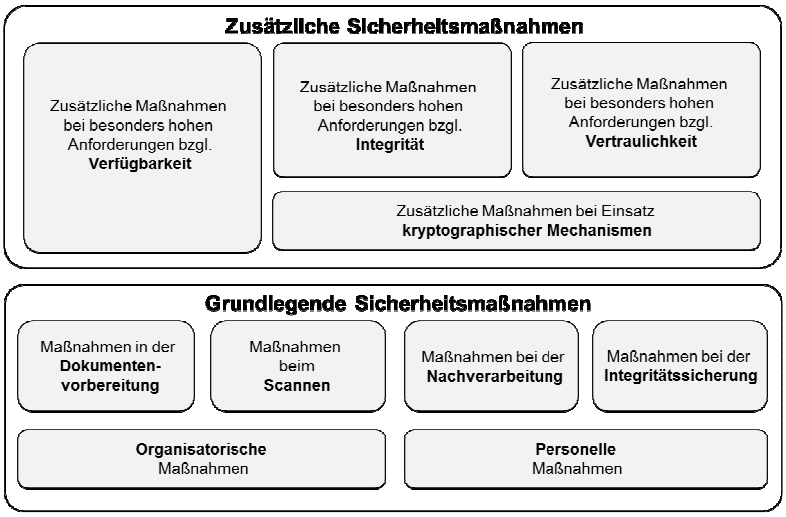

Abbildung 2: Der modulare Maßnahmenkatalog im Überblick

Der Maßnahmenkatalog sieht zunächst *grundlegende Sicherheitsmaßnahmen* vor, die für eine richtlinienkonforme Ausgestaltung des Scanprozesses notwendig 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.

Darüber hinaus sieht die Richtlinie spezifische Maßnahmen in den verschiedenen Phasen des Scanprozesses vor. Dies umfasst 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, die Verwendung geeigneter Scan-Einstellungen, die Nutzung von Metainformationen

aus der Dokumentenvorbereitung, die Durchführung geeigneter Schritte zur Qualitätssicherung sowie verschiedene Maßnahmen für Drucker, Kopierer, Scanner und Multifunktionsgeräte, wie z.B.

- die Definition von Kriterien für die Beschaffung und die geeignete Auswahl,
- die geeignete Aufstellung und Inbetriebnahme,
- die Änderung voreingestellter Passwörter,
- die sorgfältige Durchführung von Konfigurationsänderungen,
- die Beschränkung des Zugriffs und die Verwendung von sicheren Zugriffsmechanismen bei Fernadministration,
- die geeignete Protokollierung und Auswertung,
- die Netztrennung beim Einsatz von Multifunktionsgeräten und schließlich
- die sichere Außerbetriebnahme.

- *Sicherheitsmaßnahmen bei der Nachbereitung*, wie die Durchführung von geeigneten Maßnahmen zur Qualitätssicherung und Nachbearbeitung und schließlich
- *Sicherheitsmaßnahmen bei der 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 für Sozialversicherungsträger (vgl. § 110d SGB IV) oder beim Scannen besonders schützenswerter Dokumente der Einsatz qualifizierter elektronischer Signaturen 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 bzw. der Umschlüsselung zu beachten.

4 Zusammenfassung und Ausblick

Damit die Umsetzung der Vorgaben durch eine neutrale Stelle geprüft und bestätigt werden kann, wird schließlich aus dem Anforderungskatalog eine entsprechende Prüfspezifikation abgeleitet, die als Grundlage für zukünftige Prüfungen im Rahmen einer Zertifizierung dienen soll. Mit der damit möglichen Vergleichbarkeit von angebotenen Scanlösungen wird die Transparenz am Markt erhöht. Die TR kann zudem nach dem Vorbild z.B. des elektronischen Personalausweises[13] und De-Mail[14] als zukünftiger Referenzpunkt für Rechtsvorschriften dienen, in denen auf die Einhaltung

[13] Siehe PAuswV, Anhang 4.
[14] Siehe § 18 II De-Mail-G.

technisch-organisatorischer Anforderungen nach dem Stand der Technik, der bei Erfüllung der Anforderungen der TR vermutet wird, verwiesen wird.

Schließlich können die hier entwickelten Anforderungen an eine angemessen sichere und verbindliche Scanlösung als Mindeststandard nach § 8 I BSIG das Basis-Sicherheitsniveau für Scanprozesse, bei denen das Original nach Abschluss des Scannens vernichtet wird, zur Vereinheitlichung derartiger Abläufe beitragen. Die in der Praxis aufgeworfenen und aus der skizzierten uneinheitlichen Rechts- und Sachlage resultierenden Fragestellungen werden somit durch die TR im Hinblick auf die technisch-organisatorische Umsetzung adressiert. Gleichzeitig praktikable und rechtsverbindliche Lösungen werden damit einfacher umsetzbar. Durch den strukturierten modularen Ansatz mit an die jeweilige Fachanwendung anzupassenden sinnvollen Sicherheitsmaßnahmen trägt die TR zur notwendigen Vereinheitlichung der heterogenen Landschaft und zur Rechtssicherheit beim ersetzenden Scannen bei.

Literaturverzeichnis

[BMWi-HL-571] Bundesministerium für Wirtschaft und Technologie *Handlungsleitfaden zum Scannen von Papierdokumenten*, BMWi - Dokumentation Nr. 571, 2008

[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

[DOMEA] KBSt: *DOMEA-Konzept – Erweiterungsmodul zum DOMEA-Organisationskonzept 2.0, Scan-Prozesse*, Schriftenreihe der KBSt, Band 64, Oktober 2004

[GdPDU] Bundesministerium der Finanzen: *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)*, BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -

[GoBS] Bundesministerium der Finanzen: *Grundsätze ordnung-mäßiger DV-gestützter Buchführungssysteme (GoBS)*, Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995 – IV A 8 – S 0316 – 52/95 – BStBl 1995 I S. 738

[IDW-FAIT3] IDW RS FAIT 3: *Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren*, 2006

[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.

[Mu2011] H. J. Musielak: *ZPO-Kommentar*, 8. Auflage, Franz Vahlen Verlag, 2011

[PK-DML] Verband Organisations- und Informationssysteme (VOI): *PK-DML Prüfkriterien für Dokumentenmanagement-Lösungen*, 3. Auflage, 2008

[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.

[Wi2010] D. Wilke: *Die rechtssichere Transformation von Dokumenten*, Rechtliche Anforderungen an die Technikgestaltung und rechtlicher Anpassungsbedarf, Kassel 2010.

[Zö2007] R. Zöller: *Zivilprozessordnung*, Kommentar, 26. neubearbeitete Auflage, Otto Schmidt Verlag, 2007.