

Die Prüfdienste des Bundes  
und der Länder informieren

**Leitfaden**

**Elektronische Kommunikation  
und  
Langzeitspeicherung  
elektronischer Daten**

| <b>Versionsdokumentation</b> |              |             |                                                                                       |             |
|------------------------------|--------------|-------------|---------------------------------------------------------------------------------------|-------------|
| Version:                     | Datum:       | Kap./Seite: | Grund d. Änderung:                                                                    | Bearbeiter: |
| 4.0                          | Oktober 2014 | Alle        | Einarbeitung EGovG,<br>Neustrukturierung ge-<br>samtes Dokument (aus<br>Version 3.5). | AK Signatur |

Herausgeber:

ADV-Arbeitsgemeinschaft  
Geschäftsstelle im Ministerium für  
Gesundheit, Emanzipation,  
Pflege und Alter des Landes  
Nordrhein-Westfalen  
Horionplatz 1  
40213 Düsseldorf  
Tel.: (0211) 8618-0

E-Mail: [adv-ag@mgepa.nrw.de](mailto:adv-ag@mgepa.nrw.de)

Bundesversicherungsamt  
Abteilung 6  
Friedrich-Ebert-Allee 38  
53113 Bonn  
Tel.: (0228) 619-0

Ansprechpartner:  
Peter Fischer  
Referat 621 (Außenstelle Cloppenburg)  
Tel.: (04471) 1807-16  
E-Mail: [peter.fischer@bva.de](mailto:peter.fischer@bva.de)

**Inhalt:**

|          |                                                                                                                     |           |
|----------|---------------------------------------------------------------------------------------------------------------------|-----------|
| <b>0</b> | <b>Einleitung und Anwendungshinweise .....</b>                                                                      | <b>6</b>  |
| <b>1</b> | <b>Rechtsgrundlagen .....</b>                                                                                       | <b>8</b>  |
| <b>2</b> | <b>Vorgehensweise bei Einführung neuer IT-gestützter Verfahren zur<br/>Geschäftsprozessoptimierung .....</b>        | <b>10</b> |
| 2.1      | Vorbereitende Analysen und Maßnahmen.....                                                                           | 10        |
| 2.2      | Umsetzung/Ausschreibung .....                                                                                       | 10        |
| 2.3      | Anzeige an die Aufsichtsbehörde.....                                                                                | 11        |
| <b>3</b> | <b>Elektronische Kommunikation zwischen SV-Trägern und Versicherten....</b>                                         | <b>12</b> |
| 3.1      | Grundsätze .....                                                                                                    | 12        |
| 3.1.1    | Geltungsbereich .....                                                                                               | 12        |
| 3.1.2    | Schriftformerfordernis und Ersatz der Schriftform .....                                                             | 13        |
| 3.1.3    | Lesbarkeit übermittelter Dokumente .....                                                                            | 14        |
| 3.1.4    | Barrierefreiheit.....                                                                                               | 14        |
| 3.1.5    | Datenschutzrechtliche Einschränkungen.....                                                                          | 15        |
| 3.2      | Zugang.....                                                                                                         | 16        |
| 3.2.1    | Grundsätze .....                                                                                                    | 16        |
| 3.2.2    | Zugangsmöglichkeiten bei Schriftformersatz .....                                                                    | 17        |
| 3.2.2.1  | Qualifizierte Elektronische Signatur .....                                                                          | 17        |
| 3.2.2.2  | Eingabe über Web-Formulare oder besondere Eingabegeräte.....                                                        | 17        |
| 3.2.2.3  | Kommunikation mit De-Mail.....                                                                                      | 18        |
| 3.2.2.4  | De-Mail-Versand elektronischer Verwaltungsakte oder sonstiger elektronischer<br>Dokumente durch den SV-Träger ..... | 19        |
| 3.2.2.5  | Identifizierung des Absenders durch sonstige sichere Verfahren .....                                                | 19        |
| 3.2.3    | Zugangsmöglichkeiten ohne Schriftformerfordernis .....                                                              | 19        |
| 3.3      | Elektronische Einreichung von Nachweisen.....                                                                       | 20        |
| 3.3.1    | Einreichung durch den Versicherten .....                                                                            | 20        |
| 3.3.2    | Elektronische Übermittlung von Nachweisen zwischen verschiedenen Behörden / SV-<br>Trägern .....                    | 21        |
| 3.4      | Elektronischer Posteingang .....                                                                                    | 21        |

|              |                                                                                |           |
|--------------|--------------------------------------------------------------------------------|-----------|
| <b>3.4.1</b> | <b>Behandlung eingehender Fax-Sendungen .....</b>                              | <b>21</b> |
| <b>3.4.2</b> | <b>Speicherung eingehender E-Mails im elektronischen Langzeitarchiv .....</b>  | <b>22</b> |
| <b>3.4.3</b> | <b>Speicherung eingehender DE-Mails im elektronischen Langzeitarchiv .....</b> | <b>23</b> |
| <b>3.5</b>   | <b>Elektronischer Postausgang .....</b>                                        | <b>24</b> |
| <b>3.5.1</b> | <b>Grundsätze .....</b>                                                        | <b>24</b> |
| <b>3.5.2</b> | <b>E-Mails (ohne/mit Anhang) .....</b>                                         | <b>24</b> |
| <b>3.5.3</b> | <b>De-Mails (ohne/mit Anhang) .....</b>                                        | <b>25</b> |
| <b>3.5.4</b> | <b>Erstellung und Versand von Serienbriefen .....</b>                          | <b>25</b> |
| <b>4</b>     | <b>Technische und organisatorische Verfahrensanforderungen .....</b>           | <b>26</b> |
| <b>4.1</b>   | <b>Allgemeine Anforderungen .....</b>                                          | <b>26</b> |
| <b>4.1.1</b> | <b>Verfahrensbeschreibung .....</b>                                            | <b>26</b> |
| <b>4.1.2</b> | <b>Dienstanweisung .....</b>                                                   | <b>26</b> |
| <b>4.2</b>   | <b>Qualifizierte Elektronische Signatur (QES).....</b>                         | <b>28</b> |
| <b>4.2.1</b> | <b>Signaturerstellungseinheiten und Signaturanwendungskomponenten.....</b>     | <b>28</b> |
| <b>4.2.2</b> | <b>Regelungen für das Kartenmanagement .....</b>                               | <b>29</b> |
| <b>4.2.3</b> | <b>Neusignieren nach § 17 SigV .....</b>                                       | <b>29</b> |
| <b>5</b>     | <b>Übertragung und Vernichtung des Papieroriginals .....</b>                   | <b>33</b> |
| <b>5.1</b>   | <b>Scannen von Papierdokumenten.....</b>                                       | <b>33</b> |
| <b>5.2</b>   | <b>Signaturverfahren.....</b>                                                  | <b>34</b> |
| <b>5.3</b>   | <b>Sicherheitsmaßnahmen .....</b>                                              | <b>37</b> |
| <b>5.4</b>   | <b>Technische Richtlinie TR03138 („TR-RESISCAN“).....</b>                      | <b>39</b> |
| <b>5.5</b>   | <b>Vernichtung von Originalbelegen .....</b>                                   | <b>40</b> |
| <b>6</b>     | <b>Langzeitspeicherung elektronisch erzeugter Dokumente und Daten.....</b>     | <b>42</b> |
| <b>6.1</b>   | <b>Allgemeine Anforderungen .....</b>                                          | <b>42</b> |
| <b>6.2</b>   | <b>Rechtssichere Langzeitspeicherung von elektronischen Posteingängen.....</b> | <b>43</b> |
| <b>6.3</b>   | <b>Rechtssichere Langzeitspeicherung von elektronischen Postausgängen.....</b> | <b>44</b> |
| <b>6.4</b>   | <b>Technische Richtlinie TR03125 („TR-ESOR“) .....</b>                         | <b>44</b> |
| <b>6.5</b>   | <b>Besonderheiten .....</b>                                                    | <b>45</b> |
| <b>6.5.1</b> | <b>Aufbewahrung von Fehler-/Bearbeitungslisten .....</b>                       | <b>45</b> |
| <b>6.5.2</b> | <b>Aufbewahrungsfrist von Einzeldokumenten in eAkten/Vorgängen.....</b>        | <b>45</b> |

|          |                                                                                                            |           |
|----------|------------------------------------------------------------------------------------------------------------|-----------|
| <b>7</b> | <b>Elektronischer Datenaustausch</b> .....                                                                 | <b>46</b> |
| 7.1      | Ergänzende rechtliche Grundlagen .....                                                                     | 46        |
| 7.2      | Speicherung des Originaldatensatzes .....                                                                  | 47        |
| 7.3      | Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung) .....                            | 48        |
| Anhang 1 | Auszug BSI Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch<br>signierter Dokumente“ ..... | 50        |

## 0 Einleitung und Anwendungshinweise

Im Zeitalter der Digitalisierung unserer Gesellschaft gewinnt die elektronische Kommunikation zunehmend an Bedeutung. In diesem Zusammenhang stellt sich vielfach die Frage nach der Rechtsverbindlichkeit der elektronischen Kommunikation, der Vorgangsbearbeitung und der Langzeitspeicherung elektronischer Daten. Ziel dieses Leitfadens ist es daher, die gesetzlichen Anforderungen zu dieser Thematik zusammenzutragen und die hieraus abgeleiteten Anforderungen der Prüfdienste für die praktische Umsetzung zu formulieren. Dieser Leitfaden ersetzt aber nicht die individuellen Risikoanalysen und die Ausübung des pflichtgemäßen Ermessens bei der Auswahl konkreter Maßnahmen.

Dieser Leitfaden beinhaltet

- die elektronische Kommunikation (E-Government) zwischen SV-Trägern untereinander bzw. zu den Versicherten und Arbeitgebern,
- die Verwendung von qualifizierten elektronischen Signaturen (QES) bzw. der durch das EGovG eingeführten alternativen Authentifizierungsmöglichkeiten,
- die Übertragung von Papierdokumenten in die elektronische Form,
- den Transfer von elektronischen Melde- und Abrechnungsdaten (in Datensatzform) sowie
- die elektronische Langzeitspeicherung.

Neben den durch Gesetze und Verordnungen festgelegten Rahmenbedingungen sind insbesondere folgende vom Bundesamt für Sicherheit in der Informationstechnik (BSI), vom Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) und vom Bundesinnenministerium herausgegebenen Werke in der jeweils aktuellen Fassung zu beachten bzw. einzubeziehen:

- BSI-Standard 100-1 bis 100-4
- Grundschutzkataloge
- Technische Richtlinie TR03138 „Ersetzendes Scannen“ (TR-RESISCAN)
- Technische Richtlinie TR03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ (TR-ESOR)
- „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ (BfDI vom 01.03.2013)
- „Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (BMI Referat O2 – Stand: 27.06.2013)
- Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – Leitlinien und gemeinsame Maßstäbe für IuK-Prüfungen, Stand: November 2011.

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

Bei der Einführung der o. g. Teilbereiche handelt es sich um „grundlegende Maßnahmen“ im DV-Bereich. Diese sind rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht unter Verwendung des „Grundleitfadens 85“ anzuzeigen.

Der Leitfaden wird von den Prüfdiensten des Bundes und der Länder laufend gepflegt und weiter entwickelt. Es wird als Grundlage für die Beurteilung dieser Verfahren angewendet.

Den der Prüfung nach § 274 SGB V unterliegenden Institutionen wird empfohlen, ihre Verfahren entsprechend den Ausführungen in diesem Leitfaden zu gestalten. (Die Institutionen werden im Text unter dem Begriff „**SV-Träger**“<sup>1</sup> zusammengefasst.)

Bei einer Aufgabenwahrnehmung durch Dritte (§ 197b SGB V) wird empfohlen, die den bundesunmittelbaren Krankenkassen mit Rundschreiben vom 14. Mai 2012 (Az.: II5-5422.0-5272/2011) übermittelten Grundsätze „Anforderungskatalog Outsourcing“<sup>2</sup> zu beachten.

---

<sup>1</sup> **SV-Träger** i.S.v. § 274 SGB V: Krankenkassen, Pflegekassen, Arbeitsgemeinschaften, Landesverbände der Krankenkassen, GKV-Spitzenverband, KBV, KZBV, KVen, KZVen, MDK/MDS.

<sup>2</sup>

<http://www.bundesversicherungsamt.de/fileadmin/redaktion/Krankenversicherung/Rundschreiben/Rundschreiben64.pdf>

## 1 Rechtsgrundlagen

Wesentlich sind insbesondere die folgenden Gesetze bzw. Verordnungen in der jeweils aktuellen Fassung:

- **SGB I - Sozialgesetzbuch, Erstes Buch**
  - o § 36a Elektronische Kommunikation
  
- **SGB IV – Sozialgesetzbuch, Viertes Buch**
  - o § 69 Abs. 2 (Wirtschaftlichkeit und Sparsamkeit)
  - o § 110a (Aufbewahrungspflicht)
  - o § 110b (Rückgabe, Vernichtung und Archivierung von Unterlagen)
  - o § 110c (Verwaltungsvereinbarungen, Verordnungsermächtigung)
    - Vereinbarung der Spitzenverbände der Krankenkasse zu den Grundsätzen ordnungsgemäßer Aufbewahrung im Sinne des § 110a SGB IV, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen (Stand: 23.06.2008)
    - Ergänzende Vereinbarung der Spitzenverbände der Krankenkassen zur Rückgabe und Vernichtung von Unterlagen (Stand: 23.06.2008)
  - o § 110d (Beweiswirkung)
  
- **SGB V – Sozialgesetzbuch, Fünftes Buch**
  - o § 197b (Aufgabenerledigung durch Dritte)
  - o § 274 (Prüfung der Geschäfts-, Rechnungs- und Betriebsführung)
  - o §§ 284 ff. (Grundsätze der Datenverwendung)
  
- **SGB X – Sozialgesetzbuch, Zehntes Buch**
  - o § 9 (Nichtförmlichkeit des Verwaltungsverfahrens)
  - o § 33 (Bestimmtheit und Form des Verwaltungsaktes)
  - o §§ 67-78 (Schutz der Sozialdaten)
  - o § 78a und Anlage (Technische und organisatorische Maßnahmen)
  
- **Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG)**
  - o § 1 Abs. 1, 2, 4 Geltungsbereich
  - o § 2 Elektronischer Zugang zur Verwaltung
  - o § 4 Elektronische Bezahlungsmöglichkeiten
  - o § 5 Nachweise
  - o § 6 Elektronische Aktenführung
  - o § 7 Übertragen und Vernichten des Papieroriginals
  - o § 8 Akteneinsicht
  - o § 9 Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand
  - o § 13 Elektronische Formulare
  - o § 16 Barrierefreiheit
  
- **Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)**
  
- **Verordnung zur Elektronischen Signatur (Signaturverordnung – SigV)**
  
- **De-Mail-Gesetz (DeMailG)**
  - o § 4 Anmeldung zu einem De-Mail-Konto
  - o § 5 Postfach- und Versanddienst



- **Verordnung über das Haushaltswesen in der Sozialversicherung (SVHV)**
  - o § 22 (Öffentliche Ausschreibung)
  
- **Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (SVRV)**
  - o § 5 (Belegpflicht)
  - o § 6 Abs. 3 (Belege für Einzahlungen, Auszahlungen und Buchungen ohne Zahlungsvorgang)
  - o § 7 Abs. 3 (Zahlungsanordnung)
  - o § 17 (Dienstabweisungen)
  - o § 19 (Outsourcing)
  
- **Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV)**
  - o § 9 (Allgemeines)
  - o § 11 (Anordnung der Zahlung)
  - o § 12 (Zahlungsbegründende Unterlagen)
  - o § 13 (Änderung der Zahlungsanordnung)
  - o § 19 Abs. 5 (Feststellung der Belege)
  - o § 20 (Sachliche Feststellung)
  - o § 21 (Rechnerische Feststellung)
  - o § 22 (Form und Führung der Bücher und Aufzeichnungen)
  - o § 35 (Aufbewahrungsfristen)
  - o § 36 (Aufbewahrung)
  - o § 40 (Sicherheit bei Einsatz der automatisierten Datenverarbeitung, Grundsätze ordnungsgemäßer Datenverarbeitung - GoD)
  - o § 41 (qualifizierte elektronische Signatur)
  - o § 42 (Outsourcing)
  - o § 44 (Übergangsregelungen)
  
- **Risikostrukturausgleichsverordnung (RSAV)**
  - o Begründung zur Änderung des § 30 und Einführung des § 42 RSAV (Bundesratsdrucksache 446/12 vom 07.08.2012)

## **2 Vorgehensweise bei Einführung neuer IT-gestützter Verfahren zur Geschäftsprozessoptimierung**

### **2.1 Vorbereitende Analysen und Maßnahmen**

Eine prozessorientierte elektronische Verwaltungsarbeit setzt die systematische und ganzheitliche Untersuchung und Dokumentation von Prozessen voraus. Vor Einführung neuer bzw. Änderung vorhandener IT-gestützter Verfahrensabläufe sind daher mindestens folgende Schritte zwingend zu durchlaufen:

#### **Durchführung einer Geschäftsprozess- und Schwachstellenanalyse**

Aus deren Ergebnis ist ein Anforderungskatalog zu erstellen, der u. a. die im Abschnitt 1 (Rechtsgrundlagen) aufgeführten gesetzlichen Vorgaben zu beachten hat.

#### **Analysen und Festlegungen zu Datenschutz und Datensicherheit**

Ergänzend zur Geschäftsprozess- und Schwachstellenanalyse sind die Verfahrensabläufe sowie die Datenobjekte bezüglich des Datenschutzes und der Datensicherheit zu analysieren und notwendige Maßnahmen zu deren Sicherung festzulegen. Hierzu sind folgende Teilschritte notwendig:

- Schutzbedarfsanalyse (fachlich und technisch)
- Bedrohungsanalyse
- Risikoanalyse
- Sicherheitsmaßnahmen

Nähere Ausführungen hierzu sind den in der Einleitung aufgeführten Dokumenten des BSI zu entnehmen.

#### **Erstellung einer Wirtschaftlichkeitsberechnung**

Vor einer Entscheidung über den Einsatz elektronischer Verfahren ist die Wirtschaftlichkeit des Gesamtverfahrens festzustellen (§§ 69 Abs. 2, 110a Abs. 2 SGB IV, 6 Satz 2 EGovG). Hierfür sind die gängigen Verfahren zur Wirtschaftlichkeitsberechnung<sup>3</sup> (§ 69 Abs. 3 SGB IV) anzuwenden. Einzubeziehen sind auch Fragen zur Nachhaltigkeit und zu den Auswirkungen/Kosten bei einem Systemwechsel.

Zu beachten ist hierbei, dass die Erfüllung gesetzlicher Vorgaben – insbesondere aus §§ 110 a - d SGB IV sowie § 78a SGB X – Vorrang vor dem Gebot des wirtschaftlichen Handelns hat.

### **2.2 Umsetzung/Ausschreibung**

#### **Vergabeverfahren**

Nach § 22 SVHV muss dem Abschluss von Verträgen über Lieferungen und Leistungen mit Ausnahme der Verträge, die der Erbringung gesetzlicher oder satzungsmäßiger Versicherungsleistungen dienen, eine öffentliche Ausschreibung vorausgehen. Hiervon kann abgesehen werden, sofern die Natur des Geschäfts oder besondere Umstände dies rechtfertigen.

Landesspezifische Regelungen sind ggf. zu beachten.

---

<sup>3</sup> Band 18 der Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung BWV (Präsident des Bundesrechnungshofes): „Anforderungen an Wirtschaftlichkeitsuntersuchungen finanzwirksamer Maßnahmen nach § 7 Bundeshaushaltsordnung“.

### **Hinweis:**

Die Beauftragte der Bundesregierung für Informationstechnik ([www.cio.bund.de](http://www.cio.bund.de)) hat für die Beschaffung von IT-Leistungen für die Bundesverwaltung ergänzende Vertragsbestimmungen (EVB-IT) für den Abschluss von Verträgen mit externen Anbietern erarbeitet. Die Verträge sollen den öffentlichen Auftraggeber davor schützen, durch die allgemeinen Vertragsbedingungen des Anbieters benachteiligt zu werden.

Die Prüfdienste des Bundes und der Länder raten dringend, die Empfehlungen zu beachten.

Näheres über die jeweiligen Vertragswerke sind der o.g. Internetseite zu entnehmen.

## **2.3 Anzeige an die Aufsichtsbehörde**

Gemäß § 85 Abs. 1 Satz 2 ff SGB IV ist die Absicht, sich zur Aufgabenerfüllung an Einrichtungen mit Ausnahme von Arbeitsgemeinschaften im Sinne dieses Gesetzbuches zu beteiligen, sowie die Absicht, Datenverarbeitungsanlagen und -systeme anzukaufen, zu leasen oder anzumieten oder sich an solchen zu beteiligen, der Aufsichtsbehörde vor Abschluss verbindlicher Vereinbarungen anzuzeigen. Dies gilt auch für die Beschaffung von Datenverarbeitungsprogrammen. Solange das Systemkonzept der Datenverarbeitung nicht grundlegend verändert wird, ist eine Anzeige nicht erforderlich. Jede Anzeige hat so umfassend und rechtzeitig zu erfolgen, dass der Aufsichtsbehörde vor Vertragsabschluss ausreichend Zeit zur Prüfung und Beratung des Versicherungsträgers bleibt.

Bei der Einführung von E-Government-Verfahren, elektronischer Vorgangsbearbeitungssysteme oder der elektronischen Langzeitspeicherung handelt es sich in der Regel um grundlegende Maßnahmen im DV-Bereich. Diese sind rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht anzuzeigen.

Die Aufsichtsbehörden haben den „Grundleitfaden 85“ (Grundleitfaden für Anzeigen zur Beschaffung bzw. Entwicklung von Datenverarbeitungsanlagen und –systemen sowie –programmen nach § 85 Abs. 1 Sätze 2 – 6 SGB IV) erstellt. Dieser bildet den Rahmen für die Anzeige und die Wirtschaftlichkeitsbetrachtung.

Soweit sich der Versicherungsträger bei der Erfüllung seiner gesetzlich vorgeschriebenen Aufgaben zulässigerweise eines Dritten bedient, kann er mit Genehmigung der Aufsichtsbehörde auch die damit notwendigerweise verbundenen Aufgaben des Rechnungswesens durch diesen Dritten wahrnehmen lassen (§ 19 SVRV). Die ausschließliche elektronische Aufbereitung der Rechnungsbelege durch den Dienstleister ist genehmigungsfrei (aber anzeigepflichtig).

## **3 Elektronische Kommunikation zwischen SV-Trägern und Versicherten**

### **3.1 Grundsätze**

Das zum 01.08.2013 in Kraft getretene „Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ sieht vor, dass durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung erleichtert wird. Medienbruchfreie Prozesse vom Antrag bis zur Langzeitspeicherung sollen möglich werden.

Artikel 1 des **E-Government-Gesetzes (kurz: EGovG)** präzisiert die wesentlichen Verfahrensschritte, die eine vereinfachte aber rechtssichere Informationsbeschaffung, Kommunikation und Antragstellung über das Internet zulassen.

Nachfolgend werden die Abschnitte aus dem EGovG dargestellt, die eine erhebliche Relevanz im Hinblick auf die Online-Kommunikation zwischen SV-Trägern und ihren Versicherten / Arbeitgebern haben. Zur Auslegung der Rechtsvorschriften wird auf die Ausführungen des BMI in seinem „Minikommentar“ zum EGovG verwiesen.

#### **3.1.1 Geltungsbereich**

Gemäß § 1 Abs. 1 gilt das EGovG für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Bundes einschließlich bundesunmittelbarer Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Der Begriff der Behörde lehnt sich an die weite Definition des § 1 Abs. 2 SGB X an. Der Begriff der öffentlich-rechtlichen Verwaltungstätigkeit wird hier ebenso verwendet wie im SGB X.

Das EGovG gilt nicht, soweit Rechtsvorschriften des Bundes inhaltsgleiche oder entgegengesetzte Bestimmungen enthalten (§ 1 Abs. 4 EGovG).

Hierunter fallen z. B. die Regelungen zur rechtssicheren Übertragung von Papierdokumenten in die elektronische Form sowie die Langzeitspeicherung elektronisch erzeugter Dokumente unter Verwendung der qualifizierten elektronischen Signatur (QES) gem. §§ 110a – d SGB IV. Diese sind vorrangig gegenüber den in § 7 EGovG getroffenen Regelungen zum Übertragen und Vernichten des Papieroriginals.

Darüber hinaus sind insbesondere Regelungen des SGB I, SGB IV, SGB V und des SGB X zum Sozialdatenschutz vorrangig.

Weitere Vorschriften des Sozialversicherungsrechtes, die Berührungspunkte zum EGovG enthalten, sind u.a. §§ 35 SGB I i.V.m. § 80 SGB X, 36a SGB I, §§ 21, 25 SGB X.

Soweit das Gesetz den Anwendungsbereich einzelner Regelungen nicht explizit auf Behörden des Bundes beschränkt, gelten sie für alle Behörden, wenn sie Bundesrecht ausführen.

| Nur für Behörden des Bundes/bundesunmittelbare Körperschaften geltende Regelungen: | Für Behörden des Bundes/Landes und für bundes-/landesunmittelbare Körperschaften geltende Regelungen: |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| § 2 Abs. 2: Eröffnung De-Mail-Zugang                                               | § 2 Abs. 1: Eröffnung eines Zugangs zur elektronischen Kommunikation                                  |
|                                                                                    | § 3: Information über Behörden und ihre Verfahren                                                     |
|                                                                                    | § 4: Elektronische Bezahlungsmöglichkeiten                                                            |
|                                                                                    | § 5: Nachweise                                                                                        |
| § 6: Elektronische Aktenführung                                                    |                                                                                                       |
| § 7: Übertragung und Vernichtung des Papieroriginals                               |                                                                                                       |
| § 8: Akteneinsicht                                                                 |                                                                                                       |
| § 9: Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand       |                                                                                                       |
| § 11: Gemeinsame Verfahren                                                         |                                                                                                       |
|                                                                                    | § 12: Anforderungen an das Bereitstellen von Daten                                                    |
|                                                                                    | § 13: Elektronische Formulare                                                                         |
|                                                                                    | § 14: Georeferenzierung                                                                               |
|                                                                                    | § 15: Amtl. Mitteilungs- u. Verkündungsblätter                                                        |
| § 16: Barrierefreiheit                                                             |                                                                                                       |

Sofern landesunmittelbare SV-Träger diese Verfahren einführen wollen, sollten die im EGovG aufgeführten Grundlagen und Bedingungen beachtet werden. Weiterhin sollten die SV-Träger laufend beobachten, ob einzelne Länder gleichlautende Vorschriften einführen.

### 3.1.2 Schriftformerfordernis und Ersatz der Schriftform

Nach § 126a BGB muss eine Urkunde vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden, wenn durch Gesetz die schriftliche Form vorgeschrieben ist. Der Umkehrschluss, dass immer dann, wenn eine Unterschrift vorgeschrieben ist, damit die gesetzliche Schriftform angeordnet ist, kann weder aus dem Wortlaut noch aus dem Zweck der Norm hergeleitet werden. Unterschriften werden im täglichen Leben auch außerhalb gesetzlicher Schriftformerfordernisse zu verschiedensten Zwecken geleistet und sind insbesondere als Feld für die Unterschrift des Erklärenden üblicher Bestandteil jeglicher Art von Formularen.

In **§§ 36a Abs. 2a SGB I, 13 EGovG** wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird:

*„Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.“*

Ist eine solche Schriftform explizit angeordnet, kann in der „elektronischen Welt“ auch künftig eine Unterzeichnung **ausschließlich** über die QES oder eine der mit dem EGovG eingeführten schriftformersetzenden Technologien abgebildet werden.

Diese sind (nach § 36a Abs. 2 Satz 4 SGB I):

- Bereitstellung **elektronischer Formulare über Web-Portale** der Behörde, die der Versicherte online „ausfüllen“ kann. Die Authentifizierung des Absenders muss hierbei über die eID-Funktion des neuen Personalausweises (nPA) oder den elektronischen Aufenthaltstitel (eAT) erfolgen.
- Die **Übersendung von elektronischen Dokumenten per De-Mail** mit der Versandoption „absenderbestätigt“, welche eine „sichere Anmeldung“ voraussetzt. Dabei ist der Sender der Nachricht durch ein sicheres Anmeldeverfahren identifiziert und die Nach-

richt einschließlich aller Metadaten durch eine vom De-Mail-Provider aufgebrachte QES (des De-Mail-Providers) gegen Veränderungen geschützt.

- In der Kommunikation zwischen dem Versicherten und seiner Krankenkasse kann die Identität auch mit der **elektronischen Gesundheitskarte** nachgewiesen werden.
- Daneben können per Rechtsverordnung weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden.

Für alle anderen Formulare, für die **kein Schriftformerfordernis** besteht und die der Behörde elektronisch übermittelt werden sollen, ist dies **ohne Unterschrift** möglich (z.B. am Bildschirm ausgefüllte PDF-Dokumente). Für diese Dokumente/Daten können jedoch erhöhte Anforderungen bzgl. des Nachweises der Authentizität des Absenders und die Integrität bei der Datenübermittlung gegeben sein. Nähere Ausführungen sind der Tz. 3.2.3 zu entnehmen.

Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das Übersenden per Post sind nicht mehr erforderlich.

Bei in **Papierform ausgegebenen Formularen** ist weiterhin das in der Rechtsnorm abgedruckte Format samt Unterschriftenfeld zu verwenden (§ 13 Satz 2 EGovG)!

### 3.1.3 Lesbarkeit übermittelter Dokumente

Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, übermittelt sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück (§ 36a Abs. 3 SGB I).

### 3.1.4 Barrierefreiheit

Nach § 16 EGovG sollen die Behörden des Bundes die barrierefreie Ausgestaltung der elektronischen Kommunikation und der Verwendung elektronischer Dokumente nach § 4 des Behindertengleichstellungsgesetzes (BGG) in angemessener Form gewährleisten.

In diesem Gesetz hat der Bund Regeln zur Herstellung von Barrierefreiheit in der Informationstechnik für seine Verwaltung gesetzt. Damit ist die Bundesverwaltung verpflichtet, ihre öffentlich zugänglichen Internetangebote grundsätzlich barrierefrei zu gestalten. Die entsprechende Rechtsverordnung „Barrierefreie Informationstechnikverordnung“ (BITV) vom Bundesinnenministerium und Bundesministerium für Arbeit und Sozialordnung regelt die Vorgaben hierzu. Die Länder haben entsprechende Regelungen erlassen.

Danach sollen einzelne Komponenten der elektronischen Verwaltung, z. B. der elektronische Zugang zur Verwaltung und die elektronische Aktenführung, so gestaltet werden, dass die elektronischen Kommunikationseinrichtungen und elektronischen Dokumente für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind. Das ist dann der Fall, wenn ihnen der Zugang mit den hierfür vorhandenen, der jeweiligen Behinderung entsprechenden Hilfsmitteln möglich ist.

Hieraus ergeben sich folgende Grundsätze:

- Inhalte und Erscheinungsbild sind so zu gestalten, dass sie für alle wahrnehmbar sind.

- Die Benutzeroberflächen der Angebote sind so zu gestalten, dass sie für alle bedienbar sind.
- Inhalte und Bedienung sind so zu gestalten, dass sie allgemeinverständlich sind.
- Die Umsetzung der Inhalte soll so erfolgen, dass sie mit heutigen und zukünftigen Technologien funktionieren.

### 3.1.5 Datenschutzrechtliche Einschränkungen

Die mit dem EGovG eingeführten Erleichterungen bei der Übermittlung elektronischer Dokumente oder Daten erreichen dort ihre Grenze, wo es sich um besonders schützenswerte Inhalte handelt. Hierunter fallen insbesondere sensible medizinische Angaben und Dokumente.

Sowohl bei der Beantwortung von Gesundheitsfragen in der Bildschirmmaske einer Web-Anwendung als auch beim Hochladen ärztlicher Dokumente werden bestimmte technische Zusatzmaßnahmen gefordert, die über die im EGovG genannten Bedingungen hinausgehen.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat in einer am 01.03.2013 herausgegebenen „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ hierzu einige grundsätzliche Aussagen getroffen, die die Versicherungsträger beachten sollten.

Es ist ein Grundsatz des Datenschutzes, dass bei der elektronischen Übertragung personenbezogener Daten die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein muss. Je schützenswerter ein Datum ist, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte sollen in keinen Fall Kenntnis von diesen Daten erhalten. Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen.

Im Wege einer Schutzbedarfsfeststellung und Risikoanalyse ist grundsätzlich festzulegen, welcher Schaden bei Verletzung der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit entstehen kann. Dabei sollten die Daten in die Schutzbedarfskategorien „normal“, hoch“ und „sehr hoch“ unterschieden werden.

Nach Auffassung des BfDI unterliegen Gesundheitsdaten dem Schutzbedarf „sehr hoch“. Bei diesen **ist** eine Ende-zu-Ende-Verschlüsselung (§ 5 Abs. 3 Satz 3 DeMailG) zwingend notwendig! Auch das Bundesinnenministerium (BMI) weist hierauf in seinem „Minikommentar“ zum EGovG ausdrücklich hin.

Weitere Ausführungen hierzu sind dem o. g. Dokument zu entnehmen, das über die Internetseite des BfDI eingesehen werden kann.

## 3.2 Zugang

### 3.2.1 Grundsätze

Der Austausch elektronischer Dokumente zwischen Versicherten und Versicherungsträger wird im § 36a SGB I geregelt. Danach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat.

Für die Kommunikation **SV-Träger** → **Versicherter** bedeutet dies, dass der Versicherte gegenüber dem SV-Träger ausdrücklich seine Zustimmung für die Übermittlung erteilt haben muss. Die bloße Angabe einer E-Mail-Adresse reicht nicht aus.

Dagegen ist für eine Kommunikation in Gegenrichtung **Versicherter** → **SV-Träger** die Bekanntgabe einer E-Mail-Adresse des SV-Trägers als Zustimmung anzusehen.

Ergänzend wird in § 2 EGovG festgelegt, wie die verschiedenen Zugänge bei den Behörden zu schaffen sind.

Absatz 1 gibt vor, dass **jede Behörde** – spätestens ab 01.07.2014 – einen Zugang für die Übermittlung elektronischer Dokumente zu schaffen hat, die auch mit einer QES versehen sind. Eine Festlegung auf ein bestimmtes Verfahren erfolgt hierdurch nicht. Soweit die Behörde ein E-Mail-Postfach hat, kann sie unverschlüsselte, qualifiziert signierte elektronische Dokumente empfangen. Neben dem E-Mail-Postfach ist z. B. auch ein elektronischer Zugang über Verwaltungspostfächer oder über Online-Formulare und Web-Anwendungen möglich.

Eine Verpflichtung zur Überprüfung einer Signatur oder zur Annahme von verschlüsselten Dokumenten wird durch das EGovG nicht begründet. Eine solche kann sich jedoch aus anderen gesetzlichen Vorschriften ergeben, z. B. aus § 110d SGB IV.

Absatz 2 verpflichtet **Behörden des Bundes** zusätzlich, ein De-Mail-Konto im Sinne von § 5 De-Mail-Gesetz zu eröffnen. Diese Verpflichtung trifft nur die Bundesbehörden und Körperschaften, die künftig einen Zugang zu dem zentral im internen Verbindungsnetz des Bundes geplanten „De-Mail-Gateway“ haben.

De-Mail-Nachrichten gelten als beim SV-Träger eingegangen, sobald sie sich im De-Mail-Postfach des SV-Trägers beim zugehörigen De-Mail-Provider befinden.

Eine Verpflichtung des SV-Trägers, dem Versicherten auf dem De-Mail-Wege zu antworten, besteht nicht, wenn der Versicherte mehrere Zugänge gegenüber dem SV-Träger eröffnet hat. Außerdem ist der SV-Träger nicht verpflichtet, per De-Mail zu antworten, wenn es sich um Sozialdaten mit sehr hohem Schutzbedarf handelt und hierbei zusätzliche Sicherheitsmaßnahmen (z. B. Ende-zu-Ende-Verschlüsselung) einzusetzen sind.

In Absatz 3 werden die **Behörden des Bundes** darüber hinaus verpflichtet, in Verwaltungsverfahren, in denen sie aufgrund einer Rechtsvorschrift die Identität des Versicherten festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachten, dies über einen elektronischen Identitätsnachweis nach § 18 Personalausweisgesetz bzw. § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten. Bei gesetzlich Krankenversicherten kann dieser Nachweis zusätzlich auch mit der elektronischen Gesundheitskarte erfolgen (§ 36a Abs. 2 Satz 5 SGB I).



## 3.2.2 Zugangsmöglichkeiten bei Schriftformersatz

### 3.2.2.1 Qualifizierte Elektronische Signatur

In § 36a Abs. 2 Satz 1 – 3 SGB IV wird geregelt, dass eine durch Rechtsvorschrift angeordnete Schriftform – soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist – durch die elektronische Form ersetzt werden kann. In diesem Fall **ist** das ausgehende Dokument **vom Absender** mit einer QES nach SigG zu versehen. Die Verwendung von Pseudonymen ist hierbei nicht zulässig.

Nähere Erläuterungen zur QES enthält der Abschnitt 4.2, zum Schriftformerfordernis die Tz. 3.1.2.

### 3.2.2.2 Eingabe über Web-Formulare oder besondere Eingabegeräte

Eine durch Rechtsvorschrift angeordnete Schriftform kann – neben der Verwendung einer QES – auch „durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular“ ersetzt werden, welches der SV-Träger „in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung stellt“ (§ 36a Abs. 2 Satz 4 Nr. 1 SGB I).

Die Formulierung stellt klar, dass hiermit nicht elektronische Formulare gemeint sind, die der Versicherte über das Internet herunterlädt, am Bildschirm ausfüllt (z. B. ausfüllbares PDF-Formular) und anschließend ausdruckt und an den SV-Träger schickt. Die Regelung betrifft die „Direktausfüllung“, also die unmittelbare Eingabe von Daten in eine vom SV-Träger zur Verfügung gestellte unveränderbare elektronische Maske (Formular). Die Eingabe kann erfolgen über Web-Anwendungen oder in vom SV-Träger (z.B. in seinen Kundenzentren) zur Verfügung gestellten Eingabegeräten<sup>4</sup>. Die elektronische Anwendung fungiert wie ein Formular, das aus der Ferne ausgefüllt wird.

Der SV-Träger kann durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können.

Der Versicherte muss sich zusätzlich identifizieren. Dies kann (gem. § 36a Abs. 2 Satz 5 SGB I) über die eID-Funktion des neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT) oder die elektronische Gesundheitskarte (eGK) erfolgen. Der SV-Träger **hat** dabei insbesondere **sicherzustellen**, dass die vom Versicherten **einggegebenen Erklärungen (Daten) mit den Identifikationsdaten des nPA / der eGK („Metadaten“, z. B. Personalausweisdaten, Eingabezeit) dauerhaft verknüpft werden**. Abgeleitet aus den §§ 110a – d SGB IV sind diese Daten revisionssicher zu archivieren.

Die technische und organisatorische Ausgestaltung des Gesamtverfahrens (von der Eingabe durch den Versicherten bis zur Übergabe der Daten an die Fachanwendung und das Langzeitarchiv) ist in einer ausführlichen Verfahrensbeschreibung zu dokumentieren. Hierzu gehört auch die Beschreibung des Verfahrens zum Auslesen der über die Web-Anwendung eingegangenen Daten/Dokumente (einschließlich Metadaten).

In der Verfahrensbeschreibung sind insbesondere die erforderlichen technischen Sicherheitsstandards zu beschreiben. Der SV-Träger hat hierbei u.a. die datenschutzrechtlichen Vorschriften des SGB und BDSG sowie die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgestellten Grundsätze zur Datensicherheit zu beachten.

---

<sup>4</sup> Eine (teilweise/vollständig) kostenlose Überlassung von elektronischen Eingabegeräten (z.B. Kartenleser) für Versicherte **durch den Versicherungsträger** ist gem. § 30 Abs. 1 SGB IV nicht zulässig!

### 3.2.2.3 Kommunikation mit De-Mail

Nach § 36a Abs. 2 Satz 4 Nr. 2 SGB I kann eine durch Rechtsvorschrift angeordnete Schriftform auch durch Versendung eines elektronischen Dokuments an den Versicherungsträger mit der **Versandart nach § 5 Abs. 5 DeMailG** ersetzt werden.

Nach der o.g. Vorschrift muss der akkreditierte De-Mail-Diensteanbieter dem Nutzer ermöglichen, seine „**sichere Anmeldung**“ im Sinne von § 4 DeMailG in der Nachricht so bestätigen zu lassen, dass die Unverfälschtheit der Bestätigung jederzeit nachprüfbar ist. Um dieses dem Empfänger der Nachricht kenntlich zu machen, bestätigt der akkreditierte Diensteanbieter des Senders die Verwendung der sicheren Anmeldung nach § 4 durch eine qualifizierte elektronische Signatur.

Der akkreditierte De-Mail-Diensteanbieter hat zu gewährleisten, dass der Nutzer (Absender) zwischen mindestens zwei Verfahren zur sicheren Anmeldung wählen kann. Eines kann z.B. über die eID-Funktion des neuen Personalausweises (nPA) erfolgen (§ 4 Abs. 2 DeMailG).

Das bedeutet:

- Bei einem bestehenden **Schriftformerfordernis** muss sich der Absender an seinem De-Mail-Konto „sicher angemeldet“ haben. Hierzu muss er für die Anmeldung zwei geeignete und voneinander unabhängige Sicherungsmittel einsetzen.  
Dies können sein:
  1. Sicherungsmittel = Benutzername und Passwort
  2. Sicherungsmittel = eID-Funktion des nPAHierzu muss der Absender über die für die Nutzung der eID-Funktion des nPA erforderliche technische Ausstattung (Kartenlesegerät) und einen hierzu geeigneten Browser verfügen.
- Der De-Mail-Diensteanbieter des Absenders muss in den Metadaten der Nachricht bestätigen, dass der Absender die sichere Anmeldung gem. § 5 Abs. 5 DeMailG gewählt hat. Diese Wahl muss aus der gesendeten Mail in der Form, wie sie beim Empfänger angekommen ist, dauerhaft erkennbar sein.
- Die mit der Versandoption „absenderbestätigt“ versendete De-Mail wird automatisch mit einer QES versehen. Diese wird nicht durch den Absender selbst sondern seinen De-Mail-Provider angebracht. Die QES muss die Nachricht selbst, alle angehängten Dateien und die Metadaten umfassen. Durch die QES wird bestätigt, dass die Nachricht des Absenders mit diesem Inhalt versandt wurde. Der Empfänger der Nachricht hat diese einschließlich der Metadaten und der QES zu archivieren. Die Form der Signierung bleibt hierbei nur solange erhalten, wie das Dokument mit der jeweiligen De-Mail-Nachricht verbunden bleibt. Die Nachricht sowie ihre Anhänge können nach dem Versand nicht unerkannt verändert werden (Integritätsschutz).
- Um die Nachprüfbarkeit der Signatur zu erhalten, dürfen auf der Empfängerseite die Nachricht und die Anhänge (z. B. PDF-Dokumente) nicht getrennt werden sondern müssen als Ganzes aufbewahrt werden.
- Für die QES dürfen ausschließlich Zertifikate von freiwillig akkreditierten Zertifizierungsdiensteanbietern verwendet werden. Nur diese bieten die Gewähr, dass die Signaturen dauerhaft überprüfbar bleiben.

### 3.2.2.4 De-Mail-Versand elektronischer Verwaltungsakte oder sonstiger elektronischer Dokumente durch den SV-Träger

Nach § 36a Abs. 2 Satz 4 Nr. 3 SGB I können SV-Träger elektronische Verwaltungsakte oder sonstige elektronische Dokumente – sofern ein gesetzlich festgelegtes Schriftformerfordernis besteht – als De-Mail-Nachricht mit der Versandoption „absenderbestätigt“ (gem. § 5 Abs. 5 DeMailG) an Versicherte und Arbeitgeber versenden.

Hierbei muss der De-Mail-Provider bei seiner in der Nachricht mitzusendenden Bestätigung (der sicheren Anmeldung) auch den erlassenden SV-Träger als Nutzer erkennen lassen. Beide Daten sind als Metadaten Bestandteil der Nachricht.

### 3.2.2.5 Identifizierung des Absenders durch sonstige sichere Verfahren

Der Gesetzgeber hat in § 36a Abs. 2 Satz 4 Nr. 4 SGB I festgelegt, dass auch andere sichere Verfahren die Authentizität des Datenübersmitters (Absender der Daten) und die Integrität des elektronisch übermittelten Datensatzes (Inhalt) sowie die Barrierefreiheit gewährleisten können.

Derartige Verfahren können nur über eine Rechtsverordnung festgestellt werden, die durch die Bundesregierung – mit Zustimmung des Bundesrates – erlassen wird.

### 3.2.3 Zugangsmöglichkeiten ohne Schriftformerfordernis

Auch bei Dokumenten, für die kein Schriftformerfordernis gesetzlich festgelegt ist, kann eine Übermittlung an den SV-Träger über die vorgenannten Zugangsmöglichkeiten (Web-Portal, De-Mail) erfolgen. In diesen Fällen ist jedoch grundsätzlich keine Authentifizierung über die in § 36a Abs. 2 Satz 4 SGB I genannten Zugangsmöglichkeiten erforderlich. Gleichwohl kann es erforderlich sein, dass die Authentizität des Absenders und die Integrität der Originaldaten aus anderen Gründen (z. B. für RSA-Prüfungen) nachzuweisen sind.

Ist der SV-Träger nicht bereit, auch für diese Daten die in § 36a Abs. 2 SGB I genannten sicheren Zugangsmöglichkeiten anzuwenden, muss der Nachweis der Authentizität und Integrität der Daten / Dokumente auf andere Weise erbracht werden.

Beispielhaft seien hier Mindestanforderungen für die Eingabe, Übermittlung und Archivierung von Daten des **Fragebogens zur Überprüfung der Familienversicherung** über ein Online-Portal aufgeführt (keine abschließende Aufzählung). Für diesen Fragebogen besteht – in der elektronischen Form – kein Schriftformerfordernis. Die Kasse hat jedoch einen Nachweis darüber zu führen, dass die Daten durch den Versicherten abgegeben wurden, wann sie in ihren Zugangsbereich gelangt und dort nicht verändert worden sind:

Online-Portal:

- Der SV-Träger hat im Rahmen einer Schutzbedarfsanalyse festzulegen, welche Daten über das Online-Portal übermittelt werden können. Hierbei sind insbesondere die Ausführungen des BfDI („Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“) im Hinblick auf die Übermittlung von Sozial- und Gesundheitsdaten zu beachten.
- Das Anmelde- und Nutzungsverfahren ist in einer detaillierten Verfahrensbeschreibung ausführlich darzustellen.
- Gesicherter Zugang zum „Versichertenkonto“ über Benutzername und Passwort. Der Nutzer kann sein Versichertenkonto erst nach Eingabe eines ihm postalisch zugestellten Freischaltcodes nutzen. Das Passwort ist beim erstmaligen Anmelden am Portal vom Versicherten zu ändern und darf keine Trivialnamen/-ziffern sondern

muss mindestens Buchstaben + Ziffern + Sonderzeichen enthalten. Passworte, die diese Kriterien nicht erfüllen, müssen bei der Änderung (online) abgewiesen werden.

- Alternativer Zugang (ohne „Versichertenkonto“) über dem Nutzer schriftlich mitgeteiltem Einmalpasswort, über das nur ein festgelegter Vorgang aufgerufen werden kann. Das Einmalpasswort verliert nach der Nutzung seine Gültigkeit.

Datenübermittlung:

- Die Datenübermittlung hat über eine SSL-verschlüsselte Verbindung (mindestens 128 Bit) zu erfolgen.
- Neben den Nutzdaten sind sog. Metadaten mitzusenden und zu archivieren. Diese können z. B. sein KV-Nummer, Benutzername, Eingabeart (z.B. über „Versichertenkonto“ oder „Einmal-Passwort“), Eingabe-/Übermittlungsdatum/-zeit.

Archivierung:

- Die vom Versicherten online eingegebenen Daten müssen als „Datensatz“ in einem Standarddatenformat (z.B. XML) zusammen mit den o.g. Metadaten unmittelbar nach Eingang beim SV-Träger/Dienstleister und vor dem Einspielen in eine Fachanwendung auf nicht wieder beschreibbaren Datenträgern oder in einem revisionssicheren Archiv gespeichert werden. Zur Sicherung der Datenintegrität ist jeder Datensatz mit einer qualifizierten elektronischen Signatur (QES) oder einem qualifizierten Zeitstempel gegen Integritätsverlust zu sichern.
- Die Datensätze müssen während der Aufbewahrungsfristen lesbar gemacht bzw. für eine Auswertung über Prüftools zur Verfügung gestellt werden können.
- Neben den Datensätzen wird empfohlen, ein PDF-Dokument zu erstellen, in dem die vom Versicherten beantworteten Fragen aufgeführt worden sind. Dieses sollte dem Versicherten am Ende seiner Eingabe angezeigt und zum speichern/ausdrucken zur Verfügung gestellt werden. Darüber hinaus wird der Kasse empfohlen, dieses Dokument mit einer QES zu versehen und im revisionssicheren Archiv zu speichern.
- Der Zugriff auf die archivierten Daten ist in einem Benutzerkonzept festzulegen. Administrationsrechte mit der Möglichkeit der Veränderung / Löschung von Daten sind restriktiv zu vergeben.
- Es wird empfohlen, die in der „Technischen Richtlinie TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) enthaltenen Anforderungen an eine beweiswerterhaltende Archivierung elektronischer Daten / Dokumente zu berücksichtigen (siehe Tz. 6.4).

Das gesamte Verfahren ist ausführlich in Verfahrensbeschreibungen darzustellen. Dies betrifft sowohl die fachlich-funktionalen als auch die sicherheitstechnischen Anforderungen / Abläufe von der Eingabe durch den Versicherten bis zur Übergabe der Daten an das revisionssichere Archiv.

### **3.3 Elektronische Einreichung von Nachweisen**

#### **3.3.1 Einreichung durch den Versicherten**

Nach § 5 Abs. 1 EGovG können vorzulegende Nachweise (Dokumente, Bescheinigungen, Urkunden etc.) auch elektronisch eingereicht werden. Dabei entscheidet der SV-Träger nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist.

Von diesem Grundsatz gibt es zwei Ausnahmen:

- Eine (andere) Rechtsvorschrift bestimmt, dass die Nachweise im Original (Papierform) vorzulegen sind.

- Der Versicherungsträger verlangt – nach pflichtgemäßem Ermessen – für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals.

In der Verwaltungspraxis wird bereits heute häufig die Vorlage von (unbeglaubigten) Kopien zugelassen. Nach dem Willen des Gesetzgebers soll dies zur Regel werden, wenn die Vorlage eines Originals nicht durch Rechtsvorschrift angeordnet ist oder der SV-Träger sie in Ausübung seines Verfahrensermessens (§ 21 SGB X) für bestimmte Verfahren oder im Einzelfall verlangt.

Für den Fall, dass Zweifel an der Echtheit der elektronischen Kopie bzw. der Übereinstimmung mit dem Original bestehen, kann der SV-Träger die Vorlage im Original verlangen.

Die vom SV-Träger zu bestimmende Art der Einreichung umfasst auch die technikkoffen gestaltete Frage, in welchem Format ein elektronisches Dokument einzureichen ist.

Die durch Versicherte übermittelten elektronischen Nachweise sind vom SV-Träger mit einer qualifizierten (Eingangs-)Signatur (QES) gegen Integritätsverlust zu versehen und revisionssicher zu archivieren (§§ 110a + d SGB IV).

### **3.3.2 Elektronische Übermittlung von Nachweisen zwischen verschiedenen Behörden / SV-Trägern**

In § 5 Abs. 2 EGovG ist geregelt, dass die zuständige Behörde bei der Durchführung eines elektronischen Verfahrens erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit Einwilligung des Verfahrensbeteiligten (Versicherter) direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen kann. Zusätzlich wird in Absatz 2 die Form der elektronischen Einwilligung festgelegt.

Für den Bereich der gesetzlichen Sozialversicherung ist der Schutz der Sozialdaten in den §§ 67 – 78 SGB X geregelt. Nach § 67a Abs. 2 SGB X sind Sozialdaten grundsätzlich beim Betroffenen (Versicherter/Mitglied) zu erheben<sup>5</sup>. Ohne seine Mitwirkung dürfen die Daten nur unter den in § 67a Abs. 2-5 SGB X genannten Voraussetzungen erhoben werden.

Da das SGB X im Verhältnis zum EGovG hinsichtlich der Erhebung von Daten gleich- oder entgegenstehende Regelungen enthält, haben diese Vorrang (§ 1 Abs. 4 EGovG). Für die Übermittlung elektronischer Nachweise zwischen SV-Trägern gelten somit die in § 5 Abs. 2 und 3 EGovG enthaltenen Bedingungen nicht. Für die Form der Einwilligung geht die in § 67b Abs. 2 SGB X enthaltene Regelung der im EGovG vor.

## **3.4 Elektronischer Posteingang**

### **3.4.1 Behandlung eingehender Fax-Sendungen**

Der SV-Träger hat die Einsatzbedingungen über die Fax-Nutzung in einer Sicherheitsleitlinie detailliert festzulegen.

#### **Analog-/Papier-Faxe**

Fax-Sendungen, die bei der Kasse auf einem Stand-alone-Faxgerät eingehen und ausgedruckt werden, müssen – sofern der Absender keine Header-Informationen mitgesandt hat –

---

<sup>5</sup> Erheben ist das Beschaffen von Daten über den Betroffenen (§ 67 Abs. 5 SGB X).

mit einem Eingangs- und Faxstempel gekennzeichnet werden. Derartige Dokumente werden von den Prüfdiensten uneingeschränkt anerkannt, sofern

- das ausgedruckte Fax archiviert wird, oder
- die Ausdrücke unmittelbar nach dem Ausdruck eingescannt und das Image mit einer QES versehen im elektronischen Langzeitarchiv gespeichert werden.

Werden eingehende Papier-Faxe ausgedruckt und an eine andere Dienststelle per Fax weitergesandt, so können diese „Fax-Kopien“ bei einer Prüfung nicht anerkannt werden. Bei diesen Dokumenten ist nicht feststellbar, ob zwischen Ausdruck und „weiterfaxen“ eine bildhafte Änderung am Original-Fax vorgenommen worden ist.

### **Elektronische Faxe**

Auch die auf einem Fax-Server eingehenden Faxe müssen – sofern keine Header-Informationen des Absenders vorhanden/sichtbar sind – mit einem elektronischen Fax-Stempel versehen werden.

Diese Faxe können wie folgt archiviert werden:

- a) In Papierform (Ausdruck des Fax) oder
- b) als Image, sofern dieses nach Eingang (und ggf. Anbringung eines Fax-Stempels) und vor der ersten Zugriffsmöglichkeit durch einen Mitarbeiter automatisch mit der qualifizierten Signatur eines (System-)Verantwortlichen oder einem qualifizierten Zeitstempel (der eine QES beinhaltet) versehen wurde (es gelten die Ausführungen zu „E-Mails“ in Ziff. 6.2)

#### Bitte beachten:

Bei dem unter b beschriebenen Verfahren besteht **keine Beweiswerterleichterung** i.S. von § 110d SGB IV. Die Anbringung der QES dient ausschließlich dem Integritätsschutz des Dokumentes.

#### Interne Weiterleitung von elektronischen Faxen

Die interne Weiterleitung elektronischer Faxe bzw. das elektronische Weiterfaxen an eine andere Dienststelle ist unter folgenden Voraussetzungen unkritisch:

- a) Die Faxserver befinden sich in einer gesicherten Umgebung. Zugriff hat ausschließlich der zuständige Administrator.
- b) Die Übermittlungswege zwischen Faxserver und Clients sind gegen innere und äußere Eingriffsmöglichkeiten durch Unbefugte geschützt. Maßgeblich sind hier die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den BSI-Grundschutzkatalogen festgelegten Empfehlungen zur Netzsicherheit.
- c) Die jeweils zuständigen Mitarbeiter (Fax-Server-Admin, Sachbearbeiter) verfügen über keine Bildbearbeitungssoftware, mit der der Faxinhalt verändert werden könnte.

### **3.4.2 Speicherung eingehender E-Mails im elektronischen Langzeitarchiv**

Grundsätzlich müssen elektronisch bei der Kasse eingehende Nachrichten/Dokumente, die eine rechtliche Wirkung entfalten, im elektronischen Langzeitarchiv gespeichert werden (§§ 110a + d SGB IV). Dies gilt auch für E-Mails.

Bei einer „normalen“ **E-Mail** (ohne QES) ist die Authentizität des Absenders nicht nachprüfbar. Somit kann aus dieser zunächst keine rechtliche Wirkung gezogen werden. Aufgrund der grundsätzlich bestehenden Formfreiheit kann sie jedoch für die Ingangsetzung eines

Verwaltungsverfahren herangezogen werden, in dessen Verlauf dann Angaben beweissicher erhoben werden müssen.

Enthält eine solche Mail einen Anhang, der die QES des Absenders beinhaltet, sind Mail und Anhang zu speichern.

Elektronische Dokumente, die der **Absender nicht qualifiziert signiert** hat, sind vor der Langzeitspeicherung mit der QES eines (System-)Mitarbeiters zu versehen, der für die „Betreuung“ des E-Mail-/Fax-Servers verantwortlich ist. Die Signatur kann im Wege der Massensignatur erfolgen. Alternativ ist auch eine Einzelsignatur durch den Empfänger (Sachbearbeiter) möglich.

Voraussetzung hierfür ist, dass der SV-Träger/Dienstleister detailliert die nachfolgend genannten technischen und organisatorischen Maßnahmen festlegt und umsetzt:

- Ausführliche Verfahrensbeschreibung (einschl. Festlegung des Datenformates, z. B. automatische Umwandlung des Text- in ein PDF/A-Format).
- Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv.
- Bei Einsatz einer Einzelsignatur (durch den SB) vor der Archivierung ist ein Verfahren zu entwickeln, dass eine Manipulationsmöglichkeit des Dokumentes verhindert.
- Festlegung, was mit Dokumenten zu geschehen hat, die nicht in das Langzeitarchiv gehören (z. B. unzuständiger Empfänger, SPAM, Dokumente mit extremen oder sexistischen Inhalten).

Es wird ausdrücklich darauf hingewiesen, dass die an diesen Dokumenten angebrachte QES eines Mitarbeiters zu **keiner Beweiswerterleichterung** i. S. des § 110d SGB IV führt. Sie dient ausschließlich der Integritätssicherung des eingegangenen elektronischen Dokumentes.

### 3.4.3 Speicherung eingehender DE-Mails im elektronischen Langzeitarchiv

#### Nachrichten mit Schriftformerfordernis:

De-Mail-Nachrichten, die mit der Versandart nach § 5 Abs. 5 DeMailG (absenderbestätigt) beim SV-Träger eingehen, sind mit einer QES des De-Mail-Diensteanbieters des Absenders versehen. Diese Nachrichten enthalten außerdem die Daten der „sicheren Anmeldung“ als Metadaten. Die Nachricht ist zusammen mit den Metadaten und der QES im elektronischen Langzeitarchiv des SV-Trägers zu speichern.

Es wird ausdrücklich darauf hingewiesen, dass die durch den Provider angebrachte QES zu **keiner Beweiswerterleichterung** i. S. des § 110d SGB IV führt. Sie dient ausschließlich der Integritätssicherung des eingegangenen elektronischen Dokumentes.

#### Nachrichten ohne Schriftformerfordernis:

Diese müssen gem. DeMailG keine Absenderbestätigung und somit auch keine QES enthalten. Der Absender muss zur Erstellung auch keine „sichere Anmeldung“ am De-Mail-Account wählen.

Um der geltenden Archivierungspflicht gem. §§ 110a-d SGB IV zu genügen, sollten die SV-Träger diese De-Mail-Nachrichten (einschließlich etwaiger Metadaten) mit einer serverbasierten Eingangssignatur (QES) versehen und im Langzeitarchiv speichern.

Es wird ausdrücklich darauf hingewiesen, dass die an diesen Dokumenten angebrachte QES eines Mitarbeiters zu **keiner Beweiswerterleichterung** i. S. des § 110d SGB IV führt. Sie dient ausschließlich der Integritätssicherung des eingegangenen elektronischen Dokumentes.

## 3.5 Elektronischer Postausgang

### 3.5.1 Grundsätze

Für den Bereich der gesetzlichen Krankenversicherung gilt grundsätzlich das Prinzip der Formfreiheit. So kann der **Erllass eines Verwaltungsaktes (VA)** z. B. auch mündlich erfolgen (siehe § 33 Abs. 2 Satz 1 SGB X). Es müssen lediglich die in § 33 Abs. 3 Satz 1, Abs. 5 SGB X genannten Anforderungen (Erkennbarkeit der erlassenden Behörde) gewahrt werden. Dementsprechend kann z.B. bei einer Postausgangssignatur auf die qualifizierte elektronische Signatur grundsätzlich verzichtet werden.

Von der beschriebenen Rechtslage hinsichtlich des VA-Erlasses ist allerdings die Frage der **Langzeitspeicherung der Verwaltungsunterlagen** (zu denen auch der VA selbst gehört) zu unterscheiden. Insoweit verfolgt das Gesetz andere Zielsetzungen als beim VA-Erlass. Es geht nicht um die rechtssichere Bekanntgabe gegenüber dem Adressaten sondern um die zuverlässige Langzeitspeicherung von Unterlagen. Hierzu setzt § 110d Nr. 1 u. 2 SGB IV i. V. m. § 110a Abs. 2 SGB IV für die (erleichterte) Beweiswirkung der archivierten Unterlagen die qualifizierte elektronische Signatur (QES) dessen voraus, der

1. die Wiedergabe auf dem dauerhaften Datenträger hergestellt oder die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe unmittelbar nach der Herstellung der Wiedergabe geprüft hat, oder
2. bei urschriftlicher Aufzeichnung des Textes nur in gespeicherter Form diese mit einer QES nach dem SigG versehen hat.

Dies gilt nach dem ausdrücklichen Willen des Gesetzgebers für alle Unterlagen, also auch die elektronischen Verwaltungsakte, obwohl deren Bekanntgabe – wie oben dargelegt – unter geringeren Anforderungen erfolgen konnte.

Eine Aufbewahrung und Langzeitspeicherung in elektronischer Form ohne qualifizierte elektronische Signatur (QES) ist aufsichtsrechtlich bedenklich, da diesen Dokumenten im Rechtsverkehr keine Beweiskraft i.S.d. § 110d SGB IV zukommt und zumindest die Möglichkeit besteht, dass ihr Inhalt ggf. gerichtlich dargelegt oder sogar bewiesen werden muss.

Der gesetzeskonforme Einsatz der QES ist für die SV-Träger mit erheblichem organisatorischem und finanziellem Aufwand verbunden. Sie bevorzugen daher die Verwendung der sog. **Massensignatur** (z. B. durch einen für die Erstellung der Briefe im Batch-Betrieb verantwortlichen IT-Mitarbeiter). Deren Einsatz ist allerdings wegen der in § 110d SGB IV formulierten Anforderungen an die Beweiswirkung elektronisch gespeicherter Dokumente aufsichtsrechtlich nicht vertretbar. Die automatische Anbringung einer QES im Wege der Stapel-/Massensignatur ist daher beim elektronischen Postausgang **unzulässig!**

Es wird empfohlen, elektronische Dokumente immer dann mit einer QES des Erstellers zu speichern, wenn es sich um Dokumente mit „Beweiswertcharakter“ (z. B. Verwaltungsakte) handelt und zu erwarten ist, dass deren Inhalt zu einem späteren Zeitpunkt gerichtsfest dargelegt/bewiesen werden muss. Eine Differenzierung kann hierbei nicht nach einzelnen Dokumenttypen (z.B. E-Mail, Fax) sondern nur inhaltlich erfolgen.

### 3.5.2 E-Mails (ohne/mit Anhang)

E-Mails bzw. deren Anhänge müssen – sofern sie beweiswerterhaltende Inhalte haben – mit der QES des verantwortlichen Mitarbeiters (Einzelsignatur) versehen und im Langzeitarchiv gespeichert werden.



### 3.5.3 De-Mails (ohne/mit Anhang)

De-Mails, die schriftformersetzende Inhalte haben, müssen vom SV-Träger über eine „sichere Anmeldung“ und die Versandart nach § 5 Abs. 5 DeMailG versendet werden. Diese De-Mails werden vom De-Mail-Provider des SV-Trägers mit einer QES versehen.

Bei Verwaltungsakten muss gem. § 33 Abs. 3 Satz 3 SGB X die Bestätigung nach § 5 Abs. 5 DeMailG die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.

Bei der vom De-Mail-Provider angebrachten QES handelt es sich nicht um eine Willenserklärung des Absenders. Eine solche ist jedoch gemäß den Regelungen aus §§ 110a und d SGB IV für die revisionssichere Speicherung beim KV-Träger zwingend erforderlich. Daher gelten die in Ziff. 3.5.1 dargestellten Grundsätze.

Für De-Mails ohne schriftformersetzende Inhalte gilt die Regelung zu Ziff. 3.5.2.

### 3.5.4 Erstellung und Versand von Serienbriefen

Im Rahmen von elektronischen Workflows ist es üblich, Serienbriefe unter Verwendung vorgefertigter Textbausteine z. B. als Bescheid zu versenden. Aufgrund der Regelungen in §§ 110a und d SGB IV ist es erforderlich, bei der Langzeitspeicherung die „Durchschriften“ derartig erzeugter Briefe mit einer QES des Absenders zu versehen. Nach § 110a Abs. 2 Satz 3 SGB IV ist bei der Langzeitspeicherung nicht erforderlich, dass die Wiedergabe auf dem dauerhaften Datenträger mit der erstellten Unterlage (Brief an Versicherten) bildlich übereinstimmt. Das bedeutet, dass die elektronische „Durchschrift“ z. B. unter Aufführung der verwendeten Textbausteinnummern sowie der Variablen erfolgen kann. Die inhaltliche Übereinstimmung mit dem ursprünglich versandten Brief muss jedoch nachvollziehbar sein.

## 4 Technische und organisatorische Verfahrensanforderungen

### 4.1 Allgemeine Anforderungen

#### 4.1.1 Verfahrensbeschreibung

Zur Beurteilung der vom Versicherungsträger vorgesehenen Verfahren ist die Vorlage von ausführlichen, nachvollziehbaren Verfahrensbeschreibungen unumgänglich. Solche müssen insbesondere detaillierte Informationen zu den Arbeitsabläufen (Geschäftsprozesse), den betroffenen Dokumentarten und Formularen, zu Datenschutz- und Datensicherheitsmechanismen, zur Karten- und Rechteverwaltung sowie zur Aufbewahrung, Löschung und Vernichtung beinhalten.

Der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte und die Innenrevision sollten bei der Erstellung beteiligt werden.

#### 4.1.2 Dienstanweisung

Nach § 17 SVRV i.V. mit § 40 SRVwV hat der Versicherungsträger bei Einsatz der automatisierten Datenverarbeitung zur Sicherheit des Verfahrens eine Dienstanweisung zu erlassen.

Die Dienstanweisung muss bei Einsatz der elektronischen Signatur, Web-Portalen, De-Mail u. a. Einzelheiten enthalten

- zur Qualifizierten Elektronischen Signatur (QES),
- zur Stapelsignatur (§ 41 Abs. 5 SRVwV),
- zu Web-Anwendungen für die Eingabe und Übermittlung von Daten und Nachweisen (z.B. Authentifizierung des Nutzers, Beschreibung der Sicherheitseinrichtungen),
- zur Nutzung von De-Mail gem. EGovG,
- zu Art und Umfang,
- über die zusätzlich zu den Belegen zu speichernden Angaben (insbesondere Namen des Speichernden und Zeitpunkt der Langzeitspeicherung),
- zur detaillierten Beschreibung des organisatorischen Ablaufs.

**Daher sind Regelungen u. a. zu folgenden Punkten zu treffen:**

#### Zertifikate

- Gültigkeit max. 10 Jahre (§ 14 Abs. 3 SigV)
- Vor Ablauf der Eignung der Algorithmen (→ Bekanntgabe durch BNetzA) Neusignatur (§ 6 Abs. 1 S. 2 SigG, § 16 SigV) mit qualifiziertem Zeitstempel
- Sperre des Zertifikats
  - auf Verlangen des Zertifikatsinhabers oder
  - wegen falscher Angaben des Inhabers
  - Telefonisches Sperrverfahren (§ 7 SigV)
- Verfahren zum Update der Sperrlisten (CLRs-Verfahren)
  - Importdatei auf eigenem Server, Häufigkeit

#### Attribute

- Bestätigung durch Dritten (hier: SV-Träger/Arbeitgeber)
- Dritter erhält auch Mitteilung bei Sperre  
Anmerkung: Nach § 41 Abs. 2 SRVwV muss das qualifizierte Zertifikat die ausschließliche Anwendung zu dienstlichen Zwecken vorsehen. Somit ist eine entsprechende Selbstbeschränkung – im Hauptzertifikat oder als getrenntes Attribut-Zertifikat - unentbehrlich.

### PIN-Regeln

- Ausreichende Länge (mindestens 6 Zeichen)
- Sofern technisch möglich: Großes Alphabet mit Ziffern und Sonderzeichen (sofern dies durch die Eingabetastatur unterstützt wird)
- Verbot der Speicherung auf programmierbaren F-Tasten
- Regelmäßiger Wechsel (ca. alle 90 Tage)
- Automatische Sperre nach 3 Fehleingaben! Folge: Neue Karte bzw. neues Zertifikat muss beantragt werden
- Hinterlegungsregelungen

### Kartenmanagement

- Kartenausgabe/-ersatz (bei Verlust, Zerstörung, Vergessen)  
Anmerkung: Gem. § 8 Abs. 2 SigG kann der SV-Träger selbst – neben dem Karteninhaber – eine Sperre der Karte bzw. des Zertifikats veranlassen. Ggf. sind entsprechende vertragliche Regelungen gem. § 8 Abs. 1 SigG mit dem Zertifizierungsdiensteanbieter zu treffen.
- Ggf. Ersatzkarten für jede/n Mitarbeiter/in
- Stellvertreterregelungen

### Beschreibung des Verfahrens zur Anmeldung und Nutzung von Web-Portalen

- z.B. Authentifizierungsmethoden mit/ohne Schriftformerfordernis
- Sicherheit der Daten von der Eingabe bis zur Übergabe an das Fachverfahren bzw. das elektronische Archiv

### Beschreibung des Verfahrens zur Anmeldung und Nutzung von De-Mail

- z.B. Unterschiedliche Anmeldeverfahren mit/ohne Schriftformerfordernis
- Sicherheit der Daten von der Eingabe bis zur Übergabe an das Fachverfahren bzw. das elektronische Archiv

### Beschreibung des Scan- und Signaturverfahrens

- Besonderheiten, z. B. Vorkehrungen/Regelungen zur Vermeidung von Doppelerfassungen

### Zugriffs- und Zutrittsregelungen

- Steuerung über Attributbeschreibungen/-inhalte
- Protokollierung und regelmäßige Auswertung der Zugriffe
- Zutritt zu den zentralen Scan-/Signaturarbeitsplätzen bei Einsatz der Stapelsignatur (Closed-Shop-Betrieb)

### Regelmäßige Stichprobenprüfung von Signaturen

- Täglich
- Umfang der Stichprobe; Auswahl der Stichprobe

### Verpflichtungserklärung der Mitarbeiter/innen

- Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Der Signaturschlüssel-Inhaber muss gegenüber dem SV-Träger zustimmen, dass sein Zertifikat beim Zertifizierungsdiensteanbieter abrufbar gehalten wird (Ausschluß Erklärung nach § 5 Abs. 1 Satz 3 SigG)
- Verhalten in besonderen Situationen, z. B. wenn die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen wird
- Prüfung arbeits-/dienstrechtlicher Konsequenzen, wenn Mitarbeiter/innen die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen haben

### Ergonomie der Arbeitsplätze

- Scan-/Signaturarbeitsplatz mit einem Bildschirm, auf dem das gesamte Dokument komplett abgebildet werden kann.
- Schulung der Benutzer und IT-Betreuer

## **4.2 Qualifizierte Elektronische Signatur (QES)**

### **4.2.1 Signaturerstellungseinheiten und Signaturanwendungskomponenten**

#### 1. Signaturerstellungseinheiten:

Die beim Signaturverfahren zu verwendenden Signaturerstellungseinheiten sind im § 17 SigG näher beschrieben. Diese müssen gem. § 17 Abs. 4 Satz 1 SigG geprüft und bestätigt sein. Eine aktuelle Liste ist auf der Homepage der Bundesnetzagentur (BNetzA) zu finden.

#### 2. Signaturanwendungskomponenten:

Für Signaturanwendungskomponenten nach § 17 Abs. 3 Nr. 2 und 3 SigG genügt eine Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG. Nach der gängigen Definition ist die Herstellererklärung eine Erklärung eines Herstellers gegenüber der zuständigen Aufsichts- und Kontrollinstitution, dass das Produkt allen hierfür relevanten technischen Standards und Spezifikationen entspricht.

Demzufolge war es auch nach der vor dem Inkrafttreten des 1. SigÄndG herrschenden Rechtslage bereits so, dass entsprechende Herstellerklärungen bei der BNetzA hätten eingereicht werden müssen. Insoweit erfolgte durch das 1. SigÄndG lediglich eine Klarstellung bereits bestehender Vorgaben.

Mit Inkrafttreten des 1. SigÄndG am 11.01.2005 besteht bei der BNetzA folgendes Verständnis von einer Herstellererklärung: Die nach § 15 Abs. 5 S. 2 SigV für Produkte nach § 17 Abs. 1 und Abs. 3 Nr. 1 SigG erforderliche Prüfung und Bestätigung muss bei Produkten nach § 17 Abs. 2, 3 Nr. 2 und 3 durch eine die Bestätigung und qualitätssichernde Prüfung der Sicherheitsanforderungen insgesamt abdeckende Herstellererklärung ersetzt werden.

Denn genauso, wie erstere geprüfte Produkte nach § 17 Abs. 1, 3 Nr. 1 SigG gemäß Anlage 1 zum SigV I. Ziff. 4 von der BNetzA zu veröffentlichen sind, folgt aus der Tatsache, dass auch Produkte nach § 17 Abs. 2, 3 Nr. 2 und 3 SigG zu veröffentlichen sind, eine Pflicht des Herstellers, in seiner Erklärung zusätzlich detailliert darzulegen, wie er das Produkt im Einzelnen geprüft hat. Möglicherweise sind zusätzlich Testspezifikationen aufzuführen, die Anwendung gefunden haben, ferner welche Qualitätssicherungssysteme (ISO 9001, ...) zum Einsatz kommen usw. Vom Detaillierungsgrad entspricht eine Herstellererklärung daher einer Bestätigungsurkunde nebst des zu Grunde liegenden Prüfberichts („Evaluation Technical Report“ - ETR).

Zur Frage bezüglich der Bewertung des Einsatzes nicht herstellereklärter Signaturprodukte, wird von der BNetzA darauf hingewiesen, dass, wenn die Produkte ohne den Vorgaben des Gesetzes entsprechende Erklärungen in Verkehr gebracht werden, die Gefahr besteht, dass mit Hilfe dieser Produkte erstellte Signaturen etwa im Rahmen von Umsatzsteuerprüfungen des Finanzamts von dort nicht als den Anforderungen von SigG und SigV gerecht werdende qualifizierte elektronische Signaturen anerkannt werden. Um hieraus resultierende Schadensersatzforderungen gegenüber den SV-Trägern vorzubeugen, ist eine den Anforderungen von SigG und SigV entsprechende Herstellererklärung einzureichen.

Der Hersteller ist verpflichtet, bei Änderung der Programmversion eine neue Herstellererklärung abzugeben.

Ergänzend wird an dieser Stelle auf eine Veröffentlichung der Bundesnetzagentur vom 06.02.2009 hingewiesen:

#### **„Hinweis im Zusammenhang mit der Nutzung von freiwilligen Prüfzeichen**

Internetpublikationen zufolge gibt es Dienstleister, welche zum Nachweis der Übereinstimmung ihres Angebots mit den gesetzlichen Bestimmungen des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) freiwillige Prüfzeichen verwenden.

Die Bundesnetzagentur weist darauf hin, dass solche freiwilligen Prüfzeichen zum Nachweis der signaturrechtlichen Konformität unzulässig sind. Die Übereinstimmung von Produkten: Signaturanwendungskomponenten und technischen Komponenten nach dem Signaturgesetz und nach der Signaturverordnung werden ausschließlich durch Produktbestätigungen und veröffentlichte Herstellererklärungen nachgewiesen. Bestätigungen werden dabei ausschließlich von nach § 18 SigG anerkannten (Prüf- und) Bestätigungsstellen erstellt, Herstellererklärungen nur durch die Hersteller des Produktes abgegeben.“

### **4.2.2 Regelungen für das Kartenmanagement**

Im Rahmen des elektronischen Geschäftsverkehrs werden Signaturkarten nur an den speziellen Arbeitsplätzen benötigt, an denen die Signatur eingescannter Belege oder elektronisch erstellte Dokumente erfolgt. Diese Arbeitsplätze sind nur funktionsfähig, wenn der Bediener auf seine gültige(n) Signaturkarte(n) zurückgreifen kann. Gemäß § 41 Abs. 2 SRVwV sind Attributzertifikate zwingend vorgeschrieben; durch diese wird die Verwendung der Karte auf den jeweiligen Einsatzbereich beschränkt.

Die Signaturkarten sollten in einem Bestandsverzeichnis verwaltet werden, so dass immer nachvollziehbar ist, wann welche Karten eingesetzt wurden. Außerdem können dann die Karten der Nutzer, die nicht mehr in dem jeweiligen Bereich tätig sind, gesperrt werden. Auf die besonderen Regelungen zur elektronischen Zahlungsanordnung (§ 11 Abs. 4 SRVwV) wird hingewiesen.

Auf Grund der Abhängigkeit von den Signaturkarten könnte für jeden Nutzer eine Reservekarte vorgehalten werden (gilt insbesondere bei „Stapelsignaturbetrieb“), sofern nicht durch andere organisatorische Regelungen die Aufrechterhaltung des Scan-/Signaturbetriebes gewährleistet ist. Die Notwendigkeit sollte der SV-Träger im Rahmen einer Risikobetrachtung feststellen. Die Verwendung einer allgemein nutzbaren Reservekarte ist nicht möglich, da die Signaturkarten personenbezogen ausgestellt werden. Mit dem Trustcenter sollten vertragliche Regelungen getroffen werden, dass Ersatzkarten in vertretbarer Zeit geliefert werden können.

Signaturkarten sollten an einem festen Platz aufbewahrt werden, z. B. in einem Schließfachsystem, aus dem die Nutzer sie bei Dienstbeginn entnehmen und bei Dienstende zurücklegen. Die Karten verlassen somit nie den gesicherten Bereich.

### **4.2.3 Neusignieren nach § 17 SigV**

#### Neusignierung von Elektronischen Signaturen

Elektronische Signaturen basieren auf mathematischen Komplexitätsproblemen. Der technische Fortschritt führt dazu, dass immer komplexere solcher Probleme im Laufe der Zeit gelöst werden können und somit ein Signaturalgorithmus insgesamt oder eine gegenwärtig als sicher angesehene Parametrisierung (hierzu zählt z. B. die Länge eines Schlüssels) ab ei-

nem bestimmten Zeitpunkt durch die Bundesnetzagentur (BNetzA) nicht mehr als sicher angesehen werden. Die BNetzA legt daher jedes Jahr die Signaturalgorithmen und die Parameter fest, die sie für die nächsten Jahre als sicher ansieht. Die elektronische Signatur verliert also durch den technischen Fortschritt im Laufe der Zeit ihre Sicherheits- und Beweiseignung, wenn nicht weitergehende Maßnahmen ergriffen werden. Insbesondere bei der Langzeitspeicherung wird sich dieser Fall häufiger ergeben.

Mit § 17 SigV hat der Gesetzgeber hierfür eine entsprechende Regelung geschaffen: "Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 2 Satz 2 des Signaturgesetzes neu zu signieren, wenn sie für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Fall sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen und zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen."

Die erneute Signatur mit neuen Algorithmen und zugehörigen Parametern muss also zu einem Zeitpunkt erfolgen, in dem die alte Signatur noch sicher ist. Um zu beweisen, dass dieses sog. Übersignieren rechtzeitig erfolgt ist, muss ein qualifizierter Zeitstempel angebracht werden. Wird dieses Verfahren regelmäßig angewendet, kann der Beweiswert und die Beweiseignung einer elektronischen Signatur noch nachgewiesen werden, auch wenn die Ursprungssignatur alleine zwischenzeitlich unsicher geworden ist. Die neu anzubringende Signatur muss dabei natürlich nicht von der Person angebracht werden, die die Ursprungssignatur erzeugt hat.

#### Neusignierung von Hashalgorithmen

Genauso wie bei der erstmaligen Signatur geht es bei der Neusignatur auch darum, sie effektiv und kostengünstig durchzuführen, das Übersignieren soll handhabbar sein und die Anzahl der notwendigen Zeitstempel gering gehalten werden.

Auch bei der Übersignatur wird nicht das Dokument selbst, sondern der Hashwert signiert. Problematisch hinsichtlich des Erhalts der dauerhaften Beweiseignung ist, dass auch die Hashalgorithmen mathematische Komplexitätsprobleme darstellen, die durch den technischen Fortschritt hinsichtlich der Sicherheit genauso beeinflusst werden, wie die elektronischen Signaturalgorithmen.

Wird ein Hashalgorithmus durch die BNetzA ab einem bestimmten Zeitpunkt nicht mehr als sicher eingestuft, so gelten auch hier die Bestimmungen aus § 17 SigV; d. h. es ist ein erneuter Hashwert mit einem als sicher beurteilten Verfahren (für jedes Dokument) zu bilden, mit einer qualifizierten Signatur (neue Signaturalgorithmen und Parameter) zu signieren und ein qualifizierter Zeitstempel anzubringen.

#### Neusignierung von Zeitstempeln

Sollte der qualifizierte Zeitstempel, sofern er selber auf einer qualifizierten Signatur beruht, unsicher werden, reicht es aus, den Hashwert über die archivierten Dokumente zu erzeugen, alle früheren Signaturen dabei mit einzuschließen und dann einen solchen sog. kryptografischen Zeitstempel (qualifizierte Zeitstempel der auf einer qualifizierten Signatur beruht) für diesen Hashwert einzuholen.

Vorausgesetzt, die Signatur, die der Zeitstempel trägt, basiert auf den neuen Algorithmen und Parametern, entfällt in diesem Fall die Notwendigkeit, nochmals eine eigene qualifizierte Signatur anzubringen.

### Hinweise:

Die Bundesnetzagentur (BNetzA) [vormals: Regulierungsbehörde für Telekommunikation und Post – RegTP] gibt einmal jährlich eine „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Übersicht über geeignete Algorithmen“ heraus, in der eine Einschätzung der Sicherheit der verwendeten Algorithmen und entsprechende Empfehlungen abgegeben werden. In ihrer Publikation vom 22. Februar 2007 (Bundesanzeiger Nr. 69, S. 3759) teilte sie mit, dass für den beim RSA-Verfahren zugrunde liegenden Berechnungsmodus eine Länge von 1024 Bit nur noch bis zum 31. Dezember 2007 ausreicht. Für den Zeitraum 2008 – 2012 wurden bis auf 1976 Bit ansteigende Mindestwerte genannt. Empfohlen wurde die grundsätzliche Erhöhung auf 2048 Bit. Gleichlautende Feststellungen bzw. Empfehlungen hat die RegTP bereits **seit dem Jahr 2003 im jährlichen Turnus** veröffentlicht. Die aktuellen Werte sind der Internetseite der BNetzA zu entnehmen.

Um die **Beweiswirkung nach 110 d SGB IV zu erhalten**, haben die Institutionen rechtzeitig eine **Nachsignatur** zu veranlassen.

Nehmen Sozialversicherungsträger die Nachsignatur bis zu dem von der BNetzA genannten Termin **nicht** vor, fällt der **Vorteil des Anscheinsbeweises** (Privileg des Beweises des ersten Anscheins) weg. Für den Sozialversicherungsträger tritt im Streitfall die Umkehr der Beweislast ein.

Aus der Literatur können verschiedene Empfehlungen zur Vorgehensweise entnommen werden, die auch zur Wirtschaftlichkeit der Maßnahmen beitragen. U.a. ist als eine technische Möglichkeit der Aufbau von Hashbäumen in Betracht zu ziehen (vgl. u.a. **ArchiSig-Konzept** in: Roßnagel/Schmücker (Hrsg.) Beweiskräftige elektronische Archivierung, Economica Verlag, Heidelberg 2006, S. 86 ff). Dazu muss das Dokument mit der Signatur, dem Zeitstempel sowie ggf. vorhandener Auskünfte aus dem Verzeichnisdienst exportiert werden. Daraus können die jeweiligen Archivcontainer gebildet werden (in diesem Fall ist im Container nur **ein Dokument** enthalten), über die dann die Hashbäume aufgebaut werden.

Als Alternative käme auch eine „große“ Containerlösung (hier sind **mehrere Dokumente** zusammengefasst) in Betracht, wenn eine an den Aufbewahrungsfristen orientierte Archivstruktur möglich ist.

Besonders für die langen Zeitspannen, wie sie für die Langzeitspeicherung notwendig sind, können keine verlässlichen Voraussagen der technischen Entwicklung getroffen werden. Das Archiv sollte daher zumindest die verschiedenen Verfahren zur Neusignierung beherrschen.

### 4.3 Web-Portale

Viele SV-Träger bieten ihren Versicherten bereits heute die Möglichkeit, über das Internet Formulare herunter zu laden, geänderte Adressdaten mitzuteilen oder Info-Material anzufordern. Es handelt sich in der Regel um einen geschützten Bereich des Internetauftritts des SV-Trägers, zu dem der Versicherte sich – nach vorheriger einmaliger Registrierung – durch Eingabe eines Benutzernamens und eines Passwortes an seinem „Konto“ anmelden kann. Der Verbindungsaufbau und die Datenübertragung erfolgen über eine mit 128 Bit SSL verschlüsselte Leitung.

Für die Übermittlung von Nachrichten oder die Übersendung von elektronischen Nachweisen, bei denen ein Schriftformerfordernis (Tz. 3.1.2) vorliegt, sind bei der Nutzung über Web-

Anwendungen zusätzliche technische Maßnahmen erforderlich, die in entsprechenden Verfahrensbeschreibungen ausführlich zu erläutern sind.

Nach § 36a Abs. 2 Satz 4 Nr. 1 i.V.m. Satz 5 SGB I hat der SV-Träger die Identität des Nutzers vor Eingabe der Daten/Nachricht festzustellen. Hierzu hat er einen Identitätsnachweis durch Verwendung der eID-Funktion des nPA bzw. mit Hilfe der eGK online vom Nutzer „anzufordern“. Das Ergebnis der Überprüfung ist zusammen mit der übermittelten Nachricht bzw. den erhobenen Daten revisionssicher zu speichern.

Nähere Ausführungen hierzu sind der Ziff. 3.2.2.2 zu entnehmen.

#### **4.4 De-Mail-Zugang**

Eine Verpflichtung zur Schaffung eines De-Mail-Zuganges besteht für bundesunmittelbare SV-Träger nur dann, wenn sie die Möglichkeit erhalten, diesen über die für Bundesbehörden einzurichtenden zentralen De-Mail-Gateway zu realisieren. Auch ohne diese Möglichkeit werden viele SV-Träger einen solchen Zugang über einen akkreditierten De-Mail-Diensteanbieter einrichten, um mit ihren Versicherten rechtssicher kommunizieren zu können.

Auch hierzu sind zur Absicherung des De-Mail-Transportes von der Erstellung der Nachricht bis zur Speicherung beim Empfänger technische Sicherungsmittel nach dem jeweiligen Stand der Technik zu verwenden und in entsprechenden Verfahrensbeschreibungen zu erläutern.

Näher Ausführungen hierzu sind der Ziff. 3.2.2.3 zu entnehmen.



## 5 Übertragung und Vernichtung des Papieroriginals

Das Übertragen von Papierdokumenten in die elektronische Form ist im neuen EGovG in § 7 geregelt. Dieser Paragraph gilt aufgrund der in § 1 Abs. 4 EGovG festgeschriebenen Vorrangregelung jedoch für SV-Träger nicht. Für diese ist das Scan-/Signaturverfahren sowie die revisionssichere Archivierung in den §§ 110a-d SGB IV geregelt.

### 5.1 Scannen von Papierdokumenten

Die Vorschriften der §§ 110a ff. SGB IV wurden durch das 3. Verwaltungsverfahrensänderungsgesetz - VwVfÄndG (BGBl I Nr. 60 S. 3322 ff. vom 21.08.2002) in das SGB IV eingefügt. Sie gelten für alle Belegarten, einschließlich der des Finanz- und Rechnungswesens.

Die Vorschriften regeln, wie mit Papierdokumenten zu verfahren ist, die vernichtet werden sollen. Diese sind durch ein maschinelles Scanverfahren in elektronische Dokumente zu übertragen. Hierbei sind folgende Besonderheiten zu beachten:

Die Wiedergabe auf einem Bildträger oder die Daten auf einem anderen dauerhaften Datenträger müssen mit der dieser zu Grunde gelegten schriftlichen Unterlage bildlich und inhaltlich vollständig übereinstimmen. Die Gesetzesbegründung führt dazu aus, dass die „Wiedergabe bei einem späteren Abruf einen vollständigen „urschrift“-getreuen Ausdruck oder eine sonstige entsprechende Reproduktion garantiert“. Daraus könnte nunmehr abgeleitet werden, dass ausschließlich eine Farbbildung mit qualifizierter elektronischer Signatur urkundliche Beweiskraft besitzt.

Die Prüfdienste des Bundes und der Länder sind der Auffassung, dass die Sozialversicherungsträger (SV-Träger) aus Gründen der Rechtssicherheit alle papiergebundenen Dokumente in Farbe einscannen sollten. Lediglich bei Vordrucken, bei denen Farbe keine Beweiskraft besitzt sondern nur als Ausfüllhilfe für die spätere Texterkennung dient (z. B. AU-Bescheinigungen, Verordnungen), ist ein Farbscan entbehrlich. Für die Prüfung von RSA-relevanten Belegen (z. B. Verordnungen) halten die Prüfdienste die Vorlage von Graustufen-Images mit allen Formatierungszeichen für ausreichend.

Die SV-Träger sollten sich an den Ergebnissen einer individuellen Risikobetrachtung orientieren, im Rahmen derer insbesondere die Gefahren des möglichen Verlustes der Beweiskraft von Graustufen-Wiedergaben mit den Folgen des größeren wirtschaftlichen Aufwandes bei der Digitalisierung in Farbe gegeneinander abzuwägen sind.

Obwohl es grundsätzlich keine eklatanten Preisunterschiede mehr zwischen Farb- und S/W-Scannern gibt - jeder Scanner beherrscht beide Verfahren - wäre jedoch erforderlich, dass der Scanner multistreamfähig ist. Das bedeutet, es werden beim Scanvorgang sowohl ein farbiges als auch ein S-/W-Image erzeugt. Während das farbiges elektronisch signiert und archiviert wird, benötigt man das S-/W-Image nur für das Auslesen und die Nachbearbeitung der Daten; dieses Image könnte nach dem Lesevorgang wieder automatisch gelöscht werden.

Zur Vermeidung einer erhöhten Netzwerkperformance wegen des Abrufs von Farbimages durch die Sachbearbeitung wäre auch eine weitere Nutzung des vorgenannten S-/W-Image möglich.

Es muss sichergestellt sein, dass die Belege urschriftgetreu gescannt werden. Dies erfordert auch, dass auf dem Original vorhandene Formatierungszeichen (z. B. Linien, Rahmen, Logos u.a.) auch auf dem signierten Image vorhanden sein müssen. Für das Auslesen der Rohdaten für die weitere maschinelle Verwendung (z. B. OCR-Lesung) kann auf diese Kriterien allerdings verzichtet werden.

Rückseiten sind beim Stapelsignaturverfahren grundsätzlich mitzuscannen. Ein automatisches Löschen leerer Rückseiten ist zulässig, sofern die Scansoftware gewährleistet, dass bereits bei einem auf der Rückseite befindlichen Zeichen (z. B. ein „Punkt“) ein automatisches Löschen ausgeschlossen ist.

Die Anbringung eines elektronischen Eingangsstempels bzw. einer automatischen Paginierung ist unmittelbar vor dem Scanvorgang zulässig. Nach dem Einscannvorgang (auf dem Image) automatisch angebrachte elektronische Eingangsstempel sind nicht zulässig, da das Image dann kein originalgetreues Abbild des Urbeleges mehr ist. Dabei ist sicherzustellen, dass der elektronische Eingangsstempel dem tatsächlichen Eingangsdatum des Papierdokumentes entspricht.

Es ist sicherzustellen, dass eingehende Schriftstücke, bei denen es sich offensichtlich um unbeglaubigte Kopien oder Papier-Faxe handelt, nicht automatisch gescannt und signiert werden. Vielmehr ist hier erforderlich, diese Schriftstücke vor dem Signiervorgang mit einem Stempelaufdruck „Kopie“ bzw. „FAX“ zu versehen.

Die Verwendung von Multi-TIFF-Dokumenten, bei denen ein aus mehreren Seiten bestehendes Dokument mit einer Elektronischen Signatur versehen wird, ist möglich. Vermieden werden sollte jedoch, mehrere unterschiedliche Dokumente mit einer einzigen Signatur zu versehen. Hierbei könnte das Problem auftreten, dass die einzelnen Dokumente unterschiedlich lange aufbewahrt werden müssen. Bei der Vernichtung eines dieser Dokumente müssten die anderen neu signiert werden.

## **5.2 Signaturverfahren**

§ 110 d Satz 1 SGB IV fordert bei strenger Auslegung die Prüfung und Signatur jedes einzelnen erfassten Beleges.

### Einzelplatzsignatur

Der Gesetzgeber ging bei der Abfassung des Signaturgesetzes (SigG) davon aus, dass eine elektronische Signatur als Ersatz einer sonst erforderlichen körperlichen Unterschrift an einem einzelnen Dokument angebracht wird. Die entsprechenden Regelungen im SGB sehen daher vor, dass derjenige, der die Signatur auf einem Dokument anbringt, sich vor der Erzeugung der Signatur davon überzeugt, dass die Daten des zu signierenden Dokumentes integer sind. Klassischer Einsatzbereich ist der Sachbearbeiter-Arbeitsplatz, an dem einzelne Dateien elektronisch signiert und versendet werden sollen.

Die Einzelplatzsignatur erfordert grundsätzlich, dass sich die hierzu benötigte Hardware (Kartenlesegerät) und Software (Signatursoftware) im direkten Zugriffsbereich des Anwenders befindet. Im Übrigen gelten hier dieselben Sicherheitsvorschriften, die auch bei sonstigen SB-Plätzen – gem. Dienstanweisung – zu beachten sind.

### Stapelsignatur

Beim Stapelsignaturverfahren werden große Mengen Beleggutes (z. B. AU-Meldungen) stapelweise eingescannt. Die erzeugten Images werden mit Hilfe einer Signaturanwendungskomponente an einen Scan-/Signaturarbeitsplatz übertragen, an dem der Signaturvorgang initiiert werden kann.

Der Vorteil dieses Verfahrens gegenüber dem der Einzelsignatur liegt im Zeitgewinn: Das Einscannen, Signieren und Speichern von Papierbelegen kann im Stapelbetrieb erfolgen.

Dies erfordert, den Übernahmeprozess effizient zu gestalten. Hier entsteht ein Problem, wenn deshalb der vollständige Übernahmeprozess bestehend aus:

- Scannen des Dokuments,
- Erstellen der Bilddatei und
- Signieren der Datei

automatisiert wird, so dass nicht davon ausgegangen werden kann, dass der Bediener jedes Dokument vor dem Signieren visuell auf Übereinstimmung prüft.

Aufgrund der in § 110 d Satz 1 SGB IV enthaltenen Vorgaben muss der Signiervorgang grundsätzlich zeitlich und räumlich in unmittelbarem Zusammenhang mit dem Einscannen erfolgen; die Signatur darf hierbei nur von dem angebracht werden, der das Dokument auch in die elektronische Form überführt hat („Stapelsignatur“).

Alternativ dazu sieht die o.g. Vorschrift die Möglichkeit vor, die Images unmittelbar nach deren Herstellung durch einen anderen als den Scan-Operator signieren zu lassen. Dieser hat aber vor dem Signiervorgang die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe zu prüfen. Das bedeutet, jedes Image ist visuell zu prüfen. Eine Stapelsignatur ist bei dieser Alternative nur zulässig, wenn im Signiertool der zu prüfende Stichprobenumfang auf 100 v.H. heraufgesetzt wird.

Die Stapelsignatur wird erstmals in § 41 Abs. 5 SRVwV als „Massensignatur“ beschrieben und an verschiedene Voraussetzungen gebunden. Das Bundesministerium für Arbeit und Sozialordnung hat mit Schreiben vom 31.05.2002 (Az.: Ib4 – 18001 – 2) in einem Einzelfall dem Einsatz von automatisch erzeugten Signaturen („Stapelsignaturen“) zugestimmt, wenn die in der Begründung<sup>6</sup> zu § 15 Abs. 2 SigV genannten Voraussetzungen vorliegen.

Da beim Stapelsignaturverfahren nicht mehr jeder einzelne eingescannte Beleg vor seiner Signatur einer visuellen Kontrolle unterzogen wird, muss durch bestimmte technische und organisatorische Vorkehrungen ein mögliches Schadensrisiko minimiert werden.

Abgeleitet aus der Begründung zu § 15 Abs. 2 SigV sowie den Vorgaben der Regulierungsbehörde für Telekommunikation und Post – BNetzA - über „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“ (Version 1.4 vom 19.07.2005) haben die Prüfdienste des Bundes und der Länder zusammen mit dem BSI hier die folgenden Rahmenbedingungen definiert:

---

<sup>6</sup> Begründung zum Entwurf einer Verordnung zur elektronischen Signatur in der Fassung des Kabinettschlusses vom 24. 10. 2001:

Die Vorschrift enthält die erforderlichen Spezifikationen für Signaturanwendungskomponenten nach § 17 Abs. 2 SigG. Dabei wird differenziert nach Erzeugung und Prüfung einer Signatur.

Damit die Erzeugung einer Signatur nur durch die berechtigte Person erfolgen kann, dürfen bei der Aktivierung der Signaturerstellungseinheit die Identifikationsdaten (z. B. die PIN) beim Vergleich mit den auf der Signaturerstellungseinheit gespeicherten Referenzdaten nicht auslesbar oder speicherbar sein (Nummer 1 Buchst. a)). Ihre Geheimhaltung ist zu jedem Zeitpunkt zu gewährleisten. Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, Signaturen sollen für ein festes Zeitfenster oder eine bestimmte Anzahl ohne jeweilige Identifizierung erzeugt werden. In diesem Falle ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können (Nummer 1 Buchst. b)). Die Erzeugung einer Signatur muss durch einen Warnhinweis vorher angezeigt werden (Nummer 1 Buchst. c)). Insbesondere bei der automatischen Erzeugung von Signaturen ("Massensignaturen") muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.

Bei der Prüfung einer Signatur muss der technische Vorgang der Prüfung zuverlässig erfolgen und das Ergebnis muss korrekt angezeigt werden (Nummer 2 Buchst. a)); es darf nicht vorkommen, dass nicht korrekte Ergebnisse vorgetäuscht werden können. Dies gilt entsprechend für die Nachprüfung von Zertifikaten (Nummer 2 Buchst. b)). Die Regelung zu Nummer 2 Buchst. b) ist technologieneutral.

## Technische Vorkehrungen

Der Einsatz von Stapelsignaturverfahren hat ausschließlich in einer abgesicherten Umgebung zu erfolgen. Die auf der Homepage der BNetzA veröffentlichten Bestätigungen zum Einsatz von Signaturanwendungskomponenten verlangen, dass der Scan-/Signatur-Bereich sich in einem geschützten Einsatzbereich befindet. Dieser darf von außen nur mit Schlüssel/Karten von Berechtigten zu öffnen sein. In diesem Bereich sind unterzubringen:

- Scanner (für die Belegung)
- Scan-/Signatur-Arbeitsplätze

Einzelheiten sind der Homepage der BNetzA zu entnehmen.

Die Signaturanwendungskomponente ist derart zu konfigurieren, dass die Signaturerstellungseinheit lediglich für die Signatur eines Stapels freigeschaltet wird; die Stapelgröße sollte 250 (bei Hash-Bäumen = 256) Dokumente (es werden einzelne Dokumente und nicht Seiten signiert) nicht überschreiten.

Um mangelhafte Scanvorgänge (z.B. fehlende Seiten, mangelnde Lesbarkeit) zu erkennen, muss eine geeignete Qualitätskontrolle und bei Bedarf eine erneute Erfassung des gesamten Stapels stattfinden. Die detaillierte Ausgestaltung dieser Kontrolle soll sich am Schutzbedarf der verarbeiteten Dokumente, am Scan-Durchsatz sowie an der Zuverlässigkeit des Scansystems orientieren.

Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf von „normal“ und bei hohem Durchsatz kann die Sichtkontrolle auf Stichproben reduziert werden, um systematische Fehler zu erkennen. Sie sollte aber mindestens das erste und das letzte Blatt des Stapels umfassen.

Hierzu muss die Signaturanwendungskomponente technische Vorkehrungen bereitstellen, wonach der Scan-Operator gezwungen wird, einen festgelegten Stichprobenumfang einer visuellen Kontrolle zu unterziehen. Erst nach Durchführung der Sichtkontrolle der im System hinterlegten Mindeststichprobe kann der Stapel signiert werden.

Für die Signatur des nächsten Stapels muss der Scan-Operator seine Signatur-PIN erneut eingeben. Eine Freischaltung der Signaturkarte für ein festgelegtes Zeitfenster ist nicht zulässig.

Um die Übersichtlichkeit für den Scan-Operator nicht zu erschweren, sollte technisch sichergestellt sein, dass maximal ein Rückstand von drei eingescannten, ungeprüften und unsignierten Stapeln vorhanden ist!

Um die Auslastung einer Scanner-Straße zu erhöhen, können abwechselnd mehrere Scan-Operatoren scannen und signieren. Hierbei ist sicher zu stellen, dass jeder Scan-Operator über eine eigene Signaturerstellungskomponente verfügt und nur die von ihm eingescannten Dokumente signiert.

Vor der endgültigen Langzeitspeicherung der signierten Images im Langzeitarchiv ist jede Signatur noch einmal (automatisch) auf Gültigkeit zu überprüfen. Dies kann durch eine Online-Abfrage beim Zertifizierungsdienstleister oder gegen die auf dem Signaturserver gespeicherten (im Hause eingesetzten) Zertifikate sowie die aktualisierten Sperllisten erfolgen. Das Ergebnis der Überprüfung ist mit zu speichern. Sollten hierbei fehlerhafte Signaturen festgestellt werden, müssen alle nach dem Zeitpunkt der fehlerhaften Signatur eingescannten Dokumente erneut gescannt und signiert werden!

Es sei besonders darauf hingewiesen, dass der Einsatz einer automatischen Signatur voraussetzt, dass die technischen Komponenten so gewählt sind, dass der Ablauf nicht unterbrochen werden kann (Transaktionssicherheit).

Rückseiten sind beim Stapelsignaturverfahren mitzuscannen. Ein automatisches Löschen leerer Rückseiten ist grundsätzlich zulässig. Die Einstellungen der Scansoftware hat so zu erfolgen, dass schon ein auf der Rückseite befindliches Zeichen ein automatisches Löschen ausschließt.

Die Anbringung eines elektronischen Eingangsstempels durch die Scansoftware ist zulässig. Nach dem Einscansvorgang automatisch angebrachte elektronische Eingangsstempel sind nicht zulässig, da das Image dann kein originalgetreues Abbild des Urbeleges mehr ist. Dabei ist sicherzustellen, dass der elektronische Eingangsstempel dem tatsächlichen Eingang des Papierdokumentes entspricht.

Das Einscannen und Signieren geringer Papiermengen kann unter der Voraussetzung, dass eine Einzelsignatur an jedem Dokument angebracht wird, auch an den normalen Arbeitsplätzen erfolgen.

### Organisatorische Vorkehrungen

Der gesamte Verfahrensablauf vom Eingang der Papierbelege im Scan-/Signaturbereich bis zur Übertragung der Images in das elektronische Archiv sowie der Verbleib bzw. die Vernichtung der Papierbelege ist in einer Dienstanweisung (DA) detailliert zu beschreiben. Diese DA ist den Scan-Operatoren zur Kenntnis zu geben.

Eine Vernichtung der Papierdokumente kann nur dann vorgenommen werden, wenn die im SGB I und IV sowie der SVRV und SRVwV aufgeführten Voraussetzungen in allen Punkten erfüllt sind.

Es wird empfohlen, die Vernichtung erst nach der Nachbearbeitung, z. B. Plausibilitäts- und Mitgliedschaftsprüfung, durchzuführen und wenn sichergestellt ist, dass das Dokument im Archiv vorliegt/angekommen ist.

Es muss sichergestellt sein, dass unsignierte elektronische Dokumente bei fehlenden Originalunterlagen nicht nachträglich ausgedruckt und erneut dem System (jetzt mit Signatur) zugeführt werden können.

Beim nachträglichen Scannen von Altbeständen muss das Image den bereits im System gespeicherten Informationen zugeordnet werden.

## **5.3 Sicherheitsmaßnahmen**

Bei Verfahren zur Übertragung von Papierunterlagen in die elektronische Form (Scan-/Signaturverfahren) sind insbesondere folgende Sicherheitsmaßnahmen erforderlich:

### Bauliche Maßnahmen

Bei der Gestaltung der baulichen Maßnahmen ist zu unterscheiden zwischen

- Einzelplatzsignatur und
- Stapelsignatur.

Darüber hinaus gelten die allgemeinen – auch durch das BSI beschriebenen – Standards für die Herstellung der erforderlichen IT-Sicherheit für die Server und das Leitungsnetz.

Das Scannen von Belegstapeln ist räumlich und DV-technisch getrennt vom übrigen Geschäftsbetrieb zu trennen. Die Räumlichkeiten sind gegenüber Unbefugten durch geeignete

Sicherheitsmaßnahmen abzuschotten. Zutritt haben ausschließlich die in diesem Bereich tätigen Mitarbeiter/innen.

#### Betriebssystem und Netzwerk

Hinsichtlich der Konfiguration und des Betriebes von Scan-/Signaturlösungen haben die Prüfdienste des Bundes und der Länder in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Rahmenbedingungen definiert, die insbesondere beim Einsatz der „Stapelsignatur“ zu beachten sind:

Grundsätzlich gelten hier die gleichen Sicherheitsstandards, die auch im täglichen „Normalgeschäft“ zu beachten sind.

Die im Stapelsignaturgeschäft erforderlichen Sicherheitsmaßnahmen erfordern, dass das Teilnetz, in dem die Scan-/Signatur-Operatoren tätig sind, vom übrigen Hausnetz zu trennen ist. Eine „Pseudotrennung“ durch Verwendung mehrerer Netzwerkkarten im Scanclient bietet aus Sicht des BSI keine hinreichende Sicherheit.

Es sind nur solche Verbindungen zulässig, die von innen nach außen aufgebaut werden können. Dies ist durch eine entsprechende Hardware-Firewall sicherzustellen. Eine Anbindung dieser Arbeitsplätze an das Internet sowie den zentralen Mail-Server ist unzulässig!

Die Verwendung einer Software-Firewall auf dem jeweiligen Rechner wird für nicht ausreichend angesehen, weil Schadsoftware dazu führen kann, dass die Maßnahme wirkungslos ist.

#### **Maßgeblich für den Betrieb der Karten sind die durch die BNetzA festgelegten Anforderungen an die Einsatzumgebung!**

Es sind grundsätzlich Kartenleser der Klasse 2 oder 3 zu verwenden.

Es sollte auf den WINS-Dienst verzichtet werden. Eine Auflösung der Rechnernamen auf IP-Adressen bzgl. Server und Mailserver sollte durch LMHOST-Eintrag sichergestellt werden.

Bei Windows-Terminal-Servern: Da das Signaturprogramm auf dem (entfernten) Server liegt, ist die PIN-Abfrage vom Terminal-PC mit einer Verschlüsselung bzw. durch den Einsatz von zugelassenen Verschlüsselungssystemen (→ [www.bsi.bund.de](http://www.bsi.bund.de)) zu schützen. Maßgeblich ist, ob die Evaluierung und Bestätigung für die eingesetzte Karte den Einsatz über Terminalserver zulassen.

Zugriff auf die Systemzeit hat ausschließlich der Administrator. Wenn dies gewährleistet wird, kann auf den Einsatz eines (kostenpflichtigen) Zeitstempeldienstes verzichtet werden.

Auf dem Rechner dürfen keine E-Mail Programme (kein Internetanschluss) und keine Grafikbearbeitungsprogramme installiert sein.

#### Nicht wiederbeschreibbare Datenträger

Die gesetzlichen Regelungen schreiben vor, dass eine elektronische Langzeitspeicherung auf Medien zu erfolgen hat, die nicht wieder beschreibbar sind.

§ 110d SGB IV spricht von dauerhaft maschinell verwertbaren Datenträgern und schränkt somit die Medienwahl nur hinsichtlich der Lebensdauer ein. Die Daten müssen während der Aufbewahrungsfristen verfügbar und jederzeit innerhalb einer angemessenen Frist wieder

herstellbar sein. Somit spricht grundsätzlich auch nichts gegen die Verwendung von Tapes oder Harddisks.

Voraussetzung für die Langzeitspeicherung auf diesen Medien ist jedoch die Gewährleistung einer Versionsintegrität (WORM-Prinzip). Ein auf Harddisks langzeitarchiviertes, qualifiziert signiertes Image darf bei Aufruf durch den User nicht verändert werden (können); in diesem Fall ist automatisch eine Kopie des Images zu erzeugen, die dann unter einer neuen Versionsnummer abgespeichert wird. Hierdurch wird die Revisionsicherheit der signierten Dokumente gewährleistet. Die Möglichkeit des physikalischen Löschens nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist muss vom SV-Träger in der Dienstanzweisung detailliert festgelegt werden (u.a. Zeitpunkte und Zuständigkeiten).

#### Fernwartung

Aufgrund der besonderen Sicherheitsanforderungen für die technische Anbindung der im Scan-Signaturbereich eingesetzten Hard- und Software erscheint eine Fernwartung der Geräte als problematisch.

Für eine Fernwartung sind die durch das BSI in den „IT-Grundschutz-Katalogen“ festgelegten Standards wie Call-Back-Verfahren und der Einsatz von Einmal-Passwörtern zu beachten. Grundlage für die zu wählenden Maßnahmen ist der jeweilige Schutzbedarf (normal, hoch, sehr hoch) der zu scannenden Dokumente.

Darüber hinaus ist organisatorisch sicherzustellen, dass eine Fernwartung ausschließlich in Zeiten erfolgt, in denen kein Scan-Signatur-Betrieb stattfindet.

#### **5.4 Technische Richtlinie TR03138 („TR-RESISCAN“)**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 17.04.2013 die Technische Richtlinie TR 03138 „Ersetzendes Scannen“ (TR-RESISCAN) [Version 1.0 vom 20.03.2013] veröffentlicht. Sie beschreibt die technischen und organisatorischen Anforderungen für Scanprozesse und –produkte, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Ziel der TR ist es, den Anwendern in Wirtschaft und Verwaltung einen Handlungsleitfaden und eine Entscheidungshilfe zum ersetzenden Scannen zu geben. Im Hinblick auf die Informationssicherheit werden die bei einem Scanprozess bedeutsamen Bedrohungen in einer Strukturanalyse für alle Datenobjekte und Kommunikationsbeziehungen systematisch dargestellt. Auf Grundlage einer darauf aufbauenden Schutzbedarfsanalyse und anhand der entlang der verschiedenen Scanphasen durchgeführten Risikoanalyse werden konkrete Sicherheitsmaßnahmen beschrieben.

Die TR enthält einen modularen Anforderungskatalog, der unterschiedliche Sicherheitsstufen umfasst. Während es in der „Basisstufe“ vor allem um einen grundsätzlich ordnungsgemäßen und mit grundlegenden Sicherheitsmaßnahmen ausgestalteten Scanprozess geht, werden in den „Ausbaustufen“ besondere Anforderungen an Integrität, Verfügbarkeit und Vertraulichkeit mit entsprechend erhöhten Sicherheitsmaßnahmen beschrieben.

Ergänzend zu diesem Leitfaden wird empfohlen, die in der TR enthaltenen **Muss- und Soll-Anforderungen** hinsichtlich eines rechtssicheren Scan- und Signierprozesses bei der Digitalisierung von Papierdokumenten zu beachten und umzusetzen.

Die Prüfdienste des Bundes und der Länder werden die sich aus diesem Leitfaden sowie der TR-RESISCAN ergebenden Anforderungen bei Prüfungen als Prüf- und Bewertungsgrundlage heranziehen.

## 5.5 Vernichtung von Originalbelegen

Für die Vernichtung von Akten gelten folgende Rechtsgrundlagen:

- § 110b SGB IV
- § 78a SGB X
- § 80 SGB X

Die Vernichtung der Originalpapierbelege ist in einer Dienstanweisung zu regeln. Frühest möglicher Zeitpunkt für die Vernichtung ist die vollständige elektronische Aufbewahrung und Sicherung der Images und zugehörigen Signaturen. Die Ordnungsmäßigkeit ist von der internen Revision in regelmäßigen Abständen zu prüfen.

In Fällen der „frühen Signatur“ (z. B. beim Posteingang) wird empfohlen, die papiergebundenen Dokumentationen solange aufzubewahren bis die Sachbearbeitung die Zuständigkeit geklärt hat.

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben eine datenschutzgerechte Verarbeitung der Daten sicherzustellen. Die letzte Phase der Datenverarbeitung ist das Löschen gespeicherter Daten bzw. das Vernichten von Datenträgern. Datenträger können z. B. Festplatten, Magnetbänder, Filmmaterial, Disketten, CDs, DVDs, USB-Sticks, Chipkarten oder Papier sein.

Die datenschutzgerechte Vernichtung ist in der DIN 66399 „Büro- und Datentechnik - Vernichtung von Datenträgern“ geregelt. Die neue dreiteilige Norm hat die seit 1995 geltende DIN 32757-1 abgelöst und wird nun auch digitalen Dokumenten bzw. Datenträgern und den damit verbundenen neuen Sicherheitserfordernissen gerecht. Ebenfalls gilt die Europäische Norm EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“. Sie enthält im Vergleich zur älteren DIN 32757-1 zwar Vorgaben für weitere Datenträger neben dem Papier, aufgrund ihrer teilweise wenig verbindlichen Formulierungen kann sie nur eingeschränkt als Maßstab heran gezogen werden.

Die Teile eins und zwei der DIN 66399 (gültig ab Oktober 2012) enthalten die Grundlagen und Begriffe sowie die Anforderungen an Maschinen; Teil drei DIN SPEC 66399-3 (gültig ab Februar 2013) gibt die Spezifizierung der während der Vernichtung zu beachtenden Prozessschritte vor, um so die Absicherung des Gesamtprozesses der Datenträgervernichtung zu gewährleisten.

Neu sind die drei Schutzklassen, die jetzt zusammen mit den Sicherheitsstufen der Klassifizierung der anfallenden Daten dienen. Bei der Ermittlung des Schutzbedarfs für die Vernichtung der Datenträger ist der Grad der Schutzbedürftigkeit dabei ausschlaggebend für die Sicherheitsstufe. Es werden insgesamt sechs unterschiedliche Materialklassifizierungen verwendet. Sie berücksichtigen auch die Größe der Informationsdarstellung auf den Datenträgern. Weiterhin werden in der DIN 66399 statt bisher fünf Sicherheitsstufen jetzt sieben definiert.

Sozialdaten sind nach derzeitiger Auffassung der Prüfdienste nach Schutzklasse 3 (sehr hoher Schutzbedarf) zu vernichten. Zusätzlich können in den jeweiligen Einsatzgebieten landes- bzw. bereichsspezifische Spezialvorschriften gelten.

Zur Vernichtung von Datenträgern kann eine andere Stelle beauftragt werden. Dabei handelt es sich um einen anzeigepflichtigen Auftrag gemäß § 80 SGB X. Hierbei ist zu gewährleisten, dass Sozialdaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisun-



gen der Auftraggeber verarbeitet werden können (Auftragskontrolle). Der Auftrag zur Löschung personenbezogener Daten, die Weisungen zu technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind daher schriftlich festzuhalten.

## 6 Langzeitspeicherung elektronisch erzeugter Dokumente und Daten

### 6.1 Allgemeine Anforderungen

Grundsätzlich sind alle elektronisch vom SV-Träger erzeugten bzw. von Versicherten oder Dritten übersandten elektronische Dokumente, die für den jeweiligen Bearbeitungsvorgang bzw. das „Versicherungsleben“ des Versicherten rechtserheblichen Charakter („Beweischarakter“) haben, in einem elektronischen Langzeitarchiv aufzubewahren.

Hierzu gehören

#### *Eingehende Dokumente:*

- Elektronisch erzeugte Dokumente (z.B. im doc- oder pdf-Format), die elektronisch an den SV-Träger gesandt wurden (z.B. auf Datenträger, E-Mail-Anhang, ftp)
- Eingegangene elektronische Faxe (z.B. auf Fax-Server)
- Eingegangene E-Mails, De-Mails und deren Anhänge
- Im Web-Formular auf der Internetseite des SV-Trägers erzeugte Daten im Text- oder pdf-Format

#### *Ausgehende / erzeugte Dokumente:*

- „Durchschriften“ der vom SV-Träger oder seinen Mitarbeitern erzeugten elektronischen Dokumente, die elektronisch (und/oder in Papierform) an einen Externen versandt wurden (auch elektronische Faxe)
- Vom SV-Träger oder seinen Mitarbeitern an Externe (z.B. Versicherte, Arbeitgeber, Leistungserbringer) versandte E-Mails, De-Mails und deren Anhänge
- Interne Vermerke, Verfügungen, Notizen, Protokolle

Die Anforderungen an die rechtssichere Langzeitspeicherung für diese Dokumente sind definiert durch die §§ 110a – d SGB IV i.V.m. den Grundsätzen ordnungsgemäßer Aufbewahrung<sup>7</sup>.

Darüber hinaus gibt es technische und/oder organisatorische Vorgaben zu IT-Sicherheit / Datenschutz wie z.B. § 78a SGB X einschl. der Anlage („8 Gebote“), die ebenfalls normativen Charakter haben.

Weiterhin sind die vom VOI (Verband Organisations- und Informationssysteme e. V.) aufgestellten Merksätze zur revisionssicheren elektronischen Archivierung zu beachten:

- Jedes Dokument muss unveränderbar aufbewahrt werden.
- Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen .
- Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.
- Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.
- Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
- Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
- Jedes Dokument muss zeitnah wiedergefunden werden können.
- Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.

<sup>7</sup> „Vereinbarung der Spitzenverbände der Krankenkasse zu den Grundsätzen ordnungsgemäßer Aufbewahrung im Sinne des § 110a SGB IV, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen“ (Stand: 23.06.2008) und „Ergänzende Vereinbarung der Spitzenverbände der Krankenkassen zur Rückgabe und Vernichtung von Unterlagen“ (Stand: 23.06.2008).

- Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

## 6.2 Rechtssichere Langzeitspeicherung von elektronischen Posteingängen

Grundsätzlich müssen elektronisch bei der Kasse eingehende Nachrichten/Dokumente, die eine rechtliche Wirkung entfalten, im elektronischen Langzeitarchiv gespeichert werden. Dies entspricht dem Grundsatz der „Aktenmäßigkeit“ der Verwaltung.

Bei einer „normalen“ **E-Mail** (ohne QES) ist die Authentizität des Absenders nicht nachprüfbar. Somit kann aus dieser keine rechtliche Wirkung gezogen werden. Enthält eine solche Mail einen Anhang, der die QES des Absenders beinhaltet, sind Mail und Anhang zu speichern.

Elektronische Dokumente, die der **Absender nicht qualifiziert signiert** hat, sind vor der Langzeitspeicherung mit der QES eines (System-)Mitarbeiters zu versehen, der für die „Betreuung“ des E-Mail-/Fax-Servers verantwortlich ist. Die Signatur kann im Wege der Massensignatur erfolgen. Alternativ ist auch eine Einzelsignatur durch den Empfänger (Sachbearbeiter) möglich.

Voraussetzung hierfür ist, dass der SV-Träger/Dienstleister detailliert die nachfolgend genannten technischen und organisatorischen Maßnahmen festlegt und umsetzt:

- Ausführliche Verfahrensbeschreibung (einschl. Festlegung des Datenformates, z. B. automatische Umwandlung des Text- in ein PDF/A-Format).
- Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv.
- Bei Einsatz einer Einzelsignatur (durch den SB) vor der Archivierung ist ein Verfahren zu entwickeln, das eine Manipulationsmöglichkeit des Dokumentes verhindert.
- Festlegung, was mit Dokumenten zu geschehen hat, die nicht in das Langzeitarchiv gehören (z. B. unzuständiger Empfänger, SPAM, Dokumente mit extremen oder sexistischen Inhalten).

Es wird ausdrücklich darauf hingewiesen, dass die an diesen Dokumenten angebrachte QES eines Mitarbeiters zu **keiner Beweiswerterleichterung** i. S. des § 110d SGB IV führt. Sie dient ausschließlich der Integritätssicherung des eingegangenen elektronischen Dokumentes.

**De-Mails** sind grundsätzlich wie „normale“ E-Mails zu behandeln. Erhält der SV-Träger eine De-Mail mit der Versandoption „absenderbestätigt“ (§ 5 Abs. 5 DeMailG), ist die in ihr enthaltene Nachricht und die ggf. angehängten Dokumente mit der QES des De-Mail-Diensteanbieters des Absenders versehen. Die De-Mail-Nachricht (einschließlich der Anhänge, Metadaten und Signatur) muss im elektronischen Langzeitarchiv gespeichert werden. **Das Anbringen einer neuen „Eingangssignatur“ durch den SV-Träger ist nicht mehr erforderlich.**

Es wird ausdrücklich darauf hingewiesen, dass die durch den Provider angebrachte QES zu **keiner Beweiswerterleichterung** i. S. des § 110d SGB IV führt. Sie dient ausschließlich der Integritätssicherung des eingegangenen elektronischen Dokumentes.

### 6.3 Rechtssichere Langzeitspeicherung von elektronischen Postausgängen

Von der in Ziff. 3.5.1 beschriebenen Rechtslage hinsichtlich des VA-Erlasses ist allerdings die Frage der **Langzeitspeicherung der Verwaltungsunterlagen** (zu denen auch der VA selbst gehört) zu unterscheiden. Insoweit verfolgt das Gesetz andere Zielsetzungen als beim VA-Erlass. Es geht nicht um die rechtssichere Bekanntgabe gegenüber dem Adressaten sondern um die zuverlässige Langzeitspeicherung von Unterlagen. Hierzu setzt § 110d Nr. 1 u. 2 SGB IV i. V. m. § 110a Abs. 2 SGB IV für die (erleichterte) Beweiswirkung der archivierten Unterlagen die qualifizierte elektronische Signatur (QES) dessen voraus, der

- die Wiedergabe auf dem dauerhaften Datenträger hergestellt oder die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe unmittelbar nach der Herstellung der Wiedergabe geprüft hat, oder
- bei urschriftlicher Aufzeichnung des Textes nur in gespeicherter Form diese mit einer QES nach dem SigG versehen hat.

Dies gilt nach dem ausdrücklichen Willen des Gesetzgebers für alle Unterlagen, also auch die elektronischen Verwaltungsakte, obwohl deren Bekanntgabe – wie oben dargelegt – unter geringeren Anforderungen erfolgen konnte.

Eine Aufbewahrung und Langzeitspeicherung in elektronischer Form ohne qualifizierte elektronische Signatur (QES) ist aufsichtsrechtlich bedenklich, da diesen Dokumenten im Rechtsverkehr keine Beweiskraft i.S.d. § 110d SGB IV zukommt und zumindest die Möglichkeit besteht, dass ihr Inhalt ggf. gerichtlich dargelegt oder sogar bewiesen werden muss.

Der Einsatz der **Massensignatur** ist wegen der in § 110d SGB IV formulierten Anforderungen an die Beweiswirkung elektronisch gespeicherter Dokumente aufsichtsrechtlich nicht vertretbar. Die automatische Anbringung einer QES im Wege der Stapel-/Massensignatur ist daher derzeit nicht möglich.

Es wird empfohlen, elektronische Dokumente immer dann mit einer QES des Erstellers zu speichern, wenn es sich um Dokumente mit „Beweiswertcharakter“ (z. B. Verwaltungsakte) handelt und zu erwarten ist, dass deren Inhalt zu einem späteren Zeitpunkt gerichtsfest dargelegt/bewiesen werden muss. Eine Differenzierung kann hierbei nicht nach einzelnen Dokumenttypen (z.B. E-Mail, Fax) sondern nur inhaltlich erfolgen.

### 6.4 Technische Richtlinie TR03125 („TR-ESOR“)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit der Technischen Richtlinie TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) [Version 1.1 vom 18.02.2011] ein Dokument zur Verfügung gestellt, das Orientierung und Hilfestellung gibt, um den vielfältigen Anforderungen hinsichtlich

- Verfügbarkeit und Lesbarkeit
- Integrität und Authentizität
- Datensicherheit und Datenschutz

von elektronischen Daten aller Art über lange Aufbewahrungszeiträume hinweg zu genügen.

Gegenstand und Ziel der TR ist die Beweiswerterhaltung von kryptographisch signierten Dokumenten. Konkret enthält sie einen Katalog von verpflichtenden Muss-, von empfohlenen Soll- und von optionalen Kann-Anforderungen im Hinblick auf alle Elemente und Bereiche, in denen Gestaltungsbedarf hinsichtlich einer vertrauenswürdigen Langzeitspeicherung besteht. Die TR ist auf der Internetseite des BSI veröffentlicht.

Die Archivlösung der SV-Träger kann gegen die in der TR-ESOR aufgeführten Anforderungen geprüft und deren Konformität festgestellt werden. Dies erfolgt über vom BSI zertifizierte Bestätigungsstellen.

Bei dieser Prüfung werden alle **Muss-Anforderungen** auf ihre uneingeschränkte Umsetzung hin überprüft. Eine Abweichung von den Muss-Anforderungen ist nicht zulässig. Die Nichteinhaltung von **Soll-Anforderungen** muss durch den Antragsteller schlüssig und nachvollziehbar, schriftlich begründet werden.

Die Prüfdienste des Bundes und der Länder haben einige Inhalte der TR-ESOR im Anhang 1 zum Leitfaden dargestellt. Die Texte in der Spalte „Anforderungen“ sind aus dem Hauptdokument der TR-ESOR übernommen worden. Es sind nur die Anforderungen aufgeführt, die aufgrund entsprechender rechtlicher Vorgaben für SV-Träger (z. B. § 78a SGB X) von denen der TR-ESOR abweichen. Die sonstigen Grundanforderungen sind der TR-ESOR selbst zu entnehmen.

Es wird empfohlen, die im TR-ESOR-Hauptdokument und seiner Anlage B (Profilierung für Bundesbehörden) enthaltenen **Muss- und Soll-Anforderungen** hinsichtlich einer revisions-sicheren Langzeitspeicherung elektronischer Dokumente zu beachten und umzusetzen. Die Empfehlung gilt auch für die Langzeitspeicherung nicht signierter Dokumente/Daten.

Die Prüfdienste des Bundes und der Länder werden die in der Anlage aufgeführten Muss- und Soll-Anforderungen bei Prüfungen der revisionssicheren Langzeitspeicherung als Prüf- und Bewertungsgrundlage heranziehen.

## 6.5 Besonderheiten

### 6.5.1 Aufbewahrung von Fehler-/Bearbeitungslisten

Fehler-/Bearbeitungslisten möchten viele SV-Träger nicht mehr in Papierform ablegen, sondern in elektronischer Form speichern. Sofern diese Listen im Aufbewahrungskatalog der Vereinbarung der Spitzenverbände zu den Grundsätzen ordnungsgemäßer Aufbewahrung aufgeführt sind, müssen sie aufbewahrt werden. Ansonsten ist eine Aufbewahrung in das Ermessen des SV-Trägers gestellt; sie muss entscheiden, ob der Inhalt der Listen einen „rechtserheblichen Charakter“ besitzt.

In der Papierform sind die Listen einzuscannen und mit eine QES des Scan-Operators zu versehen. In der elektronischen Form muss die (Druck-)Datei ebenfalls mit der QES des Bearbeiters versehen und im Langzeitarchiv gespeichert werden.

Eine elektronische Langzeitspeicherung ohne QES des Bearbeiters in einer gesonderten Datenbank (z. B. die eines zur Bearbeitung verwendeten Tools) entspricht nicht den Vorgaben aus § 110d SGB IV.

### 6.5.2 Aufbewahrungsfrist von Einzeldokumenten in eAkten/Vorgängen

Für die in einer elektronischen Akte (eAkte) aufzubewahrenden Einzeldokumente können gem. Aufbewahrungskatalog unterschiedliche Aufbewahrungsfristen gelten. In diesem Fall richtet sich der Endzeitpunkt der Aufbewahrungspflicht der Fallakte nach dem in ihr enthaltenen Einzeldokument mit der längsten Aufbewahrungsdauer. Diese „Verlängerung“ der Aufbewahrung verstößt nicht gegen das Löschgebot aus § 84 Abs. 2 Satz 2 SGB X, da die Fallakte einen Gesamtzusammenhang schafft, in dem eine Aufbewahrung zur allgemeinen Aufgabenerfüllung des SV-Trägers erforderlich sein kann.

## **7 Elektronischer Datenaustausch**

Der Austausch von Daten zwischen SV-Trägern und deren Partnern erfolgt in zunehmendem Umfang auf elektronischem Wege.

Die Richtlinien der Spitzenverbände der Krankenkassen zum Datenaustausch sind grundsätzlich geeignet, einen sicheren Datentransfer zu gewährleisten. Danach ist die Identität des Absenders und die Authentizität der Daten sichergestellt.

Die in den Datensätzen enthaltenen Informationen werden häufig in verschiedene Datenbanken übernommen. Der Originaldatensatz als adäquates Gegenstück zum papiergebundenen Dokument (z. B. Originalrechnung) wird in der Regel nicht gespeichert bzw. nicht dauerhaft und unveränderbar gespeichert. Insbesondere erfordern es die RSA-Prüfungen, dass die Krankenkassen den Informationsstand zum Zeitpunkt der Abgabe der amtlichen Meldungen nachweisen können.

Bei einem papiergebundenen Dokument kann der Inhalt und der Zeitpunkt des Eingangs zweifelsfrei ermittelt werden. Bei einem Datensatz ist dies in der Regel nicht sichergestellt. Theoretisch könnte er noch unmittelbar vor der Einsichtnahme angepasst worden sein. Damit geht die Beweiskraft der Information verloren.

Um den Nachweis der Datenintegrität erbringen zu können, sind die im § 110a Abs. 1 SGB IV gestellten Anforderungen zu beachten. Danach sind Unterlagen, die für ihre öffentlich-rechtliche Verwaltungstätigkeit, insbesondere für die Durchführung eines Verfahrens oder für die Feststellung einer Leistung, erforderlich sind, nach den Grundsätzen ordnungsmäßiger Aufbewahrung sicher zu speichern. Zu den „Unterlagen“ in diesem Sinne gehören auch Daten, die nur mit Hilfe einer Datenverarbeitungsanlage erstellt worden sind.

Daraus folgt, dass die Krankenkassen bei der Annahme elektronischer Datensätze den Originaldatensatz im Sinne der Aufbewahrungspflichten nach § 110a SGB IV dauerhaft und unveränderbar zu speichern haben. Hierzu sind geeignete Archivsysteme zu nutzen, die eine Versionsintegrität gewährleisten (siehe hierzu Ausführungen zu nicht wieder beschreibbaren Datenträger unter Ziffer 5.3). Der SV-Träger muss im Zweifelsfall den Nachweis erbringen, dass die Ursprungsdatensätze im Original vorliegen und nicht verändert wurden.

Die Daten müssen für Revisionszwecke zeitnah zur Verfügung stehen.

Die Auftragsdaten (Vorlaufdatensatz) und die Nutzdaten sind nach Eingang beim SV-Träger (oder beauftragten Dritten) direkt nach der Entschlüsselung elektronisch zu speichern. Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (z. B. EDIFACT, XML) in eine lesbare Form umzuwandeln.

Werden die Daten nach der Speicherung des Original-Datensatzes in den operativen DV-Systemen verarbeitet, sind die vorgenommenen Datenänderungen in den Fachverfahren im Sinne einer Historienführung nachvollziehbar zu protokollieren.

### **7.1 Ergänzende rechtliche Grundlagen**

§ 78 SGB IV bildet die Rechtsgrundlage, Grundsätze u. a. für die Zahlung, die Buchführung und die Rechnungslegung festzulegen. Die Regelung ist nach den Grundsätzen des für den Bund und die Länder geltenden Haushaltsrechts vorzunehmen. Diese hat die Besonderheiten der Sozialversicherungsträger und der einzelnen Versicherungszweige zu berücksichtigen.

Aufgrund der Regelungskompetenz nach § 78 SGB IV wurden die Grundsätze des Rechnungswesens in der SVRV und Detailregelungen in der SRVwV festgelegt. Ergänzend haben die Spitzenverbände der Krankenkassen in Zusammenarbeit mit der Informationstechnischen Servicestelle der gesetzlichen Krankenkassen GmbH (ITSG) insbesondere die folgenden Richtlinien (RiL) erarbeitet:

- Richtlinien für den Datenaustausch im Gesundheits- und Sozialwesen
- Datenaustausch mit Leistungserbringern und Arbeitgebern im Internet und per Direktwahlleitung:
  - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels File-Transfer-Protocol FTP
  - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels http und https
  - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten im XML-Format
  - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels E-Mail
- Security-Schnittstelle für das Gesundheits- und Sozialwesen
- Hinweise zur Security-Schnittstelle für das Gesundheits- und Sozialwesen

Die Richtlinien können über die Internetseiten des GKV-Spitzenverbandes heruntergeladen werden: [www.gkv-datenaustausch.de](http://www.gkv-datenaustausch.de)

Die aufgeführten RiL regeln detailliert die technischen Vorgaben der Datenfernübertragung und dem Datenträgeraustausch zwischen Arbeitgebern bzw. Leistungserbringern und SV-Trägern. Sie sind für die Beteiligten verbindlich.

Insbesondere werden die Themen

1. Datenannahme (Auftrags- und Nutzdatendatei)
2. Verifikation des Absenders
3. Prüfung Verschlüsselung
4. Technische Plausibilitätsprüfung und
5. Weiterleitung

behandelt.

Wesentlicher Kern des Sicherheitssystems ist die Verschlüsselung der in den Datensätzen übermittelten Nutzdaten. Diese erfolgt auf der Grundlage fortgeschrittener (personenbezogener) Zertifikate, die vom Trustcenter der ITSG GmbH erstellt werden. Hierdurch ist es möglich, den Absender (Ersteller) des Nutzdatensatzes zu „ermitteln“.

## 7.2 Speicherung des Originaldatensatzes

Bei elektronischen Eingängen sind entsprechende Vorschriften zur Aufbewahrung der Daten zu erfüllen. In der Sozialversicherung sind dies insbesondere § 78a SGB X und die SVHV sowie die SVRV i. V. m. der SRVwV.

Danach hat der SV-Träger

- zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle) sowie

- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

§ 6 Abs. 3 SVRV stellt klar, dass Belege auch elektronisch erzeugte Dateien oder Datensätze sein können. Somit ist sichergestellt, dass die rechtlichen Anforderungen für Belege auch für elektronische Datensätze gelten.

Ergänzend fordern § 9 Abs.1 und 3 SRVwV, dass

- die Belege zu nummerieren und geordnet und sicher aufzubewahren sind. Bei elektronisch erzeugten Dateien oder **Datensätzen** muss insbesondere sichergestellt sein, dass die Daten **verfügbar** sind und innerhalb angemessener Frist **lesbar gemacht** und **ausgedruckt** werden können. Mehrausfertigungen von Belegen müssen als solche erkennbar sein und
- Berichtigungsbuchungen sind auf dem ursprünglichen Beleg zu vermerken und durch einen neuen Beleg zu begründen; sie brauchen auf dem ursprünglichen Beleg nicht vermerkt zu werden, wenn in der Kassenordnung ein gleichwertiges Verfahren vorgesehen ist.

In § 12 Abs. 2 SRVwV ist geregelt, dass Änderungen in den zahlungsbegründenden Unterlagen so auszuführen sind, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen.

Eine Speicherung des verschlüsselten Original-Datensatzes birgt die Gefahr, dass der ursprüngliche Verschlüsselungsalgorithmus zu einem späteren Prüfzeitpunkt nicht mehr zur Verfügung steht und somit ein Entschlüsseln nicht mehr möglich wird.

Es wird daher empfohlen, die Nutzdaten nach Eingang beim SV-Träger direkt nach der Entschlüsselung elektronisch zu speichern.

Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (EDIFACT) in eine lesbare Form umzuwandeln.

### 7.3 Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung)

Automatisierte Verfahren sind durch besondere technische und organisatorische Maßnahmen vor unbemerkter und unberechtigter Veränderung zu schützen. Die zur Sicherheit dieser Verfahren zu erlassene Dienstanweisung muss die in der Anlage zu § 78a SGB X erforderlichen technischen und organisatorischen Maßnahmen regeln sowie die Einzelheiten qualifizierter digitaler Signaturen nach dem Signaturgesetz.

Insbesondere ist darauf hinzuweisen, dass Einzelheiten von Verfahrensänderungen und neu eingeführter Verfahren entsprechend der Anlage 9 zu § 40 SRVwV zu dokumentieren sind. Mit dieser Regelung wird der Einsatz moderner IT-Technik im Rechnungswesen berücksichtigt und die Prüfbarkeit von Abrechnungsverfahren (Verfahrens- und Systemprüfungen) sichergestellt. Aus der Dokumentation muss sich ergeben, dass das Verfahren entsprechend seiner Beschreibung durchgeführt worden ist.

Das gesamte Verfahren ist in einer ausführlichen Verfahrensbeschreibung darzustellen. Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind. Tabellen, über die die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln. Änderungen



von Tabellen mit Programmfunktion sind in der Weise zu dokumentieren, dass für die Dauer der Aufbewahrungsfrist der jeweilige Inhalt einer Tabelle festgestellt werden kann.

Nach den Vorschriften der SVRV sind die Grundsätze ordnungsmäßiger Buchführung zu beachten, Buchungen und Aufzeichnungen sind vollständig, richtig, zeitgerecht, geordnet und nachprüfbar vorzunehmen. Änderungen in zahlungsbegründenden Unterlagen sind so auszuführen, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen. Alle Buchungen müssen belegt sein und Belege können auch elektronisch erzeugte Dateien oder Datensätze sein. Bei der Nutzung von IT-Verfahren sind die Sicherheitsanforderungen in einer Dienstanweisung (siehe § 40 SRVwV) zu bestimmen. Dabei sind die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten.

Somit sind automatisierte Verfahren durch Regelungen von technischen und organisatorischen Maßnahmen vor unbemerkten und unberechtigten Veränderungen zu schützen. Die Anwendungen haben sicherzustellen, dass dokumentiert wird, wer zu welcher Zeit Änderungen an den Daten vorgenommen hat. Verfahrensänderungen sind so zu dokumentieren, dass die Prüfbarkeit des Abrechnungsverfahrens für einen sachverständigen Dritten darstellbar und nachvollziehbar sichergestellt ist.

**Anhang 1 Auszug BSI Technische Richtlinie 03125 „Bewiswerterhaltung kryptographisch signierter Dokumente“**  
(Version 1.1 vom 18.02.2011)

| Abschnitt aus TR-ESOR | Thema:                         | Anforderungen:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Fundstelle: |
|-----------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 4.2.1.2               | Neusignierung                  | <p>Die Signaturverordnung sieht in § 17 SigV ein Verfahren vor, wie und wann die erforderliche Neusignierung zu erfolgen hat:</p> <p><i>„Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle <b>sind</b> die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer <u>neuen qualifizierten elektronischen Signatur</u> zu versehen. Diese <b>muss</b> mit <u>geeigneten neuen Algorithmen oder zugehörigen Parametern</u> erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.“</i></p> <p>Droht der Verlust der Sicherheitseignung der verwendeten Algorithmen und der zugehörigen Parameter, so <b>sind</b> die Daten und alle bestehenden Signaturen also gemäß § 17 SigV erneut zu signieren. Dies ist die Grundlage der Bewiswerterhaltung elektronischer Dokumente.</p> | § 17 SigV   |
| 4.3.1                 | Zertifizierungsdiensteanbieter | <p>Die Vergabe qualifizierter Zertifikate ist nach § 2 Nr. 7 SigG Zertifizierungsdiensteanbietern (ZDA) vorbehalten, die mindestens die Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung erfüllen.</p> <p><b>Hinweis der Prüfdienste:</b><br/><i>Im Bereich der gesetzlichen Sozialversicherung kann es erforderlich sein, dass Dokumente / Daten über die gesamte Lebenszeit des Versicherten und darüber hinaus aufzubewahren sind. Aus diesem Grund <b>sind</b> hier <b>ausschließlich Zertifikate freiwillig akkreditierter ZDA zu verwenden!</b></i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | § 2 SigG    |

| Abschnitt aus TR-ESOR | Thema:                                                  | Anforderungen:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Fundstelle:      |
|-----------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 4.3.1                 | Integritätssicherung nicht signierter Daten             | Die Integrität nicht signierter Daten <b>muss</b> zusätzlich ab dem Zeitpunkt der Überführung in einen ECM/Langzeitspeicher durch geeignete kryptographische Sicherungsmittel wie elektronische Archiv-(eingangs)hashwerte oder -signaturen und (qualifizierte) Archiv(eingangs)zeitstempel gesichert werden.<br><br><i>Handelt es sich um rechtlich bedeutsame Dokumente bzw. erfordert die Art der Daten eine revisionssichere Archivierung, so <b>müssen</b> diese mit einer QES versehen im Langzeitspeicher abgelegt werden.</i> | §§ 110a-d SGV IV |
| 5                     | <b>Funktionen einer Middleware zum Beweiswerterhalt</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                  |
| 5.1.1                 | <b>Archivierung signierter und un-signierter Daten</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                  |
| (A5.1-4)              | Konformitätsprüfung der Datenformate                    | Die Middleware <b>muss</b> <sup>8</sup> vor der Ablage im ECM/Langzeitspeicher die Syntax der zur Aufbewahrung übergebenen Archivdatenobjekte auf Konformität mit dem für die Archivierung durch die Nutzer und Betreiber eines Archivsystems definierten und spezifizierten Datenformate (auf der Basis eines gültigen XML-Schemas) prüfen. Bei Nichtübereinstimmung <b>muss</b> dann die Ablage im ECM/Langzeitspeicher abgelehnt werden.                                                                                           |                  |
| 5.2                   | <b>Organisatorische Anforderungen</b>                   | Die organisatorischen Anforderungen legen die nicht-technischen Bedingungen fest, die vorzugsweise bereits vor oder bei der Einführung einer Middleware für den Beweiswerterhalt geschaffen werden müssen. Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware und legt keine formalen Kriterien fest. <sup>9</sup>                                                                                                                                                                                     |                  |
| 6                     | <b>Abgeleitete technische Anforderungen</b>             | Der folgende Abschnitt beschreibt abgeleitete und vornehmlich technische Anforderungen, die bei der Einrichtung und dem Betrieb einer zu dieser Richtlinie konformen Middleware zum Beweiswerterhalt zu erfüllen sind.                                                                                                                                                                                                                                                                                                                |                  |

<sup>8</sup> Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.1 vom 19.09.2011)

<sup>9</sup> Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

| Abschnitt aus TR-ESOR | Thema:                                            | Anforderungen:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Fundstelle: |
|-----------------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| (A6.1-3)              | Getrennte Mandantenverwaltung                     | Die TR-ESOR-Middleware <b>muss</b> <sup>10</sup> in der Lage sein, getrennte Mandanten zu verwalten. Dies bedeutet insbesondere eine strikte (logische) Separierung der im ECM/Langzeitspeicher abgelegten Archivdatenobjekte aber auch eine Trennung der für den Beweiswerterhalt relevanten Daten (Hashbäume).                                                                                                                                                                                                                                                                                                                                                                                                                              |             |
| (A6.2-1)              | Plattform- und herstellerunabhängige Datenformate | Im Interesse der dauerhaften Verfügbarkeit und Verkehrsfähigkeit der zu archivierenden Dokumente und Daten <b>müssen</b> <sup>11</sup> ausschließlich Datenformate eingesetzt werden, die eine plattform- und herstellerunabhängige Archivierung in langfristig verkehrsfähiger Form ermöglichen.<br>Kapitel 4 von TR-ESOR-F führt im Detail die empfohlenen Formate auf.                                                                                                                                                                                                                                                                                                                                                                     |             |
| 6.4                   | <b>IT-Infrastruktur</b>                           | Die nachfolgend genannten technischen Sicherungsmaßnahmen für die TR-ESOR-Middleware und des gesamten Archivsystems dienen dem Beweiswerterhalt und umfassen physische Sicherungsmaßnahmen, logische Zugriffskontrollen sowie Datensicherungs- und Auslagerungsverfahren für den Regel- und den Notbetrieb.<br>Dieses Kapitel versteht sich als Hinweis an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest. <sup>12</sup><br><br>Der ECM/Langzeitspeicher stellt die Datensenke des elektronischen Archivs dar. Die archivierten Daten und Dokumente sind hier sicher gespeichert, inklusive aller für die langfristige Aufbewahrung und Verfügbarkeit nötigen Verkehrs- und Verwaltungsinformationen. |             |

<sup>10</sup> Bei IT-Dienstleistern/RZ, die für mehrere SV-Träger tätig sind, **muss** eine entsprechende Trennung der Daten erfolgen!

<sup>11</sup> Änderung als Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.1 vom 19.09.2011)

<sup>12</sup> Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

| Abschnitt<br>aus<br>TR-ESOR | Thema:                                                        | Anforderungen:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Fundstelle: |
|-----------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 6.5                         | <b>IT-Anwendungen beim Einsatz von Archivierungsverfahren</b> | <p>Neben Anforderungen an die IT-Infrastruktur und natürlich der TR-ESOR-Middleware <b>müssen</b> auch diverse Anforderungen an die vorgelagerten Fachanwendungen gestellt werden.</p> <p>Dieses Kapitel versteht sich als Hinweis an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest.<sup>13</sup></p> <p>Bei den zur Archivierung eingesetzten IT-Anwendungen handelt es sich im Regelfall um Softwaresysteme, die an die organisationsspezifischen Besonderheiten und Archivierungsanforderungen anzupassen sind. Eine Anwendung im Sinn dieser Richtlinie kann aus mehreren Einzelkomponenten oder Programmen bestehen. Es ist nicht notwendigerweise ein monolithisches Programm oder ein einzelnes System. In den vorgelagerten Anwendungssystemen werden die später zu archivierenden Dokumente und Daten erzeugt und bearbeitet. Bis zum Zeitpunkt der Archivierung werden sie dabei auf den zu diesen Anwendungssystemen gehörenden Datenspeichern vorgehalten.</p> |             |
| 6.5                         | Trusted Viewer                                                | <ul style="list-style-type: none"> <li>Für die Anzeige von qualifiziert signierten elektronischen Daten und Dokumenten <b>muss</b><sup>14</sup> die Anwendung oder die Anwendungsumgebung eine <u>bestätigte vertrauenswürdige Anzeigekomponente</u> (Trusted Viewer) zur Verfügung stellen. Die Bestätigung <b>muss</b> durch eine anerkannte Bestätigungsstelle gemäß §18 SigG erfolgen.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |             |
| 8                           | <b>IT-Sicherheitskonzept</b>                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |             |
| 8.2                         | <b>Maßnahmen</b>                                              | <p>Um die oben angegebenen Sicherheitsziele für die Middleware und den ECM/Langzeitspeicher in der Ausprägung der empfohlenen Referenzarchitektur zu erfüllen, sind die folgenden Maßnahmen erforderlich.</p> <p>Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware bzw. eines ECM / Langzeitspeichers und legt keine formalen Kriterien fest.<sup>15</sup></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |             |

<sup>13</sup> Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

<sup>14</sup> SV-Träger muss in der Lage sein, die Signatur von Dokumenten/Daten zu überprüfen.

<sup>15</sup> Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

| Abschnitt<br>aus<br>TR-ESOR | Thema:                  | Anforderungen:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Fundstelle: |
|-----------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                             |                         | <p><b>HINWEIS:</b><br/>Es ist zu beachten, dass dieser generische Maßnahmenkatalog auf keinen Fall ein konkretes Sicherheitskonzept (gemäß bspw. den IT-Grundschutz-Katalogen des BSI) ersetzen kann, das den lokalen und organisationsspezifischen Bedürfnissen und Gegebenheiten angepasst ist.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |             |
| 8.2.1                       | Übergreifende Maßnahmen | <p>Vor dem Einrichten eines elektronischen Archivsystems mit dem Fokus auf dem Beweiswerterhalt muss ein die technischen Systeme und sämtliche relevanten Prozesse abdeckendes IT-Sicherheitskonzept basierend auf einer standardisierten Methodik (z. B. BSI-100 Standard) erstellt und mit der Inbetriebnahme umgesetzt werden.</p> <p>Das IT-Sicherheitskonzept <b>muss</b> regelmäßig (z. B. einmal pro Jahr) auf den aktuellen Stand gebracht werden.</p> <p>Die Maßnahmen, die sich aus dem IT-Sicherheitskonzept und dessen Überarbeitung ergeben, <b>müssen</b> - soweit wirtschaftlich vertretbar<sup>16</sup> - zeitnah umgesetzt werden. Dies gilt insbesondere für die Definition und Umsetzung der Verantwortlichkeiten und Kompetenzen, der fachlichen Prozesse sowie sicherer Administrations- und Kontrollprozesse.</p> <p>Insbesondere für Einrichtungen, Organisationen und Unternehmen der öffentlichen Verwaltung <b>soll</b> das Einrichten und der Betrieb eines Archivsystems mit einer Middleware zum Beweiswerterhalt einem IT-Grundschutz-Audit mit dem Ziel der Zertifizierung unterzogen werden, um auch die jeweiligen Prozesse und Organisationen in der Einsatzumgebung nachweislich zielgerichtet definiert zu haben.</p> |             |

<sup>16</sup> Wirtschaftliche Aspekte sind nachrangig, wenn rechtliche Vorgaben (z. B. der „UP Bund“) eine zeitnahe Umsetzung fordern.