Die Prüfdienste des Bundes
und der Länder informieren

# Leitfaden

# Elektronische Kommunikation
# und
# Langzeitspeicherung elektronischer Daten

Version 4.1
Stand: 22.04.2016

| **Versionsdokumentation** | | | | |
|---|---|---|---|---|
| Version: | Datum: | Kap./Seite: | Grund d. Änderung: | Bearbeiter: |
| 4.0 | Oktober 2014 | Alle | Einarbeitung EGovG, Neustrukturierung gesamtes Dokument (aus Version 3.5). | AK Signatur |
| 4.1 | April 2016 | Alle | Einarbeitung 5. SGB-IV-ÄndG<br>Anforderungen „Online-Geschäftsstelle“<br>Anforderungen Apps | AK el.-Kommunikation |

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

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

Ansprechpartner:

- Prüfgruppe IT des Referates 614 (Außenstelle Cloppenburg)
  Tel.: (04471) 1807-0
  E-Mail:Referat_614_IT@bvamt.bund.de

- Referat 611
  Tel.: (0228) 619-1438
  E-Mail:
  Referat_611@bvamt.bund.de

**0 Einleitung und Anwendungshinweise ... 6**

**1 Rechtsgrundlagen ... 8**

**2 Vorgehensweise bei Einführung neuer IT-gestützter Verfahren zur Geschäftsprozessoptimierung ... 10**

**2.1 Vorbereitende Analysen und Maßnahmen ... 10**

**2.2 Umsetzung/Ausschreibung ... 10**

**2.3 Anzeige an die Aufsichtsbehörde ... 11**

**3 Elektronische Kommunikation zwischen SV-Trägern und Versicherten ... 12**

**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 - Grundsatz ... 15**

**3.2 Zugang ... 17**

**3.2.1 Grundsätze ... 17**

**3.2.2 Zugangsmöglichkeiten bei Schriftformersatz ... 18**

**3.2.2.1 Qualifizierte Elektronische Signatur ... 18**

**3.2.2.2 Eingabe über Web-Formulare oder besondere Eingabegeräte ... 18**

**3.2.2.3 Kommunikation mit De-Mail ... 19**

**3.2.2.4 De-Mail-Versand elektronischer Verwaltungsakte oder sonstiger elektronischer Dokumente durch SV-Träger ... 20**

**3.2.2.5 Identifizierung des Absenders durch sonstige sichere Verfahren ... 20**

**3.2.3 Zugangsmöglichkeiten ohne Schriftformerfordernis ... 20**

**3.3 Behandlung der Online-Daten und Daten mittels Apps ... 24**

**3.3.1 Datenumfang und Dokumentation ... 24**

**3.3.2 Integritätsschutz ... 25**

**3.3.3 Revisionssichere Archivierung ... 25**

**3.3.4 Apps ... 26**

**3.4 Elektronische Einreichung von Nachweisen ... 26**

**3.4.1 Einreichung durch die Versicherten ... 26**

**3.4.2 Elektronische Übermittlung von Nachweisen zwischen verschiedenen Behörden / SV-Trägern ... 27**

**3.5 Elektronischer Posteingang ... 27**

**3.5.1 Behandlung eingehender Fax-Sendungen ... 27**

**3.5.2 Speicherung eingehender E-Mails im elektronischen Langzeitarchiv ... 28**

**3.5.3 Speicherung eingehender De-Mails im elektronischen Langzeitarchiv ... 29**

**3.6 Elektronischer Postausgang ... 29**

**3.6.1 Grundsätze ... 29**

**3.6.2 E-Mails (ohne / mit Anhang) ... 30**

**3.6.3 De-Mails (ohne / mit Anhang) ... 30**

**3.6.4 Erstellung und Versand von Serienbriefen ... 30**

**4 Technische und organisatorische Verfahrensanforderungen ... 32**

**4.1 Allgemeine Anforderungen ... 32**

**4.1.1 Verfahrensbeschreibung ... 32**

**4.1.2 Dienstanweisung ... 32**

**4.2 Qualifizierte Elektronische Signatur (QES) ... 34**

**4.2.1 Signaturerstellungseinheiten und Signaturanwendungskomponenten ... 34**

**4.2.2 Regelungen für das Kartenmanagement ... 35**

**4.2.3 Neusignieren nach § 17 Signaturverordnung (SigV) ... 35**

**5 Übertragung und Vernichtung des Papieroriginals ... 39**

**5.1 Scannen von Papierdokumenten ... 39**

**5.1.1 Klassifizierung der Papierdokumente ... 39**

**5.1.2 Bildliche und inhaltliche Übereinstimmung ... 40**

**5.2 Dokumentation des Scan-Vorgangs ... 41**

**5.3 Formen der Signatur ... 42**

**5.4 Sicherheitsmaßnahmen ... 45**

**5.5 Technische Richtlinie TR03138 („TR-RESISCAN“) ... 47**

**5.6 Vernichtung von Originalbelegen ... 47**

**6 Langzeitspeicherung elektronisch erzeugter Dokumente und Daten..... 49**

**6.1 Allgemeine Anforderungen ..... 49**

**6.2 Rechtssichere Langzeitspeicherung von elektronischer Post..... 50**

**6.3 Technische Richtlinie TR03125 („TR-ESOR“) ..... 50**

**6.4 Besonderheiten ..... 51**

**6.4.1 Aufbewahrung von Fehler- / Bearbeitungslisten ..... 51**

**6.4.2 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen..... 51**

**7 Elektronischer Datenaustausch..... 52**

**7.1 Ergänzende rechtliche Grundlagen..... 52**

**7.2 Speicherung des Originaldatensatzes ..... 53**

**7.3 Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung) ..... 54**

**Anhang 1 Auszug BSI Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ ..... 56**

# 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 Vorgaben 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 das strukturierte Vorgehen bei der Auswahl, Einführung und (gesetzesmäßigen) Umsetzung 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 Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, 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), der Bundesbeauftragten für den Datenschutz und Informationsfreiheit (BfDI) und vom Bundesinnenministerium herausgegebenen Werke, Standards und Empfehlungen in den jeweils aktuellen Fassungen zu beachten:

- 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
- Organisationskonzept elektronische Verwaltungsarbeit (Herausgeber: Bundesministerium des Innern)
- Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden (Version 1.0, Stand 2014)

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

Dieser wird von den Prüfdiensten des Bundes und der Länder laufend gepflegt und weiter entwickelt. Er wird bei Prüfungen  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**“ [1] zusammengefasst.)

Bei der Einführung der o. g. Verfahren 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 „Grundleitfaden 85“ (Grundleitfaden für Anzeigen zur Beschaffung bzw. Entwicklung von Datenverarbeitungsanlagen und -systemen sowie -programmen nach § 85 Abs. 1 Sätze 2 – 6 SGB IV, in der Fassung vom 25. November 2008)[2] anzuzeigen.

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“ [3] zu beachten.

[1] **SV-Träger** i.S.v. § 274 SGB V: Krankenkassen, Pflegekassen, Arbeitsgemeinschaften, Landesverbände der Krankenkassen, GKV-Spitzenverband, Kassenärztliche Bundesvereinigung (KBV),Kassenzahnärztliche Bundesvereinigung (KZBV), Kassenärztliche Vereinigungen (KVs), Kassenzahnärztliche Vereinigungen (KZVs), Medizinischer Dienst des Spitzenverbandes Bund der Krankenkassen (MDS) Medizinische Dienste der Krankenversicherung (MDKs).

[2] Abrufbar unter www.bundesversicherungsamt.de

[3] Abrufbar unter www.bundesversicherungsamt.de

# 1 Rechtsgrundlagen

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

- **SGB I - Sozialgesetzbuch, Erstes Buch**
  - § 36a Elektronische Kommunikation

- **SGB IV – Sozialgesetzbuch, Viertes Buch**
  - § 69 Abs. 2 (Wirtschaftlichkeit und Sparsamkeit)
  - § 110a (Aufbewahrungspflicht)
  - § 110b (Rückgabe, Vernichtung und Archivierung von Unterlagen)
  - § 110c (Verwaltungsvereinbarungen, Verordnungsermächtigung)
    - Grundsätze ordnungsmäßiger Aufbewahrung im Sinne des § 110a SGB IV, Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie Aufbewahrungsfristen für Unterlagen für den Bereich der gesetzlichen Kranken- und Pflegeversicherung (Stand: 18. 12..2015, Version 1.0)

  - **5. SGB IV Änderungsgesetz**
    - Wegfall Nachweispflicht beim Scannen von Papierdokumenten (§ 110a Abs. 2 Satz 2 Nr. 1 Buchst. a SGB IV)
    - Wegfall Beweiswirkung qualifizierter elektronischer Signaturen (§ 110d SGB IV)

- **SGB V – Sozialgesetzbuch, Fünftes Buch**
  - § 197b (Aufgabenerledigung durch Dritte)
  - §§ 284 ff. (Grundsätze der Datenverwendung)

- **SGB X – Sozialgesetzbuch, Zehntes Buch**
  - § 9 (Nichtförmlichkeit des Verwaltungsverfahrens)
  - § 33 (Bestimmtheit und Form des Verwaltungsaktes)
  - §§ 67-78 (Schutz der Sozialdaten)
  - § 78a und Anlage (Technische und organisatorische Maßnahmen)

- **Gesetz zur Förderung der elektronischen Verwaltung (EGovG)**
  - § 1 Abs. 1, 2, 4 Geltungsbereich
  - § 2 Elektronischer Zugang zur Verwaltung
  - § 4 Elektronische Bezahlmöglichkeiten
  - § 5 Nachweise
  - § 6 Elektronische Aktenführung
  - § 7 Übertragen und Vernichten des Papieroriginals
  - § 8 Akteneinsicht
  - § 9 Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand
  - § 13 Elektronische Formulare
  - § 16 Barrierefreiheit

- **Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)**

- **Verordnung zur Elektronischen Signatur (Signaturverordnung – SigV**)

- **De-Mail-Gesetz (DeMailG)**
  - § 4 Anmeldung zu einem De-Mail-Konto
  - § 5 Postfach- und Versanddienst

- **Verordnung über das Haushaltswesen in der Sozialversicherung (SVHV)**
  - § 22 (Öffentliche Ausschreibung)

- **Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (SVRV)**
  - § 5 (Belegpflicht)
  - § 6 Abs. 3 (Belege für Einzahlungen, Auszahlungen und Buchungen ohne Zahlungsvorgang)
  - § 7 Abs. 3 (Zahlungsanordnung)
  - § 17 (Dienstanweisungen)
  - § 19 (Outsourcing)

- **Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV)**
  - § 9 (Allgemeines)
  - § 11 (Anordnung der Zahlung)
  - § 12 (Zahlungsbegründende Unterlagen)
  - § 13 (Änderung der Zahlungsanordnung)
  - § 19 Abs. 5 (Feststellung der Belege)
  - § 20 (Sachliche Feststellung)
  - § 21 (Rechnerische Feststellung)
  - § 22 (Form und Führung der Bücher und Aufzeichnungen)
  - § 35 (Aufbewahrungsfristen)
  - § 36 (Aufbewahrung)
  - § 40 (Sicherheit bei Einsatz der automatisierten Datenverarbeitung, Grundsätze ordnungsgemäßer Datenverarbeitung - GoD)
  - § 41 (qualifizierte elektronische Signatur)
  - § 42 (Outsourcing)
  - § 44 (Übergangsregelungen)

- **Risikostrukturausgleichsverordnung (RSAV)**
  - 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 unter Ziffer 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 Werken, Standards und Empfehlungen des BSI zu entnehmen (siehe „Einleitung und Anwendungshinweise“ dieses Leitfadens).

**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[4] (§ 69 Abs. 3 SGB IV) anzuwenden. Einzubeziehen sind auch Fragen zur Nachhaltigkeit und zu den Auswirkungen / Kosten bei einem Systemwechsel. In die Überlegung sind bereits bestehende Verfahren einzubeziehen. Eine stringente Organisation der Abläufe ist anzustreben.

Zu beachten ist hierbei, dass die Erfüllung gesetzlicher Vorgaben – insbesondere aus §§ 110 a - c 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 in Ausnahmefällen abgesehen werden, sofern die Natur des Geschäfts oder besondere Umstände dies rechtfertigen.
Landesspezifische Regelungen sind ggf. zu beachten.

[4] 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) 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. Nur 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 somit rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht anzuzeigen.

Die Aufsichtsbehörden haben den „Grundleitfaden 85“ erstellt. Dieser bildet den Rahmen für die Anzeige und die Wirtschaftlichkeitsbetrachtung und ist demnach zu beachten.

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.

Das 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 Orientierung bei der Auslegung der Rechtsvorschriften können auch die Ausführungen des BMI in seinem „Minikommentar“ zum EGovG herangezogen werden

Neben der Kommunikation über Online-Medien, gewinnt die Kommunikation über Softwareprogramme, die speziell für die Nutzung auf mobilen Endgeräten geeignet sind (sog. Apps)[5], an Bedeutung. Allgemein gelten die Aussagen / Grundsätze zur elektronischen Kommunikation über Online-Medien auch für die Apps. Dies gilt insbesondere für folgende Anforderungen, die auch beim Angebot von Apps durch die Sozialversicherungsträger erfüllt sein müssen:

- Zugang (Authentifizierung)
- Nichtveränderbarkeit / Integrität übermittelter Daten
- Einhaltung allgemeiner und spezifischer Vorgaben zu Datenschutz und Datensicherheit
- Sichere Datenwege
- Revisionssichere Speicherung / Archivierung von übermittelten Daten.

In diesem Kapitel werden daher Ausführungen zu Apps aufgenommen und Hinweise gegeben, sofern hierzu besondere / spezielle Anforderungen bestehen .

### 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. Soweit das Gesetz den Anwendungsbereich einzelner Regelungen nicht explizit auf Behörden des Bundes beschränkt, gelten sie für alle Behörden, wenn sie Bundesrecht ausführen (§ 1 Abs. 2 EGovG).

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 entgegenstehende Bestimmungen enthalten (§ 1 Abs. 4 EGovG). Hierunter fallen z. B. die Regelungen zur rechtssicheren Übertragung von Papierdokumenten in die elektronische Form sowie

[5] Solmecke/Taeger/Feldmann (Hrsg.) Mobile Apps, Kap. 1 Rn. 14, S. 3.

die Langzeitspeicherung elektronisch erzeugter Dokumente unter Verwendung der qualifizierten elektronischen Signatur (QES) gem. §§ 110a – c SGB IV. Diese sind in ihrem jeweiligen Anwendungsbereich 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.

| 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 Bezahlmöglichkeiten |
| | § 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 landesunmittelbaren SV-Träger laufend beobachten, ob einzelne Bundesländer entsprechende 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 den §§ 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 jedoch 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.

Die Schriftform kann nach § 36a Abs. 2 Sätze 4 und 5 SGB I ersetzt werden durch:

- Die Bereitstellung **elektronischer Formulare über Web-Portale** der Behörde, die die Versicherten online „ausfüllen“ kann. Die Authentifizierung des Absenders muss hierbei über die eID-Funktion des neuen Personalausweises (nPA) oder den elektronischen Aufenthaltstitel (eAT) erfolgen (Nr. 1).
- 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 Authentifizierungsverfahren identifiziert und die Nachricht einschließlich aller Metadaten durch eine vom De-Mail-Diensteanbieter aufgebrachte QES (des De-Mail-Diensteanbieters) gegen Veränderungen geschützt (Nr. 2 und 3).
- Daneben können per Rechtsverordnung weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden (Nr. 4).
- In der Kommunikation zwischen den Versicherten und ihren Krankenkassen kann die Identität auch mit der **elektronischen Gesundheitskarte** nachgewiesen werden (Satz 5).

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 Ziffer 3.2.3 zu entnehmen.

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

**Hinweis:**
Sind in **Papierform ausgegebene Formulare** mit einem Unterschriftfeld versehen, sind diese Formulare von den Versicherten weiterhin zu unterschreiben.

### 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 dieser Vorschrift hat der Bundesgesetzgeber Regeln zur Herstellung von Barrierefreiheit in der Informationstechnik für die Verwaltung gesetzt. Damit ist die Verwaltung 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 - Grundsatz

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 können bestimmte technische Zusatzmaßnahmen der Datensicherheit und des Zugangs gefordert sein, die über die im EGovG genannten Bedingungen der datenschutzrechtlich „einfachen“ Kommunikation hinausgehen.

Die 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 SV-Träger 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 die Daten sind, 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 dürfen in keinem 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 und besondere Anforderungen an die Authentifizierung erfüllt 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 der 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.
Für den Schutzbedarf „sehr hoch“ empfiehlt die Aufsicht des Bundesversicherungsamtes bei Abruf von Gesundheitsdaten (z. B. Patientenquittung) aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren (z.B. Benutzername / Password sowie einem weiteren Sicherungsmittel wie z.B. der eID des neuen Personalausweises (nPA) / der elektronischen Gesundheitskarte, siehe Rundschreiben des Bundesversicherungsamtes vom 5. September 2014).
Die Prüfdienste empfehlen ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung vorzusehen, z. B eine qualifizierte Zwei-Wege-Authentifizierung z.B.

- Benutzername / Password **und**
- weiteres Sicherungsmittel wie (transaktions- oder zumindest sitzungsbezogenes) TAN-Verfahren oder – alternativ zu TAN-Verfahren - als besonders sicherem weiteren Sicherungsmittel die eGK bzw. den nPA (vgl. Ziffer 3.2.3.1 und 3.2.3.4).

Die Prüfdienste empfehlen, diese Vorkehrungen auch bei der Übermittlung sensibler Informationen von Versicherten an den Sozialversicherungsträger vorzusehen.

Weitere Ausführungen hierzu sind der o. g. „Handreichung“ zu entnehmen, die über die Internetseite der BfDI eingesehen werden kann.

Für Apps gelten die dargestellten Anforderungen an die Schutzbedarfsfeststellung / Risikoanalyse sowie die inhaltlichen Grundsätze in gleichem Maße. Dabei ist bei der Festlegung der Anforderungen zwischen den verschiedenen Funktionen und Inhalten von Apps zu unterscheiden:

- Anmeldung in der Online-Geschäftsstelle über die App:
  - Gleiche Schutzklassen / Anforderungen wie bei Online-Portalen
- Informationsaustausch nur über App-Server (ohne Account bei Online-Portal):
  - Serverbasierte Schutzmaßnahmen in Bezug auf
    - Integrität der App
    - Sicherung der Übertragungswege
  - Gleiche Schutzklassen wie bei Online-Portalen
- Datenabruf vom Server (z.B. allgemeine Informationen ohne personenbezogene Daten:
  - Keine Speicherung von nicht erforderlichen Daten (Zweckbindung, Datensparsamkeit)

Zu den datenschutzrechtlichen Anforderungen an die Erstellung und das Angebot von Apps verweisen die Prüfdienste auf die Veröffentlichungen der Datenschutzbehörden.[6]

[6] Z.B. Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Schwerin, 6./7. April 2016): „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ sowie Düsseldorfer Kreis der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (16. Juni 2014): „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“.

## 3.2 Zugang

### 3.2.1 Grundsätze

Der Austausch elektronischer Dokumente zwischen Versicherten und SV-Träger 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 → Versicherte** bedeutet dies, dass die Versicherten gegenüber dem SV-Träger ausdrücklich ihre Zustimmung für die Übermittlung elektronischer Dokumente (z.B. per E-Mail) erteilt haben müssen (§ 36a Abs. 1 SGB I). Die bloße Angabe einer E-Mail-Adresse reicht nicht aus.

Dagegen ist für eine Kommunikation in Gegenrichtung **Versicherte → 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 auch qualifiziert signierte elektronische Dokumente empfangen. Neben dem E-Mail-Postfach ist z. B. auch die Einrichtung eines elektronischen Zugangs 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 § 110a SGB IV i. V. m. der Anlage zu § 78a SGB X.

- 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-Diensteanbieter befinden.

  Eine Verpflichtung des SV-Trägers, den Versicherten auf dem De-Mail-Wege zu antworten, besteht nicht, wenn die Versicherten mehrere Zugänge gegenüber dem SV-Träger eröffnet haben. Außerdem ist der SV-Träger nicht verpflichtet, per De-Mail zu antworten. Wenn es sich um Sozialdaten mit sehr hohem Schutzbedarf handelt, sind bei elektronischen Antworten zusätzliche Sicherungsmaßnahmen (z. B. Ende-zu-Ende-Verschlüsselung) einzusetzen.

- In Absatz 3 werden die Behörden des Bundes darüber hinaus verpflichtet, in Verwaltungsverfahren, in denen sie aufgrund einer Rechtsvorschrift die Identität der 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 auch mit der elektronischen Gesundheitskarte erfolgen (§ 36a Abs. 2 Satz 5 SGB I).

**Hinweis:**
Nur die Informationen der Versicherten, die über Verfahren gewonnen werden, die die im folgenden genannten Anforderungen an Authentifizierung, Integrität der Daten und revisionssichere Speicherung erfüllen, werden von den Prüfdiensten zu Prüfzwecken als Beleg anerkannt.

### 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 die Ziffer 4.2, zum Schriftformerfordernis die Ziffer 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 die Versicherten über das Internet herunterladen, am Bildschirm ausfüllen (z. B. ausfüllbares PDF-Formular) und anschließend ausdrucken und an den SV-Träger schicken. 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 zur Verfügung gestellten Eingabegeräten (z.B. in seinen Kundenzentren)[7]. Die elektronische Anwendung fungiert wie ein Formular, das aus der Ferne ausgefüllt wird.
Empfehlung: Der SV-Träger sollte durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können.

Die Versicherten müssen sich zur Nutzung identifizieren (Authentifizierung). 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 von Versicherten **eingegebenen Erklärungen (Daten) mit den Identifikationsdaten des nPA / der eGK („Metadaten“, z. B. Personalausweisdaten, Eingabezeit) dauerhaft verknüpft werden**. Abgeleitet aus § 110a SGB IV i. V. m. der Anlage zu § 78a SGB X sind diese Daten revisionssicher zu archivieren.

Die technische und organisatorische Ausgestaltung des Gesamtverfahrens (von der Eingabe durch die Versicherten bis zur Übergabe der Daten an die Fachanwendung und das

[7] Eine (teilweise/vollständig) kostenlose Überlassung von elektronischen Eingabegeräten (z.B. Kartenleser) für Versicherte **durch den SV-Träger** ist gem. § 30 Abs. 1 SGB IV nicht zulässig!

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.

#### 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.

Der akkreditierte De-Mail-Diensteanbieter muss danach 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 De-Mail-Diensteanbieter des Senders die Verwendung der sicheren Anmeldung nach § 4 durch eine QES.

Der akkreditierte De-Mail-Diensteanbieter hat zu gewährleisten, dass der Nutzer (Absender) zwischen mindestens zwei Verfahren zur sicheren Anmeldung wählen kann. Ein Verfahren muss hierbei die Nutzung der eID-Funktion des neuen Personalausweises (nPA) ermöglichen (§ 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 nPA

  Hierzu 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-Diensteanbieter 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 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) versenden.

Hierbei muss der De-Mail-Diensteanbieter 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 Datenübermittlers (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 und deren revisionssichere Speicherung aus anderen Gründen (z. B. für RSA-Prüfungen) nachzuweisen sind. Sollten für diese Daten die in § 36a Abs. 2 SGB I genannten sicheren Zugangsmöglichkeiten nicht angewandt werden, muss der Nachweis der Authentizität und Integrität der Daten / Dokumente auf andere Weise erbracht werden. Das gesamte beim SV-Träger zur Anwendung kommende Verfahren ist in einer Verfahrensbeschreibung detailliert zu dokumentieren.

#### 3.2.3.1 Authentifizierungsverfahren - Allgemein

Zur Anerkennung von elektronisch übermittelten Daten ist die Identität der Absenderin / des Absenders über ein Authentifizierungsverfahren festzustellen. Hierzu hat der SV-Träger im Rahmen einer Schutzbedarfsanalyse festzulegen, welche Daten über das Online-Portal übermittelt bzw. abgerufen werden können. Hierbei können insbesondere die Ausführungen der BfDI („Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“) im Hinblick auf die Übermittlung von Sozial- und

Gesundheitsdaten als allgemein zu verstehende Anforderungen an die Schutzbedarfsfeststellung herangezogen werden.
Dies bedeutet, dass je nach Schutzbedarf innerhalb des Portals ggf. zusätzliche Authentifizierungen für den Abruf „besonders schützenswerter" Daten einzurichten sind.

Hinweise zur Klassifizierung von elektronischer Eingangspost bzw. der Anzeige von Informationen innerhalb eines Online-Portals enthalten die Technische Richtlinie des BSI („TR-03138 TR-RESISCAN") sowie das „Organisationskonzept elektronische Verwaltungsarbeit" des Bundesministeriums des Innern. In diesen Dokumenten erfolgt eine dreistufige Klassifizierung des Schutzbedarfs in „normal", „hoch" und „sehr hoch".

So kann mit dem Verfahren „Nutzername / Passwort" (Identifikationsmerkmale) nur die Sicherheit für einen normalen Schutzbedarf erreicht werden, da der Nutzername das einzige Identitätsattribut darstellt.
Um die Authentizität / Integrität / Vertraulichkeit der Identifikationsmerkmale während der Übermittlung zu schützen, muss vor der Übermittlung eine sichere Verbindung mit einem geeigneten Mechanismus etabliert werden.

Eine höhere Sicherheit (hoher / sehr hoher Schutzbedarf) kann nur erreicht werden, wenn zusätzliche Geheimnisse wie z.B. PIN und weitere Authentifizierungsfaktoren (z.B. über Softwaretoken, Hardwaretoken) sowie kryptographische Sicherungsverfahren genutzt werden. [8]

Die „Zusatz-Authentifizierung" muss bei jedem Abruf der besonders schützenswerten Daten neu erzeugt / eingegeben werden. Eine dauerhafte Freischaltung des besonders geschützten Bereichs durch einmalige Eingabe dieser „Zusatz-Authentifizierung" ist nicht zulässig.

Hieraus kann beispielhaft abgeleitet werden:

- Die Anzeige einer „Patientenquittung" (§ 305 SGB V) innerhalb eines Online-Portals ist – aufgrund der darin enthaltenen Gesundheitsdaten – zweifelsfrei dem Schutzbedarf „sehr hoch" zuzuordnen.
  Für diesen Schutzbedarf „sehr hoch" empfiehlt die Aufsicht des Bundesversicherungsamtes aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren, z.B. Benutzername / Passwort sowie einem weiteren Sicherungsmittel wie z.B. der eID des nPA / der eGK (siehe Rundschreiben des Bundesversicherungsamtes vom 5. September 2014 sowie vom 18. April 2016).
  Die einmalige Authentifizierung am Online-Portal (Benutzername / Passwort) reicht nach Auffassung auch der Prüfdienste in keinem Fall für eine Anzeige derartiger Daten aus. Die Prüfdienste empfehlen daher ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung (qualifizierte Zwei-Wege-Authentifizierung auf verschiedenen „Kanälen") vorzusehen:
  Anmeldung mit Nutzername / Passwort **und** einem weiteren (transaktionsbezogenen oder zumindest sitzungsbezogenen) Sicherungsmittel, das mindestens z.B. ein mTAN-Verfahren darstellt bzw. – als höhere Sicherheitsstufe – die Nutzung nPA / eGK.

- Änderungen sensibler Stammdaten (Adressänderungen, Bankverbindungen etc.) sind nach Auffassung der Prüfdienste ebenfalls dem Schutzbedarf „sehr hoch" zuzuordnen. Die Prüfdienste empfehlen dringend, Änderungen dieser Daten durch Versicherte über elektronische Kommunikation ebenfalls erst nach einer zusätzlichen Authentifizierung vorzusehen. Hierzu kann auch ggf. das mTAN-Verfahren (wie im Bankensektor üblich) genutzt werden.

[8] Zu „technischen" Hinweisen siehe z. B. die Ausgabe 4/2016 der Zeitschrift „Datenschutz und Datensicherheit" (DuD).

Die Prüfdienste empfehlen für die Nutzung des Online-Dienstes über mobile Endgeräte folgendes zu beachten:

- Zusätzlich zur mTAN sollte ein weiteres, sicheres Geheimnis genutzt werden (z. B. zugesandte mTAN und zusätzlich eine Ziffernfolge der eGK-Kartennummer).
  oder
- Zusendung der mTAN an ein Gerät, durch das nicht die Anforderung der mTAN erfolgte.
  oder
- Weitere Verfahren, die außerhalb des mTAN-Verfahrens ein weiteres Geheimnis liefern (z.B. Zugangstoken).

Eine Authentifizierung oder Übermittlung / Änderung eines Geheimnisses als Sicherungsmittel über Telefon (Telefonzentrale) für eine anschließende Datenübermittlung sollte nicht (Empfehlung der Prüfdienste) bzw. nur bei weiterer, sicherer / zweifelsfreier Identifizierung der/des Versicherten im Rahmen des Telefonkontaktes erfolgen (siehe Rundschreiben des Bundesversicherungsamtes vom 18. April 2016).

#### 3.2.3.2 Eröffnung eines dauerhaften Online-Zugangs („Benutzer-Konto“)

Der Antrag auf Eröffnung eines Zugangs zum Online-Portal („Online-Geschäftsstelle“) kann schriftlich oder über eine Web-Anwendung erfolgen. Die Mindestanforderung der Prüfdienste ist eine Zwei-Wege-Authentifizierung. Die Beantragung kann folgendermaßen ausgestaltet werden:

Von den Versicherten sind bestimmte Daten zur „Erstidentifikation“ abzufordern. Hierzu gehören <u>mindestens</u>

- Name, Vorname
- Geburtsdatum
- eindeutiges Identifizierungsmerkmal, z.B. KV-Nummer (Sicherer wäre z. B. die Abfrage von Teilen der eGK-Kartennummer)

Optional können an dieser Stelle bereits auch schon folgende Daten (für die spätere Nutzung des Online-Portals) von den Nutzern eingegeben werden:

- Benutzername
- Passwort
- E-Mail-Adresse

Nach Absendung der Daten erfolgt ein Abgleich der eingegebenen Mindestdaten mit den im Bestand des SV-Trägers vorhandenen Daten. Die optional bereits angegebene E-Mail-Adresse kann - nach Abgleich mit den beim SV-Träger ggf. bereits bekannten Daten - durch Zusendung einer E-Mail mit einem „Verifizierungslink“ geprüft werden.

Nach Annahme und Verifizierung der Daten durch den SV-Träger hat dieser dem Nutzer einen **Freischaltcode** postalisch zuzustellen. Dieser Freischaltcode ist vom Nutzer innerhalb einer vom SV-Träger festzulegenden Gültigkeitsdauer (maximal 60 Tage) bei der Erstanmeldung im Online-Portal einzugeben. Hierdurch wird das Online-Portal für Geschäftsprozesse des normalen Schutzbedarfs freigeschaltet.
Entsprechend den festgelegten datenschutzrechtlichen Sicherheitsanforderungen kann innerhalb des Online-Portals eine zusätzliche Authentifizierungsabfrage für „höherwertige“ Geschäftsprozesse notwendig werden (vgl. Ziffer 3.2.3.1).

Die SV-Träger dürfen nur eine einmalige Nutzung des Freischaltcode zulassen. Lässt der Nutzer die Frist zur Ersteingabe verstreichen, muss er einen neuen Freischaltcode vom SV-Träger anfordern.

Die SV-Träger haben die technischen Voraussetzungen dafür zu schaffen, dass sowohl der von ihnen zu vergebene **Freischaltcode** als auch das vom Nutzer festzulegende **Passwort** für den Online-Zugang die in den IT-Grundschutzkatalogen des BSI enthaltenen Vorgaben erfüllen, u.a.

- Mindestlänge (8 Zeichen)
- Kombination aus Buchstaben, Ziffern und Sonderzeichen
- Keine Trivialnamen/-Ziffern.

Passworte, die diese Kriterien nicht erfüllen, müssen bei der Eingabe/Änderung (online) abgewiesen werden.

Der SV-Träger hat ferner festzulegen, nach wieviel Fehleingaben des Passwortes der Zugang zum Online-Portal für diesen Nutzer gesperrt wird. Üblich sind hier maximal fünf Versuche.

Bei Übermittlung von Daten der Schutzklasse „hoch / sehr hoch“ können weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel erforderlich sein (siehe Ziffer 3.2.3.1).

#### 3.2.3.3 „Einmal-Kennwort-Verfahren“

Für Versicherte, die den vollen Funktionsumfang einer Online-Geschäftsstelle (noch) nicht nutzen, aber z. B. bei einzelnen Fragebogenaktionen die Antwortdaten online übermitteln möchten, bietet sich das „Einmal-Kennwort-Verfahren“ an. Die versicherte Person erhält auf dem Postweg ein Einmalpasswort, über das nur ein festgelegter Vorgang aufgerufen werden kann. Dies ermöglicht einen alternativen Zugang, ohne dass ein o.a. „Benutzer-Konto“ angelegt wird.

Das Einmal-Kennwort muss vom SV-Träger individuell für jede versicherte Person erzeugt werden. Es muss sichergestellt sein, dass das gleiche Kennwort nicht mehrfach für verschiedene Versicherte erzeugt wird. Die entsprechenden Vorgaben zur Generierung von Kennwörtern gemäß den IT-Grundschutzkatalogen des BSI sind zu beachten.

Das Einmal-Kennwort ist den Versicherten postalisch zu übermitteln (Zwei-Wege-Authentifizierungsverfahren), in welchem das Eingabeverfahren beschrieben werden sollte. Ferner ist über die festgelegte Gültigkeitsdauer des Kennwortes (max. 60 Tage)und dessen Verfall zu informieren, sobald die versicherte Person den damit verbundenen Online-Geschäftsprozess vollständig durchgeführt hat. Wird der mit dem Kennwort verknüpfte Eingabeprozess vorzeitig abgebrochen, sollte das Kennwort für eine Wiederaufnahme weiter genutzt werden können.
Die vergebenen Einmal-Kennwörter sind beim SV-Träger in einer geschützten Datenbank solange zu speichern, bis der dazugehörige Prozess abgearbeitet wurde oder die Verfallfrist abgelaufen ist. Es ist sicherzustellen, dass die Sachbearbeitung zu keinem Zeitpunkt Einblick in das Einmal-Kennwort hat.

Bei Übermittlung von Daten der Schutzklasse „hoch / sehr hoch“ können weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel erforderlich sein (siehe Ziffer 3.2.3.1).

#### 3.2.3.4 Authentifizierung bei Nutzung von Apps

Auch bei der elektronischen Kommunikation über Apps sind die allgemeinen Anforderungen zur Sicherung des Zugangs zur Kommunikation anzuwenden. Dies gilt insbesondere bei Übermittlung sensibler Daten.

Entsprechend der Schutzbedarfsfeststellung / Risikoanalyse (siehe Ziffer 3.1.5) sind die Anforderungen entsprechend dem Schutzbedarf der elektronischen Kommunikation auszugestalten:

- Für eine Authentifizierung bei einer Online-Geschäftsstelle über eine App gelten die Ausführungen zur Online-Kommunikation.
- Bei einer Kommunikation mit dem App-Server hat bei der Erstanmeldung zum System mindestens eine Zwei-Wege-Authentifizierung zu erfolgen. Dies kann auf folgendem Weg geschehen:
  - Erstidentifikation“ am Server
  - Mitteilung der Zugangsdaten über Post
  - Die Authentifizierung am App-Server erfolgt über die per Post mitgeteilten Geheimnisse / Zugangsdaten.
- Bei Übermittlung von Daten der Schutzklasse „hoch / sehr hoch“ sind weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel erforderlich.
- Für einfache Datenabrufe ohne personenbezogene Daten über einen App-Server empfehlen die Prüfdienste eine Nutzung der App ohne Anmeldung zu ermöglichen.

Die Mindestanforderungen für alle Fälle der Appkommunikation sind:

- Die App darf keine nutzerbezogenen Daten ungesichert auf dem Gerät speichern. Diese Daten sind auf dem Appserver gesichert vorzuhalten.
- Während der Nutzung der App gespeicherte Daten sind in einem gesicherten Bereich abzuspeichern.

## 3.3 Behandlung der Online-Daten und Daten mittels Apps

### 3.3.1 Datenumfang und Dokumentation

Zur Übermittlung der von Versicherten eingegebenen Daten ist vor Beginn der Eingabe eine verschlüsselte Verbindung zwischen dem Eingabegerät und dem Server des SV-Trägers aufzubauen. Für Daten mit einem normalen Schutzbedarf ist eine SSL-Verschlüsselung ausreichend. Bei den im Rahmen der Schutzbedürftigkeit als „hoch“ oder „sehr hoch“ zu bewertenden Daten (s. Ziffer 3.2.3.1) muss der SV-Träger entscheiden, ob hierbei zusätzliche Schutzmaßnahmen zu nutzen sind. Mindestens sind Schutzmaßnahmen zu ergreifen, die dem jeweils aktuellen Stand der Technik entsprechen, und deren kryptographische Verfahren eine angemessene Sicherheit bieten.

Der SV-Träger hat einen Nachweis darüber zu führen, dass die Daten durch die Versicherten übermittelt wurden (Authentifizierung, Nichtabstreitbarkeit), wann sie in seinen Zugangsbereich gelangt und dass sie dort nicht verändert worden sind (Integrität). Die empfangenen Daten lassen sich unterteilen in Nutzdaten und Metadaten:

<u>Nutzdaten</u> sind die von den Versicherten während des Online-Prozesses eingegebenen Angaben. Sie sind – zusammen mit der entsprechenden Frage / Bezeichnung des Eingabefeldes – zu speichern (Hinweis: Die Speicherung der <u>Frage</u> ist als Kurzform/Schlagwort möglich).

Metadaten sind systemseitig erzeugte Zusatzdaten, anhand derer der SV-Träger belegen kann, dass die Nutzdaten durch die Versicherten erzeugt wurden. Hierzu gehören insbesondere

- eindeutiges Identifizierungsmerkmal der versicherten Person (ggf. auch Benutzername)
- Eingabeweg (Benutzer-Konto oder „Einmal-Kennwort-Verfahren“)
- Systemzeit der Übermittlung der Daten (Datum, Uhrzeit)

Sowohl die im Online-Prozess erhobenen Nutzdaten als auch die Metadaten sind in einer Datendatei zu speichern. Diese Datei muss bei späteren Prüfungen (z.B. RSA-Prüfung) maschinell ausgewertet werden können. Hierzu ist es erforderlich, dass die Speicherung in einem zukunftssicheren Datenformat erfolgt. Das BSI empfiehlt hierzu u.a. das XML- oder csv-Format. Aber auch eine Speicherung als Textdatei (mit einheitlichem Trennzeichen) wäre für die Prüfdienste auswertbar. Der Satzaufbau ist einheitlich zu gestalten. Fragen, die der/die Versicherte nicht beantworten muss, sind trotzdem aufzuführen und das Ergebnisfeld mit „blank“ versehen sein.

Neben dieser Datendatei sollte der SV-Träger aus den generierten Antworten ein PDF-Dokument erstellen, welches sich der/die Versicherte anzeigen und herunterladen kann. Auch dieses muss die Nutz- und die Metadaten enthalten.

### 3.3.2 Integritätsschutz

Die unter Ziffer 3.3.1 aufgeführten Dateien (Daten- und PDF-Datei) sind unmittelbar nach ihrer Erzeugung gegen einen möglichen Integritätsverlust zu schützen. Dies kann automatisiert durch folgende Verfahren erfolgen:

- Automatische Anbringung einer QES.
- Automatische Anbringung eines qualifizierten elektronischen Zeitstempels eines akkreditierten Zertifizierungsdiensteanbieters.
- Automatische Anbringung einer fortgeschrittenen Signatur gem. SigG.
- Automatische Anbringung einer PGP-Signatur, die mit einem ausreichend sicheren Schlüssel erzeugt wurde.

Der SV-Träger hat bei der Entscheidung über die Wahl des Integritätsschutzes die Grundsätze der Wirtschaftlichkeit zu beachten. Eine Nutzen-/Kosten-Analyse ist bei der Anzeige des Verfahrens der Aufsichtsbehörde vorzulegen.

### 3.3.3 Revisionssichere Archivierung

Die unter Ziffer 3.3.1 aufgeführten Dateien (Daten- und PDF-Datei) müssen 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.

Die Datensätze müssen während der Aufbewahrungsfristen lesbar gemacht bzw. für eine Auswertung über Prüftools zur Verfügung gestellt werden können.

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 beweis-

werterhaltende Archivierung elektronischer Daten / Dokumente zu berücksichtigen (siehe Ziffer 6.4).

### 3.3.4 Apps

Die unter den Ziffern 3.3.1 bis 3.3.3 genannten Anforderungen gelten ebenso für mittels Apps an einen Appserver übermittelte Daten und auf diesem Kommunikationsweg beigefügte Dokumente.

Die Prüfdienste empfehlen, die Software und Datenströme vor der Entwicklung zu beschreiben und die damit in Verbindung stehenden Anforderungen an Datenschutz, Datensicherheit, Integritätsschutz, Dokumentation und Speicherung in einer Verfahrensdokumentation festzuhalten.

Als Mindestanforderung an die Sicherung der Übermittlungswege ist die Absicherung der Kommunikationsverbindung App / back-end durch eine geeignete Transportverschlüsselung vorzusehen.

Die Datenintegrität auf dem Transportweg und bei der Speicherung ist zu gewährleisten. Nach erfolgter Schutzbedarfsanalyse sollten bei hohem / sehr hohem Schutzbedarf auch kryptographische Maßnahmen vorgesehen werden.

## 3.4 Elektronische Einreichung von Nachweisen

### 3.4.1 Einreichung durch die 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 SV-Träger verlangt – nach pflichtgemäßem Ermessen – für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals.

In der Verwaltungspraxis wird bereits heute häufig die Vorlage von (nicht beglaubigten) 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.

Die Anforderungen an die bildliche und textliche Übereinstimmung (siehe Ziffer 5.1.2) sind auch an dieser Stelle entsprechend heran zu ziehen.

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

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

Die durch Versicherte übermittelten elektronischen Nachweise sind vom SV-Träger gegen Integritätsverlust zu schützen und revisionssicher zu archivieren.

### 3.4.2 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 Verwaltungsverfahrens erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit Einwilligung des Verfahrensbeteiligten (die Versicherten) 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 (Versicherte / Mitglieder) zu erheben[9]. 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.

## 3.5 Elektronischer Posteingang

### 3.5.1 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 dem SV-Träger auf einem „Stand-alone-Faxgerät“ eingehen und ausgedruckt werden, müssen – sofern der Absender keine Header-Informationen mitgesandt hat – mit einem Eingangs- und Faxstempel gekennzeichnet werden. Derartige Dokumente werden von den Prüfdiensten uneingeschränkt anerkannt, sofern

- das ausgedruckte Fax archiviert wird, oder
- die Ausdrucke 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.

[9] „Erheben“ ist das Beschaffen von Daten über den Betroffenen (§ 67 Abs. 5 SGB X).

**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/eine Mitarbeiterin 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 Ziffer 6.2)

**Hinweis**:
Das unter b) beschriebenen Verfahren 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:

- Die Faxserver befinden sich in einer gesicherten Umgebung. Zugriff hat ausschließlich der zuständige Administrator.
- 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.
- Die jeweils zuständigen Beschäftigten (Fax-Server-Admin, Sachbearbeiter) verfügen über keine Bildbearbeitungssoftware, mit der der Faxinhalt verändert werden könnte.

### 3.5.2 Speicherung eingehender E-Mails im elektronischen Langzeitarchiv

Grundsätzlich müssen elektronisch bei dem SV-Träger eingehende Nachrichten/Dokumente, die eine rechtliche Wirkung entfalten, im elektronischen Langzeitarchiv gespeichert werden (§ 110a 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 Verwaltungsverfahrens 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-)Beschäftigten 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. Der Integritätsschutz kann auch über die in Ziffer 3.3.2 aufgeführten alternativen Sicherungsmittel erreicht werden.

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 die Sachbearbeitung) 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).

**Hinweis**:
Die an diesen Dokumenten angebrachte QES dient ausschließlich dem Integritätsschutz des Dokumentes.

### 3.5.3 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. Das Anbringen einer neuen „Eingangssignatur“ durch den SV-Träger ist nicht erforderlich.

Es wird ausdrücklich darauf hingewiesen, dass die durch den De-Mail-Dienstanbieter angebrachte QES ausschließlich dem Integritätsschutz des Dokumentes dient.

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 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 durch die Sachbearbeitung angebrachte QES ausschließlich dem Integritätsschutz des Dokumentes dient.

## 3.6 Elektronischer Postausgang

### 3.6.1 Grundsätze

Für den Bereich der gesetzlichen Sozialversicherung gilt grundsätzlich das Prinzip der Formfreiheit. So kann der **Erlass 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 und ggf. Abs. 5 SGB X genannten Anforderungen (Erkennbarkeit der erlassenden Behörde) gewahrt werden. Dementsprechend kann z.B. bei einer Postausgangssignatur auf die QES 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 die Pflicht zur Langzeitspeicherung andere Zielsetzungen als beim VA-Erlass. Es geht nicht um die rechtssichere Bekanntgabe gegenüber dem Adressaten, sondern um die zuverlässige Langzeitspeicherung von Unterlagen.

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 zukommt und zumindest die Möglichkeit besteht, dass ihr Inhalt ggf. gerichtlich dargelegt oder sogar bewiesen werden muss.

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, Faxe) sondern nur inhaltlich erfolgen.

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

E-Mails bzw. deren Anhänge müssen – sofern sie beweiswerterhaltende Inhalte haben – mit der QES eines/einer verantwortlichen Beschäftigten (Einzelsignatur) versehen und im Langzeitarchiv bzw. unverändert und unveränderbar mit den erforderlichen Eingangsdaten in einem revisionssicheren Speichersystem gespeichert werden.

### 3.6.3 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-Diensteanbieter 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-Diensteanbieter angebrachten QES handelt es sich nicht um eine Willenserklärung des Absenders. Eine solche ist jedoch gemäß den Regelungen aus §§ 110a SGB IV i. V. m. der Anlage zu § 78a SGB X für die revisionssichere Speicherung beim KV-Träger zwingend erforderlich. Daher gelten die in Ziffer 3.5.1 dargestellten Grundsätze.

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

### 3.6.4 Erstellung und Versand von Serienbriefen

Im Rahmen von elektronischen Workflows ist es üblich, Serienbriefe unter Verwendung vorgefertigter Textbausteine, z. B. als Bescheide, zu versenden. Aufgrund der Regelungen in § 110a SGB IV ist zu empfehlen, 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 Versicherte) bildlich übereinstimmt. Das bedeutet, dass die elektronische „Durchschrift“ z. B. unter Aufführung der verwendeten Text-

bausteinnummern 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 SV-Träger vorgesehenen Verfahren ist die Vorlage von ausführlichen und 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

- zu Art und Umfang,
- zur 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 ( u.a. Eröffnung eines Zugangs gem. EGovG),
- 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 Satz 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 alle Beschäftigten
- 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 Beschäftigten*

- 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 Beschäftigte 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 Satz 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 Satz 3 Nr. 2 und 3 SigG durch eine die Bestätigung und qualitätssichernde Prüfung der Sicherheitsanforderungen insgesamt abdeckende Herstellererklärung ersetzt werden.

Denn genauso, wie erstere geprüfte Produkte nach § 17 Abs. 1 Satz 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 Satz 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, etc.) 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 herstellererklärter 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 erstellter 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 Signaturverordnung (SigV)

<u>Neusignierung von Elektronischen Signaturen</u>
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 SiG 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 zugrundeliegenden 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 eine **Beweiswirkung zu erhalten,** haben die SV-Träger rechtzeitig eine **Nachsignatur** zu veranlassen**.**

Nehmen SV-Träger 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 SV-Träger 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, oder Informationen zu übermitteln. Es handelt sich in der Regel um einen geschützten Bereich des Internetauftritts des SV-Trägers, zu dem die Versicherten sich – nach vorheriger Registrierung an ihrem „Konto“ anmelden können. Jede Verbindung über das Internet ist durch eine Transportverschlüsselung zu schützen. Die eingesetzte Transportverschlüsselung ist regelmäßig darauf hin zu prüfen, ob sie dem aktuellen Stand der Technik entspricht und den Sicherheitsanforderungen zum Schutz von Sozialdaten genügt. Die Anforderungen der Anlage des § 78a SGB X, des §13 Abs. 7 TMG sowie des „Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden“ sind zu beachten.

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

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

Nähere Ausführungen hierzu sind der Ziffer 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-Dienste-anbieter 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.

Nähere Ausführungen hierzu sind der Ziffer 3.2.2.3 zu entnehmen.

# 5 Übertragung und Vernichtung des Papieroriginals

Das Übertragen von Papierdokumenten in die elektronische Form ist in § 110a SGB IV geregelt. Dieser Paragraph gilt als spezialrechtliche Norm vorrangig gegenüber der in § 7 EGovG enthaltenen Regelung. Ergänzend enthält das EGovG Hinweise darauf, wie das Scanverfahren technisch und organisatorisch auszugestalten ist, nämlich nach dem „Stand der Technik“. Dieser kann sich z.B. aus Richtlinien des BSI ableiten (siehe Minikommentar des BMI zu § 7 EGovG).

Die Technische Richtlinie „Ersetzendes Scannen“ [BSI TR-03138 (RESISCAN)] (nachfolgend: TR) 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.

Die nachfolgend aufgeführten Anforderungen an den Scanprozess leiten sich grundsätzlich aus dieser Richtlinie ab.

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.

## 5.1 Scannen von Papierdokumenten

Der § 110a SGB IV regelt, wie mit Papierdokumenten zu verfahren ist, die gescannt werden sollen. Diese sind durch ein maschinelles Scanverfahren in elektronische Dokumente zu übertragen. Hierbei sind folgende Besonderheiten zu beachten:

### 5.1.1 Klassifizierung der Papierdokumente

Der SV-Träger hat für die einzuscannenden Dokumente eine fachliche Schutzbedarfsanalyse zu erstellen, in der hinsichtlich der Schutzziele „Integrität“, „Vertraulichkeit“ und „Verfügbarkeit“ eine Klassifizierung vorzunehmen ist. Die TR-RESISCAN schlägt hier eine dreistufige Aufteilung in „normal“, „hoch“ und „sehr hoch“ vor.

Während für ein als „normal“ klassifiziertes Dokument einfache technisch-organisatorische Schutzmaßnahmen im Scanprozess implementiert werden müssen, fordert die TR für „hoch“ und „sehr hoch“ eingestufte Dokumente die Anwendung kryptographischer Sicherungsmittel.

Für den SV-Träger bedeutet dies, dass er unterschiedliche technisch-organisatorische Verfahren für jede Dokumentenklasse einführen müsste. Aufgrund des hohen Aufwandes erscheint eine solche Lösung nicht wirtschaftlich.

Die Prüfdienste empfehlen daher, das Scanverfahren so zu gestalten, als seien nur Dokumente mit Schutzbedarf „sehr hoch“ zu scannen. Nähere Ausführungen zu den Anforderungen an ein solches Scanverfahren sind der TR-RESISCAN und ihren Anhängen zu entnehmen.

### 5.1.2 Bildliche und inhaltliche Übereinstimmung

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 Farbabbildung mit qualifizierter elektronischer Signatur urkundliche Beweiskraft besitzt.

Die Prüfdienste des Bundes und der Länder sind der Auffassung, dass die 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 <u>mit allen Formatierungszeichen</u> 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 farbige 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 auch zu scannen. 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 Einscanvorgang (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.

Die Anforderungen gelten auch für über Apps erstellte Abbilder und deren Übermittlung sowie Speicherung beim SV-Träger.

## 5.2 Dokumentation des Scan-Vorgangs

Bis zum 31.12.2015 war in § 110d SGB IV geregelt, dass die beim Scan-Vorgang erzeugten Images vom Scan-Operator mit einer qualifizierten elektronischen Signatur (QES) signiert werden mussten. Nur dann konnte nachgewiesen werden, dass das Original vorlag und in die elektronische Form übertragen wurde.

Nach Wegfall der o.g. Vorschrift besteht gleichwohl die Notwendigkeit, festzustellen, wer das Dokument in die elektronische Form übertragen hat. Eine rechtliche Verpflichtung hierzu ergibt sich aus der Anlage zu § 78a SGB X. Darin heißt es:

> „Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten geeignet sind,
> …
> 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),...“

Wie bereits in Ziffer 5.1.1 beschrieben, wird empfohlen, alle einzuscannenden Papierdokumente mit dem Schutzbedarf „sehr hoch“ zu klassifizieren und die daraus resultierenden Anforderungen gem. TR-RESISCAN umzusetzen. Hierzu gehört u.a.

- die Protokollierung, wer das Scansystem wann und in welcher Weise genutzt hat und
- der Einsatz kryptographischer Sicherungsmittel, z.B. der qualifizierten elektronischen Signatur.

Die Prüfdienste empfehlen daher eindringlich, auch nach Wegfall des § 110d SGB IV beim Scannen von Papierdokumenten weiterhin die QES als Sicherungsmittel (Integritätsschutz)

zu verwenden. Hierdurch wird gleichzeitig dokumentiert, wer die Übertragung des Dokumentes in die elektronische Form wann durchgeführt hat.

## 5.3 Formen der Signatur

### 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.

Die Prüfdienste empfehlen, unter Berücksichtigung von § 7 EGovG, dass der Signiervorgang grundsätzlich zeitlich und räumlich in unmittelbarem Zusammenhang mit dem Einscannen erfolgt. Die Signatur darf hierbei nur von der Person angebracht werden, die das Dokument auch in die elektronische Form überführt hat („Stapelsignatur“).

Alternativ dazu besteht die Möglichkeit, 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 eine voll umfängliche (100 v. H.) Prüfung erfolgt.

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[10] 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:

## 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 Beleglesung)
- 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.

[10] Begründung zum Entwurf einer Verordnung zur elektronischen Signatur in der Fassung des Kabinettbeschlusses 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.

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 beinhalten, 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 Sperrlisten 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 <u>ein</u> auf der Rückseite befindliches Zeichen ein automatisches Löschen ausschließt.

Die Anbringung eines elektronischen Eingangsstempels durch die Scansoftware ist zulässig. Nach dem Einscanvorgang 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.

## 5.4 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.

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 Beschäftigten.

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

### 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) 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.

§ 110a Abs. 2 SGB IV spricht von „dauerhaften 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 Revisionssicherheit der signierten Dokumente gewährleistet. Die Möglichkeit des physikalischen Löschens nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist muss vom SV-Träger in der Dienstanweisung 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-Passworten 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.

## 5.5 Technische Richtlinie TR03138 („TR-RESISCAN“)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 17.04.2013 die Technischen 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.

## 5.6 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. Frühester 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 herangezogen 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. Die Einstufung muss sich aus wirtschaftlichen / organisatorischen Gründen immer nach dem zu vernichtenden Gut richten, welches der höchsten Schutzklasse angehört.

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 Weisungen 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“ der 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 Beschäftigten erzeugten elektronischen Dokumente, die elektronisch (und / oder in Papierform) an Externe versandt wurden (auch elektronische Faxe)
- Vom SV-Träger oder seinen Beschäftigten 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 – c SGB IV i. V. m. den Grundsätzen ordnungsgemäßer Aufbewahrung.

Darüber hinaus gibt es technische und / oder organisatorische Vorgaben zu IT-Sicherheit / Datenschutz wie z.B. § 78a SGB X einschl. der Anlage (sog. „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.
- 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 elektronischer Post

Entsprechend dem Grundsatz der „Aktenmäßigkeit“ müssen Nachrichten / Dokumente, die elektronisch beim SV-Träger eingehen und die eine rechtliche Wirkung entfalten, grundsätzlich im elektronischen Langzeitarchiv gespeichert werden. Dies gilt nach dem ausdrücklichen Willen des Gesetzgebers für alle Unterlagen, also auch für elektronische Verwaltungsakte. Die Anforderungen zum Posteingang und zum Postausgang sind unter den Ziffern 3.5 und 3.6 beschrieben.

Eine Aufbewahrung und Langzeitspeicherung von Dokumenten in elektronischer Form ohne qualifizierte elektronische Signatur (QES) ist aufsichtsrechtlich bedenklich, da die Möglichkeit besteht, dass ihr Inhalt angezweifelt wird und ggf. gerichtlich dargelegt oder sogar bewiesen werden muss. 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 werden muss.

## 6.3 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 1.2 vom 19.12.2014) ein Dokument zur Verfügung gestellt, das Orientierung und Hilfestellung gibt, um den vielfältigen Anforderungen hinsichtlich

- Verfügbarkeit und Lesbarkeit,
- Integrität und Authentizität sowie
- 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 revisionssicheren 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.

## 6.4 Besonderheiten

### 6.4.1 Aufbewahrung von Fehler- / Bearbeitungslisten

Fehler- / Bearbeitungs- / Kontrolllisten möchten viele SV-Träger nicht mehr in Papierform ablegen, sondern in elektronischer Form speichern. Sofern diese Listen in den Grundsätzen ordnungsmäßiger Aufbewahrung aufgeführt sind, müssen sie aufbewahrt werden. Ansonsten ist eine Aufbewahrung in das Ermessen des SV-Trägers gestellt; er 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) ist aufsichtsrechtlich bedenklich, da die Möglichkeit besteht, dass ihr Inhalt angezweifelt wird und ggf. gerichtlich dargelegt oder sogar bewiesen werden muss.

### 6.4.2 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 Verwaltungsverfahrens 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 SV-Träger 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 5.4). 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, JSON) 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 hat der GKV-Spitzenverband in Zusammenarbeit mit der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherungen 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:
  - Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels File-Transfer-Protocol FTP
  - Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels http und https
  - Spezifikation der Schnittstellen für die Übermittlung von Nachrichten im XML-Format
  - 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.

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; XML, JSON) 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 „Beweiswerterhaltung kryptographisch signierter Dokumente“

(Version 1.2 vom 19.12.2014)

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

| Abschnitt aus TR-ESOR | Thema: | Anforderungen: | Fundstelle: |
|---|---|---|---|
| | | | |
| **4.3.1** | Integritätssicherung nicht signierter Daten | Die Integrität nicht signierter Daten ***muss*** 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>*Handelt es sich um rechtlich bedeutsame Dokumente bzw. erfordert die Art der Daten eine revisionssichere Archivierung, so **müssen** diese mit einer QES versehen im Langzeitspeicher abgelegt werden.* | §§ 110a ff. SGB IV |
| **5** | **Funktionen einer Middleware zum Beweiswerterhalt** | | |
| **5.1.1** | **Archivierung signierter und unsignierter Daten** | | |
| **(A5.1-4)** | Konformitätsprüfung der Datenformate | Die Middleware **muss**[11] 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 **muss** dann die Ablage im ECM/Langzeitspeicher abgelehnt werden. | |
| **5.2** | **Organisatorische Anforderungen** | 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.[12] | |
| **6** | **Abgeleitete technische Anforderungen** | 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. | |

[11] Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.2 vom 19.12.2014).

[12] 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-Middlware ***muss***[13] 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 **müssen**[14] 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** | **IT-Infrastruktur** | Die nachfolgend genannten technischen Sicherungsmaßnahmen für die TR-ESOR-Middleware und für das gesamte Archivsystem 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.[15]<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. | |

[13] Bei IT-Dienstleistern/RZ, die für mehrere SV-Träger tätig sind, **muss** eine entsprechende Trennung der Daten erfolgen!

[14] Änderung als Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.2 vom 19.12.2014)

[15] Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

| Abschnitt aus TR-ESOR | Thema: | Anforderungen: | Fundstelle: |
|---|---|---|---|
| | | | |
| **6.5** | **IT-Anwendungen beim Einsatz von Archivierungsverfahren** | Neben Anforderungen an die IT-Infrastruktur und natürlich der TR-ESOR-Middleware **müssen** auch diverse Anforderungen an die vorgelagerten Fachanwendungen gestellt werden.<br>Dieses Kapitel versteht sich als Hinweis an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest.[16]<br><br>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. | |
| **6.5** | Trusted Viewer | • Für die Anzeige von qualifiziert signierten elektronischen Daten und Dokumenten ***muss***[17] die Anwendung oder die Anwendungsumgebung eine bestätigte vertrauenswürdige Anzeigekomponente (Trusted Viewer) zur Verfügung stellen. Die Bestätigung **muss** durch eine anerkannte Bestätigungsstelle gemäß §18 SigG erfolgen. | |
| **8** | **IT-Sicherheitskonzept** | | |
| **8.2** | **Maßnahmen** | 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.<br><br>Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware bzw. eines ECM / Langzeitspeichers und legt keine formalen Kriterien fest.[18] | |

[16] Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

[17] SV-Träger muss in der Lage sein, die Signatur von Dokumenten/Daten zu überprüfen.

[18] Abweichend zur TR-ESOR können im Bereich der Sozialversicherungsträger formale Anforderungen Muss-Kriterien sein.

| Abschnitt aus TR-ESOR | Thema: | Anforderungen: | Fundstelle: |
|---|---|---|---|
| | | | |
| | | HINWEIS:<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. | |
| **8.2.1** | Übergreifende Maßnahmen | 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.<br><br>Das IT-Sicherheitskonzept **muss** regelmäßig (z. B. einmal pro Jahr) auf den aktuellen Stand gebracht werden.<br><br>Die Maßnahmen, die sich aus dem IT-Sicherheitskonzept und dessen Überarbeitung ergeben, **müssen** - soweit wirtschaftlich vertretbar[19] - zeitnah umgesetzt werden. Dies gilt insbesondere für die Definition und Umsetzung der Verantwortlichkeiten und Kompetenzen, der fachlichen Prozesse sowie sicherer Administrations- und Kontrollprozesse.<br><br>Insbesondere für Einrichtungen, Organisationen und Unternehmen der öffentlichen Verwaltung **soll** 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. | |

[19] Wirtschaftliche Aspekte sind nachrangig, wenn rechtliche Vorgaben (z. B. der „UP Bund“) eine zeitnahe Umsetzung fordern.