[redacted]

[redacted]

Leiter der Stelle zur Bekämpfung von Fehlverhalten im
Gesundheitswesen gem. § 197a SGB V des
GKV-Spitzenverbands
[redacted]
10117 Berlin

[redacted] 07.10.2022

Verdacht der zweckwidrigen Verwendung von GKV-Mitteln aufgrund des Beschlusses der Gesellschafterversammlung der gematik vom 28.02.2022 bzw. 29.08.2022 zum Konnektortausch in der Telematikinfrastruktur

Sehr geehrte[redacted]
sehr geehrte Damen und Herren,

hinsichtlich der im Betreff bezeichneten Thematik wenden wir uns an die Stelle zur Bekämpfung von Fehlverhalten im Gesundheitswesen nach § 197a SGB V beim GKV-Spitzenverband.

[redacted] Es geht uns im vorliegenden Fall um die Prüfung, ob und inwieweit eine zweckwidrige Verwendung von Mitteln der gesetzlichen Krankenversicherung vorliegen könnte.

Aufgrund des im Betreff genannten Beschlusses der Gesellschafterversammlung der gematik vom 28.02.2022 bzw. 29.08.2022 zum Konnektortausch in der Telematikinfrastruktur besteht schließlich die Vermutung, dass es - in naher Zukunft - zu Unregelmäßigkeiten bzw. einer zweckwidrigen Nutzung von Finanzmitteln der Gesetzlichen Krankenversicherung kommen wird.

Es wird insoweit angezweifelt, ob eine ordnungsgemäße Umsetzung der normativen Spezifikationsvorgaben der gematik von allen Konnektorherstellern erfolgt ist und im Rahmen der Zulassungsprozesse nach § 325 Abs. 1 SGB V durch die gematik selbst geprüft und/oder das Ergebnis der Prüfung den Gesellschaftern der gematik zur Beschlussfassung über die weitere Vorgehensweise zur Entscheidungsfindung am 28.02.2022 und 29.08.2022 hinreichend zur Kenntnis gebracht wurde. Den Konnektortausch habe die Geschäftsführung der gematik der Gesellschafterversammlung, so heißt es, als einzig verlässlich umsetzbare Lösung zur Beschlussfassung empfohlen.

[redacted]

Begründung:

Die normativen Festlegungen für den Produktivbetrieb der Telematikinfrastruktur des deutschen Gesundheitswesens für das Vorhaben Onlineproduktivbetrieb 1 (OPB1) ergeben sich aus der Dokumentenlandkarte Release 1.6.4.-1 vom 23.08.2017. Die normativen Festlegungen, entsprechend dem vorgenannten Release, bilden die Grundlage für die Zulassungs- bzw. Bestätigungsverfahren der gematik für den Produktivbetrieb der TI **(vgl. Anlage 1)**.

Die ersten zugelassenen Konnektoren des Anbieters CompuGroup Medical AG sind seit September 2017 verfügbar, sodass das o. g. Release zum OPB1 nach derartiger Kenntnislage maßgeblich für das Zulassungs- bzw. Bestätigungsverfahren u. a. von Konnektoren sein dürfte.

In der Dokumentenlandkarte enthalten ist u. a. die Spezifikation des **gSMC-K-Objektsystems** V3.10.0 vom 28.10.2016 (nachweislich S. 21 der Dokumentenlandkarte zu Abschnitt 3.5. (Kartenspezifikationen)). Dieses Dokument beschreibt die Kartenschnittstelle der gerätespezifischen Security Module Card Typ-K (gSMC-K) zum Einsatz in Konnektoren. In Abschnitt 5.5.7 **(vgl. Anlage 2)** wird zu MF/DF.NK/EF.C.NK.VPN2.xxxx ausgeführt, dass die Zertifikatsdatei angelegt ist, um ein Zertifikat mit dem öffentlichen Schlüssel PuK.NK.VPN.xxxx zu PrK.NK.VPN.xxxx (xxxx steht dabei für R2048, R3072, E256, E384) nach Ablauf der Nutzungszeit des Schlüssels PrK.AK.AuT.R2048 aufzunehmen.

Die Entscheidung, welches Verschlüsselungsverfahren aus der vorgenannten Menge R3072, E384, d. h. RSA oder ECC bei einem Wechsel des Schlüsselmaterials gewählt wird, sollte zu einem späteren Zeitpunkt folgen. Augenscheinlich musste allerdings allen Herstellern klar sein, dass eine Ablösung der Schlüssel RSA und ECC mit den ab 2023 wünschenswerten und ab 2026 obligatorischen Schlüssellängen von 3072 Bit bei RSA und 384 Bit bei ECC umzusetzen ist.

Die Dokumentenlandkarte enthält ebenfalls auf Seite 21 den Hinweis zu einer weiteren Spezifikation des **Card Operating System (COS)** Elektrische Schnittstelle in der V3.10.0 vom 21.04.2017. Diese Spezifikation definiert die Anforderung an die Funktionalität einer Betriebssystemplattform (COS-Plattform) für elektronische Karten im Gesundheitswesen. Kapitel 14 enthält dabei normative Kommandos, welche an eine Smartcard geschickt werden **(vgl. Anlage 3)**. In Abschnitt 14.9.3 (S. 356 ff.) wird beschrieben, dass das Kommando Generate Asymmetric Key Pair (GAKP) dem Erzeugen von asymmetrischen Schlüsselpaaren und dem Auslesen eines dabei erzeugten öffentlichen Schlüssels dient.

Damit dies erfolgt, müssen die Konnektoren die entsprechenden Kommandos an die gSMC-K absetzen. Dies ist wiederum in der **Konnektor-Spezifikation** V4.11.1 vom 14.12.2016 **(vgl. Anlage 4)** als Bestandteil der Dokumentenlandkarte beschrieben. Diese Spezifikation definiert die Anforderung zu Herstellung, Test und Betrieb des Produkttyps Konnektor. Unter dem Abschnitt 3.1 (S. 29 ff.) wird ausgeführt, dass der Konnektor das geheime Schlüsselmaterial zur Geräteidentität (ID. NK. VPN, ID. AK. AUT, ID. SAK. AUT) und die Rolle SAK (C.SAK. AUTD-CVC) über SmartCards des Typs gSMC-K nutzen muss. Der Konnektor muss mit einer gSMC-K bestückt sein und er kann mit mehr als einer gSMC-K bestückt sein.

Unter Rd.-Nr. 962 - 965 wird weiter ausgeführt, dass die gSMC-K über die Möglichkeit zur nachträglichen Generierung von Schlüsselpaaren und dem Nachladen der zugehörigen Zertifikate verfügen muss.

[redacted]

Des Weiteren wird ausgeführt, dass dieser Mechanismus erst in den kommenden Releases durch den Konnektor unterstützt wird. Initial sind alle Identitäten jedoch bereits einmal auf der gSMC-K vorhanden. Somit musste unseres Erachtens auch hier allen Herstellern bewusst gewesen sein, dass das Nachladen von Zertifikaten als Alternative zum Hardware-Konnektortausch in Kenntnis einer langen Vorlaufzeit umzusetzen ist.

In diesem Zusammenhang stellt sich nunmehr die Frage, zu welchem Zeitpunkt die zuvor genannte Forderung in der Spezifikation festgelegt wurde?

Am 30.06.2021 trat dann die **Konnektorspezifikation Version 5.13.0** sowie die dazugehörige **Prüfvorschrift für die Produkttypversion 5 (PTV5)** in Kraft. In der Konnektorspezifikation V 5.13.0 wird auf den Seiten 32 ff. unter Punkt 3.1.1 die Erneuerung der Zertifikate der gSMC-K verbindlich für Konnektoren erläutert **(vgl. Anlage 5)**. Danach muss der Konnektor 180 Tage vor Ablauf des aktuell verwendeten Zertifikats den Zertifikatserneuerungsprozess anstoßen. Nach BSI-Vorgaben sind selbst die aktuellen RSA-Zertifikate noch bis zum 31.12.2024 nutzbar. Diese verfügbare Zeit reicht aus, um andere alternative Lösungen zum Konnektortausch zu entwickeln. Auch im Produkttypsteckbrief Prüfvorschrift Konnektor Version 5.0.0 – 0 (**vgl. Anlage 6**) vom 30.06.2021 wird u. a. auf den Seiten 2 ff. die Einarbeitung **„Feature gSMC-K-Laufzeitverlängerung“** beschrieben.

Das Feature „gSMC-K-Laufzeitverlängerung“ in der Version 1.0.0 vom 30.06.2021 beschreibt die spezifikatorische Grundlage für eine sichere verlängerte Nutzung von Konnektoridentitäten der gSMC-K. **Die Abstimmung des Dokumentes erfolgte mit den Herstellern, dem BSI und den Gesellschaftern der gematik** (vgl. Seiten 5 ff. **Anlage 7**).

In der Zielsetzung zu Punkt 1.1 dieses Dokumentes wird beschrieben, dass das Feature „Laufzeitverlängerung gSMC-K“ als eine technische Alternative zu einem Austausch der betroffenen Geräte umgesetzt werden muss. Die Umsetzung erfolgt demnach in der Produkttypversion PTV5 des Konnektors.

Ausweislich der Zulassungsübersicht **(vgl. Anlage 8)** der gematik vom 11.08.2022 hatten zwei Konnektorenhersteller die Vorgaben PTV5 am 29.12.2021 (Fa. RISE) und am 11.01.2022 (Fa. Secunet) umgesetzt. Auf Veranlassung der gematik mussten die Anbieter secunet und RISE das Feature Laufzeitverlängerung gSMC-K aus dem Release PTV 5 wieder entfernen. Mit diesem Feature wäre es dann auch möglich gewesen, neben den RSA-Zertifikaten, die bis zum 31.12.2024 nach BSI-Vorgaben wirksam sind, auch Zertifikate einzuspielen, sog. ECC-Zertifikate, die nach BSI-Vorgaben eine über den 31.12.2024 hinausgehende Wirksamkeit entfalten. Die Fa. CompuGroup Medical hat die normativen Forderungen nicht umgesetzt. Mit Beschluss der Gesellschafterversammlung der gematik vom 28.02.2022 (PM März 2022) wurde der Konnektortausch insgesamt als **sicherste Lösung** erklärt **(vgl. Anlage 9)**.

Mit Pressemitteilung der gematik vom 30.08.2022 **(vgl. Anlage 10)** wurde der zuvor genannte Beschluss vom 28.02.2022 (Pressemitteilung aus März 2022) dahingehend abgeändert, dass das alternativlose Szenario des Konnektortausches nur noch für Konnektoren gilt, deren Zertifikate bis August 2023 ablaufen. Ab September 2023 werden dann Alternativen wie die Laufzeitverlängerung gSMC-K oder ein Anschluss über ein Rechenzentrum angeboten, obgleich die Hersteller RISE und secunet bereits vor ihrer Zulassung am 29.12.2021 bzw. 11.01.2022 zu PTV5 den Nachweis der implementierten Laufzeitverlängerung erbracht hatten. Mit der Entscheidung gegen die Umsetzung der Laufzeitverlängerung wurden die Anbieter RISE und secunet sogar aufgefordert, das Feature Laufzeitverlängerung aus der relevanten Spezifikation zu PTV5 wieder zu entfernen.

[redacted]

Unter diesem Aspekt erscheint der Beschluss der Gesellschafterversammlung der gematik vom 28.02.2022 bzw. 29.08.2022 für den alternativlosen Austausch der Konnektoren mehr als fraglich.

Von dem Konnektortausch sind somit nur Konnektoren der Fa. CompuGroup Medical betroffen. Ursächlich hierfür ist die fehlende Umsetzung der Spezifikation vom 30.06.2021 zur Laufzeitverlängerung der gSMC-K. Ausweislich der Übersicht „Hardwaretausch der Fa. CompuGroup" vom 24.05.2022 **(vgl. Anlage 11)** sind alleine im Zeitraum 01.09.2022 - 31.03.2023 im ärztlichen Bereich 24.146 Konnektoren und im zahnärztlichen Bereich 11.295 Konnektoren, mithin 35.441 Konnektoren insgesamt zu tauschen.

Nach den jeweiligen Grundsatzfinanzierungsvereinbarungen der KBV und der KZBV mit dem GKV-Spitzenverband werden für den jeweiligen Konnektortausch 2.300,00 Euro/brutto erstattet.

Das Update auf PTV5 wird mit 250,00 Euro/brutto vergütet (vgl. **Anlage 12** für den zahnärztlichen Bereich).

Somit ergibt sich ein Unterschiedsbetrag in Höhe von 2.050,00 Euro/brutto pro Konnektorstandort.

Die - jetzt unnötigerweise entstehenden - Mehrausgaben bei dem Konnektortausch im Vergleich zur Software-Laufzeitverlängerung nach PTV5 zulasten der Versichertengemeinschaft in der gesetzlichen Krankenversicherung (GKV) belaufen sich demnach allein im Zeitraum vom 01.09.2022 - 31.03.2023 auf **72.654.050,00 Euro/brutto.**

Insoweit besteht der Verdacht der zweckwidrigen Verwendung von GKV-Mitteln aufgrund des Beschlusses der Gesellschafterversammlung der gematik vom 28.02.2022 bzw. 29.08.2022 zum Konnektortausch in der Telematikinfrastruktur.

Bitte bestätigen Sie uns den Eingang dieses Schreibens samt Anlagen.

Mit freundlichen Grüßen

[redacted]