
Stellungnahme: Sicherheit bei eGK Kartenlesegeräten

Stellungnahme von SCM Microsystems und BSI zur angeblichen Sicherheitslücke in eGK Kartenlesegeräten

Die eGK Kartenlesegeräte sind sicher – die Schwachstelle ist der Internet-Zugang des Praxis-PCs, wenn er nicht durch Antivirensoftware geschützt ist

Bensheim, 16. Juni 2011– In einer gemeinsamen Pressemitteilung teilten die Kassenärztliche Bundesvereinigung (KBV), Kassenärztliche Bundesvereinigung (KZBV), die Bundesärztekammer (BÄK) und die Bundeszahnärztekammer (BZÄK) am 25.05.2011 mit, dass die eGK-Kartenlesegeräte des laufenden Basis-Rollouts eine Schwachstelle aufweisen. Theoretisch sei es für Hacker möglich, von außen an die PIN des Arztes zu gelangen. Die darauf folgenden Medienberichte sorgten für erhebliche Verwirrung unter Ärzten, in die wir hier Klarheit bringen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dies in einer Stellungnahme berichtigt: Für die im Rahmen des Basis-Rollouts vorgesehene **Verarbeitung der** auf der elektronischen Gesundheitskarte gespeicherten **Versichertendaten durch die Kartenterminals (eHealth-BCS-Terminals) bestehen** nach aktueller Kenntnis **keine Sicherheitsrisiken**. Die **Eingabe einer PIN ist** in der Basis-Anwendung **nicht vorgesehen**.

SCM Microsystems, der Hersteller der von Concat ausgelieferten eGK-Kartenlesegeräte, nimmt Stellung: Die eGK Kartenlesegeräte von SCM Microsystems sind von dieser Sicherheitslücke nicht betroffen.

Wie das BSI SCM Microsystems bestätigt hat, handelt es sich bei der durch die Medien kommunizierten angeblichen Sicherheitslücke, die zum Ausspähen der PIN von Heilberufsausweis oder Signaturkarte dienen könnte, um ein unter speziellen Laborbedingungen durch gezieltes Einbringen von Schadsoftware auf dem Primärsystem eines Praxiscomputers erzeugtes Szenario. Hinter dem angeblichen Sicherheitsproblem steckt ein Angriffsszenario, welches zwingend einen erfolgreichen Angriff auf die IT-Sicherheit der Praxis-EDV voraussetzt. Schützt der Arzt seine EDV pflichtgemäß gegen solche Attacken, ist der beschriebene Angriff auf PINs nicht möglich. Wir empfehlen daher grundsätzlich und nicht nur zum Schutz von Patientendaten den Einsatz von aktuellen Versionen von Virenschanner und Firewall-Software.

Was die Kartenlesegeräte von SCM angeht, ist folgendes festzustellen:

Die sichere PIN-Eingabe beim **stationären eHealth200 eGK Kartenlesegerät ist bei Beachtung der Sicherheitsanweisungen** für den Praxiscomputer **gewährleistet**.

Kontakt für Journalisten:

Concat AG

Claudia E. Petrik

Telefon +49 (6157) 91 94-260

Telefax + 49 (6157) 91 94-220

E-Mail claudia.petrik@concat.de

Die PIN des **mobilen eHealth500** ist eine reine Geräte-PIN, die in keinem Zusammenhang mit einer PIN für Heilberufsausweis oder Signaturkarte steht. Das Gerät ist also prinzip-bedingt **nicht von der angeblichen Sicherheitslücke betroffen**.

Die beschriebene Sicherheitslücke steht damit in keinem kausalen Zusammenhang mit eGK Lesegeräten von SCM Microsystems, sondern betrifft die Sicherheit des Praxiscomputers des Arztes im Allgemeinen.

Das Szenario kann so aktuell auch nicht eintreten, da eine PIN-Abfrage bei stationären Geräten in der Offline-Phase (eGK Basis-Rollout) nicht vorgesehen ist. Wird ein für den Basis-Rollout zugelassenes stationäres Kartenterminal wie das eHealth200 zusätzlich für qualifizierte elektronische Signaturen genutzt, gelten gemäß SigG/SigV besondere Anforderungen an die Einsatzumgebung. Die Anwendung QES hat in einem „geschützten Bereich“ zu erfolgen. Das heißt, das Primärsystem ist durch geeignete Maßnahmen frei von Schadsoftware zu halten. Im Rahmen der Zertifizierung nach QES ist ein Verfahren für die sichere PIN-Eingabe vorgeschrieben, das optisch oder akustisch eindeutig den sicheren Status signalisiert. Zum Ausschluss des Restrisikos empfehlen wir dringend, die im Handbuch beschriebene Anzeige des Gerätes zu beachten.

Beim mobilen eGK Lesegerät eHealth500 handelt es sich um ein Gerät, das autark, ohne Verbindung zu einem PC, Daten von Versichertenkarten und elektronischen Gesundheitskarten einliest und diese Daten dann bei Anschluss an einen PC nach Aufforderung durch das Praxisverwaltungssystem an dieses kommuniziert. Ein Kommando zum Start der Verifizierung einer PIN ist hier zwar vorhanden, es handelt sich bei dieser PIN aber um die Geräte-PIN für den Leser selbst, die das Lesen der gespeicherten Daten autorisiert. Keine Ziffer dieser PIN kann an den PC und darauf befindliche Schadsoftware weitergereicht werden. Ein Kommando zur Eingabe einer Karten-PIN und Mitteilung derselben an einen PC/eine Schadsoftware wird von diesem Gerät nicht unterstützt.

Über die Concat AG:

Die [Concat AG](#) ist seit 1990 als innovativer Systemintegrator am deutschsprachigen Markt aktiv und gehört seit 2006 zur international renommierten [Meridian-Gruppe](#). Das ganzheitliche Portfolio des Unternehmens umfasst Planung, Realisierung und Betrieb komplexer IT-Infrastrukturlösungen für mittelständische Firmen und Großkonzerne. Die Schwerpunkte liegen in den Bereichen Virtualisierung, Speicherung, Sicherung, Archivierung und Netzwerke für hochverfügbare, heterogene Datenlandschaften. Der Hauptsitz des Unternehmens ist in Bensheim. Eine deutschlandweite Betreuung der Kunden vor Ort ermöglichen die Geschäftsstellen in Köln, Pfungstadt, München und Hamburg sowie die Niederlassungen in Siegen, Dortmund, Stuttgart, Freiburg, Berlin und Wendelsheim. Im Geschäftsjahr 2010 erwirtschafteten 135 Mitarbeiter einen Umsatz von gut 60 Millionen Euro.

Kontakt für Journalisten:

Concat AG

Claudia E. Petrik

Telefon +49 (6157) 91 94-260

Telefax + 49 (6157) 91 94-220

E-Mail claudia.petrik@concat.de