

Die Prüfdienste des Bundes
und der Länder informieren

Langzeitspeicherung elektronischer Daten

Version 3.5
Stand: 14.11.2011

Inhalt:

Vorwort	4
1 Rechtsgrundlagen	5
2 Hinweise und Definitionen	7
2.1 Definition „Elektronische Signaturen“	7
2.2 Anforderungen an elektronische Signaturen.....	7
2.3 Unterschied zwischen „Elektronischer Signatur“ und „Verschlüsselung“	7
2.4 Stapelsignaturen	8
2.5 Zeitstempel.....	8
2.6 Langzeitspeicherung - Beweiswerterhalt durch Neusignierung	8
2.7 Normierung bei elektronischen Signaturen	13
2.8 Sonderformen der elektronischen Signatur.....	13
2.8.1 Unterschrift auf einem elektronischen Pad	13
3 Vorgehensweise bei der Einführung	14
3.1 Wirtschaftlichkeitsbetrachtung/Geschäftsprozessanalyse	14
3.2 Umsetzung/Ausschreibung	15
3.3 Anzeige an die Aufsichtsbehörde.....	15
4 Elektronische Langzeitspeicherung papiergebundener Dokumente	16
4.1 Verfahrensbeschreibung.....	16
4.2 Dienstanweisung	16
4.3 Scanverfahren	17
4.4 Regelungen für das Kartenmanagement	19
4.5 Signaturerstellungseinheiten und Signaturanwendungskomponenten.....	19
4.6 Sicherheit, Betriebssystem und Netzwerk.....	20
4.7 Stapelsignaturverfahren	22
4.8 Neusignieren nach § 17 SigV	25

4.9	Vernichtung von Originalbelegen	27
4.10	Grundsätze zu Aufbewahrung/Fristen/Reproduktion/Löschung.....	28
4.11	Übernahme von Altbeständen	29
4.12	Übergangsregelungen	29
5	Langzeitspeicherung elektronisch erzeugter Dokumente	31
5.1	Qualifizierte elektronische Signatur von elektronischen Postausgängen.....	31
5.2	Rechtssichere Langzeitspeicherung von elektronischen Postausgängen	32
5.3	Rechtssichere Langzeitspeicherung von elektronischen Posteingängen	32
5.4	Besonderheiten.....	33
5.4.1	Erstellung und Versand von Serienbriefen.....	33
5.4.2	Aufbewahrung von Fehler-/Bearbeitungslisten.....	33
5.4.3	Aufbewahrungsfrist von Einzeldokumenten in eAkten/Vorgängen	33
5.4.4	Behandlung eingehender Fax-Sendungen.....	33
5.4.4.1	Analog-/Papier-Faxe.....	33
5.4.4.2	Elektronische Faxe.....	34
6	Elektronischer Datentransfer	35
6.1	Ergänzende rechtliche Grundlagen.....	36
6.2	Speicherung des Originaldatensatzes.....	37
6.3	Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung)	38
7	Anforderungen an die elektronische Langzeitspeicherung	39
7.1	Besonderheiten / Abweichungen zur TR 03125	39
8	Glossar	40
9	Anlagen	43
9.1	Zusammenfassung: Behandlung elektronischer Dokumente.....	43

Vorwort

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 Aufbewahrungsverfahren und der Einbeziehung der elektronischen Vorgangsbearbeitung.

Dieser Leitfaden beinhaltet

- die Verwendung von qualifizierten elektronischen Signaturen,
- den Transfer von elektronischen Melde- und Abrechnungsdaten (in Datensatzform) sowie
- die elektronische Langzeitspeicherung.

Er beschreibt die Anforderungen entsprechend den gesetzlichen Vorschriften und die Rechtspositionen der Aufsichtsbehörden und Prüfdienste nach § 274 SGB V.

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

Das Handbuch wird von den Prüfdiensten des Bundes und der Länder laufend gepflegt und weiter entwickelt. Es wird als Grundlage für die Beurteilung dieser Verfahren angewandt.

Den Sozialversicherungsträgern wird empfohlen, ihre Verfahren entsprechend den Ausführungen in diesem Handbuch zu gestalten.

Herausgeber:

ADV-Arbeitsgemeinschaft
Geschäftsstelle im Ministerium für
Gesundheit, Emanzipation,
Pflege und Alter des Landes
Nordrhein-Westfalen
Kopstadtplatz 13
45127 Essen
Tel.: 0201/8134-0

E-Mail: adv-ag@mgepa.nrw.de

Bundesversicherungsamt
Abteilung K
Prüfdienst Krankenversicherung
Friedrich-Ebert-Allee 38
53113 Bonn
Tel.: 0228/619-0

Ansprechpartner:
Peter Fischer
Referat K 3 (Außenstelle Cloppenburg)
Tel.: 04471/1807-16
E-Mail: peter.fischer@bva.de

1 Rechtsgrundlagen

Wesentlich sind die folgenden Gesetze bzw. Verordnungen:

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.05.2001 i.d.F. vom 17.07.2009
- Verordnung zur Elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 i.d.F. vom 17.12.2009
- SGB I - Sozialgesetzbuch, Erstes Buch -
 - o § 36a (Elektronische Kommunikation)
- SGB IV – Sozialgesetzbuch, Viertes Buch -
 - o § 69 Abs. 2 (Wirtschaftlichkeit und Sparsamkeit)
 - o § 110a (Aufbewahrungspflicht)
 - o § 110b (Rückgabe, Vernichtung und Archivierung von Unterlagen)
 - o § 110c (Verwaltungsvereinbarungen, Verordnungsermächtigung)
 - Vereinbarung der Spitzenverbände der Krankenkasse zu den Grundsätzen ordnungsgemäßer Aufbewahrung im Sinne des § 110a SGB IV, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen (Stand: 23.06.2008)
 - Ergänzende Vereinbarung der Spitzenverbände der Krankenkassen zur Rückgabe und Vernichtung von Unterlagen (Stand: 23.06.2008)*
 - o § 110d (Beweiswirkung)
- SGB V – Sozialgesetzbuch, Fünftes Buch –
 - o § 274 (Prüfung der Geschäfts-, Rechnungs- und Betriebsführung)
- SGB X – Sozialgesetzbuch, Zehntes Buch –
 - o § 9 (Nichtförmlichkeit des Verwaltungsverfahrens)
 - o § 33 (Bestimmtheit und Form des Verwaltungsaktes)
- Verordnung über das Haushaltswesen in der Sozialversicherung (SVHV) – vom 21.12.1977, i.d.F. vom 19.12.2007 (BGBl I S. 3024)
 - o § 22 (Öffentliche Ausschreibung)
- Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (SVRV) – i.d.F. vom 17.07.2009 (BGBl I S.2046)
 - o § 7 Abs. 3 (Zahlungsanordnung)
 - o § 17 (Dienstanweisungen)
 - o § 19 (Outsourcing)
- Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV) – i.d.F. vom 10.06.2005 (BAnz. S. 9087)
 - o § 11 (Anordnung der Zahlung)
 - o § 12 (Zahlungsbegründende Unterlagen)
 - o § 20 (Sachliche Feststellung)
 - o § 21 (Rechnerische Feststellung)
 - o § 35 (Aufbewahrungsfristen)
 - o § 36 (Aufbewahrung)
 - o § 40 (Sicherheit bei Einsatz der automatisierten Datenverarbeitung)
 - o § 41 (qualifizierte elektronische Signatur)
 - o § 42 (Outsourcing)

- § 44 (Übergangsregelungen)

*Anmerkungen zu den Vereinbarungen der Spitzenverbände nach § 110c SGB IV (Stand: 23.06.2008):

Die ehemaligen Spitzenverbände der KV-Träger haben den Krankenkassen Empfehlungen für die Mindestdauer der Aufbewahrung gegeben. Gleichwohl sind Anforderungen, wie sie sich z. B. aus § 15a RSAV ergeben, zusätzlich zu berücksichtigen.

Nach § 15a RSAV haben die Prüfdienste die Richtigkeit der gemeldeten Leistungsausgaben, die Personenidentität und das Bezugsjahr zu prüfen. Dies ist zweifelsfrei nur durch Einsicht der Originalbelege oder der mit einer qualifizierten elektronischen Signatur versehenen Images (vom Ursprungsbeleg) möglich. Diese Belege sind für die betroffenen Versicherten entsprechend aufzubewahren. Kann die Krankenkasse den Nachweis in der o. g. Form nicht erbringen, sind die für den RSA gemeldeten Daten ungültig und deshalb aus der Meldung herauszunehmen. Die Krankenkasse trägt somit allein das Risiko.

2 Hinweise und Definitionen

2.1 Definition „Elektronische Signaturen“

Elektronische Signaturen sind von Personen elektronisch erstellte Willenserklärungen oder Bestätigungen. Sie können im eigenen Namen oder im Auftrag erfolgen, sind jedoch immer personengebunden.

Aus technischer Sicht gesehen stellen elektronische Signaturen verschlüsselte Hashwerte dar. Durch erneute Erstellung eines Hashwertes und dessen Vergleich gegen den ursprünglichen Hashwert kann die Integrität von signierten Daten ermittelt und somit eventuelle Veränderungen an Daten bzw. Dokumenten erkannt werden.

2.2 Anforderungen an elektronische Signaturen

Aus den Anforderungen an ein zu signierendes elektronisches Dokument ergeben sich die Anforderungen an elektronische Signaturen.

Im Geschäftsverkehr zwischen den Institutionen sind vom Papier abgeleitet bei Einsatz von elektronischen Signaturen einige Anforderungen an die Signaturen zu beachten:

- Der Unterzeichner muss identifizierbar sein (Authentizität).
- Der Inhalt des Dokuments und das Identifizierungsmerkmal des Unterzeichners gehören zusammen. Eine Person kann die von ihr erstellte Signatur nicht abstreiten (Verbindlichkeit).
- Nachträgliche Veränderungen am Dokument müssen erkennbar sein (Integrität).
- Der Unterzeichner muss den Prozess kontrollieren können.

Soweit nach § 36a Abs. 2 SGB I oder § 41 Abs. 1 SRVwV eine Unterschrift verlangt wird, kann diese ausschließlich durch eine qualifizierte elektronische Signatur eines akkreditierten Zertifizierungsdiensteanbieters nach § 15 SigG geleistet werden. Die hierzu eingesetzten Produkte müssen die in § 17 Abs. 1-3 SigG aufgeführten Eigenschaften besitzen; dies ist gem. § 17 Abs. 4 SigG nachzuweisen.

Bei der Wahl des Speicherformats ist darauf zu achten, dass die umgebenden Systeme die Objekte vor Manipulation schützen. Die Auswahl des Formates wird bestimmt durch

- rechtliche Vorschriften
- technisch-funktionale Kriterien und
- betriebswirtschaftliche Kriterien.

2.3 Unterschied zwischen „Elektronischer Signatur“ und „Verschlüsselung“

Elektronische Signaturen dienen nicht der Geheimhaltung und somit auch nicht der Verschlüsselung von Dokumenten. Sie bieten daher auch keinen Schutz vor Veränderungen signierter Dokumente. Erst mit der Erstellung einer fortgeschrittenen oder einer qualifizierten Elektronischen Signatur wird mit Hilfe eines geheimen Schlüssels (Private Key) der Hashwert (Prüfsumme) der signierten Daten verschlüsselt. Der Hashwert kann mit Hilfe des öffentlichen Schlüssels (Public Key) zu einem späteren Zeitpunkt entschlüsselt und gegen einen neu erstellten Hashwert überprüft werden, um festzustellen, ob das Dokument unverändert vorliegt.

Bei der Verschlüsselung werden Dokumente mit dem Public Key des Empfängers verschlüsselt und können nur mit dessen Private Key wieder entschlüsselt werden.

2.4 Stapelsignaturen

Elektronische Signaturen sind per Gesetz an Personen gebunden und müssen daher einzeln erstellt werden. Allerdings können Ausnahmegenehmigungen erteilt werden, damit elektronische Signaturen auch im Batchverfahren automatisiert erstellt werden können. Dabei ist die Auslösung eines automatisierten Signiervorgangs an die signierende Person gebunden.

2.5 Zeitstempel

Zeitstempel werden technisch wie elektronische Signaturen erzeugt, sind jedoch keine personengebundene Signatur (z. B. Willenserklärung), sondern werden lediglich zum Nachweise dafür genutzt, dass der Inhalt eines elektronischen Dokuments zu einem bestimmten Zeitpunkt vorlag.

Zeitstempel werden entweder online von Zeitstempeldiensten oder von entsprechenden Servern, die im Sinne einer Black Box ins Netz gestellt werden, erstellt. Die Datenstruktur eines Zeitstempels beinhaltet u. a. folgende wesentliche Inhalte:

- Erstellungsdatum und Uhrzeit des Zeitstempels
- Hashwert (Prüfsumme des „gestempelten“ Dokumenteninhalts)

Zeitstempel werden im Allgemeinen durch entsprechende Dienste angeboten, die die aktuelle Uhrzeit gewährleisten. Zeitstempel werden vorrangig automatisiert wie Stapelsignaturen erzeugt.

Qualifizierte Zeitstempel können nur durch freiwillig akkreditierte Zertifizierungsdiensteanbieter und mit gem. § 17 SigG erfolgreich evaluierten und bestätigten Geräten, erzeugt werden.

Zeitstempel können für das Einfrieren eines Dokumentenstatus sowie für die Speicherung von Dokumenten in elektronischen Archiven genutzt werden. Zweck der Stempelung ist der spätere Nachweis des Dokumenteninhalts zum Zeitpunkt seiner Stempelung. Zeitstempel können elektronische Signaturen als Willenserklärung nicht ersetzen.

Zeitstempel dienen auch als Ergänzung zu qualifizierten Signaturen, da mit qualifizierten Signaturen die Signaturerstellungszeit nicht gesichert festgehalten wird. Mit einem Zeitstempel kann der Nachweis geführt werden, dass eine zertifikatsbasierte Signatur vor demjenigen Zeitpunkt erstellt wurde, an dem das Zertifikat ungültig wurde und somit die Verwendung des Private Keys zur Signaturerstellung erlaubt war.

2.6 Langzeitspeicherung - Beweiswerterhalt durch Neusignierung

Der unter diesem Abschnitt folgende Text wurde mit freundlicher Genehmigung der Verlagsgruppe Hüthig Jehle Rehm GmbH aus der Veröffentlichung „Beweiskräftige Elektronische Archivierung- Ergebnisse des Forschungsprojektes AchiSig“, Herausgeber: Roßnagel/Schmücker, ISBN 3-87081-427-6, Abschnitt 3.5.1.2 entnommen:

„Die Signaturverordnung sieht in § 17 SigV ein Verfahren vor, wie und wann diese Neusignierung zu erfolgen hat. Auf europäischer Ebene ist das deutsche Signaturrecht neben dem österreichischen das einzige, das diese Problematik überhaupt aufgreift und normiert. Weder aus dieser noch aus sonstigen Regelungen des Signaturgesetzes oder anderer Gesetze ergibt sich aber eine explizite Rechtspflicht, die Daten bei drohendem Verlust der Sicherheitseignung neu zu signieren. Sie kann sich aber implizit als Amts- oder Vertragspflicht ergeben,

wenn entsprechende Sorgfaltspflichten für die ordnungsgemäße Aufbewahrung als Beweismittel bestehen.¹ Die Erfüllung der Voraussetzungen des § 17 SigV ist nämlich, soweit erforderlich, für die Anwendung des § 371a Abs. 1 Satz 2 ZPO notwendig, da gemäß dieser Bestimmung der positive Verlauf einer Prüfung nach dem Signaturgesetz auch von der weiterhin gegebenen Algorithmeignung abhängt und bei drohendem Verlust die Neusignierung entsprechend dem Verfahren nach § 17 SigV verlangt wird.

Droht der Verlust der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter, so sieht das Signaturrecht in § 17 SigV ein normiertes Verfahren für eine erneute Signatur vor. Danach folgt für die Neusignierung, dass die Daten unter Einbeziehung aller bestehenden Signaturen vorher mit einem qualifizierten Zeitstempel zu versehen und erneut zu signieren sind.

Ein qualifizierter Zeitstempel ist dabei nach § 2 Nr. 14 SigG als elektronische Bescheinigung eines qualifizierten Zertifizierungsdiensteanbieters darüber zu verstehen, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

Wichtig für den Erfolg und die Durchsetzung technischer Konzepte ist ein gemeinsames, einheitliches Verständnis der gesetzlichen Regelungen, die ihnen zugrunde liegen. Die folgende Interpretation des § 17 SigV entspricht dem Sinn und Zweck der Regelung, ist mit deren Wortlaut vereinbar und ermöglicht eine effektive, wirtschaftliche Realisierung der Neusignierung in großen Langzeitspeichersystemen.² Im Folgenden wird die Regelung entsprechend der im Rahmen des Projekts „ArchiSig“ entwickelten Auslegung als These dargelegt. Jeder These folgt eine Kurzerläuterung.

1. Die Beweiswerterhaltung qualifizierter elektronischer Signaturen nach § 17 SigV erfordert den Einsatz erneuter qualifizierter elektronischer Signaturen und qualifizierter Zeitstempel. Andere Sicherungsmittel, wie z. B. die Speicherung auf einmal beschreibbaren Datenträgern, die Hinterlegung bei Notaren oder ähnliche technisch-organisatorische Maßnahmen, erfüllen nicht die Anforderungen der Vorschrift.

Der Gesetzgeber hat mit § 17 SigV ein bestimmtes Verfahren normiert, wie mögliche technisch bedingte Unsicherheiten von Signaturen ausgeglichen werden sollen. Nur durch eine erneute qualifizierte elektronische Signatur und einen qualifizierten Zeitstempel kann die durch die ursprüngliche Signatur geschaffene faktische Sicherheit dauerhaft aufrechterhalten werden. Die faktische Sicherheit einer Signatur ist aus sich heraus dauerhaft gewährleistet und soll nicht von Dritten oder einer weiteren Infrastruktur abhängig sein, deren Sicherheitsgrad immer ein anderer ist – unabhängig von seiner Qualität – und jeweils neu zu bestimmen wäre. Dadurch entstehenden Unsicherheiten soll durch die Festlegung eines bestimmten, objektiven Verfahrens entgegengewirkt werden.

2. Die erneute qualifizierte elektronische Signatur ist keine Willenserklärung, sondern ein Sicherungsmittel vorhandener Willenserklärungen. Sie muss daher keine persönliche Signatur z. B. eines Archivars sein.

¹ Siehe näher Roßnagel, A. / Pordesch, U., Kommentierung, in: Roßnagel, A. (Hrsg.), Recht der Multimediadienste, Loseblatt-Kommentar, C. H. Beck, München 2004, § 17 SigV, Rn. 1.

² Siehe zum Folgenden auch Roßnagel, A. / Fischer-Dieskau, S. / Pordesch, U. / Brandner, R.: Erneuerung elektronischer Signaturen, CR Computer und Recht 4 / 2003, 276 ff. Maßgeblich für die Auslegung sind der Wortlaut, die aus der Begründung zur Verordnung erkennbare Intention des Ordnungsgebers und auch die teleologische Reduktion des Wortlauts als anerkannte Interpretationsmethode. Die Durchsetzung einzelner Interpretationen von Rechtstexten ergibt sich erst durch ein breites gemeinsames Verständnis einzelner Regelungen. Die Auslegung unterliegt immer der richterlichen Überprüfung und kann daher nicht als abschließend verstanden werden.

Einzigste Intention der Neusignierung ist die Sicherstellung der Integrität und Authentizität des ursprünglich signierten Dokuments. Durch die Neusignierung wird dem drohenden Verlust der Sicherheitseignung der eingesetzten Algorithmen und Parametern ein weiteres Sicherungsmittel entgegengehalten und auf diese Weise das ursprüngliche Dokument gesichert.

Eine weitere Funktion kommt der Neusignierung nicht zu, so dass es daher unerheblich ist, wer die erneute qualifizierte elektronische Signatur anbringt.³

3. Werden elektronisch signierte Daten mit einem qualifizierten Zeitstempel versehen, der mindestens eine qualifizierte elektronische Signatur enthält, so genügt dies für eine erneute elektronische Signatur im Sinn des § 17 Satz 3 SigV. Eine weitere qualifizierte elektronische Signatur ist nicht notwendig, da sie keinen Mehrwert an Sicherheit bietet.

Streng dem Wortlaut folgend, sind die Daten mit einer neuen qualifizierten elektronischen Signatur zu versehen, die einen qualifizierten Zeitstempel tragen muss. Ein qualifizierter Zeitstempel ist dabei entsprechend § 2 Nr. 14 SigG die elektronische Bescheinigung eines qualifizierten Zertifizierungsdiensteanbieters darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Im Gegensatz zum Signaturgesetz 1997 beinhaltet ein qualifizierter Zeitstempel somit nicht mehr per Definition eine qualifizierte elektronische Signatur. Allein die Verwendung eines qualifizierten Zeitstempels ist somit für die Neusignierung nicht ausreichend.⁴ Werden dafür jedoch Zeitstempel eingesetzt, die eine qualifizierte elektronische Signatur beinhalten, bietet eine weitere Signatur keinen zusätzlichen Mehrwert an Sicherheit und ist daher überflüssig.⁵

4. Die Daten müssen entsprechend der fehlenden Eignung des Sicherungsmittels, d. h. der eingesetzten Algorithmen und Parameter, neu signiert werden. Da die Daten durch einen Hashwert repräsentiert werden, reicht es aus, allein die Signaturen des elektronischen Dokuments erneut mit einem Zeitstempel zu versehen und somit neu zu signieren, vorausgesetzt der verwendete Hashalgorithmus ist noch sicherheitsgeeignet und nur der asymmetrische Verschlüsselungsalgorithmus ist in seiner Sicherheitseignung gefährdet. In diesem Fall repräsentiert der Hashwert die Daten weiterhin, und die erneute elektronische Signatur umfasst damit auch die ursprünglich signierten Daten. Die Berechnung eines neuen Hashwerts der gesamten Daten mit einem neuen sicherheitsgeeigneten Hashalgorithmus und ein erneuter Zeitstempel unter Einbeziehung einer erneuten qualifizierten elektronischen Signatur ist dagegen dann notwendig, wenn auch der eingesetzte Hashalgorithmus in seiner Sicherheitseignung gefährdet ist. In diesem Fall ist nicht mehr sichergestellt, dass der Hashwert die ursprünglichen Daten repräsentiert und die erneute elektronische Signatur diese damit umfasst.

Diese Differenzierung greift den Repräsentationsgedanken auf, der Signaturverfahren grundsätzlich zugrunde liegt. Bereits bei der Erstellung einer Signatur wird nicht das eigentliche Dokument, sondern nur ein dieses Dokument repräsentierender Hashwert signiert.

Das Dokument (eventuell in Verbindung mit weiteren Daten) wird in einem oder mehreren Schritten gehasht, und im Anschluss daran wird mit Hilfe eines Public-Key-Algorithmus aus dem so gebildeten Hashwert und einem Signaturschlüssel ein Signaturwert berechnet.⁶ Wird

³ Siehe näher Roßnagel, A. / Pordesch, U., Kommentierung, in: Roßnagel, A. (Hrsg.), Recht der Multimediadienste, Loseblatt-Kommentar, C. H. Beck, München 2004, § 17 SigV, Rn. 52.

⁴ Insofern unzutreffend: Schneider, R.: Neusignatur – Anforderungen und Praxis, DuD Datenschutz und Datensicherheit 27 (2) / 2003, 91 ff.

⁵ Siehe näher Roßnagel, A. / Pordesch, U., Kommentierung, in: Roßnagel, A. (Hrsg.), Recht der Multimediadienste, Loseblatt-Kommentar, C. H. Beck, München 2004, § 17 SigV, Rn. 54.

⁶ Siehe Kapitel 2.3.1: „Grundprinzip von Signaturverfahren“.

der PKI-Algorithmus oder ein Parameter unsicher, ist der Hashalgorithmus aber noch sicher, so repräsentiert der Hashwert nach wie vor das Ausgangsdokument. Er muss für die Bildung einer neuen Signatur nicht erneut berechnet werden. Ein Zugriff auf das Dokument zu solch einer erneuten Berechnung ist unnötig.⁷

Dieser Repräsentationsgedanke kann auch bei der Neusignierung elektronischer Signaturen entsprechend § 17 SigV herangezogen werden. Solange alle verwendeten Hashverfahren als sicher gelten, reicht es für die Neusignierung aus, für die weitere Betrachtung allein auf die Signaturen bzw. Zeitstempel abzustellen. Ein initialer Archivzeitstempel, der das Dokument und seine Signatur umschließt, weil er den Hashwert des Dokuments enthält, kann somit selbst auch gehasht und erneut mit einem Zeitstempel versehen werden. In diesem Fall repräsentiert der erneute Zeitstempel nicht mehr unmittelbar, sondern nur noch mittelbar den ursprünglichen Hashwert des Dokuments. Dieser Repräsentationsgedanke kann so lange zur Anwendung kommen, wie die verwendeten Hashverfahren sicher sind.⁸

5. Die erneute Signatur muss rechtzeitig, d. h. vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter und mit neuen nach der Bewertung der zuständigen Behörde sicherheitsgeeigneten Algorithmen und zugehörigen Parametern erfolgen.

Entsprechend § 17 SigG sowie Anlage 1 Abschnitt I Nr. 2 zur SigV veröffentlicht die zuständige Behörde im Bundesanzeiger eine Übersicht der sicherheitsgeeigneten Algorithmen und zugehörigen Parameter sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Die Eignung wird durch eine Expertenkommission festgestellt und soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Da die in die Zukunft reichende Vorhersage jedoch auf Grund neuer technischer Entwicklungen nicht mit abschließender Sicherheit erfolgen kann, ist die Eignung jährlich sowie zusätzlich bei Bedarf neu zu bestimmen. Signaturanwender sind somit verpflichtet, sich regelmäßig über die Eignung der verwendeten Algorithmen und zugehörigen Parameter zu informieren, um rechtzeitig vor Ablauf der verwendeten Verfahren eine Neusignierung vornehmen zu können.⁹

6. Die erneute elektronische Signatur muss mindestens die gleiche Qualitätsstufe haben wie die Ausgangssignatur, um deren ursprüngliche Qualität zu erhalten. Qualifizierte elektronische Signaturen mit Anbieterakkreditierung müssen durch qualifizierte Zeitstempel akkreditierter Zertifizierungsdiensteanbieter erneuert werden; für die Neusignierung qualifizierter elektronischer Signaturen muss der Zertifizierungsdiensteanbieter, der den qualifizierten Zeitstempel zur Neusignierung erzeugt, nicht akkreditiert sein.

Akkreditierte Zeitstempeldiensteanbieter wurden im Gegensatz zu nur qualifizierten Anbietern vor Aufnahme ihres Betriebs durch die zuständige Behörde überprüft. Ihre Sicherheitsvorkehrungen entsprechen demnach den Anforderungen des Signaturgesetzes. Mit dem erhaltenen Gütesiegel wird nach § 15 Abs. 1 Satz 4 SigG „der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für Zertifizierungsdiensteanbieter entsprechend den Anforderungen des Signaturgesetzes zum Ausdruck gebracht“. Diese nachgewiesene Sicherheit, die im Rahmen einer Signaturprüfung einbezogen werden kann, bleibt nur bei Erneuerung durch akkreditierte Signaturen erhalten.

⁷ Siehe näher Roßnagel, A. / Pordesch, U., Kommentierung, in: Roßnagel, A. (Hrsg.), Recht der Multimediendienste, Loseblatt-Kommentar, C. H. Beck, München 2004, § 17 SigV, Rn. 49.

⁸ Siehe hierzu detaillierter Kapitel „Archivzeitstempelung und Neusignierung“.

⁹ Weiterführend hierzu Frye, C. / Pordesch, U.: Berücksichtigung der Sicherheitseignung von Algorithmen qualifizierter Signaturen, DuD Datenschutz und Datensicherheit 27 (2) / 2003, 73 ff.

7. Die erneute elektronische Signatur muss alle vorherigen qualifizierten elektronischen Signaturen zu den Daten umschließen, d. h. sowohl parallele und sequentielle Mehrfachsignaturen als auch frühere erneute elektronische Signaturen. So bleibt der Beweiswert der Daten in vollem Umfang erhalten. Selbst ein nachträgliches Löschen einzelner zu den Daten gehörender Signaturen wird erkennbar, so dass nach der ersten Neusignierung der Beweiswert sogar zunimmt.

Elektronische Dokumente können nicht nur einfach signiert sein, sondern können mehrere Signaturen tragen. Dabei kann es sich um parallele (nicht unmittelbar aufeinander bezogene) und um sequentielle Signaturen (Gegenzeichnungssignaturen, d. h. unmittelbar aufeinander bezogene Signaturen) handeln. Daneben kann ein signiertes Dokument bereits früher erneut elektronisch signiert worden sein und daher mehrere Signaturen beinhalten. Die Neusignierung muss alle diese vorhandenen Signaturen umschließen. Nur so lässt sich die Gesamtstruktur des Dokuments und der dazugehörigen Signaturen und Informationen erhalten.

Darüber hinaus bringt dieses Verfahren eine Erhöhung des Beweiswerts zum ursprünglich signierten Dokument mit sich. Ansonsten könnten Signaturen unbemerkt und ohne dass Spuren zurückblieben, von einem elektronischen Dokument entfernt werden. Dagegen wird ein nachträgliches Löschen einzelner zum gesamten Dokument gehörender Signaturen nach einer Neusignierung, die alle Signaturen umschließt, erkennbar.¹⁰

8. Eine erneute elektronische Signatur kann beliebig viele Daten umschließen. Dies müssen nicht die Daten eines, sondern können die Daten vieler Dokumente sein. Auch verschlüsselte Daten, die qualifizierte elektronische Signaturen enthalten, können erneut elektronisch signiert werden, wenn die verschlüsselten Daten die signierten Daten eindeutig repräsentieren.

Die Neusignierung dient lediglich als Sicherungsmittel und verfolgt keinen weiteren Zweck. Daher können beliebig viele Daten durch die Neusignierung umschlossen werden. Es muss sich lediglich beweisen lassen, dass ein bestimmtes Dokument in der Umschließung enthalten ist, d. h. (gemeinsam mit anderen) erneut signiert wurde. Dabei muss nicht unbedingt das Dokument selbst direkt erneut signiert werden. Auch eine vorhergehende Verschlüsselung ist möglich. Voraussetzung hierfür ist, dass eine nachweislich eineindeutige Abbildung zwischen chiffriertem Dokument und Ausgangsdokument besteht.

Der Wortlaut der Regelung ist in allen Fällen nicht immer eindeutig, wird aber durch diese Interpretation, die Probleme der Technik und der Praxis berücksichtigt, dem Anspruch des Gesetzes gerecht, eine Technikoffenheit sicherzustellen. Die rechtswissenschaftlichen Methoden der Auslegung gesetzlicher Regelungen ermöglichen, den Interpretations- und Gestaltungsspielraum von § 17 SigV ausreichend zu nutzen, um eine signaturgesetzkonforme Neusignierung verhältnismäßig kostengünstig und effizient einzusetzen. Auch wenn eine Verpflichtung zur Neusignierung nach § 17 SigV dem Signaturrecht nicht zu entnehmen ist,¹¹ so folgt aus der Aufbewahrungspflicht und dem Erfordernis, geeignete Maßnahmen für die dauerhafte Integrität der Dokumente zu treffen, die Pflicht, dem Erfordernis der durch § 17 SigV ausgestalteten Neusignierung nachzukommen. Ohne korrekte Neusignierung kann die Beweiserleichterung nach § 371a Abs. 1 Satz 2 ZPO nicht in Anspruch genommen werden und der Nachweis der Integrität misslingt.“

¹⁰ Siehe hierzu Roßnagel, A.: Gutachten zur Signaturgesetzkonformität des Standardisierungsvorschlags „Long-Term Conservation of Electronic Signatures“ für die ISIS-MTT Spezifikation vom 30.6.2004,

¹¹ Brandner, R. / Pordesch, U. / Roßnagel, A. / Schachermayer, J.: Langzeitsicherung qualifizierter elektronischer Signaturen, DuD Datenschutz und Datensicherheit 26 (2) / 2002, 97 ff.

2.7 Normierung bei elektronischen Signaturen

In Deutschland gab es bisher zwei Gruppen, die sich mit Spezifikationen zum Thema „elektronische Signaturen“ beschäftigt haben. Im TeleTrust Deutschland e. V. haben sich Industrieunternehmen und Forschungsinstitute zusammengeschlossen und eine Serie von Standards unter der Bezeichnung MailTrust (MTT) herausgegeben. Anbieter von Zertifizierungsdienstleistungen haben sich zur Gruppe T7 zusammengeschlossen und den Industrial Signature Interoperability Standard (ISIS) herausgegeben. Um die vorhandenen Spezifikationen in einem gemeinsamen Industriestandard zu harmonisieren, haben sich der TeleTrust e.V. und T7 für eine Zusammenarbeit entschieden. Der in einer ersten Version seit Oktober 2001 vorliegende Standard greift weitestgehend auf existierende internationale Standards zurück und berücksichtigt die Anforderungen des SigG in Form von Profilen. Für die Langzeitsicherung relevante Teile des so genannten ISIS-MTT-Standards sind:

Part 3: Message Formats, weil hier (CMS-basiert) Datenstrukturen für die Speicherung von Verifikationsdaten festgelegt werden,

Part 5: Certificate Path Validation, weil hier die Algorithmen zur Verifikation von Zertifikatsketten (Gültigkeitsmodell) festgelegt werden,

Profile: SigG-conforming Systems and Applications und Optional Enhancements to the SigG-Profile, weil hier SigG-spezifische Erweiterungen und Einschränkungen festgelegt werden.

Eine speziell auf die Langzeitaufbewahrung signierter Dokumente referenzierende Spezifikation gibt es allerdings noch nicht.

2.8 Sonderformen der elektronischen Signatur

2.8.1 Unterschrift auf einem elektronischen Pad

Leistungserbringer im Bereich Rehasport setzen z. T. ein Softwareprodukt ein, durch welches die Unterschrift des Versicherten (als Bestätigung der erbrachten Leistung) auf einem Unterschriften-Pad erzeugt wird. Hierbei handelt es sich nicht um eine qualifizierte elektronische Signatur i.S. des Signaturgesetzes.

Weder der § 302 SGB V noch die Richtlinie der früheren Spitzenverbände der Krankenkassen über Form und Inhalt des Abrechnungsverfahrens mit „Sonstigen Leistungserbringern“ (AbrechVerfRL) enthalten Vorgaben, die dem Einsatz des Unterschriften-Pads entgegenstehen.

Die Unterschrift als Bestätigung ist in diesem Fall nicht mit dem gesetzlichen Schriftformerfordernis (§ 126 BGB) gleichzusetzen. Insofern ist der Einsatz einer qualifizierten elektronischen Signatur i.S.d. Signaturgesetzes nicht erforderlich. Durch seine Unterschrift gibt der Versicherte keine formbedürftige Willenserklärung ab, durch die er ein neues Rechtsverhältnis eingeht oder auf ein bestehendes Rechtsverhältnis einwirkt. Die Auswirkungen seiner Unterschrift sind allein auf das Abrechnungsverhältnis von Krankenkasse und Leistungserbringer beschränkt und daher für ihn nicht rechtserheblich.

Solange die Unterschrift des Versicherten zu dem in der Richtlinie vorgesehenen Zeitpunkt erfolgt, ist die Verwendung eines Unterschriften-Pads aus formalrechtlichen Gründen unproblematisch.

3 Vorgehensweise bei der Einführung

3.1 Wirtschaftlichkeitsbetrachtung/Geschäftsprozessanalyse

Folgende Vorgehensweise wird empfohlen:

Schritt 1: Durchführung einer Geschäftsprozessanalyse:

Der Detaillierungsgrad ist abhängig davon, ob Massengut nur eingescannt, signiert und elektronisch archiviert oder eine papierarme Verwaltung im Rahmen eines Workflows eingeführt werden soll.

Ergebnis der Geschäftsprozessanalyse (GPA) ist u. a. ein Anforderungskatalog, der u. a. die gesetzlichen Vorgaben hinsichtlich

- § 110 a SGB IV (Aufbewahrungspflicht)
- § 110 b SGB IV (Rückgabe, Vernichtung und Archivierung von Unterlagen)
- § 110 d SGB IV (Beweiswirkung)
- § 9 SGB X (Nichtförmlichkeit des Verwaltungsverfahrens)
- § 33 SGB X (Bestimmtheit und Form des Verwaltungsaktes)

zu beachten hat.

Die GPA sollte folgende Rahmenbedingungen hinsichtlich der Dokumentenerfassung beinhalten

- o Festlegen der zu erfassenden Belegarten bzw. Dokumenttypen,
- o Herkunft der relevanten Dokumente,
- o Menge und Zuwachs des Dokumentenvolumens,
- o Dokumentenformate/-qualität
- o Ort und Zeitpunkt der Dokumentenerfassung und
- o Rechtliche Rahmenbedingungen (z. B. Unterschriftenregelung, Aufbewahrungsfristen).

Hinsichtlich der Wirtschaftlichkeitsanalyse sollte die bisherige Aufbewahrungspraxis in Frage gestellt werden.

Schritt 2: Erstellung einer Wirtschaftlichkeitsberechnung:

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

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

Sofern diese die Wirtschaftlichkeit des geplanten Verfahrens bestätigt, kann die Maßnahme in Angriff genommen werden.

Schritt 3: Entscheidung Zertifizierungsdienst (TrustCenter):

Die Möglichkeit, selbst ein TrustCenter zu betreiben, scheidet i.d.R. wegen des hohen Aufwandes (Auflagen gem. SigG / SigV) und den daraus folgenden Kosten aus. Als Alternative bietet sich hier die Inanspruchnahme privater Dritter an. Hierbei ist zu beachten, dass nur freiwillig akkreditierte TrustCenter Sicherheiten bieten, die für den Bereich der gesetzlichen

Sozialversicherung erforderlich sind. Eine Liste dieser TrustCenter ist auf der Internet-Seite der BNetzA zu ermitteln.

3.2 Umsetzung/Ausschreibung

Vergabeverfahren:

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

Landesspezifische Regelungen sind ggf. zu beachten.

Hinweis:

Der Beauftragte der Bundesregierung für Informationstechnik 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 (Link: http://www.cio.bund.de/cln_102/DE/IT-Angebot/IT-Beschaffung/it-beschaffung_node.html).

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.

3.3 Anzeige an die Aufsichtsbehörde

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

Bei der Einführung der elektronischen Langzeitspeicherung/elektronischen Signatur handelt es sich um grundlegende Maßnahmen im DV-Bereich. Diese sind rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht anzuzeigen.

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).

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

4 Elektronische Langzeitspeicherung papiergebundener Dokumente

4.1 Verfahrensbeschreibung

Zur Beurteilung des vom Versicherungsträger vorgesehenen Verfahrens ist die Vorlage einer ausführlichen, nachvollziehbaren Verfahrensbeschreibung unumgänglich. Eine solche muss insbesondere Informationen zum Ablauf des Signaturverfahrens, der betroffenen Dokumentarten, zur Karten- und Rechteverwaltung sowie zur Aufbewahrung, Löschung und Vernichtung beinhalten.

Der Datenschutzbeauftragte und die Innenrevision sollten bei der Erstellung beteiligt werden.

4.2 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 u. a. Einzelheiten enthalten

- zur Qualifizierten Elektronischen Signatur (QES)
- zur Stapelsignatur (§ 41 Abs. 5 SRVwV)
- zu Art und Umfang
- über die zusätzlich zu den Belegen zu speichernden Angaben (insbesondere Namen des Speichernden und Zeitpunkt der Langzeitspeicherung)
- zur detaillierten Beschreibung des organisatorischen Ablaufs

Daher sind Regelungen zu folgenden Punkten zu treffen:

Beschreibung des Scan- und Signaturverfahrens

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

Zugriffs- und Zutrittsregelungen

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

Zertifikate

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

Attribute

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

PIN-Regeln

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

Kartenmanagement

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

Regelmäßige Stichprobenprüfung von Signaturen

- Täglich
- Umfang der Stichprobe; Auswahl der Stichprobe

Verpflichtungserklärung der Mitarbeiter/innen

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

Ergonomie der Arbeitsplätze

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

4.3 Scanverfahren

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

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

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

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

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

Obwohl es grundsätzlich keine eklatanten Preisunterschiede mehr zwischen Farb- und S/W-Scannern gibt - jeder Scanner beherrscht beide Verfahren - wäre jedoch erforderlich, dass der Scanner multistreamfähig ist. Das bedeutet, es werden beim Scanvorgang sowohl ein farbiges als auch ein Graustufen-Image erzeugt. Während das farbige elektronisch signiert und archiviert wird, benötigt man das Graustufen-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 Graustufen-Images möglich.

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

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

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

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

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

4.4 Regelungen für das Kartenmanagement

Im Rahmen des elektronischen Geschäftsverkehrs werden Signaturkarten nur an den speziellen Arbeitsplätzen benötigt, an denen die Signatur eingescannter Belege oder elektronisch erstellte Dokumente erfolgt. Diese Arbeitsplätze sind nur funktionsfähig, wenn der Bediener auf eine gültige Signaturkarte 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.

4.5 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 BNetzA zu finden.

2. Signaturanwendungskomponenten:

Für Signaturanwendungskomponenten nach § 17 Abs. 3 Nr. 2 und 3 SigG genügt eine Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG. Nach der gängigen Definition ist die Herstellererklärung eine Erklärung eines Herstellers gegenüber der zuständigen Aufsichts- und

Kontrollinstitution, dass das Produkt allen hierfür relevanten technischen Standards und Spezifikationen entspricht.

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

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

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

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

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

Ergänzend weisen wir an dieser Stelle auf eine Veröffentlichung der Bundesnetzagentur vom 06.02.2009 hin:

„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 Herstellerklärungen nachgewiesen. Bestätigungen werden dabei ausschließlich von nach § 18 SigG anerkannten (Prüf- und) Bestätigungsstellen erstellt, Herstellerklärungen nur durch die Hersteller des Produktes abgegeben.“

4.6 Sicherheit, Betriebssystem und Netzwerk

Bauliche Maßnahmen

Bei der Gestaltung der baulichen Maßnahmen ist zu unterscheiden zwischen

- Einzelplatzsignatur und
- Stapelsignatur.

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

Das Scannen von Belegstapeln ist räumlich und DV-technisch getrennt vom übrigen Geschäftsbetrieb zu trennen. Die Räumlichkeiten sind gegenüber Unbefugten durch geeignete Sicherheitsmaßnahmen abzuschotten. Zutritt haben ausschließlich die in diesem Bereich tätigen Mitarbeiter/innen.

Betriebssystem und Netzwerk

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

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

Die im Stapelsignaturgeschäft erforderlichen Sicherheitsmaßnahmen erfordern, dass das Teilnetz, in dem die Scan-/Signatur-Operatoren tätig sind, vom übrigen Hausnetz zu trennen ist. 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!

In der Registry sollte ein Eintrag zum Löschen der Auslagerungsdatei erfolgen, damit eine Zwischenspeicherung der PIN beim Herunterfahren unterbunden wird. Ersatzweise könnte bei einem Arbeitsspeicher > 256 MB die Auslagerungsdatei abgeschaltet werden.

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 kein e-Mail Programme (kein Internetanschluss) und keine Grafikbearbeitungsprogramme installiert sein.

Nicht wiederbeschreibbare Datenträger

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

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

Somit spricht grundsätzlich auch nichts gegen die Verwendung von Tapes oder Harddisks. Voraussetzung für die Langzeitspeicherung auf diesen Medien ist jedoch die Gewährleistung einer Versionsintegrität (WORM-Prinzip). Ein auf Harddisks langzeitarchiviertes, qualifiziert signiertes Image darf bei Aufruf durch den User nicht verändert werden (können); in diesem Fall ist automatisch eine Kopie des Images zu erzeugen, die dann unter einer neuen Versionsnummer abgespeichert wird. Hierdurch wird die Revisionsicherheit der signierten Dokumente gewährleistet. Die Möglichkeit des physikalischen Löschens nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist muss vom SV-Träger in der 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 im GSHB festgelegten Standards wie Call-Back-Verfahren und der Einsatz von Einmal-Passworten zu beachten.

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

4.7 Stapelsignaturverfahren

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

Einzelplatzsignatur

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

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

Stapelsignatur

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

Der Vorteil dieses Verfahrens gegenüber dem der Einzelsignatur liegt im Zeitgewinn: Das Einscannen, Signieren und Speichern von Papierbelegen kann im Stapelbetrieb erfolgen. Dies erfordert, den Übernahmeprozess effizient zu gestalten. Hier entsteht ein Problem, wenn deshalb der vollständige Übernahmeprozess bestehend aus:

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

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

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

Alternativ dazu sieht die o.g. Vorschrift die Möglichkeit vor, die Images unmittelbar nach deren Herstellung durch einen anderen als den Scan-Operator signieren zu lassen. Dieser hat aber vor dem Signiervorgang die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe zu prüfen. Das bedeutet, jedes Image ist visuell zu prüfen (Einzelsignatur). [Eine Stapelsignatur ist bei dieser Alternative nur zulässig, wenn im Signiertool der zu prüfende Stichprobenumfang von 2 v.H. auf 100 v.H. heraufgesetzt wird.]

Die Stapelsignatur wird erstmals in § 41 Abs. 5 SRVwV als „Massensignatur“ beschrieben und an verschiedene Voraussetzungen gebunden. Das Bundesministerium für Arbeit und Sozialordnung hat mit Schreiben vom 31.05.2002 (Az.: Ib4 – 18001 – 2) in einem Einzelfall dem Einsatz von automatisch erzeugten Signaturen („Stapelsignaturen“) zugestimmt, wenn die in der Begründung¹² 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:

¹² Begründung zum Entwurf einer Verordnung zur elektronischen Signatur in der Fassung des Kabinettschlusses vom 24. 10. 2001:

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

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

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

Technische Vorkehrungen

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

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

Einzelheiten sind der Homepage der BNetzA zu entnehmen.

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

Die Signaturanwendungskomponente sollte technische Vorkehrungen bereitstellen, wonach der Scan-Operator gezwungen wird, einen festgelegten Stichprobenumfang einer visuellen Kontrolle zu unterziehen. Erst nach erfolgreicher Kontrolle der Stichprobenbelege und entsprechender Bestätigung durch den Scan-Operator darf der Stapel signiert werden.

Sofern bei der visuellen Kontrolle ein fehlerhaftes Dokument entdeckt wird, sind technische Vorkehrungen derart zu treffen, dass der gesamte Stapel neu eingescannt werden muss.

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. Erst nach erfolgreicher Prüfung des Mindeststichprobenumfangs von 2 v. H., - mindestens aber von 2 Dokumenten - wird der Stapel signiert. Es wird empfohlen, jeweils den ersten und letzten Beleg eines Stapels zusätzlich mit einzubeziehen. 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 un-signierten Stapeln vorhanden ist!

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 ein auf der Rückseite befindliches Zeichen ein automatisches Löschen ausschließt.

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

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 von Originalbelegen 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.

4.8 Neusignieren nach § 17 SigV

Neusignierung von Elektronischen Signaturen

Elektronische Signaturen basieren auf mathematischen Komplexitätsproblemen. Der technische Fortschritt führt dazu, dass immer komplexere solcher Probleme im Laufe der Zeit gelöst werden können und somit ein Signaturalgorithmus insgesamt oder eine gegenwärtig als sicher angesehene Parametrisierung (hierzu zählt z. B. die Länge eines Schlüssels) ab einem bestimmten Zeitpunkt durch die Bundesnetzagentur (BNetzA) nicht mehr als sicher angesehen werden. Die BNetzA legt daher jedes Jahr die Signaturalgorithmen und die Parameter fest, die sie für die nächsten Jahre als sicher ansieht. Die elektronische Signatur verliert also durch den technischen Fortschritt im Laufe der Zeit ihre Sicherheits- und Beweiseignung, wenn nicht weitergehende Maßnahmen ergriffen werden. Insbesondere bei der Langzeitspeicherung wird sich dieser Fall häufiger ergeben.

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

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

Neusignierung von Hashalgorithmen

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

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

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

Neusignierung von Zeitstempeln

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

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

Hinweise:

Die Bundesnetzagentur (BNetzA, vormals Regulierungsbehörde für Telekommunikation und Post – RegTP -) gibt einmal jährlich eine „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Übersicht über geeignete Algorithmen“ heraus, in der eine Einschätzung der Sicherheit der verwendeten Algorithmen und entsprechende Empfehlungen abgegeben werden. In ihrer Publikation vom 22. Februar 2007 (veröffentlicht im Bundesanzeiger Nr. 69, S. 3759, ebenfalls im Internet veröffentlicht unter „<http://www.bundesnetzagentur.de/media/archive/9655.pdf>“ teilt sie mit, dass für den beim RSA-Verfahren zugrunde liegenden Berechnungsmodus eine Bitlänge von 1024 bit nur noch bis zum 31. Dezember 2007 ausreicht. Für den Zeitraum 2008 – 2012 werden bis auf 1976 bit ansteigende Mindestwerte genannt. Empfohlen wird die grundsätzliche Erhöhung auf 2048 bit. Gleichlautende Feststellungen bzw. Empfehlungen hat die RegTP bereits **seit dem Jahr 2003 im jährlichen Turnus** veröffentlicht.

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

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

Aus der Literatur können verschiedene Empfehlungen zur Vorgehensweise entnommen werden, die auch zur Wirtschaftlichkeit der Maßnahmen beitragen. U.a. ist als eine techni-

sche 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.

4.9 Vernichtung von Originalbelegen

Für die Vernichtung von Akten gelten folgende Rechtsgrundlagen:

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

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

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

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben eine datenschutzgerechte Verarbeitung der Daten sicherzustellen. Die letzte Phase der Datenverarbeitung ist das Löschen gespeicherter Daten bzw. das Vernichten von Datenträgern.

Datenträger können z. B. Magnetbänder, Disketten, Filmmaterial oder Papier sein. Soweit es sich um personenbezogene Daten handelt, gelten bestimmte gesetzliche Regelungen, die Zeitpunkt und die Art und Weise der Löschung festlegen.

Zusätzlich können in den jeweiligen Einsatzgebieten landes-/bereichsspezifische Spezialvorschriften gelten.

Eine datenschutzgerechte Vernichtung von Informationsträgern (Papier und Mikrofilm) ist in der DIN 32757 geregelt. DIN 32757-1 konzentriert sich ganz auf die Vernichtung von personenbezogenen Daten. Für Schriftgut werden Sicherheitsstufen für die Aktenvernichtung festgelegt. Diese orientieren sich entsprechend der Sensitivität der zu vernichtenden Informationen an dem für eine Reproduktion erforderlichen Aufwand:

Stufe 1: Allgemeines Schriftgut, das unlesbar gemacht werden soll. Eine Reproduktion ist ohne besondere Hilfsmittel und ohne Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich. Zulässig ist eine Materialteilchenfläche von $\leq 1000 \text{ mm}^2$ (bei CrossCut) bzw. einer Streifenbreite von $\leq 12 \text{ mm}$ (bei Streifenschnitt).

Stufe 2: Internes Schriftgut, das unlesbar gemacht werden soll. Eine Reproduktion ist mit Hilfsmitteln und nur mit besonderem Zeitaufwand möglich. Zulässig ist eine Materialteilchenfläche von $\leq 400 \text{ mm}^2$ (bei CrossCut) bzw. einer Streifenbreite von $\leq 6 \text{ mm}$ (bei Streifenschnitt).

Stufe 3: Vertrauliches Schriftgut. Eine Reproduktion ist nur unter erheblichem Aufwand (Personen, Hilfsmitteln, Zeit) möglich. Zulässig ist bei CrossCut eine Materialteilchenfläche von max. 240 mm^2 (bei einer Breite von max. 4 mm und einer Länge von max. 60 mm) bzw. bei Streifenschnitt einer Streifenbreite von max. 2 mm .

Stufe 4: Geheimzuhaltendes Schriftgut. Eine Reproduktion ist nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich. Zulässig ist (bei CrossCut) eine Materialteilchenfläche von $\leq 30 \text{ mm}^2$ (bei einer Breite von max. 2 mm und einer Länge von max. 15 mm).

Stufe 5: Geheimzuhaltendes Schriftgut, wenn außergewöhnlich hohe Sicherheitsanforderungen zu stellen sind. Eine Reproduktion ist nach dem Stand der Technik unmöglich. Zulässig ist eine Materialteilchenfläche (bei CrossCut) von $\leq 12 \text{ mm}^2$ (bei einer max. Breite von $\leq 0,8 \text{ mm}$ und einer max. Länge von 15 mm).

Die Angaben gelten in gleicher Weise für Polyesterfilm und Kunststoff mit einer Informationsdarstellung in Originalgröße. Für Mikrofilm und Chipkarte ist für die Stufe 3 eine Materialteilchenfläche von $\leq 1 \text{ mm}^2$, für die Stufe 4 von $\leq 0,5 \text{ mm}^2$ und für die Stufe 5 von $0,2 \text{ mm}^2$ vorgeschrieben.

Geeignete Aktenvernichter tragen eine Bezeichnung, welche die erfüllte Sicherheitsstufe für die Art des Informationsträgers wiedergibt, z. B. Aktenvernichter DIN 32757 – S 3 P (P = Papier).

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 personenbezogene Daten, 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.

Ein Transport von Datenträgern mit personenbezogenen Daten zu einem Aktenvernichter darf nur in geschlossenen Behältnissen und in geschlossenen Fahrzeugen durchgeführt werden, um zu gewährleisten, dass Daten während des Transports von Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

4.10 Grundsätze zu Aufbewahrung/Fristen/Reproduktion/Löschung

Papierdokumente, die in eine elektronische Form überführt und elektronisch signiert worden sind, existieren nach Vernichtung des Originals nur noch ein Mal (in Dateiform). Wie bei der normalen Sicherung der mit Hilfe der EDV erstellten Daten sind auch von den elektronischen Archivdaten Kopien zu erstellen und an einem außerhalb der Kassenräume liegenden Ort sicher aufzubewahren.

Manipulationen und Veränderung müssen ausgeschlossen sein und es dürfen keine Daten verloren gehen oder manipuliert werden können. Dies gilt auch auf dem Übertragungsweg.

Es muss sichergestellt sein, dass die Daten während der Aufbewahrungsfrist (Katalog der Aufbewahrungsfristen) verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht und ausgedruckt werden können. Dabei muss die Wiedergabe mit der Originalunterlage bildlich übereinstimmen.

Nach § 41 Abs. 4 SRVwV ist bei elektronisch signierten Daten vor einer weiteren Verarbeitung die qualifizierte elektronische Signatur und anhand des betreffenden Zertifikats die Unterschriftsberechtigung zu prüfen.

Für die Prüfung eines signierten Images muss ein Programm bereitgestellt werden, das eine Verifikation ermöglicht: Neben der Anzeige des Dokuments (über einen Viewer) wird die Signatur geprüft und als Ergebnis „ok“ oder „Signatur fehlerhaft“ zurückgeliefert.

Zur revisionssicheren elektronischen Archivierung (Langzeitspeicherung) stammen vom VOI (Verband Organisations- und Informationssysteme e. V.) die folgenden 10 Merksätze:

- 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

4.11 Übernahme von Altbeständen

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.

4.12 Übergangsregelungen

Die Übergangsregelung gemäß § 44 Abs. 1 SRVwV ist am 07.08.1999 in Kraft getreten und zum 23.12.2004 (Bundesanzeiger Nr. 243 vom 22.12.2004) sowie zum 17.06.2005 (Bundesanzeiger Nr. 110 vom 16.06.2005) geändert worden. Sie betrifft Scanverfahren, die vor dem 07.08.1999 bereits begonnen wurden und bei denen die Originalbelege trotz fehlender elektronischer Signatur vernichtet werden dürfen.

Die fünfjährige Übergangsfrist endete am 21. Mai 2006. Seit diesem Zeitpunkt ist eine elektronische Langzeitspeicherung – bei gleichzeitiger Vernichtung der Originalbelege – ausschließlich unter Verwendung qualifizierter elektronischer Signaturen gem. § 2 Nr. 3 Signa-

turgesetz zulässig

5 Langzeitspeicherung elektronisch erzeugter Dokumente

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

Hierzu gehören

Eingehende Dokumente:

- Elektronisch erzeugte Dokumente (z.B. im doc- oder pdf-Format), die elektronisch an den SV-Träger gesandt wurden (z.B. auf Datenträger, E-Mail-Anhang, ftp)
- Eingegangene elektronische Faxe (z.B. auf Fax-Server)
- Eingegangene E-Mails 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 deren Mitarbeitern erzeugten elektronischen Dokumenten, die elektronisch (und/oder in Papierform) an einen Externen versandt wurden (auch elektronische Faxe)
- Vom SV-Träger oder seinen Mitarbeitern an Externe (z.B. Versicherte, Arbeitgeber, Leistungserbringer) versandte E-Mails und deren Anhänge
- Interne Vermerke, Verfügungen, Notizen, Protokolle

Die Anforderungen an die rechtssichere Langzeitspeicherung für diese Dokumente sind definiert durch die §§ 110a – d SGB IV i.V.m. den Grundsätzen ordnungsgemäßer Aufbewahrung¹³.

In einer Tabelle (Abschnitt 9, Anlage 1) sind die wesentlichen Dokumentarten aufgeführt, die bei einem Sozialversicherungsträger eingehen oder von ihm selbst erstellt werden. In der Spalte „Beschreibung“ werden u. a. die charakteristischen Eigenheiten der einzelnen Dokumentarten dargestellt sowie die aus den gesetzlichen Vorschriften abgeleiteten Vorgaben zum Verwaltungsverfahren nach dem SGB X.

5.1 Qualifizierte elektronische Signatur von elektronischen Postausgängen

Der Austausch elektronischer Dokumente zwischen Versicherten und Versicherungsträger wird im § 36a SGB I geregelt.

Danach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat. Für die Kommunikation **SV-Träger → Versicherter** bedeutet dies, dass der Versicherte gegenüber dem SV-Träger ausdrücklich seine Zustimmung für die Übermittlung erteilt haben muss. Die bloße Angabe einer E-Mail-Adresse reicht nicht aus. Dagegen ist für eine Kommunikation in Gegenrichtung **Versicherter → SV-Träger** die Bekanntgabe einer E-Mail-Adresse des SV-Trägers als Zustimmung anzusehen.

¹³ „Vereinbarung der Spitzenverbände der Krankenkasse zu den Grundsätzen ordnungsgemäßer Aufbewahrung im Sinne des § 110a SGB IV, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen“ (Stand: 23.06.2008) und „Ergänzende Vereinbarung der Spitzenverbände der Krankenkassen zur Rückgabe und Vernichtung von Unterlagen“ (Stand: 23.06.2008)*

In § 36a Abs. 2 SGB IV wird weiterhin 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 mit einer qualifizierten elektronischen Signatur nach SigG zu versehen. Die Verwendung von Pseudonymen ist hierbei nicht zulässig.

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

5.2 Rechtssichere Langzeitspeicherung von elektronischen Postausgängen

Von der in Ziff. 5.1 beschriebenen Rechtslage hinsichtlich des VA-Erlasses ist allerdings die Frage der **Langzeitspeicherung der Verwaltungsunterlagen** (zu denen auch der VA selbst gehört) zu unterscheiden. Insoweit verfolgt das Gesetz andere Zielsetzungen als beim VA-Erlass. Es geht nicht um die rechtssichere Bekanntgabe gegenüber dem Adressaten sondern um die zuverlässige Langzeitspeicherung von Unterlagen. Insofern setzt § 110d Nr. 1 SGB IV i. V. m. § 110a Abs. 2 SGB IV für die Beweiswirkung der archivierten Unterlagen die qualifizierte elektronische Signatur voraus. Dies gilt nach dem ausdrücklichen Willen des Gesetzgebers für alle Unterlagen, also auch die elektronischen Verwaltungsakte, obwohl deren Bekanntgabe – wie oben dargelegt – unter geringeren Anforderungen erfolgen konnte.

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

Der gesetzeskonforme Einsatz der QES ist für die KV-Träger mit erheblichem organisatorischen und finanziellem Aufwand verbunden. Sie bevorzugen daher die Verwendung der sog. **Massensignatur**. Deren uneingeschränkter Einsatz ist allerdings wegen der in § 110d SGB IV formulierten Anforderungen an die Beweiswirkung elektronisch gespeicherter Dokumente aufsichtsrechtlich nicht vertretbar.

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

5.3 Rechtssichere Langzeitspeicherung von elektronischen Posteingängen

Posteingänge, die den SV-Träger auf elektronischem Wege erreichen (z.B. als Mail-Anhang) und die eine QES des Absenders/Erstellers enthalten, sind im elektronischen Langzeitarchiv zu speichern.

Dokumente, die der Absender nicht qualifiziert signiert hat, sind vor der Langzeitspeicherung mit der QES eines Mitarbeiters des SV-Trägers zu versehen. Im übrigen gelten hier die Ausführungen zu Ziff. 5.2 .

5.4 Besonderheiten

5.4.1 Erstellung und Versand von Serienbriefen

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

5.4.2 Aufbewahrung von Fehler-/Bearbeitungslisten

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

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

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

5.4.3 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.

5.4.4 Behandlung eingehender Fax-Sendungen

Die Kasse hat die Einsatzbedingungen über die Fax-Nutzung in einer Sicherheitsleitlinie detailliert festzulegen.

5.4.4.1 Analog-/Papier-Faxe

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

5.4.4.2 Elektronische Faxe

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

Diese Faxe können wie folgt archiviert werden:

- a) In Papierform (Ausdruck des Fax) oder
- b) als Image, sofern dieses nach Eingang (und ggf. Anbringung eines Fax-Stempels) und vor der ersten Zugriffsmöglichkeit durch einen Mitarbeiter automatisch mit einem qualifizierten Zeitstempel (der eine QES beinhaltet) versehen wurde.

Bitte beachten:

Bei dem unter b beschriebenen Verfahren besteht keine Beweiswirkung i.S. von § 110d SGB IV. Die Kassen mögen daher nach Durchführung einer Risikobewertung selbst entscheiden, ob sie elektronische Faxe beim Eingang mit einer QES des Empfängers (Sachbearbeiter) versehen wollen.

Interne Weiterleitung von elektronischen Faxen

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

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

6 Elektronischer Datentransfer

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

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

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

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

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

Daraus folgert, dass die Krankenkassen bei der Annahme elektronischer Datensätze den Originaldatensatz im Sinne der Aufbewahrungspflichten nach § 110a SGB IV dauerhaft und unveränderbar zu speichern haben. Hierzu sind geeignete Archivsysteme zu nutzen, die eine Versionsintegrität gewährleisten (siehe hierzu Ausführungen zu nicht wieder beschreibbaren Datenträger unter Ziffer 5.6). 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. EDI-FACT, XML) in eine lesbare Form umzuwandeln.

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

Die Prüfdienste werden bei ihren Prüfungen Informationen aus Datenbeständen nur anerkennen, wenn die genannten Voraussetzungen erfüllt werden.

Die Prüfdienste werden bei ihren Prüfungen – auch im RSA-Bereich – Informationen aus Datenbeständen ab dem Berichtsjahr 2010 nur anerkennen, wenn die genannten Voraussetzungen erfüllt werden. Die Softwareentwickler wurden entsprechend informiert.

6.1 Ergänzende rechtliche Grundlagen

Neben den rechtlichen Anforderungen aus §§ 110a - d SGB IV sind für den elektronischen Datentransfer die folgenden rechtlichen Grundlagen u. a. zu beachten:

§ 78a SGB X und Anlage	Technische und organisatorische Maßnahmen
§ 5 SVRV	Belegpflicht
§ 6 Abs. 3 SVRV	Belege für Einzahlungen, Auszahlungen und Buchungen ohne Zahlungsvorgang
§ 9 SRVwV	Allgemeines
§ 12 SRVwV	Zahlungsbegründende Unterlagen
§ 13 SRVwV	Änderung der Zahlungsanordnung
§ 19 Abs. 5 SRVwV	Feststellung der Belege
§ 22 SRVwV	Form und Führung der Bücher und Aufzeichnungen
§ 40 Abs. 3 SRVwV	Sicherheit bei Einsatz der automatisierten Datenverarbeitung Grundsätze ordnungsgemäßer Datenverarbeitung (GoD)

Darüber hinaus sind die Aufbewahrungsfristen (Löschung von Daten) einzuhalten. Dabei stellt § 78 SGB IV die Rechtsgrundlage dar, Grundsätze u. a. über die Zahlung, die Buchführung und die Rechnungslegung festzulegen. Die Regelung ist nach den Grundsätzen des für den Bund und die Länder geltenden Haushaltsrechts vorzunehmen. Diese hat die Besonderheiten der Sozialversicherungsträger und der einzelnen Versicherungszweige zu berücksichtigen.

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

- Richtlinien für den Datenaustausch mit den gesetzlichen Krankenkassen (Version 4.09.12 vom 13.08.2010 – gültig ab 01.07.2010)
- Datenaustausch mit Leistungserbringern und Arbeitgebern im Internet:
 - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels http (Version 1.0 vom 19.05.2009 – gültig ab 01.07.2009)
 - o Spezifikation der Schnittstellen für die Übermittlung von Nachrichten mittels E-Mail (Version 1.6.1 vom 01.06.2007 – gültig ab 01.03.2010)
- Security-Schnittstelle für das Gesundheitswesen (Version 1.5.1 von Oktober 2008 – gültig ab 01.10.2008)
- Hinweise zur „Security-Schnittstelle für das Gesundheitswesen Version 1.5“ (Version 1.7.2 vom 28.07.2008)

Die Richtlinien können über die Internetseiten des GKV-Spitzenverbandes heruntergeladen werden: <http://www.gkv-datenaustausch.de/Home.gkvnet>

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“.

Die Verschlüsselung erfolgt sowohl im PEM-Format (befristet bis 30.06.2010) als auch im PKCS#7-Format.

6.2 Speicherung des Originaldatensatzes

Bei elektronischen Eingängen sind Vorschriften zur Aufbewahrung des Eingangs 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 Sozialversicherungsträger

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

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

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

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

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

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

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

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

6.3 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.

7 Anforderungen an die elektronische Langzeitspeicherung

Die fachlichen Grundanforderungen zur Langzeitspeicherung elektronischer Dokumente im Bereich der Sozialversicherung ergeben sich aus den §§ 110 a – d SGB IV. Sie werden ergänzt durch die Verwaltungsvereinbarung gem. § 110 c SGB IV „Vereinbarung der Spitzenverbände der Krankenkasse zu den Grundsätzen ordnungsgemäßer Aufbewahrung im Sinne des § 110a SGB IV, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen“ (Stand: 23.06.2008) und die „Ergänzende Vereinbarung der Spitzenverbände der Krankenkassen zur Rückgabe und Vernichtung von Unterlagen“ (Stand: 23.06.2008).

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

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit der Technischen Richtlinie TR 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) [Version 1.1 vom 18.02.2011] einen Leitfaden zur Verfügung gestellt.

Diese Richtlinie gibt Orientierung und Hilfestellung, um den vielfältigen Anforderungen hinsichtlich

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

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

Konkret enthält die Richtlinie 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 Prüfdienste empfehlen die dort genannten Anforderungen zu beachten und werden diese bei ihren Erhebungen mit einbeziehen.

Die TR 03125 kann von den Internetseiten des BSI unter folgendem Link abgerufen werden:

https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index.htm.html

7.1 Besonderheiten / Abweichungen zur TR 03125

- Ziffer 5.2.3: Die Verwendung eines Pseudonyms ist gem. § 36a Abs. 1 Satz 3 SGB I nicht zulässig.
- Ziffer 7.3.1: Zusätzliche Schnittstellen zum Ändern von bereits archivierten (signierten) Dokumenten sind nicht zulässig, weil sie die Signatur zerstören würden.
- Ziffer 8.2.2: Bei mehrfachen fehlgeschlagenen Authentifizierungsversuchen ist der Zugang zu sperren.

8 Glossar

- **Akte**

Als Akte bezeichnet man in der Schriftgutverwaltung eine Sammlung von Aufzeichnungen, die bei der eigenen Verwaltungs- oder Geschäftstätigkeit anfallen und aufgrund eines gemeinsamen Merkmals zusammengefügt aufbewahrt werden.

- **Anschein der Echtheit**

Zwar wird angenommen, dass der Signierende auch der rechtmäßige Karteninhaber ist, doch beweisen kann man dies nicht. Aus diesem Grunde wurde für qualifizierte Signaturen der Anschein der Echtheit (ZPO § 371a) eingeführt. Die Beweisführung bei qualifizierten Signaturen, dass der Zertifikatsinhaber nicht signiert hat, obliegt damit dem Zertifikatsinhaber.

- **Anforderungen an elektronische Signaturen**

Folgende Anforderungen sind beim Einsatz von elektronischen Signaturen zu beachten:

- Der Unterzeichner muss identifizierbar sein
- Der Inhalt des Dokuments und das Identifizierungsmerkmal des Unterzeichners gehören zusammen.
- Nachträgliche Veränderungen am Dokument müssen erkennbar sein
- Der Unterzeichner muss den Prozess kontrollieren können

- **Datensicherung**

Die Datensicherung dient dem Schutz vor Datenverlust durch Hardware-Schäden, Diebstahl, Feuer, Fluten, versehentliches oder absichtliches Löschen oder Überschreiben und logischen Fehlern innerhalb der Daten. Die Datenspeicherung erfolgt in der Regel verdichtet. Durch die kurzfristige Aufbewahrung (in der Regel 3 bis 6 Monate) unterscheidet sie sich von der längerfristigen Datenspeicherung.

- **Dokument**

von lat: documentum = beweisende Urkunde.

Ein Dokument ist

- eine Urkunde
(ist die mit einem Gegenstand fest verbundene Gedankenerklärung, die einen bestimmten Tatbestand bzw. Sachverhalt fixiert und zumeist auch ihren Aussteller erkennen lässt. Dazu gehören in erster Linie Schriftstücke.)

- in der EDV eine Datei, die nicht ausführbar ist
(Eine Datei ist ein strukturierter Bestand inhaltlich zusammengehöriger Daten, der auf einem Datenträger, einem externen Speichermedium abgelegt ist. Diese Daten existieren über die Laufzeit eines Programms hinaus und werden als persistent bezeichnet.)
- in der Datenanalyse ein Begriff für Daten, die schriftlich niedergelegt sind.
- **E-Government**
Unter E-Government (elektronisches Regieren und Verwalten) versteht man die Vereinfachung und Durchführung von Prozessen durch den Einsatz von Informations- und Kommunikationstechnologien. Dies wird nicht nur innerhalb und zwischen Institutionen der Exekutive (Behörden) durchgeführt, sondern auch zu Bürgern, Unternehmen sowie zu weiteren staatlichen Institutionen.
- **Elektronische Speicherung**
Elektronische Speicherung steht für die unveränderbare, langzeitige Aufbewahrung elektronischer Information. Dies bedeutet, dass die Daten vollständig, auch mit Meta-Daten in eine andere Ebene übernommen werden. Die Informationen befinden sich nicht mehr im Online-Bereich.
- **Elektronische Signaturen**
Von Personen elektronisch erstellte Willenserklärungen oder Bestätigungen. Elektronische Signaturen erfolgen im eigenen Namen oder im Auftrag, sind jedoch immer personengebunden.
Dabei unterscheidet das Signaturgesetz aufsteigend nach Sicherheitsanforderungen zwischen:
 - einfacher elektronischer Signatur,
 - fortgeschrittener elektronischer Signatur und
 - qualifizierter elektronischer Signatur
- **Geschäftsprozess**
Ein Geschäftsprozess beschreibt eine Folge von Aktivitäten mit dem Ziel einer Leistungserstellung.
- **Gültigkeit von Zertifikaten**
Der dem Unterzeichner zugeordnete Private Key darf nur während der Gültigkeit des Zertifikats für eine Signaturerstellung verwendet werden und muss nach Ablauf dann im Trust Center, nicht jedoch auf der Karte selbst, als gesperrt markiert werden. Nach der Sperre müssen Zertifikate für qualifizierte Signaturen noch weitere 5 Jahre vom ZDA (Zertifizierungsdienst-Anbieter) zur Identifizierung vorgehalten werden, Zertifikate für qualifizierte Signaturen mit Anbieterakkreditierung sogar 30 Jahre.
- **Hash oder Hashwert**
Dieser ist letztlich eine kryptographische Prüfsumme (Fingerabdruck) eines Dokuments. Bei der Elektronischen Signatur wird nicht das komplette Dokument, sondern nur dieser Hashwert signiert.
- **LangzeitLangzeitspeicherung**
Die elektronische L. stellt auf eine dauerhafte und unveränderbare Aufbewahrung von Dokumenten ab, bei der sich die Aufbewahrungsdauer an den gesetzlichen Regelungen ausrichtet.

- **Migration**
Der Vorgang der Migration ist eine Verlagerung von Datenbeständen auf ein langsameres und nicht so teures Medium. Meta-Daten verbleiben auf der Originalebene. Die Informationen befinden sich weiterhin im Online-Bereich.
- **Neusignierung**
Unter Neusignierung (teilweise auch Über- oder Nachsignierung genannt) versteht man die erneute Signierung elektronischer Dokumente, unter Einschluss der ursprünglichen Signaturen.
- **Qualifizierte elektronische Signatur**
Der Unterzeichner muss bei einer qualifizierten Elektronischen Signatur Inhaber eines qualifizierten zugewiesenen Zertifikats sein und ihm somit vom ZDA der Public Key eines asymmetrischen Schlüsselpaares zugewiesen worden sein. Auf einer Signaturkarte werden der Private Key sowie eine 6-stellige PIN abgelegt und diese dem Antragsteller ausgehändigt.
- **Selbstbeschränkung**
Selbstbeschränkung stellt sicher, dass die Karte nicht für andere als die vorgesehenen Zwecke genutzt werden kann. Hierfür werden vom Trustcenter entsprechende Attribute auf die Karte angebracht.
- **Workflow**
Ein Arbeitsablauf (engl. Workflow) ist eine Menge von automatisiert ablaufenden Aktivitäten. Ein Geschäftsprozess wird also automatisiert, elektronisch unterstützt, abgewickelt. Das Ziel ist hierbei weniger eine Dokumentation für die Mitarbeiter als eine mögliche (Teil-)Automatisierbarkeit der Ausführung.
- **Workflow-Management-System**
Ein Workflow-Management-System ist ein Softwaresystem, das die Durchführung von Workflows ermöglicht, indem es die Workflow-Instanzen nach einem vorgegebenen, im Rechner abgebildeten Schema steuert und dazu benötigte Daten und Applikationen bereitstellt.
- **Zeitstempel**
Zeitstempel werden entweder online von Zeitstempeldiensten oder von entsprechenden Servern, die im Sinne einer Black Box ins Netz gestellt werden, erstellt. Die Datenstruktur eines Zeitstempels beinhaltet u.a. folgende wesentliche Inhalte:
 - Erstellungsdatum und Uhrzeit des Zeitstempels
 - Hashwert

9 Anlagen

9.1 Zusammenfassung: Behandlung elektronischer Dokumente

Lfd. Nr.		Beschreibung	Bemerkungen	Aufbewahrung
1	Dokumente (Papierform)			
1.1	eingehend:			
1.1.1	Briefe / Formulare / Vordrucke / Urkunden	In Papierform eingehende Unterlagen (Briefe, Formulare, Vordrucke, zahlungsbegründende Unterlagen) werden durch Einscannen in die elektronische Form überführt.	Das Dokument (Image) wird durch den Scan-Operator durch Anbringung einer qualifizierten elektronischen Signatur (QES) nach SigG gegen Veränderungen geschützt (Authentizität / Integrität). Außerdem wird hierdurch bestätigt, dass das Original vorgelegen hat und urschriftgetreu in eine elektronische Form umgewandelt wurde.	Alle Dokumente sind entsprechend den jeweils geltenden Aufbewahrungsfristen zu speichern. Zur Sicherstellung einer ggf. notwendigen Neusignierung gem. § 17 SigV sollte die Langzeitspeicherung nach dem im ArchiSig-Konzept entwickelten Hashbaum-Verfahren erfolgen.
1.1.2	FAX Kopien	In Papier ausgedruckte Faxe werden wie Papierunterlagen behandelt. Vor dem Einscannen sind sie (z.B. durch Stempelaufdruck „FAX“) besonders zu kennzeichnen. In Papierform eingehende Dokumente, bei denen ersichtlich ist, dass es sich um Kopien handelt, sind vor dem Einscannvorgang besonders zu kennzeichnen (z.B. durch Stempelaufdruck „Kopie“).	siehe 1.1.1	siehe 1.1.1
1.2	ausgehend:			
1.2.1	Bescheide / Formulare / Vordrucke / Papier-Faxe	<ul style="list-style-type: none"> Briefe / Formulare, die der SVTr an Versicherte, Arbeitgeber, Leistungserbringer oder Behörden in Papierform verschickt, werden i.d.R. unterschrieben. Bei mit Hilfe automatischer Einrichtungen erlassenen Briefen/Bescheiden sind Unterschrift bzw. Namenswiedergabe entbehrlich (§ 33 Abs. 5 SGB X). 	<ul style="list-style-type: none"> (masch.)Versand des Papierdokumentes über „Poststraße“ (ggf. ohne Unterschrift) 	<ul style="list-style-type: none"> Aufbewahrung des Original-(Papier)-Dokuments oder Aufbewahrung der mit der QES des Absenders/Erstellers versehenen Datei. <p>Die Zusendung von Fragebögen / Formularen ist in der eAkte bzw. im Fachverfahren zu speichern. Ein Abbild des leeren Formulars ist nicht zu speichern. Erst das zurückgesandte (ausgefüllte) Formular wird gem. Ziff. 1.1.1 eingescannt und archiviert.</p>
2	Elektronische Dokumente (Datei, E-Mail, Anhang, Elektronisches FAX)			
2.1	eingehend:			
2.1.1	Allg. Anfrage	<ul style="list-style-type: none"> E-Mails mit allg. Anfragen gehen i.d.R. nur mit einer einfachen Namensnennung des Absenders beim SVTr ein. Dies entspricht einer „einfachen“ Signatur i. S. § 2 Nr. 1 SigG. 	<ul style="list-style-type: none"> Eingehende E-Mails müssen den Absender erkennen lassen, damit sie der E-Akte des Versicherten zugeordnet werden können. 	Sofern die E-Mail für den Bearbeitungsvorgang von Bedeutung ist, muss sie aufbewahrt werden (Einzelfallentscheidung durch SB). In diesem Fall ist sie mit einer QES des Empfängers (Bearbeiters) zu versehen.
2.1.2	Antrag (Mitgliedschaft, Leistungen), Leistungsabrechnung	<ul style="list-style-type: none"> Anträge von Kunden gehen meist als E-Mail bzw. Mail-Anhang ein. Hierbei handelt es sich insbesondere um Dateien in den Formaten „doc“, „pdf“ oder „tif“, bei denen der Absender neben Text ggf. auch eine eingescannte Unterschrift verwendet hat. Anträge in elektronischer Form (z.B. Mail-Anhang) müssen – aufgrund der Nichtförmlichkeit des Verwaltungsverfahrens § 9 SGB X - grundsätzlich nicht signiert sein. Ausnahme: Bei durch Rechtsvorschrift angeordneter Schriftform muss der Antrag mit einer QES des Absenders versehen sein. Fehlt eine solche, ist die fehlende 	<ul style="list-style-type: none"> Siehe 2.1.1 Elektronische Dokumente (z.B. Mail-Anhänge), mit denen eine Mitgliedschaft oder Leistung beantragt wird, für die (in Papierform) eine körperliche Unterschrift vorgeschrieben ist, müssen mit einer QES des Absenders versehen sein. Eine Verschlüsselung kann dazu führen, dass der Empfänger die Nachricht nicht lesen kann. In diesem Fall ist § 36a Abs. 3 SGB I anzuwenden. Bei unverschlüsselt eingehenden Anträgen hat der SV-Träger den Absender auf den Schutz der Sozialdaten auf dem Transportweg hinzuweisen. 	<ul style="list-style-type: none"> Alle Vorgänge sind mit der QES des Absenders zu speichern. Ist eine solche nicht vorhanden, muss das Dokument vor der Langzeitspeicherung mit einer QES des Empfängers (Bearbeiters) signiert werden.

Lfd. Nr.		Beschreibung	Bemerkungen	Aufbewahrung
		Unterschrift u.U. auf einem „Papiervordruck“ nachträglich einzuholen.		
2.1.3	Elektronisches FAX	<ul style="list-style-type: none"> Eingang auf einem zentralen Fax-Server oder direkt im Postfach des zuständigen Mitarbeiters 	<ul style="list-style-type: none"> Das elektronische Fax muss als solches gekennzeichnet werden. Dies kann erfolgen durch <ul style="list-style-type: none"> die vom Absender übermittelten Header-Informationen, einen elektronischen Eingangsstempel oder eine sonstige elektronische Kennzeichnung (z.B. „FAX“) durch den SV-Träger unmittelbar nach dem Eingang. 	<ul style="list-style-type: none"> Das eingegangene elektronische Fax ist - sofern es rechtserheblichen Charakter hat - gem. §§ 110a + d SGB IV mit einer QES des Empfängers (Bearbeiter) zu versehen und zu speichern. Durch technische Maßnahmen ist sicherzustellen, dass die auf dem Fax-Server eingehenden Faxe vor der Signatur nicht manipuliert werden können.
2.1.4	E-Mail	<ul style="list-style-type: none"> Eingang auf einem zentralen Mail-Server oder direkt im Postfach/E-Mail-Client des zuständigen Mitarbeiters 		<ul style="list-style-type: none"> Mails und Anhänge ohne QES sind (zur Sicherung der Integrität) gem. §§ 110a + d SGB IV mit einer QES des Empfängers (Bearbeiter) zu versehen und zu speichern, sofern es sich um ein Dokument mit rechtserheblichem Inhalt handelt. Durch technische Maßnahmen ist sicherzustellen, dass die auf dem Mail-Server eingehenden Mails vor der Signatur nicht manipuliert werden können.
2.2	ausgehend:			
2.2.1	Extern:	<ul style="list-style-type: none"> Eine elektronische Kommunikation zum Versicherten / Leistungserbringer ist nur zulässig, wenn dieser hierfür einen Zugang eröffnet hat. Hierzu muss dieser eine entsprechende Erklärung gegenüber dem SVTr abgeben; die bloße Angabe einer E-Mail-Adresse reicht nicht aus. 		
2.2.1.1	Allg. Informationen	<ul style="list-style-type: none"> Aufgrund der Nichtförmlichkeit des Verfahrens gem. § 9 SGB X ist eine Signatur durch den SV-Träger nicht erforderlich. 		<ul style="list-style-type: none"> Bei sog. Mailing-Aktionen (elektronische Post mit gleichem Inhalt) muss der KV-Träger entscheiden, ob eine Langzeitspeicherung zu Beweis Zwecken notwendig ist.
2.2.1.2	Entscheidungen des SV-Trägers	<ul style="list-style-type: none"> Verwaltungsakte, die von einem elektronischen Rechner erzeugt und vom SV-Träger an den elektronischen Rechner eines Versicherten, Arbeitgebers, Leistungserbringer oder eine Behörde in elektronischer Form (als E-Mail-Anhänge) verschickt werden, müssen i.d.R. nicht unterschrieben werden (§ 33 Abs. 5 SGB X). Sie müssen lediglich die erlassende Stelle und die Unterschrift oder Namenswiedergabe des Leiters, seines Vertreters oder eines Beauftragten enthalten (§ 33 Abs. 3 SGB X). Grundsätzlich keine Signatur erforderlich (§ 9 SGB X) Ausnahme: Bei durch Rechtsvorschrift angeordneter Schriftform muss das der Signatur zugrunde liegende qualifizierte Zertifikat die erlassende Behörde erkennen lassen. (§ 33 Abs. 3 S. 2 SGB X). 	<ul style="list-style-type: none"> Verschlüsselung zur Sicherung der Vertraulichkeit. Zum Beweis des Zugangs eines elektronischen Dokuments beim Empfänger ist eine (elektronische) Quittung anzufordern. Alternative Zustellung: Ablage des Dokumentes in einem persönlichen Postfach, das dem Empfänger auf den Internet-Seiten des SVTr zur Verfügung gestellt wird. Zugriff über SSL-Verbindung (128-Bit-Verschlüsselung). 	<ul style="list-style-type: none"> Die E-Mail und Datei (-Anhang) müssen mit einer QES des Erstellers (Bearbeiter) versehen und aufbewahrt werden. Dies gilt auch für elektronisch erzeugte Faxe.
2.2.2	Intern:	<ul style="list-style-type: none"> Intern zum Bearbeitungsvorgang gehörige / versandte Dokumente, Protokolle, Verfügungen, Entscheidungsvorlagen oder E-Mails. 	<ul style="list-style-type: none"> Durch edv-technische und organisatorische Maßnahmen ist sicher zu stellen, dass nur die Systemadministration User bzw. E-Mail-Accounts anlegen / löschen 	<ul style="list-style-type: none"> Diese Dokumente sind grundsätzlich als Teil eines Bearbeitungsvorganges aufzubewahren. Sofern in ihnen für das Verwal-

Lfd. Nr.		Beschreibung	Bemerkungen	Aufbewahrung
			<p>schen / bearbeiten kann.</p> <ul style="list-style-type: none"> • Der Ersteller / Bearbeiter des Vermerks muss systemseitig nachvollziehbar dokumentiert werden. • User dürfen im Workflow von ihnen erstellte Dokumente nicht mehr nachträglich ändern / löschen können, sobald der zugehörige Bearbeitungsvorgang abgeschlossen und archiviert worden ist. 	tungsverfahren rechtserhebliche Sachverhalte beschrieben oder entschieden werden („Beweischarakter“), sind sie mit einer QES des Erstellers (Bearbeiter) zu versehen.
2.2.3	Buchungs- / Kassenanordnungen	<ul style="list-style-type: none"> • Für Buchungs- / Kassenanordnungen besteht nach SVRV und SRVwV grundsätzlich ein Schriftformerfordernis. Sofern derartige Verwaltungsvorgänge vollelektronisch abgewickelt werden, sind die erforderlichen Unterschriften durch die QES zu ersetzen. 	<ul style="list-style-type: none"> • QES als Ersatz für die sonst in körperlicher Form zu leistenden Unterschriften. • Gilt auch für die Feststellung der sachlichen und rechnerischen Richtigkeit von zahlungsbe gründenden Unterlagen. 	<ul style="list-style-type: none"> • Aufbewahrung mit QES des Erstellers (Bearbeiter) zwingend erforderlich.
3	Web-Formular			
	Vorbemerkungen	<ul style="list-style-type: none"> • SVTr stellen auf ihren Internetseiten für Versicherte, Arbeitgeber und Leistungserbringer Web-Formulare zur Verfügung, über die z.B. Anschriftänderungen, Kontoverbindungen oder Entgeltmeldungen elektronisch übermittelt werden können. • Die Daten gehen beim SVTr auf unterschiedliche Weise ein: <ol style="list-style-type: none"> 1. Am Bildschirm wird lediglich ein PDF-Formular erzeugt, dass der Absender dort ausfüllen, ausdrucken und per Post versenden muss. 2. Die am Bildschirm eingegebenen Daten erzeugen systemintern eine Text-Mail, die an den SVTr übermittelt wird. 3. Die am Bildschirm eingegebenen Daten erzeugen systemintern einen Datensatz, der in die Host-Anwendung beim SVTr automatisch einfließt. 	<p>Folgende Grundanforderungen müssen bei direktem Datenfluss in das DV-System des SVTr mindestens erfüllt sein:</p> <ul style="list-style-type: none"> • Zugang nur über vom SVTr vergebene Benutzer-ID und Kennwort • Zugangssicherung mindestens SSL-verschlüsselt (HTTPS) • Direkt in das System einfließende Daten(-Änderungen) sind zu historisieren und zu speichern. 	
3.1	Allgemeines/Info-Anforderung	<ul style="list-style-type: none"> • Der Versicherte fordert allgemein zugängliches Informationsmaterial an. 	<ul style="list-style-type: none"> • Keine besonderen Sicherungsmaßnahmen erforderlich. 	<ul style="list-style-type: none"> • Keine Aufbewahrung notwendig.
3.2	Antrag (Mitgliedschaft, Leistungen), Leistungsabrechnung	<ul style="list-style-type: none"> • Anträge in elektronischer Form (z.B. im Web-Formular) müssen – aufgrund der Nichtförmlichkeit des Verfahrens § 9 SGB X –grundsätzlich nicht signiert sein. • Ausnahme: Bei durch Rechtsvorschrift angeordneter Schriftform (z.B. Antrag frw. Mitgliedschaft, Fami-Bogen) muss der Antrag mit einer QES des Absenders versehen sein. Fehlt eine solche, ist die fehlende Unterschrift u.U. auf einem „Papiervordruck“ nachträglich einzuholen. 	<ul style="list-style-type: none"> • Verschlüsselung zur Sicherung der Vertraulichkeit. • Der Zugang des Versicherten zu seinem persönlichen Online-Bereich über Benutzerkennung, Passwort und ggf. iTAN's und Übermittlung eines ausgefüllten Online-Fragebogens über eine gesicherte Leitung (z.B. Verschlüsselung HTTPS) ersetzt bei einem Schriftformerfordernis (z.B. Prüfung freiwillige Versicherung) nicht die QES gem. § 36a Abs. 2 SGB I ! 	<ul style="list-style-type: none"> • Alle Vorgänge sind mit einer QES des Absenders zu versehen und aufzubewahren. • Ist eine QES des Absenders nicht vorhanden, muss das Dokument mit einer QES des Empfängers (Bearbeiter) versehen werden, um es vor Integritätsverlust zu schützen.