www.jusletter-it.eu

Astrid Schumacher

Das deutsche E-Government-Gesetz — MaSSnahmen des BSI zur Umsetzung

Mit dem wachsenden Angebot von E-Government-Dienstleistungen durch Bund, Länder und Kommunen steigt auch der Bedarf an sicheren elektronischen Identitäten, um vertrauenswürdiges, authentisches und rechtsverbindliches Handeln im Internet zu ermöglichen und Identitätsdiebstahl abzuwehren. Die Aufgabe des BSI als zentraler Dienstleister für Informationssicherheit in Deutschland ist hierbei einerseits Entwicklung und Bereitstellung, andererseits Analyse und Bewertung sicherer eID-Technologien, also Technologien für die Gewährleistung elektronischer Identitäten, in enger Kooperation mit Verwaltung, Wirtschaft und Forschung. Insbesondere mit Technischen Richtlinien stellt das BSI Orientierungshilfen und Handlungsleitfäden nicht nur für die Verwaltung zur Verfügung, und leistet damit durch die Standardisierung von Prozessen einen praktischen Beitrag zur Erhöhung der Informationssicherheit. Dieser Artikel beschreibt einige MaSSnahmen des BSI im Rahmen des aktuellen eGovernment-Rahmens in Deutschland.

Sammlung: Tagungsband IRIS 2015
Kategorie: Beiträge
Rechtsgebiete: E-Government
Region: Deutschland

Zitiervorschlag: Astrid Schumacher, Das deutsche E-Government-Gesetz — MaSSnahmen des BSI zur Umsetzung, in: Jusletter IT IRIS

Inhaltsübersicht

1 Das deutsche E-Government-Gesetz von 2013

[Rz 1] Das am 1. August 2013 in Kraft getretene deutsche Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, EGovG)[1] definiert die gesetzliche Grundlage und damit das Handwerkszeug, mit dem der Staat wesentliche Schritte in die digitale Verwaltung unternehmen soll. So enthält das EGovG als wesentliche Änderung für das Verwaltungsverfahren neben der qualifizierten elektronischen Signatur die Einführung von zwei weiteren technischen Möglichkeiten, um die Schriftform in der elektronischen Kommunikation zu ersetzen: nämlich einerseits De-Mail mit der Versandoption «absenderbestätigt», die eine «sichere Anmeldung» voraussetzt, andererseits Web-Anwendungen der Verwaltung in Verbindung mit sicherer elektronischer Identifizierung durch die Online-Ausweisfunktion (eID-Funktion) des Personalausweises.

[Rz 2] De-Mail wird darüber hinaus nach dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (FördElRV, EJusticeG)[2] als sicherer Übermittlungsweg für elektronische Schriftsätze zum Gericht anerkannt.

[Rz 3] Das Regierungsprogramm Digitale Verwaltung 2020 vom September 2014 setzt wesentliche Eckpunkte auch zur Umsetzung des EGovG. Dieses ist Bestandteil der Digitalen Agenda 2014—2017[3]: «Mit dem Programm Digitale Verwaltung 2020 schafft die Bundesregierung die Rahmenbedingungen für die Verwaltung der Zukunft. Diese nutzt die Potenziale der Digitalisierung, ist effektiv, transparent, effizient, barrierefrei, bürger- und unternehmensfreundlich. Die Agilität der Verwaltung, aber auch die Finanzierbarkeit und die Sicherheit der Informationstechnik des Bundes sollen langfristig gesichert werden»[4].

[Rz 4] Inhalt des Programms ist also die Unterstützung der Bundesverwaltung bei der Digitalisierung der Verwaltung. Dies umfasst u.a. technische Infrastrukturen an der Schnittstelle zu Bürgern und Unternehmen (De-Mail, eID-Service, ePayment und Formularmanagement), die im Rahmen des Programms «Gemeinsame IT» entwickelt werden. Ein «Aktionsplan E-Akte» bündelt daneben die Aktivitäten bei der elektronischen Aktenführung. Mit dem Normenscreening, also der Prüfung und Streichung von Formerfordernissen, insbesondere der Schriftform, im Bun-

1 http://www.gesetze-im-internet.de/egovg/.

2 http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/Gesetz_zur_Foerderung_des_elektronischen_Rechtsverkehrs_mit_den_Gerichten.pdf aufgerufen: 3. Februar 2015.

3 www.digitale-agenda.de.

4 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/regierungsprogramm-digitale-verwaltung-2020.html aufgerufen: 3. Februar 2015.

desrecht, werden der Einsatz und die Verbreitung einfacherer elektronischer Verfahren insgesamt erleichtert.

1.1 Wesentliche Regelungen des EGovG

[Rz 5] Das EGovG ist ein sog. Artikelgesetz. Während Art. 2 bis Art. 7 des EGovG Regelungen zur Ersetzung der Schriftform durch andere technische Verfahren als die qualifizierte elektronische Signatur enthalten (s.o.), beinhaltet Art. 1 das E-Government-Gesetz als solches, das im Wesentlichen folgende Regelungen enthält[5]:

- Verpflichtung der Verwaltung zur Eröffnung eines elektronischen Kanals und zusätzlich der Bundesverwaltung zur Eröffnung eines De-Mail-Zugangs,
- Grundsätze der elektronischen Aktenführung und des ersetzenden Scannens,
- Erleichterung bei der Erbringung von elektronischen Nachweisen und der elektronischen Bezahlung in Verwaltungsverfahren,
- Erfüllung von Publikationspflichten durch elektronische Amts- und Verkündungsblätter,
- Verpflichtung zur Dokumentation und Analyse von Prozessen,
- Regelung zur Bereitstellung von maschinenlesbaren Datenbeständen durch die Verwaltung («open data»)

1.2 Technische Richtlinien als Orientierungshilfe und Stand der Technik

[Rz 6] Technische Richtlinien (TR) des BSI haben originär Empfehlungscharakter. Eine Verbindlichkeit entsteht erst durch individuelle Vorgabe des Bedarfsträgers (z.B. in Vergabeverfahren), oder konkret durch gesetzliche Referenzierung, wie z.B. beim Personalausweis mit Online-Ausweisfunktion und De-Mail, bei denen die funktionalen und sicherheitstechnischen Eigenschaften durch direkte gesetzliche Regelung nach den Richtlinien des BSI erfolgen muss, die im Bundesanzeiger veröffentlicht werden. Oftmals spricht die gesetzliche Regelung dagegen vom «Stand der Technik», dessen Einhaltung bei TRs des BSI als vermutet gilt — wie z.B. bei der elektronischen Aktenführung.

[Rz 7] Das Ziel der TR des BSI ist die Verbreitung von angemessenen IT-Sicherheitsstandards.[6] Sie richten sich daher in der Regel an alle, die mit dem Aufbau oder der Absicherung von IT-Systemen zu tun haben. Sie ergänzen die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen. Für zahlreiche TRs besteht beim BSI die Möglichkeit, die Konformität eines Produkts/Systems zu einer solchen Richtlinie durch eine Zertifizierung nachzuweisen.[7]

- Als Alternativen zu einem Zertifikat kommen Auditor-Testate und Konformitätserklärungen

5 Zitiert nach: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Gesetz/e-government-gesetz_node.html aufgerufen: 3. Februar 2015.

6 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html aufgerufen: 3. Februar 2015.

7 https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachTR/zertifiz_tr.html aufgerufen: 3. Februar 2015.

in Betracht. Dies kann etwa dann sinnvoll sein, wenn es sich um kleinere Organisationseinheiten handelt, für die das Durchlaufen des gesamten Zertifizierungsprozesses mit Dokumentationserstellung, Erstellung von Auditberichten sowie deren Abnahme durch die Zertifizierungsstelle unverhältnismäSSig erscheint, gleichwohl für den betroffenen Prozess dessen OrdnungsgemäSSheit und das Befolgen der BSI-Empfehlungen nachgewiesen werden soll.

2 Online-Ausweisfunktion und die AusweisApp2

[Rz 8] §2 EGovG verpflichtet jede Behörde, gemäSS Abs. 1 auch einen Zugang für die Übermittlung elektronischer Dokumente zu eröffnen, sowie nach Abs. 3 in Verwaltungsverfahren, in denen sie die Identität einer Person festzustellen hat, die Online-Ausweisfunktion anzubieten.

[Rz 9] Mit der Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels in Verbindung mit einer Software und einem Kartenlesegerät wird das sichere Online-Ausweisen ermöglicht. Für die Nutzung dieser eID-Funktion wird eine Software benötigt, mit deren Hilfe eine sichere Verbindung zwischen Kartenlesegerät, dem Ausweis und der Webanwendung (Diensteanbieter) hergestellt werden kann. Diese Software ermöglicht den gesicherten Datenaustausch zwischen Personalausweis und Diensteanbieter.

[Rz 10] Seit der Einführung des Personalausweises mit eID-Funktion in 2011 stellt der Bund mit der AusweisApp eine kostenlose Software für den Datenaustausch zur Verfügung, die seit dem 1. November 2014 in einer neuen und verbesserten Version als AusweisApp2 bereitgestellt wird. Diese steht zum Download für die Betriebssysteme Windows 7 und 8 sowie OS X zur Verfügung. Nach derzeitiger Planung soll die AusweisApp2 ab April 2015 auch für die mobilen Betriebssysteme iOS und Android verfügbar sein.

Abbildung 1: Startscreen der AusweisApp2

[Rz 11] Mit der neuen AusweisApp2 stellt der Bund allen Bürgerinnen und Bürgern eine schlanke, performante, browserunabhängige und nutzerfreundliche Software für die Online-Ausweisfunktion zur Verfügung. Die Entwicklung dieser Software wurde hinsichtlich der Nutzerfreundlichkeit und Barrierefreiheit durch das Zentrum für Angewandte Informatik der Hochschule Darmstadt untersucht. Um ein HöchstmaSS an Sicherheit zu gewährleisten, erfolgte die Entwicklung in enger Abstimmung mit dem BSI. Eine anerkannte Prüfstelle hat die AusweisApp2 entwicklungsbegleitend geprüft, das BSI hat die AusweisApp2 gemäSS Technischer Richtlinien zertifiziert.

[Rz 12] Um eine schnelle Datenverarbeitung zu erreichen, beschränkt sich der Funktionsumfang der neuen App auf das Online-Ausweisen, also den elektronischen Identitätsnachweis mit der Online-Ausweisfunktion. In der schlanken Software ist zudem die Möglichkeit enthalten, sich die Daten im eigenen Online-Ausweis anzeigen zu lassen, eine Auflistung der mit der AusweisApp2 nutzbaren Anbieter sowie die Möglichkeit, sich den Verlauf der bereits vorgenommenen Authentisierungsvorgänge anzeigen zu lassen. Darüber hinaus wird der Quellcode der Software offengelegt.

3 De-Mail

[Rz 13] Die in §2 Abs. 2 EGovG festgelegte Verpflichtung der Bundesbehörden zur Eröffnung eines elektronischen Zugangs durch eine De-Mail-Adresse ist abhängig von dem «Zugang zu dem zentral für die Bundesverwaltung angebotenen IT-Verfahren» und damit vom De-Mail-Gateway, das den Bundesbehörden zentral in 2015 zur Verfügung gestellt werden soll. Ein Kalenderjahr nach Aufnahme des Betriebs des zentralen De-Mail-Gateways muss der De-Mail-Zugang dann

realisiert werden.

[Rz 14] Zudem kann nach §3a Abs. 2 Satz 4 Nr. 2 VwVfG die Schriftform auch durch eine De-Mail ersetzt werden, wenn der Nutzer sich «sicher» an seinem De-Mail-Konto angemeldet hat, also etwa mit der Online-Ausweisfunktion des Personalausweises.

[Rz 15] De-Mail ermöglicht den verbindlichen und vertraulichen Versand elektronischer Dokumente und Nachrichten. Das De-Mail-Gesetz, das am 3. Mai 2011 in Kraft trat[8], sorgt dafür, dass alle De-Mail-Anbieter nach den gleichen Kriterien in einem transparenten Verfahren geprüft und akkreditiert werden. Somit wird De-Mail von allen De-Mail-Diensteanbietern auf einem einheitlichen Sicherheitsniveau angeboten.

[Rz 16] Im Unterschied zu herkömmlichen E-Mails werden De-Mails auf verschlüsselten Transportwegen versendet. Zudem kann die Identität der Kommunikationspartner ebenso wie Versand und Eingang von De-Mails nachgewiesen werden. Dadurch können viele Vorgänge auch elektronisch abgewickelt werden, für die bisher nur der — klassische — Postweg infrage kam.

[Rz 17] Das BSI hat die wesentlichen funktionalen und sicherheitsrelevanten Anforderungen in einem umfangreichen Richtlinienwerk beschrieben: BSI TR-01201 De-Mail[9]. Zudem gewährleistet ein durch die Bundesbeauftragte für den Datenschutz (BfDI) erteiltes Datenschutzzertifikat die Erfüllung der datenschutzrechtlichen Anforderungen[10]. Das BSI übernimmt darüber hinaus als zuständige Behörde die Akkreditierung von De-Mail-Diensteanbietern[11]. Im Rahmen der Akkreditierung muss jeder De-Mail-Diensteanbieter nachweisen, dass er die durch das De-Mail-Gesetz geforderten hohen Anforderungen an die organisatorische und technische Sicherheit der angebotenen De-Mail-Dienste erfüllt. Zur Akkreditierung der De-Mail Dienste sind u.a. das ISO 27001-Zertifikat auf Basis von IT-Grundschutz für den Informationsverbund des Anbieters nötig sowie ein Zertifikat nach den sonstigen Anforderungen der TR-01201 De-Mail.

---

8 De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), zuletzt durch Art. 3 Abs. 8 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert, http://www.gesetze-im-internet.de/de-mail-g/ aufgerufen: 3. Februar 2015.

9 https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/TechnischeRichtlinien/TechnRichtlinien_node.html aufgerufen: 3. Februar 2015.

10 GemäSS dem entsprechenden De-Mail-Kriterienkatalog, http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailKriterienkatalog.pdf?__blob=publicationFile aufgerufen: 3. Februar 2015.

11 https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/Akkreditierung/Akkreditierung_node.html aufgerufen: 3. Februar 2015; gegenwärtig sind als De-Mail-Dienstleister akkreditiert: 1&1 De-Mail GmbH, Mentana-Claimsoft GmbH, T-Systems International GmbH und Telekom Deutschland GmbH.

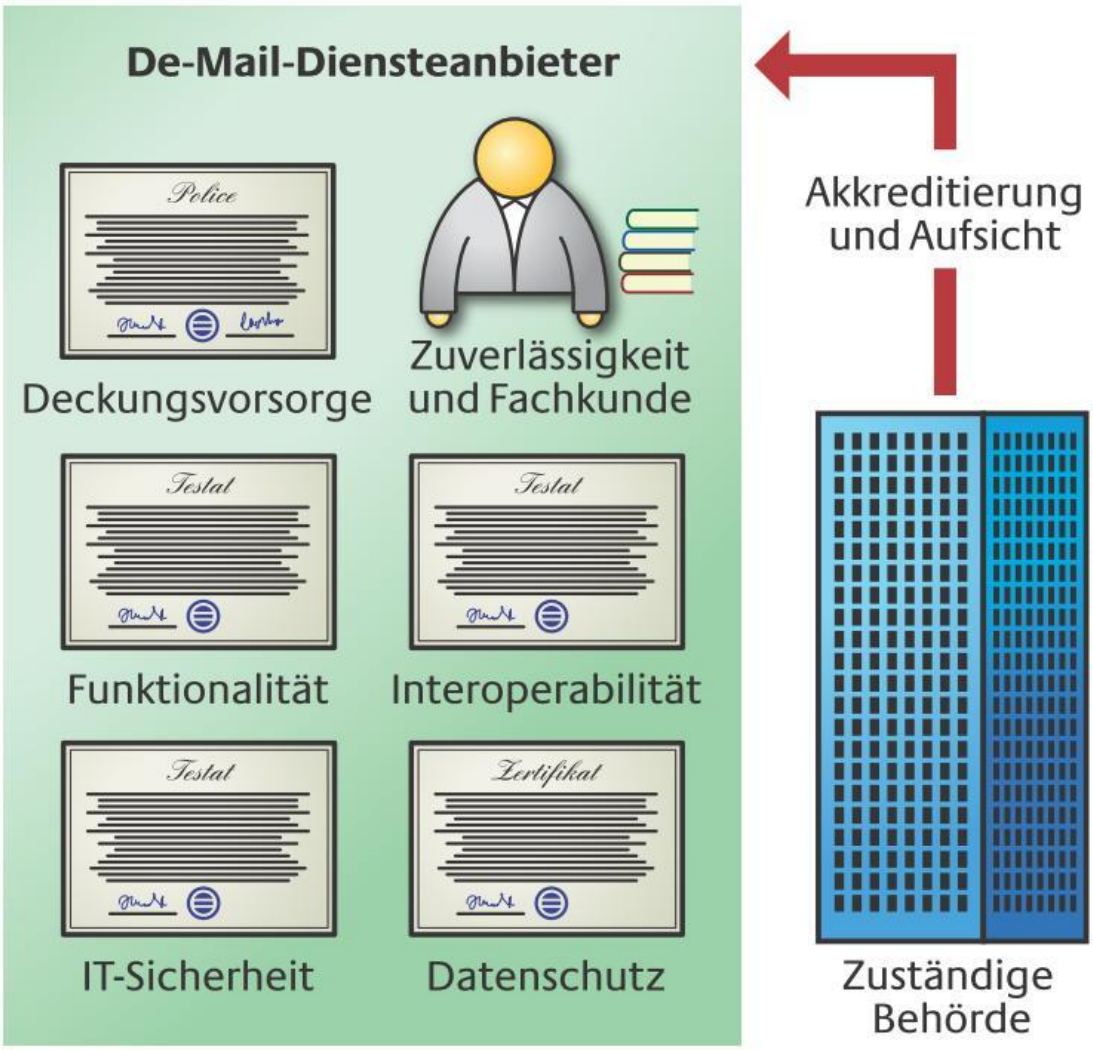

Abbildung 2: Illustration zur TR-01201 De-Mail

[Rz 18] Darüber hinaus wurde — nach einer erfolgreichen Pilotierung in der Praxis — eine TR für die Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente erstellt, die BSITR-03146 E-Bild hD[12]. Diese erlaubt es den Fachverfahrensherstellern, Fotografensoftwareherstellern und De-Mail-Providern, das Verfahren umzusetzen. Dieses dient dazu, das digital aufgenommene Lichtbild für die Beantragung eines Personalausweises auf sicherem elektronischen Weg direkt in die Personalausweisbehörde zu senden und somit einerseits dem Bürger ein schlankeres Antragsverfahren und andererseits der Behörde die Einsparung administrativer Schritte zur Einbettung des Passbildes in das Antragsverfahren zu ermöglichen, da das Einscannen des Lichtbilds in der Behörde entfällt.

[12] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03146/index_htm.html aufgerufen: 3. Februar 2015.

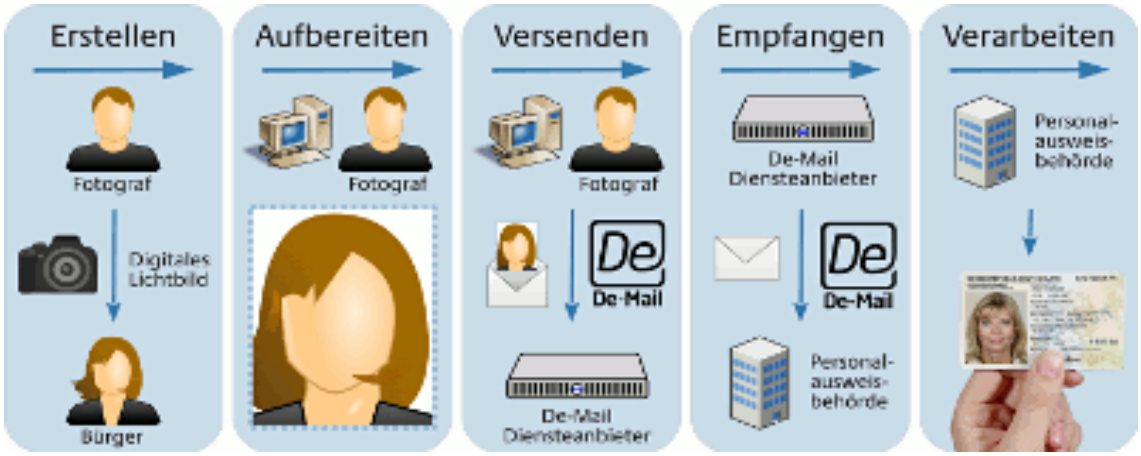

Abbildung 3: Illustration zur TR-03146 E-Bild hD

4 Elektronische Aktenführung

[Rz 19] Ein weiteres wesentliches Ziel des EGovG sind medienbruchfreie Prozesse vom Antrag bis zur Archivierung. Sowohl im eGovernment als auch bei der Justiz wird für den jeweils geforderten «Stand der Technik» bzgl. der Umsetzung entsprechender gesetzlicher Regelungen auf Technische Richtlinien des BSI verwiesen. Dies betrifft etwa §6 EGovG, wonach die Bundesbehörden ihre Akten bis zum 1. Januar 2020 elektronisch führen sollen, was auch die Archivierung beinhaltet. Nach §7 EGovG sind die Behörden angehalten, ersetzend zu scannen, und zwar nach Abs. 1 «nach dem Stand der Technik». Weitere in der ZPO erfolgte Änderungen durch das EJusticeG verweisen u.a. hinsichtlich der Beweisführung mit gescannten Dokumenten ebenfalls — jeweils in der Gesetzesbegründung — auf den Stand der Technik und diesbzgl. auf TRs des BSI (vgl. §§371 b, 298a ZPO).

4.1 Ersetzendes Scannen und vertrauenswürdige Langzeitaufbewahrung

[Rz 20] Die beiden hier referenzierten Richtlinien standen zum Inkrafttreten der gesetzlichen Regelungen bereits zur Verfügung, was die Umsetzung des entsprechenden Verweises im Gesetzgebungsverfahren erleichterte. Diese bieten mit ihren strukturierten Anforderungen pragmatische Orientierungshilfen für Verwaltung und Wirtschaft zur Einhaltung ordnungsgemäSSer Prozesse, unter besonderer Berücksichtigung der Wahrung des jeweiligen Beweiswerts. Die BSI-TR 03138 «Ersetzendes Scannen — RESISCAN»[13] hat zum Ziel, Anwendern in Verwaltung, Justiz, Wirtschaft und Gesundheitswesen als Handlungsleitfaden und Entscheidungshilfe zu dienen, wenn es darum geht, Papierdokumente nicht nur einzuscannen, sondern nach Erstellung des Scanproduktes auch zu vernichten.

[Rz 21] Mit der BSI-TR 03125 «Beweiswerterhaltung kryptographisch signierter Dokumente»[14]

[13] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html aufgerufen: 3. Februar 2015.

[14] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html aufgerufen: 3. Febru-

steht ein Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume — bis zum Ende der Aufbewahrungsfristen — vertrauenswürdig gespeichert werden können.

[Rz 22] Während die TR-RESISCAN somit Anforderungen für eine ordnungsgemäSSe und Risikominimierende 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[15] für die langfristige Aufbewahrung von qualifiziert signierten Daten gefordert ist.

[Rz 23] Sowohl hinsichtlich dem, TR-ESOR zugrundeliegenden, ArchiSig-Modell als auch hinsichtlich eines nach TR-RESISCAN produzierten Scanproduktes wurden Simulationsstudien durchgeführt, die in rechtlicher Hinsicht nachgewiesen haben, dass mit dem Befolgen der TR-Empfehlungen der jeweilige Beweiswert optimiert und die Beweisführung vor Gericht entsprechend vereinfacht werden kann[16].

[Rz 24] Das BSI hat bereits Zertifikate mit der Konformitätsbestätigung nach diesen TRs ausgestellt. Diese werden zudem zunehmend in Vergabeverfahren als Grundlage der zu erfüllenden Anforderungen zugrundegelegt.

4.2 Einige Umsetzungsbeispiele aus der Praxis

[Rz 25] Am 23. Mai 2014 wurden die «Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis» von der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung im Deutschen Ärzteblatt veröffentlicht. Diese referenzieren u.a. auf die BSI-TR 03138 und BSI-TR 03125.[17]

[Rz 26] Am 12. März 2014 hat der Deutsche Steuerberaterverband e.V. die «Gemeinsame Muster-Verfahrensdokumentation () zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege» veröffentlicht[18].

[Rz 27] Die Justiz gibt ebenfalls Standardisierungsvorgaben vor, deren Ziel es ist, unter Beachtung des pragmatisch Leistbaren eine verlässliche und wirtschaftliche Grundlage für Verfahrensentwicklungen zur elektronischen Kommunikation zu bieten. In den Organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften (OT-Leit ERV)[19] werden technische Rahmenvorgaben u.a. hinsichtlich Dokumentenformaten,

---

ar 2015.

15 Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Art. 4 Abs. 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154), http://www.gesetze-im-internet.de/sigv_2001/index.html aufgerufen: 3. Februar 2015.

16 RoSSnagel/Nebel, Simulationsstudie Ersetzendes Scannen, 2014; Fischer-Dieskau et.al., Die Simulationsstudie ArchiSig, 2005.

17 Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis und Addendeum zur Technischen Anlage, Deutsches Ärzteblatt, Jg. 111, Heft 21 vom 23. Mai 2014, S. A-963-A972. Die Technische Anlage in der Fassung von 2008 — diese Fassung findet unter Berücksichtigung der Ergänzungen durch das Addendeum 2014 weiterhin Anwendung.

18 https://www.bstbk.de/export/sites/standard/de/ressourcen/Dokumente/04_presse/publikationen/03_berufsrecht/49_Musterverfahrensdokumentation_Digitalisierung_und_Aufbewahrung_von_Belegen.pdf aufgerufen: 3. Februar 2015.

19 http://www.justiz.de/BLK/regelungen/ot_leit.pdf aufgerufen: 3. Februar 2015.

Übertragungsstandards und Architekturvorgaben für den elektronischen Rechtsverkehr gemacht. Unter Zugrundlegung der TR-RESISCAN werden seit Anfang 2014 von der «Bund-Länder-Kommission für Informationstechnik in der Justiz» Verfahrensanweisungen zum Scannen erarbeitet, auf die in einer dahingehend angepassten Muster-Rechtsverordnung verwiesen werden soll.

5 Orientierungshilfe für vertrauenswürdige Verwaltungsdienstleistungen und Schriftformersatz

[Rz 28] Um die Verwaltung bei der Konzeption und Realisierung von eGovernment-Verwaltungsdienstleistungen im Rahmen der Umsetzung des EGovG zu unterstützen, wurde die TR 03107 «Elektronische Identitäten und Vertrauensdienste im E-Government» entwickelt. Teil 1 ist ein wesentlicher Beitrag zum sicheren Identitätsmanagement, indem dort verschiedene Vertrauensniveaus sowie BewertungsmaSSstäbe aufgearbeitet werden, die die Behörden in die Lage versetzen, ihre Dienstleistungen entsprechend sicher und datenschutzgerecht zu gestalten. Teil 2 beinhaltet die Verknüpfung sicherer Formulare mit der Nutzung der Online-Ausweisfunktion des Personalausweises.

[Rz 29] Der zunehmende Bedarf an sicheren elektronischen Identitäten spiegelt sich aktuell z.B. im BSI-Bericht zur Lage der IT-Sicherheit[20] wieder, der den Diebstahl und Missbrauch von Identitäten als stetige Bedrohung feststellt. Auch in diesem Zusammenhang wurde vom IT-Planungsrat[21] die eID-Strategie beschlossen, die 10 konkrete MaSSnahmen enthält, und weitere Vertrauensdienste wie Bürgerkonten betrachtet[22]. Als eine der ersten MaSSnahmen wurde vom BSI die hier genannte TR-03107 entwickelt.

[Rz 30] Die dort getroffenen Empfehlungen werden auch in die Umsetzung der EU-Verordnung zu elektronischen Identitäten und Vertrauensdiensten[23] (eIDAS-VO) eingebracht. Das BSI hat hier von Beginn an mitgewirkt und ist auch bei der Erarbeitung der nun anstehenden Durchführungsrechtsakte sowie in der maSSgeblichen Standardisierungsarbeit aktiv beteiligt, um die hier angestrebte europaweite Interoperabilität bei der sicheren elektronischen Identifizierung sowie weiteren Vertrauensdiensten in der grenzüberschreitenden Nutzung gleichermaSSen pragmatisch wie sicher zu erreichen.

---

[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf aufgerufen: 3. Februar 2015.

[21] http://www.it-planungsrat.de/DE/Home/home_node.html aufgerufen: 3. Februar 2015; der IT-Planungsrat steuert als zentrales Gremium für die föderale Zusammenarbeit in der Informationstechnik die Zusammenarbeit von Bund und Ländern in der Informationstechnik und im E-Government.

[22] http://www.it-planungsrat.de/DE/Projekte/Steuerungsprojekte/Steuerungsprojekte_NEGS/eIDStrategie/eID_strategie_node.html aufgerufen: 3. Februar 2015; durch die eID-Strategie soll «ein flächendeckendes Angebot von sicheren elektronischen Verfahren zur Gewährleistung von Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit (Vertrauensdienste) in elektronischen Transaktionen erreicht werden, das von Bürgerinnen, Bürgern, Unternehmen und der Verwaltung selbst umfassend akzeptiert wird».

[23] EU-Verordnung 910/2014 des europäischen Parlaments und des Rats vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

6 Literatur

Berlit, Uwe, eJustice — was soll denn das? JurPC WebDok. 117/2014.

Bundesärztekammer/Kassenärztliche Bundesvereinigung, Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis und Addendeum zur Technischen Anlage, Deutsches Ärzteblatt, Jg. 111, Heft 21 vom 23. Mai 2014, S. A-963-A972.

Bundessteuerberaterkammer (BstBK), Deutscher Steuerberaterverband (DstV), Muster-Verfahrensdokumentation zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege, 2014.

Bundesamt für Sicherheit in der Informationstechnik, Mit Sicherheit — BSI-Magazin 2013/2014, erschienen 12/2014.

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2014, Stand November 2014.

Bundesamt für Sicherheit in der Informationstechnik, De-Mail, Sicherer elektronischer Nachrichtenverkehr — einfach und nachweisbar, Februar 2014.

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 2013.

Bund-Länder-Kommission für Informationstechnik in der Justiz, Arbeitsgruppe Elektronischer Rechtsverkehr: Organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften vom 21. April 2005, Arbeitsgruppe IT-Standards in der Justiz: Technische Rahmenvorgaben für den elektronischen Rechtsverkehr vom 15. Januar 2014.

Bundesregierung, Digitale Agenda 2014—2017, hrsg. von: Bundesministerium für Wirtschaft und Energie, Bundesministerium des Innern, Bundesministerium für Verkehr und digitale Infrastruktur, August 2014.

Bundesregierung, Digitale Verwaltung 2020 — Regierungsprogramm 18. Legislaturperiode, hrsg. vom Bundesministerium des Innern, September 2014.

Fischer-Dieskau, Stefanie/Pordesch, Ulrich/RoSSnagel, Alexander/Steidle, Roland, Die Simulationsstudie ArchiSig — Simulationsstudie zur Beweistauglichkeit elektronisch signierter Dokumente, in: Alexander RoSSnagel, Paul Schmücker (Hrsg.), Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente, Heidelberg 2005.

Hühnlein, Detlef/Korte, Ulrike/Schumacher, Astrid, Die BSI-Richtlinien TR-Esor und TR-Resiscan, D-A-CH Security 2012, Tagungsband.

Physikalisch-Technische Bundesanstalt, ArchiSafe, http://www.archisafe.de.

RoSSnagel, Alexander, Auf dem Weg zur elektronischen Verwaltung — Das E-Government-Gesetz, NJW 2013 Heft 37, 2710—2716.

RoSSnagel, Alexander/Nebel, Maxi, Simulationsstudie Ersetzendes Scannen — Ergebnisse, Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnik-Gestaltung (IteG) der Universität Kassel, 30. Januar 2014.

RoSSnagel, Alexander/Nebel, Maxi, Beweisführung mittels ersetzend gescannter Dokumente, NJW 2014, 886 ff.

RoSSnagel, Alexander/Fischer-Dieskau, Stefanie/Jandt, Silke/Wilke, Daniel, Scannen von Papierdokumenten — Anforderungen, Trends und Empfehlungen, Band 18 der Reihe «Der elektronische Rechtsverkehr», Nomos 2008.

Schumacher, Astrid/Grigorjew, Olga/Hühnlein, Detlef/Jandt, Silke, Die Entwicklung der

BSI-Richtlinie für das rechtssichere ersetzende Scannen, in: Tagungsband der FTVI, Gesellschaft für Informatik, LNI 2012, http://www.ftvi.de.

Wilke, Daniel, Die rechtssichere Transformation von Dokumenten, Rechtliche Anforderungen an die Technikgestaltung und rechtlicher Anpassungsbedarf, Kassel 2010.

Astrid Schumacher, Leiterin des Referats S11-Sicherheit in eID-Anwendungen, Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185—189, 53175 Bonn, DE, astrid.schumacher@bsi.bund.de; www.bsi.bund.de