Spitzenverband Bund der Krankenkassen, Berlin

Deutsche Rentenversicherung Bund, Berlin

Deutsche Rentenversicherung Knappschaft-Bahn-See, Bochum

Bundesagentur für Arbeit, Nürnberg

Deutsche Gesetzliche Unfallversicherung e.V., Berlin

26.10.2017

Gemeinsame Grundsätze Technik für die elektronische Datenübermittlung gemäß § 95 SGB IV

in der vom 01.01.2018 an geltenden Fassung[1]

Der Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband), die Deutsche Rentenversicherung Bund, die Deutsche Rentenversicherung Knappschaft-Bahn-See, die Bundesagentur für Arbeit sowie die Deutsche Gesetzliche Unfallversicherung haben Standards für die elektronische Datenübermittlung an die oder innerhalb der Sozialversicherung in dem nachfolgenden Dokument aufgestellt. Sie kommen damit ihrer Verpflichtung gemäß § 95 SGB IV nach. Die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau sowie die Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen (ABV) haben an der Erstellung dieser Gemeinsamen Grundsätze Technik mitgewirkt.

Die „Gemeinsamen Grundsätze Technik für die elektronische Datenübermittlung an die oder innerhalb der Sozialversicherung“ sind nach Anhörung des Bundesministeriums für Gesundheit sowie der Bundesvereinigung der Deutschen Arbeitgeberverbände e.V. durch das Bundesministerium für Arbeit und Soziales genehmigt worden.

Die gemeinsamen Grundsätze werden durch gemeinsame Verlautbarungen der Spitzenorganisationen der Sozialversicherung erläutert.

---

[1] Das Bundesministerium für Arbeit und Soziales hat die Gemeinsamen Grundsätze nach Anhörung des Bundesministeriums für Gesundheit und der Bundesvereinigung Deutscher Arbeitgeberverbände e.V. am 14.11.2017 genehmigt.

Inhaltsverzeichnis

Anlagen

Anlage	Titel
1	Krankenkassenkommunikationssystem
2	Auftragsdatei
3	eXTra (Einheitliches XML-basiertes Transportverfahren)
4	Verfahrenskennungen
5	Datenaustausch mit der Rentenversicherung
6	Datenaustausch mit der GKV
7	E-Mail
8	HTTP
9	FTP
10	FTAM over IP
11	Nicht belegt
12	XML
13	GKV-Kommunikationsserver
14	Datenträger
15	Zeichensätze
16	Security Schnittstelle
17	Kommunikationsserver der Deutschen Rentenversicherung
18	Begriffe und Abkürzungsverzeichnis

1. Allgemeines

Der GKV-Spitzenverband, die Deutsche Rentenversicherung Bund, die Deutsche Rentenversicherung Knappschaft Bahn-See, die Bundesagentur für Arbeit sowie die Deutsche Gesetzliche Unfallversicherung bestimmen in den nachfolgenden, gemeinsamen Grundsätzen

- die Datenaustauschverfahren,
- die Parameter für den Datenaustausch,
- die Datenaustauscharten,
- das Sicherheitsverfahren für den Datenaustausch und
- das Rückmeldeverfahren (soweit es nicht ein Verfahren des Datenaustauschs mit Arbeitgebern betrifft).

Der weiter fortschreitende Wechsel von der papierbasierenden Kommunikation zur Datenfernübertragung stellt die Systeme im Gesundheits- und Sozialwesen vor die besondere Anforderung, die technischen Rahmenbedingungen so zu gestalten, dass eine effiziente und auch effektive Kommunikation betrieben werden kann. So ist es von besonderer Bedeutung, dass die Kommunikationsverfahren möglichst einheitlich und transparent sind. Je einheitlicher diese Kommunikationssysteme sind, umso zuverlässiger und flexibler kann die Kommunikation betrieben werden.

Zusätzliche Voraussetzung für den elektronischen Datenaustausch personenbezogener Daten ist, dass Vertraulichkeit, Integrität und Verbindlichkeit in gleicher Weise sichergestellt werden, wie beim herkömmlichen papiergebundenen Abrechnungsverfahren, z. B. durch verschlossene Umschläge und persönliche Unterschriften. Im Gesundheits- und Sozialwesen werden hierfür zum Datenaustausch der beteiligten Partner Verschlüsselungsverfahren und elektronische Signaturen auf der Grundlage kryptographischer Verfahren eingesetzt. Die Nutzdaten müssen mit einem gültigen Zertifikat elektronisch signiert und verschlüsselt werden.

2. Datenaustauschverfahren

2.1 Grundlagen

Der Datenaustausch im Sinne dieser gemeinsamen Grundsätze bedeutet, dass Daten zwischen einer abgebenden Stelle und einer empfangenden Stelle per Datenfernübertragung (DFÜ) oder soweit noch erforderlich, mittels Datenträger ausgetauscht werden. Bei der Gestaltung der Datenfernübertragung und des Datenträgeraustausches ist die Vollständigkeit der regelungsbedürftigen Sachverhalte anhand der folgenden Liste zu prüfen:

- Rechtliche Grundlage
- Zweck und Anwendungsbereich
- Teilnahmeberechtigte oder -verpflichtete
- Anmeldeverfahren
- Testverfahren
- Beginn und Turnus des Datenaustausches
- Bearbeitungsfristen, Verfügbarkeit
- Datenaustauschart und ihre technischen Anforderungen
- Zeichenvorrat / Code
- Dateinamen, Verfahrenskennungen
- Komprimierungsverfahren
- Datenschutzmaßnahmen
- Versandwege, Datenfernübertragungswege
- Datenträgeraustausch, Datenfernübertragungsdienste, Datenübertragungssteuerung und höhere Kommunikationsfunktionen
- Bereitstellung, Pflege, Löschen und Verbleib der Datenträger
- Datensicherung und Dokumentation
- Prüfung und Fehlerbehandlung
- Haftung
- Kostenregelung
- Übergangsbestimmung

2.2 Steuerung der Datenaustauschverfahren

Der Datenaustausch zwischen den beteiligten Partnern steuert sich im Wesentlichen über den Dateinamen der Datenlieferung. Dieser Dateiname ist codiert und ergibt sich aus einer Kombination aus Verfahrensmerkmalen und einer eindeutigen Ziffernfolge. Somit lässt sich, ohne auf den Dateiinhalt zurück zu greifen, eine Zuordnung für die Weiterverarbeitung der Datenlieferung erkennen. Eine detailliertere Beschreibung dieser Steuerung folgt im Kapitel 3.

2.3 Krankenkassenkommunikationssystem (KKS)

Das Krankenkassenkommunikationssystem beschreibt eine universelle Struktur von Daten, die per Datenfernübertragung wie auch per Datenträger übertragen werden können. Der Aufbau der Dateilieferung im KKS Verfahren ist so definiert, dass unabhängig voneinander zwei korrespondierende Dateien übertragen werden. Dabei enthält die erste Datei die sog. Nutzdaten, welche in binärer Form vorliegen und verschlüsselt sein müssen. Die Dateistruktur bzw. der Satzaufbau dieser Nutzdatendatei wird von der jeweiligen Fachanwendung definiert. Die zweite, sog. Auftragsdatei (Auftragssatz) wird unverschlüsselt übertragen und enthält die notwendigen Informationen, um die Nutzdatendatei transportieren (weiterleiten) und verarbeiten zu können. Dabei können je nach Übertragungsweg eine oder mehrere Stellen als Vermittlungsstellen (physikalische Empfänger) fungieren, nur die letztendlich adressierte Datenstelle (logischer Empfänger) kann die Nutzdaten entschlüsseln, weiterleiten oder verarbeiten. Das KKS Verfahren erlaubt, mehrere Datenlieferungen in Form von Dateipärchen (Nutzdaten und Auftragsdatei) auf einem Datenträger zu übertragen.

- Anlage 1- Krankenkassenkommunikationssystem
  und
- Anlage 2 - Auftragsdatei

2.4 Einheitliches XML-basiertes Transportverfahren (eXTra)

Das „einheitliche XML-basierte Transportverfahren (eXTra-Standard)“ ist ein frei verfügbarer, von der „Arbeitsgemeinschaft für wirtschaftliche Verwaltung“ redaktionell gepflegter Standard für den Datenaustausch zwischen Wirtschaft und Verwaltung. In ihm wird der technische Rahmen, allerdings nicht der Übertragungsweg für standardisierte XML-Pakete festgelegt, die zwischen den Verfahrensbeteiligten übermittelt werden. Der eXTra-Standard kennt 6 unterschiedliche Rollen und 3 Ebenen:

- Rollen
  - Erzeuger (Fachlicher Sender)
  - Logischer Sender
  - Physischer Sender
  - Physischer Empfänger
  - Logischer Empfänger
  - Verwerter (fachlicher Empfänger)
- Ebenen:
  - Nachrichtenebene
  - Transportebene
  - Logistikebene

Der eXTra-Standard trifft keine Festlegungen zur Registrierung, Authentifizierung, zu Format und Struktur der fachlichen Nutzdaten, zu Übertragungsverfahren- und protokollen, zur Archivierung und zur Kommunikation innerhalb der Sender- bzw. Empfängerseite.
Der eXTra Standard beschreibt einen Baukasten an technischen Komponenten für den Datenaustausch. Für die einzelnen Fachverfahren können aus diesem Baukasten die notwendigen oder gewünschten Komponenten profiliert werden. Diese eXTra Profile werden von der AWV abgenommen und auf der Seite www.extra-standard.de ebenso wie die jeweils gültige Version des Standards veröffentlicht.

Die Dokumente zum eXTra-Standard werden bei der Datenstelle der Deutschen Rentenversicherung Bund, Berner Straße 1, 97084 Würzburg archiviert.

- Anlage 3 – eXTra

3. Parameter für den Datenaustausch

3.1 Verfahrenskennung

Die Verfahrenskennung ist ein wichtiger Baustein bei der Generierung des (Transfer-) Dateinamens der Nutzdatendatei und zur Identifikation der empfangenen Datei bei der Datenannahmestelle. Die Verfahrenskennungen werden von den Fachverfahren beantragt und in einer Zusammenfassung veröffentlicht. Das Feld VERFAHREN_KENNUNG ist in den Stellen 20-24 des Auftragssatzes festgelegt.

- Anlage 4 – Verfahrenskennungen

3.2 Weitergehende Beschreibung in den Verfahren

In den Verfahren wird der Dateityp und die Übertragungsrichtung eindeutig pro Verfahren (bei Datenaustausch z. B. der Nachrichtentyp, sofern eindeutig pro Lieferung) im Feld VERFAHREN_KENNUNG_SPEZIFIKATION festgelegt. Damit ist pro Verfahren eine weitere Unterscheidung der Nachrichtenart möglich. Dieses Feld kann benutzt werden, um die Verarbeitungspriorität auszudrücken. Das Feld VERFAHREN_KENNUNG_SPEZIFIKATION ist in den Stellen 28-32 des Auftragssatzes festgelegt.

- Anlage 4 – Verfahrenskennungen

3.3 Verfahrensteilnehmer

Zur Sicherstellung aller Funktionen im Datenaustausch müssen alle teilnehmenden Kommunikationspartner bekannt sein. Ebenso die untereinander auszutauschenden Daten, die sich über die Verfahrenskennungen identifizieren. Für festgelegte Verfahren haben die Teilnehmer Besonderheiten definiert, siehe dazu folgende Anlagen:

- Anlage 5 – Datenaustausch mit der Rentenversicherung
  und
- Anlage 6 – Besonderheiten des GKVinternen Datenaustauschs und des Datenaustauschs der GKV mit Leistungserbringern

4. Datenaustauscharten

4.1 Allgemeines

Grundsätzlich ist die Datenfernübertragung (DFÜ) als Austauschart zu verwenden. Das verwendete Datenaustauschverfahren wird bilateral und einvernehmlich zwischen Datenlieferant und Datenempfänger nach Maßgabe dieser Gemeinsamen Grundsätze Technik inkl. aller Anlagen vereinbart. Soweit eine Fernübertragung aus technisch/wirtschaftlichen Gründen nicht realisiert werden kann, können die beteiligten Stellen auf einvernehmlicher Basis Datenträger vereinbaren.

Im KKS-Verfahren erfolgt die Übertragung jeder verschlüsselten Nutzdatendatei als separate Datei. Nach der Übertragung einer Nutzdatendatei wird die dazugehörige Auftragsdatei übertragen. Ein Übertragungsvorgang besteht aus der Übertragung dieser zwei Dateien in der festgelegten Reihenfolge.

Im eXTra-Verfahren werden die Routinginformationen im Header, die verschlüsselte, Base64 codierte Nutzdatendatei im Nachrichtenbody in einer einzigen XML-Nachricht übertragen.

Die unter den Punkten 4.2 und 4.3 aufgeführten Datenaustauscharten unterliegen verfahrensabhängig folgender Gültigkeit:

	Arbeitgeberverfahren	Verfahren der Leistungserbringer
Internet-E-Mail-Kommunikation	-	zulässig
Internet-http(s)-Kommunikation	-[2]	zulässig
Internet-(s)ftp(s)-Kommunikation	-	zulässig
FTAM	-	zulässig
X.400	-	zulässig
GKV-Kommunikationsserver (eXTra)	zulässig	-
DSRV-Kommunikationsserver (eXTra)	zulässig	zulässig
Datenträger	-	zulässig

4.2 Datenfernübertragung

4.2.1 Internet - E-Mail-Kommunikation

Mit dem standardisierten E-Mail Verfahren wird die bisherige elektronische Kommunikation zwischen Leistungserbringern und Annahmestellen als dateiorientierte Übertragung beibehalten. Es werden eine verschlüsselte Nutzdatendatei mit den eigentlichen Meldungen und ein Auftragssatz mit Routinginformationen als Anhang an die E-Mail gehängt und versendet.

[2] Zulässig im Rahmen der Kommunikation über die Kommunikationsserver und ausschließlich https

Um zu verhindern, dass die Meldungen verfälscht oder von Unberechtigten gelesen werden, werden sie nach den Vorgaben im Gesundheits- und Sozialwesen verschlüsselt.

Pro E-Mail darf immer nur eine Nutzdaten- und eine Auftragsdatei übermittelt werden. Es ist nicht möglich, mehrere Dateipaare mit einer E-Mail zu versenden. Die E-Mail wird an die Annahmestelle adressiert, dort empfangen, geprüft und weiter verarbeitet.

Das E-Mail Verfahren sieht eine Antwort-E-Mail vor, ebenfalls werden fehlerhafte Datenlieferungen per E-Mail quittiert.

- Anlage 7 – E-Mail

4.2.2 Internet – http(s)-Kommunikation

Es werden die beiden Übertragungsverfahren HTTP und HTTPS[3] zur Kommunikation über das Internet angeboten. Die elektronische Kommunikation zwischen Arbeitgebern, Leistungserbringern und Annahmestellen ist dateiorientiert. Es werden eine Nutzdaten-Datei mit den eigentlichen Nachrichten und ein Auftragssatz mit Routinginformationen gebildet.

Um zu verhindern, dass Meldungen verfälscht oder von Unberechtigten gelesen werden, werden die Nutzdaten verschlüsselt. Hier werden im Gesundheits- und Sozialwesen etablierte Verfahren verwendet, die jeweils gültige Security Schnittstelle ist bindend.

Das Übermittlungsverfahren über HTTP bzw. HTTPS kommt sowohl bei Übermittlungen an die GKV-Annahmestellen als auch bei Rückmeldungen an die Teilnehmer zur Anwendung. Die Übermittlungen und Rückmeldungen erfolgen separat, da die Rückmeldungen nur auf eine Anfrage eines Teilnehmers von den Datenannahmestellen bereitgestellt werden.

Gemäß den Vorgaben des Gesundheits- und Sozialwesen verschlüsselt der Absender die Datei für den Empfänger, erstellt den dazugehörigen Auftragssatz und überträgt die Dateien mittels HTTP/HTTPS-Upload zu einem Server des Empfängers im Internet.

Zur weiteren Erhöhung der Sicherheit des Datenaustauschs im Gesundheits- und Sozialwesen ist ab dem 01.01.2019 zwingend eine Transportverschlüsselung bei der Nutzung des http-Protokolls vorgeschrieben. Diese kann durch die Nutzung von https oder eines VPN-Tunnels sichergestellt werden.

- Anlage 8 – http https

[3] Für die Verfahren im Datenaustausch mit Arbeitgebern ist ausschließlich die Verwendung von https zugelassen.

4.2.3 Internet – (s)ftp(s)-Kommunikation

Das File Transfer Protocol ist ein standardisiertes Netzwerkprotokoll zur Übertragung von Dateien über TCP/IP-Netzwerke. FTP wird benutzt, um Dateien vom Server zum Client (Herunterladen), vom Client zum Server (Hochladen) oder clientgesteuert zwischen zwei Endgeräten zu übertragen. Außerdem können mit FTP Verzeichnisse angelegt und ausgelesen, sowie Verzeichnisse und Dateien umbenannt oder gelöscht werden.

Auch bei der FTP Übertragung werden immer eine verschlüsselte Nutzdaten- und eine Auftragsdatei übermittelt; es ist allerdings möglich, mehrere Dateipaare in einer Übertragung zu übermitteln.

Die FTP Übertragung beginnt mit einer Anmeldung vom Client (Absender) beim FTP Server des Empfängers. Über diese Verbindung werden Befehle zum Server gesendet. Der Server antwortet auf jeden Befehl mit einem Statuscode, oft mit einem angehängten, erklärenden Text.

Um eine geschützte Verbindung aufzubauen, können die erweiterten Protokolle SFTP und FTPS genutzt werden.

Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht.

FTP über SSL, kurz FTPS, ist eine Methode zur Verschlüsselung des File Transfer Protocol (FTP); im Unterschied zu SFTP ist FTPS eine Kombination von FTP und dem Transport Layer Security (TLS).

Zur weiteren Erhöhung der Sicherheit des Datenaustauschs im Gesundheits- und Sozialwesen ist ab dem 01.01.2019 zwingend eine Transportverschlüsselung bei der Nutzung des FTP-Protokolls vorgeschrieben. Diese kann durch die Nutzung von FTPS, SFTP oder eines VPN-Tunnels sichergestellt werden.

- Anlage 9 – ftp sftp ftps

4.2.4 File Transfer, Access und Management over IP – FTAM over IP

FTAM dient sowohl der Unterstützung des Austauschs vollständiger Dateien als auch dem Lesen und Ändern von Dateiausschnitten, Dateiattributen und Inhaltsverzeichnissen. Um dies unabhängig von der jeweilig im System implementierten Dateiorganisation zu gewährleisten, verwendet FTAM ein logisches Dateisystem, den Virtual Filestore. Dieser Virtual Filestore wird durch die jeweilige Herstellerimplementation auf das reale System abgebildet.

Der Zugang zu den entfernten Dateien erfolgt dabei nicht unmittelbar, sondern über Dienste der dort installierten FTAM Software, ist also nicht mit einem allgemeinen Zugang zum entfernten System gleichzusetzen.

Auch bei der FTAM Übertragung werden immer eine verschlüsselte Nutzdaten- und eine Auftragsdatei übermittelt; es ist allerdings möglich, mehrere Dateipaare in einer Übertragung zu übermitteln.

Die Verbindungsaufnahme zwischen FTAM-Initiator und Responder erfolgt über eine Anmeldeprozedure. Dabei wird entschieden, ob der Nutzer berechtigt ist, Zugriff auf das System zu erhalten. Im Anschluss daran erfolgt die protokollierte Dateiübertragung.

Ab dem 01.01.2018 ist ausschließlich die Nutzung von FTAM over IP zulässig.

- Anlage 10 – FTAM over IP

4.2.5 XML-Empfehlung

Durch die Schaffung einer einheitlichen XML-Empfehlung sollen sämtliche XML-Aktivitäten im Umfeld der Sozialversicherung zentralisiert und gebündelt werden. Durch deren modularisierten Aufbau sollen so zukünftig einheitliche und integrierte XML-Schnittstellen entwickelt werden können. Dies kann mittel- und langfristig zu Effizienzsteigerungen und Kosteneinsparungen führen. Insbesondere lassen sich durch dieses Vorgehen die Implementierungsaufwände drastisch reduzieren.

Durch die XML-Empfehlung wird für den Datenaustausch auf Basis von XML ein standardisiertes und einheitliches Rahmenwerk geschaffen, mit dessen Hilfe alle zukünftigen XML-Schnittstellenimplementierungen vollständig beschrieben werden können. Hierbei werden nicht nur die Sprachelemente und konkreten Entwurfsprinzipien vorgeschrieben, sondern auch die Grundstrukturen verfahrensneutral festgelegt.

- Anlage 12 – XML Empfehlung

4.2.6 GKV-Kommunikationsserver

Die Spitzenorganisationen der Krankenkassen auf Bundesebene haben die Einrichtung und den Betrieb eines zentralen GKV-Kommunikationsservers umgesetzt, um ein zentrales „Tor“ sowohl für die Annahme der Meldungen der AG, als auch zum Abruf der Rückmeldungen von den DAVn bereit zu stellen.

Dieser Kommunikationsserver etabliert ein zentrales elektronisches Verfahren, um Arbeitgeber Meldungen zu den Datenannahmestellen und deren Rückmeldungen zurück an den Arbeitgeber zu senden.

Die Übertragung zum Kommunikationsserver erfolgt über das HTTPS Protokoll, die übertragenen Daten werden dabei nach dem eXTra Standard aufbereitet.

Der eXTra-Standard stellt alle Elemente, die heute bereits im Auftragssatz existieren, im XML-Format zum Transport zur Verfügung. Somit können die Transportinformationen aus dem Auftragssatz und die verschlüsselten Nutzdaten wie bisher geliefert werden.

- Anlage 13 – GKV-Kommunikationsserver

4.2.7 DSRV-Kommunikationsserver

Die Datenstelle der Träger der Rentenversicherung (DSRV) betreibt ebenfalls einen zentralen Kommunikationsserver. Dieser DSRV-Kommunikationsserver nimmt damit als zentrales "Tor" die für die Rentenversicherung registrierten Verfahren nach dem allgemeinen eXTra Standard entgegen.

Der Datenaustausch erfolgt über das HTTPS Protokoll. Bei HTTPS erfolgt eine Verschlüsselung auf Transportebene. Zusätzlich sind die Daten nach den jeweils geltenden Anforderungen der Anlage 16 verschlüsselt.

- Anlage 17 – RV-Kommunikationsserver

4.3 Datenträger

Grundsätzlich ist die Datenfernübertragung (DFÜ) als Austauschart zu verwenden. Soweit eine Fernübertragung aus technisch/wirtschaftlichen Gründen nicht realisiert werden kann, können die beteiligten Stellen auf einvernehmlicher Basis Datenträger vereinbaren, soweit dies nicht durch gesetzliche oder vertragliche Regelungen ausgeschlossen ist.

- Anlage 14 – Datenträger

4.4 Zeichensätze

Zur Vermeidung von technischen Problemen bei der Übertragung von Daten zwischen Systemen unterschiedlicher Basis ist es unabdingbar, sich vor dem vereinbarten Datenaustausch auf einen, der in der Anlage 15 aufgeführten, für alle beteiligte Systeme gültigen Zeichensatz zu verständigen.

- Anlage 15 – Zeichensätze

5. Sicherheitsverfahren

5.1 Verschlüsselung und Signatur

Eine zwingende Voraussetzung für den sicheren elektronischen Datenaustausch personenbezogener Daten ist, dass Vertraulichkeit, Integrität und Verbindlichkeit in gleicher Weise gewährleistet werden, wie beim herkömmlichen papiergebundenen Meldeverfahren, z. B. durch verschlossene Umschläge. Im Gesundheits- und Sozialwesen werden hierfür zum Datenaustausch mit Arbeitgebern und Leistungserbringern Verschlüsselungsverfahren und die digitale Signatur auf der Grundlage kryptographischer Verfahren eingesetzt. Dabei nutzt jeder Beteiligte zwei Schlüssel; einen öffentlichen und einen privaten Schlüssel. Die Nachrichten werden von dem Absender zunächst mit seinem privaten Schlüssel signiert, bei der folgenden Verschlüsselung unter Nutzung des öffentlichen Schlüssels des Empfängers unkenntlich gemacht. Dieser kann nun als einziger die Nachricht unter Nutzung seines privaten Schlüssels auslesen; über die Signatur wird zusätzlich die Identität des Absenders geprüft. Mit diesem Verfahren wird sichergestellt, dass nur die vom Absender berechtigten Empfänger Nachrichten lesen können.

5.2 Gültigkeitsprüfung der Zertifikate

Bei der Datenannahme muss das Zertifikat des Absenders auf Gültigkeit überprüft werden.

- Anlage 16 – Security Schnittstelle

5.3 Überprüfung und Fortschreibung der IT-Sicherheit

Um die Sicherheit des Datenaustauschs im Gesundheits- und Sozialwesen langfristig zu gewährleisten, ist es von Zeit zu Zeit erforderlich, die kryptographischen Verfahren hinsichtlich der Notwendigkeit von Änderungen zu prüfen. Grundlage bei der Ermittlung der Änderungsbedarfe bilden die strengen Empfehlungen aus der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Algorithmenkatalog) der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn sowie aus der Technischen Richtlinie TR-02102-1 der des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Aktuell sind folgende Dokumente maßgeblich:

- Die Verordnung (EU) Nr. 910/2014 (eiDAS-Verordnung) sowie ergänzend das Vertrauensdienstegesetz in seiner aktuellen Version vom 29.07.2017
- BSI Technische Richtlinie TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Version 2017-01 vom 8. Februar 2017

Beide o. g. Dokumente werden im Jahresrhythmus veröffentlicht und anschließend in einem Gremium, welches sich aus Experten aller Träger der Sozialversicherung und externen Spezialisten

zusammensetzt, auf ihre Relevanz für die Security Schnittstelle im Gesundheits- und Sozialwesen analysiert.

Auf Grund der Gültigkeit der PCA-Zertifikate von 7 Jahren und der CA-Zertifikate von 5 Jahren, ist turnusgemäß eine Erneuerung dieser Zertifikate erforderlich. Da sich Änderungen an den genutzten kryptografischen Verfahren meist nur in Verbindung mit neuen CA-Zertifikaten realisieren lassen, ist deren Erneuerung in der Regel ein geeigneter Zeitpunkt zur Umsetzung dieser Änderungen, zumal auch das BSI seine Bewertung und Empfehlung zur Sicherheit dieser Verfahren für einen Zeitraum von 6 bis 7 Jahre erstellt.

In diesem Dokument werden keine Aussagen hinsichtlich des Datenschutzes bei den Trägern im Gesundheits- und Sozialwesen getroffen. Dieser liegt in deren eigenen Verantwortung und wird in den Paragrafen 67 bis 85a im Zweiten Kapitel des SGB X geregelt.