

Konnektoraustausch in Arztpraxen: 300-Millionen-Grab ohne stichhaltige Gründe

| 15.07.2022 07:00 Uhr Lorenz Schönberg, Thomas Maus



130.000 Konnektoren sollen in Kliniken und Arztpraxen "aus Sicherheitsgründen" ausgetauscht werden – mit fragwürdigen und lückenhaften Begründungen.

(This article is also available in English [1])

Rund 130.000 Kliniken und Arztpraxen in Deutschland tauschen ihre Gesundheits- und Patientendaten über die Telematikinfrastruktur (TI) mit den Krankenkassen aus. Da die Daten sehr sensibel sind, gelten strenge Sicherheitsvorgaben. So stellen speziell abgesicherte Router – sogenannte Konnektoren – die Verbindung zur TI her. Deren Krypto-Zertifikate laufen nach fünf Jahren aus.

Verantwortlich für die TI ist die Digitalisierungsagentur Gematik, die maßgeblich vom Bundesgesundheitsministerium (BMG) gesteuert wird. Gematik und BMG zufolge lassen sich die Zertifikate nicht erneuern, sodass die Konnektoren nach fünf Jahren komplett ausgetauscht werden müssen. **Aus den Altgeräten wird "Elektroschrott" [2]**, wie es Thomas Kriedel, Vorstandsmitglied der Kassenärztlichen Bundesvereinigung (KBV), beschreibt. Wir haben nun einen Konnektor

geöffnet und geprüft, ob es nicht auch anders geht.

Streitpunkt Zertifikatsverlängerung

Derzeit gibt es drei Hersteller, die Konnektoren anbieten: CGM, RISE und Secunet. 2017 hatte CGM die KoCoBox bereitgestellt. Von diesen Konnektoren wurden damals 15.000 installiert, die dieses Jahr erneuert werden müssen. Für die ungefähr 115.000 übrigen Konnektoren – darunter auch neuere Modelle von RISE und Secunet – gilt derselbe Austauschzwang. Sie folgen in den kommenden Jahren.

"Aus den Altgeräten wird Elektroschrott"

Die KBV hat als einer der Gesellschafter der Gematik dem Austausch zugestimmt: "Die Gematik hat uns nach ausreichender Prüfung auch mit den Herstellerfirmen der Konnektoren keine sichere Alternative anbieten können", **erklärte Kriedel in einem von der KBV veröffentlichten Interview [3]**. Die Hersteller könnten bei einer Softwarelösung nicht garantieren, dass kein Konnektor ausfalle.

Der Hersteller CGM schrieb in einer FAQ zum Hardwaretausch auf seiner Webseite: "Da die Zertifikate in den Konnektoren fest verbaut sind und aus Sicherheitsgründen nicht entfernt oder ersetzt werden können, ist deren Austausch technisch nicht möglich." Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) wäre immerhin eine zweijährige Verlängerung der Zertifikate per Software ausreichend sicher, ohne die Konnektoren jetzt tauschen zu müssen.

LESEN SIE AUCH

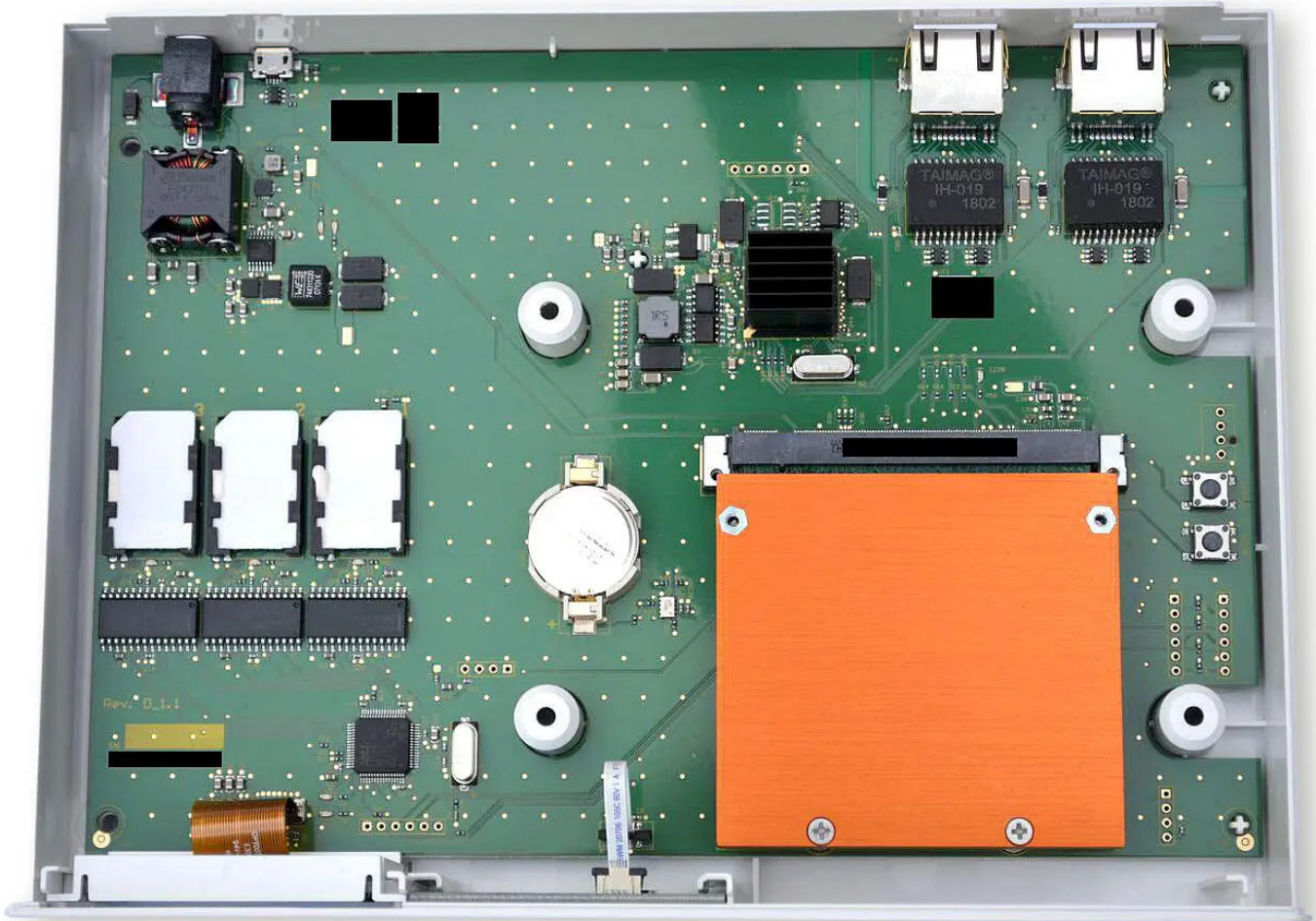
Teure Intensivmedizin für ein totes Pferd: Der TI-Konnektor-Tausch

[4]

KoCoBox unboxed

Wir haben die Aussage des Herstellers CGM geprüft und eine KoCoBox genauer untersucht. Um an das Innere einer KoCoBox zu gelangen, mussten wir sechs Sicherheitsschrauben vom Typ "Torx Plus Security" entfernen. Das gelang uns mit einem simplen Klingenschraubendreher.

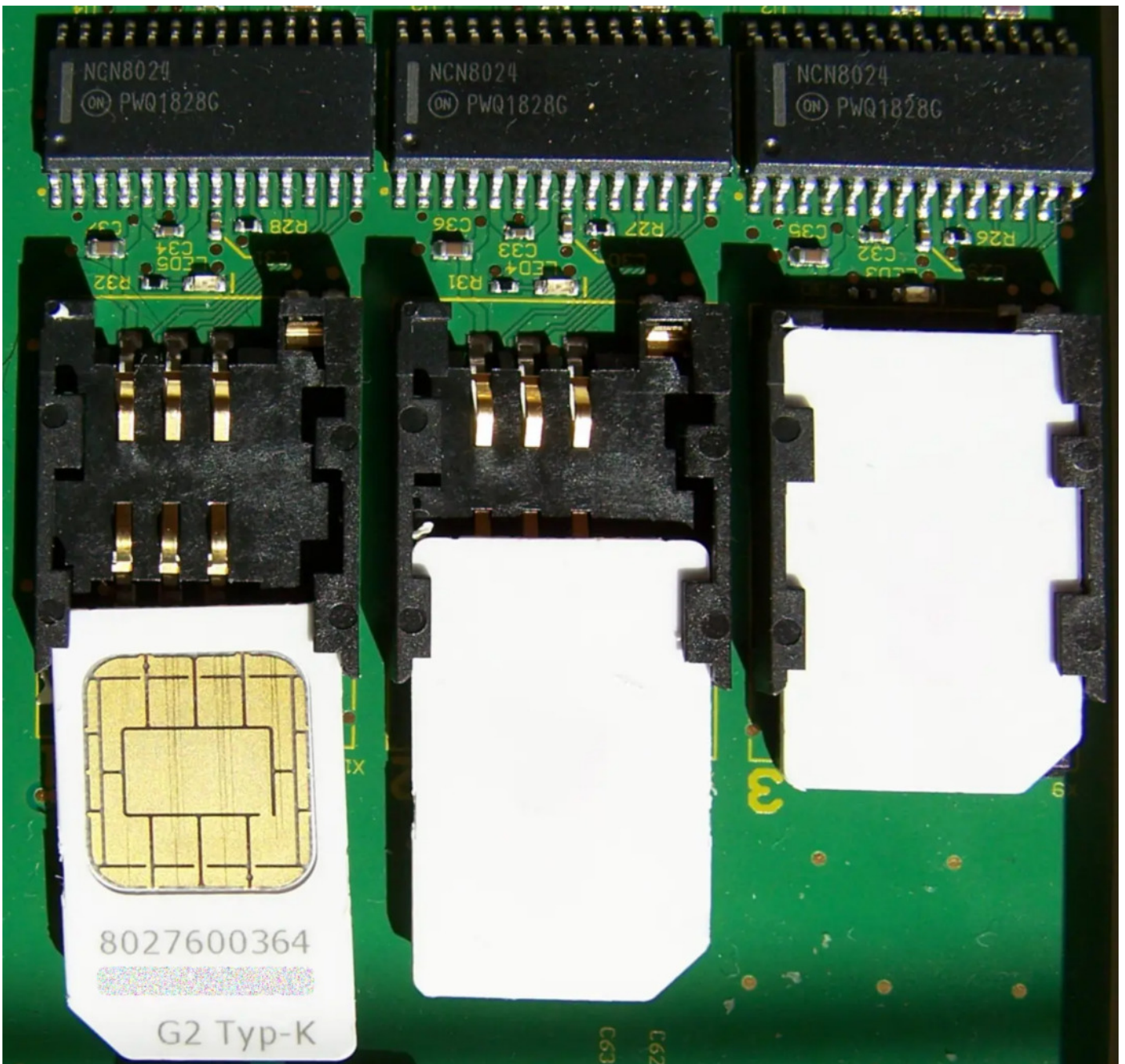
Im Unterschied zu den Kartenterminals in den Arztpraxen wurden beim Konnektor nur einzelne Software-Komponenten nach dem internationalen IT-Sicherheitsstandard Common Criteria zertifiziert und nicht die Hard- und Software als Ganzes. Das mag ein Grund dafür sein, dass bei der KoCoBox im Unterschied zu den Terminals kein elektronischer Manipulationsschutz vorhanden ist. Es gibt darauf nur zwei Klebesiegel, die sich spurlos und leicht entfernen lassen und von einem Techniker bei einer Reparatur erneuert werden können.



Die Hauptplatine der KoCoBox stammt von os-cillation. Auf ihr sitzen links drei Halterungen für gSMC-K-Karten – diese enthalten die ablaufenden Krypto-Zertifikate. Rechts der orange Kühlkörper des CPU-Boards – kein Rotgold, wie man angesichts der Preise vermuten würde.

Im Inneren der KoCoBox füllt eine Hauptplatine das Gehäuse aus. Auf ihr sind Spannungsversorgung, Pufferbatterie, Ethernet-Zugänge und ein Treiberbaustein für das Display zu finden. Auf der linken Seite sitzen drei SIM-Kartenaufnahmen, in denen kleine gerätespezifische Security Module Cards (gSMC-K) stecken. Die gSMC-K-Karten sind Mini-Smart-Cards mit eben jenen Krypto-Zertifikaten, die nach fünf Jahren ablaufen. Die Krypto-Aufgaben wurden auf drei Secure Module Cards (SMC) verteilt, weil die Prozessorleistung einer einzelnen SMC für den Alltagsbetrieb des Konnektors zu schwach wäre.

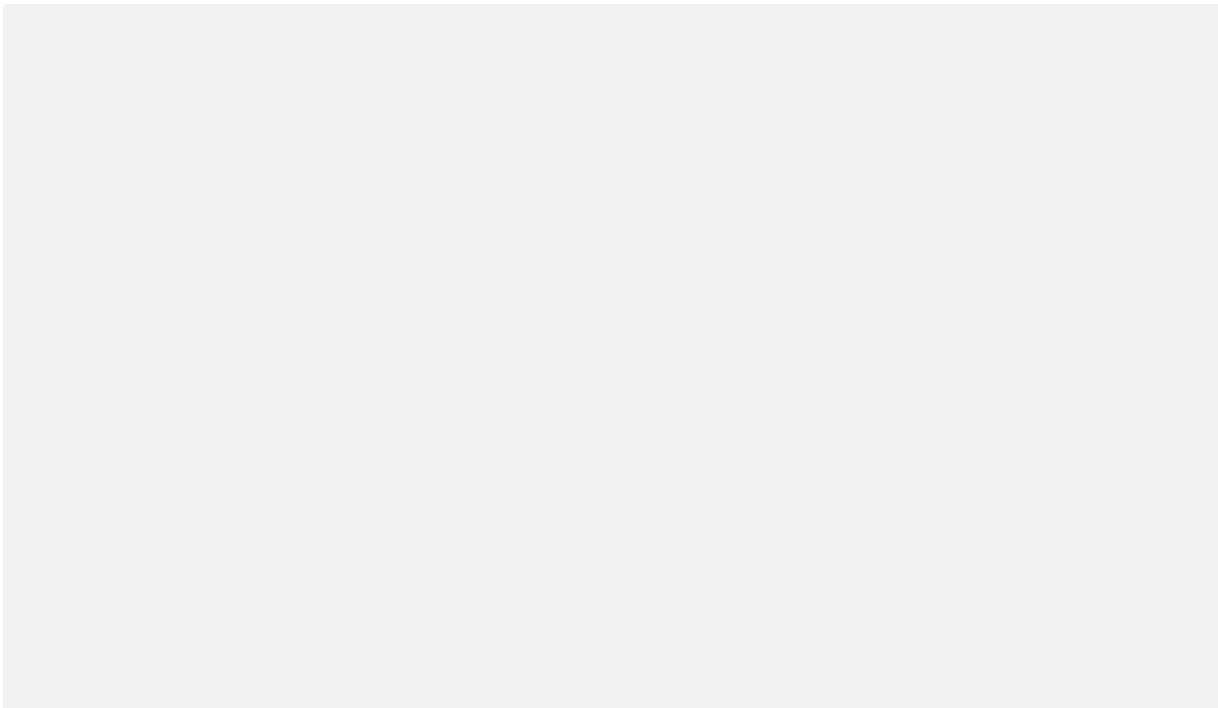
Die drei gSMC-K-Karten konnten wir zusammen mit der Stützbatterie problemlos entfernen und wieder einsetzen. Die KoCoBox bootete anschließend klaglos und konnte weiterverwendet werden. Dies widerspricht der Aussage von CGM, die Zertifikate seien fest verbaut. Als wir den Hersteller konfrontierten, **änderte er den Text auf seiner Webseite [5]** in "Das Zertifikat auf der Karte und der Konnektor sind untrennbar miteinander verbunden. Es ist möglich, sie physisch voneinander zu trennen, beide sind anschließend aber ohne Funktion." In einem weiteren **FAQ zur KoCoBox MED+ [6]** ist ebenfalls noch von fest verbauten Zertifikaten die Rede.



Die drei qSMC-K-Karten mit den Krypto-Zertifikaten lassen sich kinderleicht herausziehen und wieder einsetzen.

Auch hier müssen wir widersprechen: Wir konnten sogar eine KoCoBox reanimieren, die nicht mehr bootete, indem wir gSMC-K-Karten und Stützbatterie kurz entfernten und wieder einsetzten. Wir fanden keinerlei Security-Fuses oder ähnliche Sicherungen, die ein erneutes Pairing der Konnektor-Hardware mit einem frischen Satz gSMC-K-Karten verhindern würden. Wir fragten CGM nach derartigen Sicherungen. Eine Antwort wollte uns der Hersteller jedoch nicht geben.

Nach unseren Erkenntnissen spricht alles dafür, dass die gSMC-K-Karten zwar an die Konnektor-Hardware gebunden sind, aber offenbar nicht die Konnektor-Hardware an die gSMC-K-Karten. Demnach könnte man einen neuen Kartensatz mit frischen Zertifikaten für den Konnektor erstellen und den teuren Hardware-Tausch vermeiden.

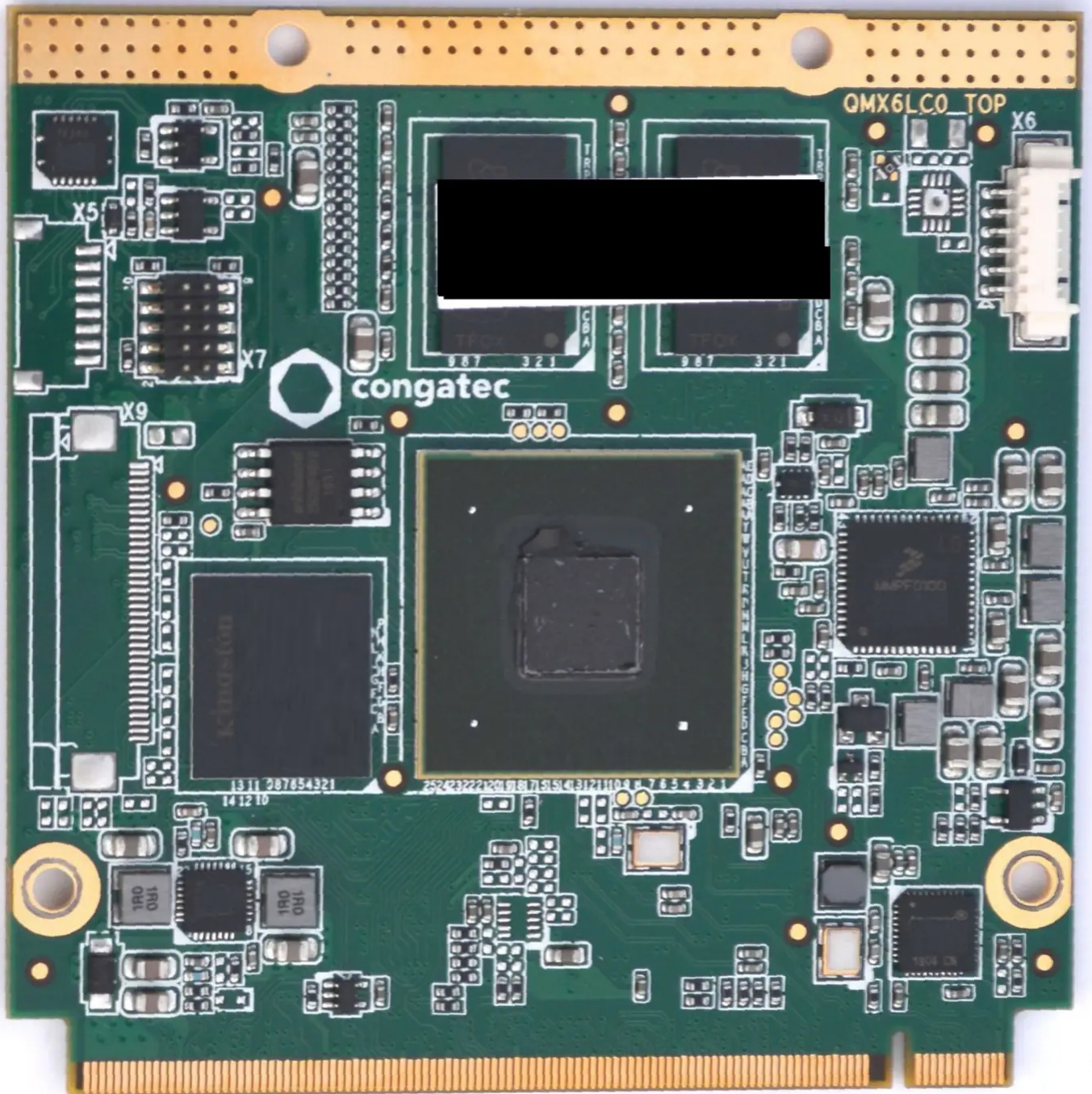


[7]

Lukrativer Austausch

Für CGM ist der komplette Hardwaretausch der Konnektoren durchaus lukrativ: Laut offizieller Preisliste verlangt der Hersteller für einen Vor-Ort-Austausch seiner KoCoBox zwischen 2161 Euro und 2330 Euro netto. Davon entfallen 1586 Euro allein auf die Hardware. Zwar haben die Hersteller RISE und Secunet noch keine Austauschpreise genannt, in der Vergangenheit unterschieden sich die Preise der Hersteller aber nur marginal.

Auf Nachfrage begründete CGM die hohen Preise mit dem Einsatz "hochsicherer und hochspezialisierter Komponenten" – eine Angabe, die sich mit unseren Untersuchungsergebnissen nicht deckt. Denn das Mainboard entspricht weitgehend einem Standard-Industriemodell, das die os-cillation GmbH aus Siegen unter dem Namen BaseBoard für Qseven-Module verkauft. Für die KoCoBox wurden lediglich der HDMI- und ein dritter Ethernet-Anschluss entfernt sowie der SMC-Einschub um zwei weitere ergänzt.



Herzstück der KoCoBox ist diese Prozessorplatine von Congatec. Im Handel sind Serienmodelle zum Einzelpreis von 250 Euro zu haben.

Zum Mainboard gehört ein Congatec-CPU-Board mit der Bezeichnung QMX6LC0. Es ist eine leicht abgespeckte Sonderversion des Serienmodells "Conga QMX6/QC-2G eMMC4" das aktuell einzeln für 250 Euro zu haben ist. Setzt man für die übrigen Komponenten wie Hauptplatine mit Anschlüssen, Gehäuse, Display, Tastenfeld sowie Zusammenbau, Endkontrolle und Verpackung noch einmal 150 Euro an, dann lassen sich 400 Euro als Obergrenze für die Herstellungskosten der Konnektor-Hardware schätzen.

Zertifikatsverlängerung per Software

In den Konnektoren von RISE und Secunet befinden sich ebenfalls gSMC-K-Karten, die jedoch nicht

ausgetauscht werden müssten. Denn beide Konnektoren unterstützen eine Zertifikatsverlängerung per Software.

RISE teilte uns mit: "Ein Konzept zum Tausch wurde mit der Gematik abgestimmt und die Machbarkeit war für RISE natürlich möglich. Dabei sollte der kryptographische private Schlüssel auf der gSMC-K weitergenutzt und ein neues Zertifikat dazu erstellt werden. Das würde für den Konnektor ausreichen, um weiterhin genutzt werden zu können und allen Anforderungen zu entsprechen."

Vermeidbarer Hardwaretausch

Setzt man für drei gSMC-K-Karten einen Herstellungspreis von zusammen 30 Euro an, ließen sich pro ausgetauschter KoCoBox etwa 1556 Euro sparen. Bei den Arbeitskosten für den Kartentausch, Aufspielen neuer Firmware, Rekonfiguration der Praxis-IT sowie An- und Abfahrt unterstellen wir in etwa dieselben wie bei der Kalkulation für den Konnektortausch von CGM.

Unverständlich ist, warum die Gematik trotzdem auf einen Austausch aller Konnektoren besteht und keine Unterscheidung zwischen den Modellen der drei Hersteller macht. Statt 300 Millionen Euro für den Tausch von 130.000 Konnektoren, würde der Tausch der gSMC-K-Karten der KoCoBoxen nur einen Bruchteil kosten. Die Software-Verlängerung der übrigen Konnektoren von RISE und Secunet wäre deutlich günstiger. Nach den Gründen für den Komplettaustausch gefragt, antwortete die Gematik lediglich: "Die Konnektoren müssen ausgetauscht werden", ohne weitere Erläuterungen.

Die Ärzte könnten vielleicht auf den Kosten sitzen bleiben, da die Krankenkassen bislang nur die Erstausrüstung für den Anschluss an die TI erstatten. Allerdings verhandeln die Ärztevertretungen derzeit noch mit dem Spitzenverband der Krankenkassen um eine Beteiligung. Dennoch entzieht der offenbar vermeidbare Hardware-Austausch dem Gesundheitssystem unnötigerweise viel Geld.

C'T AUSGABE 16/2022



(Bild: c't 16/22 [8])

In c't 16/2022 erklären wir, wie Datenhändler Sie beim Surfen durchleuchten, Ihre Daten verarbeiten und zu Geld machen. Sie erfahren, wie Sie sich gegen Tracking wehren und Ihre Privatsphäre schützen. Auf dem Prüfstand behaupten sich neben USB-Sticks und SSDs bis 1 TByte auch A3-Multifunktionsdrucker und das neue MacBook Pro 13" mit M2-CPU. Außerdem stellen wir eine Reihe von nützlichen Tools für Security-Recherchen vor.

- [Wie Datenhändler Sie ausspionieren \[9\]](#)
- [Abwehrmaßnahmen gegen Datenhaie \[10\]](#)
- [Vergleichstest: USB-Medien mit 1 TByte Speicherplatz \[11\]](#)
- [Multifunktionsdrucker bis DIN A3 \[12\]](#)
- [OSINT: Tools für Security-Recherchen \[13\]](#)
- [Test: Apple MacBook Pro 13" mit M2-Prozessor \[14\]](#)
- [Test: Ultrabreitmonitore fürs Büro \[15\]](#)
- [Linux-Praxis: JACK durch PipeWire ersetzen \[16\]](#)
- [Raspberry Pi als Webcam mit Motion \[17\]](#)
- [FAQ: Kontakt zur c't-Redaktion \[18\]](#)
- [c't 16/2022 im Heise-Shop \[19\]](#)

(hag [20])

URL dieses Artikels:

<https://www.heise.de/-7168522>

Links in diesem Artikel:

- [1] <https://www.heise.de/hintergrund/eHealth-Connector-replacement-is-a-EUR300-000-000-grave-without-valid-reason-7179008.html>
- [2] <https://www.heise.de/news/Telematikinfrastruktur-Austausch-von-Konnektoren-mit-auslaufenden-Zertifikaten-6583285.html>
- [3] <https://www.heise.de/news/Kassenaerztliche-Vereinigung-Austausch-von-Konnektoren-in-Praxen-alternativlos-7077403.html>
- [4] <https://www.heise.de/meinung/Teure-Intensivmedizin-fuer-ein-totes-Pferd-Der-TI-Konnektor-Tausch-7121805.html>
- [5] https://www.cgm.com/deu_de/plattformen/telematikinfrastruktur/service-und-updates/ti-erneuern.html
- [6] https://www.kococonnector.com/deu_de/kocobox-med/faq.html
- [7] <https://www.heise.de/ct/>
- [8] <https://www.heise.de/select/ct/2022/16>

- [9] <https://www.heise.de/select/ct/2022/16/2215109062905263714>
- [10] <https://www.heise.de/select/ct/2022/16/2215109093935760801>
- [11] <https://www.heise.de/select/ct/2022/16/2211708044768746862>
- [12] <https://www.heise.de/select/ct/2022/16/2213109155430529183>
- [13] <https://www.heise.de/select/ct/2022/16/2216412463166966563>
- [14] <https://www.heise.de/select/ct/2022/16/2216109395271701245>
- [15] <https://www.heise.de/select/ct/2022/16/2214510423127163877>
- [16] <https://www.heise.de/select/ct/2022/16/2217115093399431691>
- [17] <https://www.heise.de/select/ct/2022/16/2215414371932960277>
- [18] <https://www.heise.de/select/ct/2022/16/2200714215315134477>
- [19] https://shop.heise.de/ct-16-2022/Print?wt_mc=intern.shop.shop.ct_2216.ctde.textlink.textlink
- [20] <mailto:hag@ct.de>

Copyright © 2022 Heise Medien