Konnektor

Die Nutzung von Einbox-Konnektoren ist maximal bis 2030 möglich: https://www.gematik.de/newsroom/news-detail/aktuelles-gesellschafter-beschliessen-ende-der-nutzung-von-einbox-konnektoren

PTV 6: erzwingt die Nutzung von ECC. Grundsätzlich bedarf es jedoch keines PTV-6-Konnektors, um bei korrekter Primärsystemimplementierung eine ECC-Signatur durchzuführen.

Über den Konnektor werden medizinische Einrichtungen an die TI angebunden.

Neben der Hardware-Variante in der medizinischen Einrichtung gibt es zunehmend auch Serviceangebote, bei denen man eine TI-Anbindung quasi „abonnieren“ kann, ohne einen Konnektor selbst anschaffen zu müssen. Diese Anbieter betreiben dann Einboxkonnektoren in einem Rechenzentrum und „verschalten“ diese miteinander („Konnektor-Farming“). Anbieter dieser Lösungen sind. bspw. RedMedical und Akquinet. Regulatorisch werden diese Angebote geduldet, offiziell zugelassen sind sie nicht. Mittlerweile gibt es jedoch auch spezifizierte Varianten eines „TI as a Service“ als TI-Gateway mittels Highspeedkonnektor (HSK) anbieten. Anbieter eines TI-Gateway sind zugelassen und nutzen den zugelassen Produkttyp HSK in ihrem Rechenzentrum. Mit ersten Angeboten wird im Herbst 2024 gerechnet.

Finanzierung

- Erstausstattungspauschale (für Konnektor und Kartenterminal)
  - bis zu 3 Ärzt:innen/Psychotherapeut:innen in der Praxis: 1549 € (neu: 1661,50 €)
  - 4 bis 6 Ärzt:innen/Psychotherapeut:innen in der Praxis: 2084 € (neu: 2309 €)
  - mehr als 6 Ärzt:innen/Psychotherapeut:innen in der Praxis: 2619 € (neu: 2956,50 €)
- **Neu**: Austausch defekter Konnektoren: Wird bei Bedarf über KVen erstattet (bundesweites Budget von 4 Millionen Euro vereinbart)

Finanzierung Konnektortausch

- Erstattungen voraussichtlich ab Oktober 2022
- Verhandlungen sind beim Schiedsamt geendet: Entscheidung: 2300 €. KBV lehnt den Schiedsspruch ab.[1)]
- CGM bietet Praxen und Kliniken den Konnektortausch zunächst insgesamt für 2330 € an.[2)] Nach dem Schiedsspruch und rechtzeitig vor der Gesellschafterversammlung der gematik, wo der Konnektortausch erneut thematisiert wird, senkte CGM die Preise auf 2300 €, was genau der per Schiedsspruch verordneten Pauschale entspricht.[3)]
- Im Zusammenhang mit der Konnektortauschthematik ist eine neue Finanzierungslogik für die TI geplant (Beschluss der GSV im August). Vermutlich wird es ein zwischen den Bundesmantelvertragspartnern auszuhandelndes Digitalisierungsbudget für Leistungserbringer geben, über das diese dann selbst entscheiden können

- Die BReg bringt einen Änderungsantrag zum RegE des KHPflEG ein, der eine TI-Monatspauschale für Leistungserbringer vorsieht.[4)]
- Die Reaktionen von BÄK und KBV fallen eher negativ aus. Die KBV bringt einen eigenen Vorschlag ein.

Neue Vertrauenslisten BNetzA

Zulassungsrelevante Firmware-Aktualisierung der Konnektoren notwendig aufgrund irgendeines Implementing Acts der EU. Wird sich voraussichtlich verzögern.

Die Vertrauensliste der Bundesnetzagentur (BNetzA) wird zukünftig an den neuen Standard ETSI TS 119 612 Version 2.3.1 angepasst. Diese Anpassung erfolgt im Rahmen der Aktualisierung des Implementing Acts CID 2015/1505.

Um sicherzustellen, dass Konnektoren auch weiterhin qualifizierte elektronische Signaturen (QES) erstellen und prüfen können, werden neue Firmware-Versionen bereitgestellt, die das aktualisierte Schema der Vertrauensliste unterstützen. Die Hersteller haben in Zusammenarbeit mit der gematik entsprechende Updates entwickelt, die von den Herstellern ab Mitte Mai/ Mitte Juni 2025 zur Verfügung gestellt werden.

Was bedeutet das konkret?

Einboxkonnektoren: Betreiber und Kunden von Einboxkonnektoren können die neuen Firmware-Versionen nach deren Verfügbarkeit installieren. Sofern der Konnektor keine Auto-Update-Funktion besitzt, kann das Update manuell durchgeführt oder über den Vertriebspartner bzw. DVO organisiert werden. TI-Gateway: Für Highspeedkonnektoren, die über ein TI-Gateway angebunden sind, ist kein Handeln erforderlich. Das Update wird zentral bereitgestellt und automatisch verfügbar gemacht.

Derzeit dient die Bereitstellung der neuen Firmware-Versionen als Vorbereitung auf den Wechsel zur aktualisierten Vertrauensliste. Sobald die Einführung der neuen Vertrauensliste konkreter wird, werden wir an dieser Stelle erneut informieren und weitere Hinweise zur Umsetzung geben.[5)]

Konnektortausch

In dieser Kleinen Anfrage werden einige Hintergründe erklärt und zentrale Fragen (teils im ausweichenden Regierungsstil 😉) beantwortet.

Mittlerweile gibt es eine Info-Seite der gematik zum Thema Konnektortausch.

Die gSMC-K trägt die kryptographische, angeblich logisch und physisch fest mit dem Konnektor verbundene, Identität des Konnektors. Die gSMC-Ks gehen nur an zugelassene Konnektorhersteller und werden dort in einem auditierten Staging-

Prozess verbaut.

Die offizielle Einordnung des Gesamtthemas durch die gematik: https://www.gematik.de/datensicherheit/konnektortausch.

Hintergrund

- Die Sicherheitszertifikate der Konnektoren (bzw. der Identitätskarte gSMC-K) laufen gemäß Spezifikation spätestens nach 5 Jahren ab. Es gibt aus Performancegründen drei gSMC-Ks pro Konnektor - die Prozessorleistung einer einzigen gSMC-K wäre für den Alltagsbetrieb zu schwach.
- Die ersten Konnektoren wurden Ende 2017 ausgegeben.
- Eine Laufzeitverlängerung (über ein Online-Update) der Zertifikate ist maximal bis Ende 2025 möglich (BSI bzw. europäische Regelungen lassen nicht mehr zu).
- Die Gesellschafter hatten im Lenkungsausschuss (91. Sitzung am 28.03.2019) auf ausdrückliche Empfehlung der gematik beschlossen, den Lösungsansatz einer Laufzeitverlängerung nicht mehr zu verfolgen und neue Lösungen (in Richtung „Zukunfts-Konnektor“) zu verfolgen.
- Ein Zukunfts-Konnektor (oder Software-Konnektor) steht nicht zur Verfügung. Auch die TI 2.0, die zukünftig (angeblich) ganz ohne Hardware-Konnektoren auskommen soll, steht zu diesem Termin nicht zur Verfügung. Ursprünglich wurde zwar der 1.1.2025 angekündigt, inzwischen ist aber von 2026 die Rede und im Grunde ist es ein offenes Geheimnis, dass auch dieser Termin nicht realistisch ist, wie viele der Termine und Fristen in diesem Umfeld.
- Anforderungen für eine Laufzeitverlängerung per Online-Aktualisierung waren in den Spezifikationen für den Konnektor vorgesehen für PTV 5, die auch ePA 2.0 beinhaltet.
- Nach 2025 müssten nicht nur die Zertifikate verlängert, sondern auch die zugehörigen privaten Schlüssel auf der Karte (gSMC-K) „ausgetauscht“ (neu generiert) werden. Grund: BSI-Vorgaben[6] (und europäische Vorgaben[7] zur Gültigkeit von Algorithmen, hier im Speziellen der RSA-Algorithmus.[8] Die gSMC-Ks sind darauf - bis auf die ersten ausgelieferten in CGM-Konnektoren - allerdings ebenfalls vorbereitet, da sie neben dem alten (RSA) auch neues Schlüsselmaterial (ECC) „mitbringen“.
- Die Laufzeitverlängerung wurde von secunet und RISE implementiert, allerdings gab es keine Zulassung für diese Funktionalität. Somit waren zwar PTV5-Konnektoren zugelassen (für ePA 2.0), aber ohne Laufzeitverlängerung.
- CGM hat nix implementiert.
- Neben einer Anpassung der Konnektoren ist allerdings auch eine Beauftragung einer Zertifikatssenke bei arvato als TSP notwendig.[9]
- In einem heise-Artikel wird von den Autoren behauptet die gSMC-Ks der CGM-Konnektoren ließen sich entfernen und austauschen, ohne dass der Konnektor seine Funktion einstelle. Er ließe sich anschließend problemlos neu starten (booten). In einer Stellungnahme zweifelt die gematik an, dass es sich um einen Austausch gegen eine neue - nicht dieselbe - gSMC-K handele. Alle Hersteller hätten der gematik bestätigt, ein Tausch sei nicht möglich. Zudem verstieße ein solcher Tausch gegen Sicherheitsvorgaben. Das ist richtig: Im Security Target des CGM-Konnektors heißt es explizit: „Die kryptographischen Identitäten des Konnektors werden durch drei Smart Card basierte Sicherheitsmodule (gSMC-K) bereitgestellt, die in den internen Kartensteckplätzen des Konnektors installiert sind. Diese Smart Cards werden im Produktionsprozess eingebaut und sind nicht austauschbar. Weder Endbenutzer noch geschultes Service-Personal können die gSMC-K ersetzen. Die Manipulation oder das Entfernen der Smart Cards führt zur Außerbetriebssetzung des Geräts.“[10] Falls ein Austausch also möglich

wäre, wäre das eigentliche Thema eher der dadurch vorliegende Sicherheitsvorfall und die Frage, wie ein solcher Konnektor durch die Sicherheitszertifizierung gelangen konnte.
- Der Flüpke-"Hack" (CCC) weist zwar praktisch nach, dass es keine hardwareseitige Verknüpfung zwischen gSMC-K und Konnektor (zumindest für die Konnektoren von secunet und CGM) gibt und eine Aktualisierung bzw. ein Austausch der Zertifikate (oder Karten) machbar wäre[11], aber im Kern ist das eigentlich nichts Neues, da eine Aktualisierung ja ohnehin ursprünglich geplant und spezifiziert war.

Chronologie

- **20.11.2020** In einer Antwort auf eine kleine Anfrage der Grünen heißt es noch: „Die Gesellschaft für Telematik analysiert derzeit verschiedene technische Lösungen, mit denen ein Konnektoraustausch mit Ablauf der Zertifikate vermieden werden kann. In die Analyse wird das Bundesamt für Sicherheit in der Informationstechnik eng eingebunden.“[12]
- Am **28.2.2022** beschließt die Gesellschafterversammlung der gematik, alle Konnektoren im Feld zu tauschen und die Laufzeitverlängerung aus der Konnektorspezifikation zu entfernen
- **21.4.2022** Laut gematik finden Gespräche mit den Herstellern RISE und secunet bzgl. praktikablerer Lösungen statt.[13], am **19.5.2022** gibt die gematik allerdings keine weiteren Auskünfte zu diesen Verhandlungen.[14]
- **15.7.2022** heise online behauptet in einem Artikel, die gSMC-Ks der CGM-Konnektoren ließen sich problemlos austauschen.[15]
- **21.7.2022** Die gematik veröffentlicht eine kurze Stellungnahme zum heise-Artikel. Wörtlich heißt es dort: „Die im Bericht von heise / c’t vorgeschlagene Lösung, die gSMC-K auszutauschen, ist unserer Einschätzung nach keine Lösung für den Einsatz in den Praxen, da unter anderem die Sicherheitsvorgaben verletzt werden. Wie uns auf Anfrage bei allen Herstellern nochmals bestätigt wurde, ist der geschilderte Austausch der gSMC-K zudem technisch nicht möglich. Es liegt demnach die Vermutung nahe, dass bei dem im Artikel beschriebenen Entfernen der gSMC-K dieselbe (!) Karte auch wieder in den Konnektor hineingesteckt wurde – demnach also KEIN Austausch der Karte selbst stattfand. Wäre dies der Fall, so ist es auch nicht verwunderlich, dass der Konnektor danach weiterhin funktionierte, schließlich hat sich an seiner Konfiguration nichts geändert. Festzuhalten bleibt: Der Austausch einer gSMC-Karte im Konnektor ist laut übereinstimmender Herstellerangaben nicht möglich.“
- **22.7.2022** KBV fordert gematik in einer Pressemitteilung auf, zunehmend aufkommende Fragen - auch im Zusammenhang mit dem Artikel von heise online am 15.7.2022 zum Konnektortausch zu beantworten und kündigt an einen entsprechenden Beschlussvorschlag in der kommen Gesellschafterversammlung am 2.8.2022 einzubringen.
- **26.7.2022** c't/heise bestätigen, dass es sich um dieselben Karten handelte, die wieder eingebaut wurden.[16]
- **28.7.2022** gematik veröffentlicht Antworten auf die Fragen der gematik als Stellungnahme. Frage 4 behauptet, dass das erfolgreiche Entfernen und Widereinsetzen der gSMC-K nicht den Vorgaben widerspreche. Die folgen Sätze aus dem PP und Security Target (des CGM-Konnektors) lassen sich auch anders lesen:
  - „Sicher bedeutet in diesem Fall, dass die gSMC-K nicht unbemerkt vom Netzkonnektor getrennt werden kann.“[17]
  - „Die Manipulation oder das Entfernen der Smart Cards führt zur Außerbetriebssetzung des Geräts.“[18]
- **29.7.2022** KBV hält gestrige Antwort der gematik für nicht befriedigend und kündigt die Thematisierung in der GSV am nächsten Dienstag (2.8.2022) an. Die KBV fordert, dass die gematik herausarbeitet, unter welchen Bedingungen die gSMC-Ks ggf. austauschbar wären.[19]
- **2.8.2022** Gesellschafterversammlung der gematik. Das BMG lehnt den eingereichten Beschluss

der KBV/BÄK mit der Begründung ab, dass es keine neue Faktenlage gem. gematik gäbe und man sich besser auf die Anpassung des Finanzierungsmodells fokussiere, um keine Fehlanreize für die Industrie zu schaffen und neue nicht hardwaregebundene Lösungen besser zu unterstützen.[20] Die gematik wurde aber beauftragt für die nächste Gesellschafterversammlung eine Bewertung aller Alternativen vorzulegen, um die Faktenlage - ob nun geändert oder nicht - transparent zu machen.[21]

- **29.8.2022** Gesellschafterversammlung der gematik bestätigt die Entscheidung zum Konnektortausch.[22] Allerdings müssen nur die Geräte, die bis September 2023 auslaufen ausgetauscht werden, für die folgenden Geräte soll es ein technikneutrales Finanzierungsmodell geben, dass drei Optionen ermöglicht: Tausch, Laufzeitverlängerung der Zertifikate in den Karten bzw. Anschluss an Rechenzentrumslösung (vgl. dazu den avisierten neuen zentralen Dienst der TI: TI-Gateway).
- **Sept./Okt. 2022** Flüpke (CCC) weist für die beiden Konnektoren von secunet und CGM durch Reengineering nach, dass es keine hardwareseitige Verknüpfung zwischen Konnektor und gSMC-K gibt.[23].
- **17.10.2022** Die gematik reagiert mit einer Stellungnahme, die auf den GSV-Beschluss vom 29.8.2022 verweist auf die Veröffentlichungen der CCC-Hacks durch heise.[24]
- **25.10.2022** Veröffentlichung einer Änderungsliste, die die Laufzeitverlängerung wieder in die Spezifikation der gematik aufnimmt, zumindest als Option.
- **8.12.2022** Veröffentlichung der aktualisierten Konnektorspezifikaton mit der (maximal dreijährigen) Laufzeitverlängerung (für ECC-fähige Konnektoren) als verpflichtende Funktionalität.[25]
- **16.12.2022** Sieben Kassenzahnärztliche Vereinigungen (KZV) - Baden-Württemberg, Bayern, Hessen, Niedersachsen, Rheinland-Pfalz, Schleswig-Holstein und Westfalen-Lippe - haben eine Anzeige bei der Stelle zur Bekämpfung von Fehlverhalten im Gesundheitswesen eingereicht. Die Stelle ist beim Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) angesiedelt. Die Anzeige wird derzeit geprüft.[26]
- **22.12.2022** Bundeskartellamt leitet aufgrund eingegangener Beschwerde kein Verfahren ein.[27]
- **02.03.2023** Kleine Anfrage der AfD zu „Hintergründe[n] des Konnektortauschs im Gesundheitswesen“.[28]
- **30.03.2023** Antwort der BReg auf die Kleine Anfrage der AfD zu „Hintergründe[n] des Konnektortauschs im Gesundheitswesen“.[29]

Zahlen

- Nach einer Antwort der Bundesregierung auf eine schriftliche Frage vom Abgeordneten Erwin Rüddel (CDU/CSU) wurde eine Laufzeitverlängerung bisher in 18.450 Fällen durchgeführt (Stand Juni 2024). Verglichen mit der im September 2023 geschätzten Zahl an auslaufenden Konnektoren wurde ungefähr die Hälfte der betroffenen Konnektoren verlängert.[30]
- In einer Antwort auf eine kleine Anfrage der Grünen[31] wird folgende Verteilung der Ablaufdaten der Zertifikate auf Basis von Schätzungen der gematik angegeben:

Jahr	Prozentualer Anteil der gSMC-K-Zertifikat, die in dem aufgeführten Jahr ablaufen
2022 (ab September)	8 %
2023	31 %
2024	29 %
2025	32 %

- **CGM**: 2022 sollen rund 30.000 Konnektoren ausgetauscht werden. In dieser Zahl sind auch die

Konnektoren inbegriffen, deren Zertifikate erst im Januar oder Februar 2023 auslaufen, die aber schon im ersten Schwung mit getauscht werden sollen. Weitere rund 30.000 Konnektoren werden in den Folgejahren getauscht.
- **RISE**-Konnektoren müssen frühestens im Oktober 2023 getauscht werden. Dazu wie viele Konnektoren in welchen Zeiträumen getauscht werden müssen, macht RISE keine Angaben
- Der allererste **Secunet**-Konnektor wurde im Dezember 2018 zugelassen. Nach aktuellem Stand laufen zum Ende 2023 ca. 4.000 bis 7.000 Zertifikate und 2024 über das Jahr verteilt ca. 25.000 bis 34.000 Zertifikate aus, insgesamt sind ca. 80.000 Zertifikate im Einsatz.

- Die ersten CGM-Konnektoren laufen Ende 2022 aus. Das Bestellportal der CGM für die neuen Konnektoren ist bereits online gegangen. CGM geht von einem halben Jahr Vorlauf aus für den Tausch. Also frühzeitig melden. CGM wird die Kunden laut Portal frühzeitig informieren. Detailinfos hier.
- Die ersten RISE-Konnektoren sind erst im Oktober 2023 betroffen.
- Die ersten Secunet-Konnektoren im Dezember 2023.
- Eine Finanzierungsvereinbarung für den Konnektortausch existiert noch nicht.

Eine Alternative zum Konnektortausch sind übrigens Konnektor-Hosting-Angebote von Red telematik und Akquinet, bei denen der Konnektor (und teils sogar das Kartenterminal mit der SMC-B) als Dienstleistung im Rechenzentrum betrieben wird.

Funktionalität

- In der Datensatzbeschreibung KVDT der KBV ist seit der Version 5.50 (13.5.2022) ein Feld (FK 0227) vorgesehen, welches das Ablaufdatum des Konnektorzertifikats beinhaltet.[32)] Mit der Version 5.54 (13.5.2022) des Anforderungskatalog KVDT[33)] wird begleitend gefordert, dass PS das Datum anzeigen können.[34)]
- Zudem ist im ILF für PS mit dem Änderungsrelease „Konnektor: Maintenance 22.2 (Stand: 13.05.2022)“ vorgesehen, das PS, einen Warnhinweis geben, wenn das Ablaufdatum der Konnektorzertifikats in den nächsten drei Monaten liegt.

Potentielle Alternativen

- Online-Aktualisierung RSA-Zertifikate (hilft bis Ende 2024) plus weitere Online-Aktualisierung mit ECC-Zertifikaten (hilft nicht bei einigen früh ausgerollten CGM-Konnektoren, ohne doppelt personalisierte gSMC-Ks)
- Ablösung Konnektoren durch Software-Konnektor bzw. TI2.0 (hilft nix, weil zu spät)
- Anbindung neuer Nutzergruppen mit HSK und TIaaS (HSMs der HSK lassen sich einfacher aktualisieren, Spec und Zulassung HSKs durch gematik nötig, hilft nix für alte ausgerollte Konnektoren)
- Ablösung alter Konnektoren durch TIaaS-Lösungen (Kosten vermutlich ähnlich wie Tausch)
- Tausch der gSMC-Ks(?)

Literatur

- Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Kathrin Vogler, Petra Pau, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Ates Gürpinar, Dr. André Hahn, Susanne Hennig-Wellsow, Ina Latendorf, Cornelia Möhring, Sören Pellmann, Martina Renner, Dr. Petra Sitte und der Fraktion DIE LINKE: Konnektoren im Gesundheitswesen – Software-Update statt Hardware-Tausch, 3.11.2022, BT-Drs. 20/4271 und die zugehörige Antwort der BReg (BT-Drs. 20/4745).
- Kleine Anfrage der Fraktion der CDU/CSU: Konnektoren im Gesundheitswesen - Verwendung von Mitteln der gesetzlichen Krankenversicherung, 17.11.2023. Antwort der Bundesregierung steht noch aus.

Sicherheit

Flüpke-"Hack"

Kurzbeschreibung

Flüpke (CCC) hat im Sept./Okt. 2022 nachgewiesen, dass es **keine hardwareseitige Verknüpfung** zwischen Konnektor und gSMC-Ks gibt (zumindest bei den Konnektoren von CGM und secunet).

- Die Karten lassen sich mechanisch aus ihren Steckplätzen im Gehäuse herausziehen. Ohne die Karten lassen sich bestimmte geschützte Partitionen des Konnektors nicht mehr entschlüsseln, nach Wiedereinsetzen funktioniert der Konnektor jedoch wieder reibungslos.
- Mittels Replay-Attacke gegen die unverschlüsselte Kommunikation zwischen Konnektor-Hardware und gSMC-Ks gelang es Flüpke alle Dateisysteme des Konnektors in eine virtuellen Maschine zu kopieren und dort zu mounten und auszulesen.
- Zudem konnte er relativ leicht die PINs der gSMC-Ks ermitteln, die zur Initialisierung der Konnektoren mit einer neuen SMC-K-Karte notwendig sind.
- Flüpke spielte zudem eine neue Version des Softwaretools „pcsd“ in seine Referenzumgebung ein, mit der die gSMC-Ks Befehle senden und empfangen. Wird ein Befehl zum Auslesen abgelaufener Zertifikate gesendet, antwortet die geänderte Version mit einem verlängerten Zertifikat aus dem Dateisystem.[35)]

Was sagt die Spezifikation?

Im CC-Schutzprofil für den Konnektor heißt es explizit:

> Der Netzkonnektor hat Zugriff auf ein Sicherheitsmodul (gSMC-K), das sicher mit dem Netzkonnektor verbunden ist. Sicher bedeutet in diesem Fall, dass die gSMC-K nicht unbemerkt vom Netzkonnektor getrennt werden kann und dass die Kommunikation zwischen gSMC-K und Netzkonnektor weder mitgelesen noch manipuliert werden kann.[36)]

Genau dies hat der CC allerdings demonstriert.

Das Schutzprofil umfasst jedoch weitere organisatorische Maßnahmen, die verhindern sollen, dass überhaupt erst Unberechtigten einen Konnektor bzw. eine gSMC-K gelangen:

> Die Sicherheitsmaßnahmen in der Umgebung müssen den Konnektor (während aktiver Datenverarbeitung im Konnektor) vor physischem Zugriff Unbefugter schützen. Befugt sind dabei nur durch den Betreiber des Konnektors namentlich autorisierte Personen (z. B. Leistungserbringer, ggf. medizinisches Personal). Sowohl während als auch außerhalb aktiver Datenverarbeitung im Konnektor müssen die Sicherheitsmaßnahmen in der Umgebung sicherstellen, dass ein Diebstahl des Konnektors und/oder Manipulationen am Konnektor so rechtzeitig erkannt werden, dass die einzuleitenden materiellen, organisatorischen und/oder personellen Maßnahmen größeren Schaden abwehren.[37)]

Gematik und die Hersteller (CGM und secunet) sehen hier kein Fehlverhalten gegen eine Spezifikation, die als ganzes zu betrachten sei.[38)]

Generelles Sicherheitsproblem für die TI?

Ein Zugriff mittels eines nicht ordnungsgemäß außer Betrieb genommenen oder gestohlenen Konnektors in die TI ist allerdings nur möglich, wenn zusätzliche ein SMC-B vorhanden ist. Neben dem IPsec-Verbindungsaufbau, bei sich der Konnektor über seine Geräteidentität (gSMC K) gegenüber dem sog. VPN Konzentrator des VPN Zugangsdienstes authentifiziert, muss der Konnektor initial beim VPN Zugangsdienst registriert werden. Dabei erfolgt eine Prüfung der SMC-B der Einrichtung. Auf diese Weise wird gewährleistet, dass nur berechtigte Institutionen Zugang zur TI über einen Konnektor erlangen. Der Konnektor überprüft darüber hinaus einmal täglich die Zertifikate der SMC-B der Einrichtung.[39)]

Im Falle eines erkannten(!) physischen Angriffs können Konnektoren über den Hersteller gesperrt werden. So lange der Angriff unbemerkt abläuft, bestünde ein gewisses Restrisiko, dass mit Hilfe eines manipulierten Konnektors Daten gesammelt werden könnten.

Ist es so easy wie dargestellt?

Das Vorgehen von Flüpke zeigt instruktiv, dass es möglich ist - und wohl auch einfacher als von Spezifikationen und Kommunikation der Hersteller/gematik bisher suggeriert, hier eine Zertifikatsverlängerung durchzuführen.

Allerdings ist dieses Vorgehen an sich nicht neu und ja bereits von der gematik spezifizeirt gewesen, nur viel die Entscheidung trotzdem anders aus.

Zudem muss neben dem „einfachen“ Einspielen eines Softwareupdates eine Zertifizierung des BSI eingeholt werden und auch die Zertifikatssenke bei arvato beauftragt werden, was natürlich auch bereits hätte geschehen können.

Details

SignDocument und RSA/ECC

- Seit Version 5.6.0 gibt es den Parameter `Crypt`, über den man steuern kann, welcher private Schlüssel (RSA oder ECC) ausgewählt wird. Standardmäßig wird RSA ausgewählt, möchte man

ECC wählen, muss man explizit ECC setzen über diesen Parameter.
- Seit der Version 5.23.0 ist der wieder abgeschafft und es wird der SChlüssel anhand der Kartengeneration ausgewählt, also wenn Karte ECC unterstützt immer ECC.

1) Pressemitteilung der KBV vom 22.7.2022.
2) Preisliste TI-Hardwaretausch CGM und Konnektoraustausch: Erstattungsbetrag erhöht, KBV unzufrieden, aerzteblatt, 20.7.2022 (abgerufen am 20.7.2022).
3) CGM senkt Preise für Austausch-Konnektor, ÄrzteZeitung online, 1.8.2022 (abgerufen am 3.8.2022) u. Pressemitteilung CGM v. 1.8.2022 (abgerufen am 3.8.2022).
4) Digitalisierungsfinanzierung für Arztpraxen soll auf Monatspauschale umgestellt werden, aerzteblatt.de, 16.11.2022 (abgerufen am 17.11.2022).
5) Quelle: https://fachportal.gematik.de/ti-status/wartungen-sonstige-informationen#c12, Meldung vom 16.05.2025.
6) s. Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.2.0, 21.9.2018.
7) gemeint ist der SOGIS-Algorithmenkatalog, der allerdings den 31.12.2025 als Endtermin festlegt; europäische und deutsche Vorgaben sind hier nicht immer einheitlich, was das Ganze nicht erleichtert.
8) Die gematik fasst alle diese externen Vorgaben in der übergreifenden Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur zusammen.
9) s. Featurespezifikation der gematik „Laufzeitverlängerung gSMC-K“, 7.6.2021.
10) S. 10.
11) [23] ,
Gesundheitsnetz: CCC-Hacker entschlüsseln TI-Konnektor von CompuGroup Medical, heise online, 14.10.2022.
12) [31] ,
BT-Drs. 19/24527, S. 3.
13) Austausch von Konnektoren wird geprüft, Handelsblatt Inside - Digital Health, 21.4.2022.
14) Intensive Verhandlung über Konnektoren-Finanzierung, Handelsblatt Inside - Digital Health, 19.5.2022.
15) Maus, Thomas; Schönberg, Lorenz. Konnektoraustausch in Arztpraxen: 300-Millionen-Grab ohne stichhaltige Gründe. heise online, 15.7.2022 (abgerufen am 18.7.2022).
16) Streit um Konnektoraustausch eskaliert, zm online, 26.7.2022 (abgerufen am 28.7.2022).
17) Common Criteria Schutzprofil (Protection Profile) - Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP) BSI-CC-PP-0047, Version 3.2.1, 29.10.2014, S. 55.
18) Security Target Netzkonnektor: KoCoBox MED+ OPB 2.1 Konnektor, Version 2.3.24, Dokumentenversion 1.27, 16.7.2020, S. 10.
19) Debatte um Konnektortausch dauert an: KBV hält an Forderung nach Neubewertung fest, KBV

Praxisnachrichten, 29.7.2022 (abgerufen am 29.7.2022).
20)

s. Tweet von Susanne Ozegowski v. 2.8.2022.
21)

s. Tweet vom KBV-Sprecher, Roland Stahl, v. 2.8.2022 u. Pressestatement der KBV v. 2.8.2022.
22)

Pressemitteilung gematik vom 30.8.2022.
24)

s. dazu auch Gematik reagiert auf CCC-Hack: Gerätetausch bleibt "kurzfristig" beste Lösung, heise online, 17.10.2022 (abgerufen am 18.10.2022).
25)

s. Pressemitteilung gematik v. 91.12.2022.
26)

s. https://www.heise.de/news/Korruptionsverdacht-beim-Konnektortausch-Aerzte-erstatten-Anzeige-7396953.html.
27)

vgl. https://www.heise.de/news/Bundeskartellamt-beschaeftigt-sich-mit-Konnektoren-im-Gesundheitswesen-7441005.html.
28)

BT-Drs. 20/5879.
29)

BT-Drs. 20/6266.
30)

https://dserver.bundestag.de/btd/20/117/2011712.pdfBT-Drs. 20/11712, S. 102.
32)

S. 21, FK 0227.
33)

S. 16f.
34)

s. gematik-gemmunity-Artikel
35)

s. dazu inbes. GIESELMANN, Hartmut, 2022. Der 300-Millionen-Hack: CCC-Hacker stellen Software zur Laufzeitverlängerung der Konnektoren im Gesundheitswesen vor. In: *heise online* [online]. 15.10.2022 [Zugriff am: 24.10.2022]. Verfügbar unter: https://www.heise.de/news/300-Millionen-Hack-CCC-praesentiert-Gratis-Laufzeitverlaengerung-fuer-Konnektoren-7308896.html.
36)

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, 2018. *BSI-CC-PP-0098: Common Criteria Schutzprofil (Protection Profile) - Schutzprofil 2: Anforderungen an den Konnektor* [online]. Version 1.3. 09.05.2018 [Zugriff am 17.10.2022]. Verfügbar unter: https://www.commoncriteriaportal.org/files/ppfiles/pp0098b_pdf.pdf, S. 76.
37)

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, 2018. *BSI-CC-PP-0098: Common Criteria Schutzprofil (Protection Profile) - Schutzprofil 2: Anforderungen an den Konnektor* [online]. Version 1.3. 09.05.2018 [Zugriff am 17.10.2022]. Verfügbar unter: https://www.commoncriteriaportal.org/files/ppfiles/pp0098b_pdf.pdf, S. 105.
38)

vgl. dazu Gesundheitsnetz: CCC-Hacker entschlüsseln TI-Konnektor von CompuGroup Medical, heise online, 14.10.2022 und die dort zitierte Stellungnahme von CGM sowie die Stellungnahme secunet und die Stellungnahme secunet.
39)

gemSpec_VPN_ZugD, S. 36 ff.