

## **eGK: Kein Sicherheitsrisiko durch Software-Schwachstelle – Auslieferung der eHealth-BCS-Kartenterminals wie geplant**

Die kürzlich bei den Kartenterminals zum Einlesen der elektronischen Gesundheitskarte (eGK) festgestellte Schwachstelle in der Software birgt kein Sicherheitsrisiko für die PIN des elektronischen Heilberufsausweises sowie der eGK. Das ist das Ergebnis der Sicherheitsprüfung durch eine Steuerungsgruppe, der neben der Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) auch Vertreter des Bundesministeriums für Gesundheit (BMG) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angehören.

Zum Hintergrund: Die gematik hatte vor Kurzem bei Routineuntersuchungen entdeckt, dass es über eHealth-BCS-Terminals für Hacker potentiell möglich ist, von außen an die PIN des elektronischen Heilberufsausweises zu gelangen. Die persönliche Identifikationsnummer wird zum Beispiel genutzt, um eine elektronische Unterschrift zu erstellen. Um daraufhin eine elektronische Unterschrift des Arztes fälschen zu können, müsste der Angreifer aber auch noch den Heilberufsausweis in seinen Besitz bringen.

### **Kein Sicherheitsrisiko bei Eingabe im „sicheren PIN-Modus“**

Bei korrekter Nutzung der eHealth-BCS-Kartenterminals und Karten im sogenannten „sicheren PIN-Modus“ besteht jedoch keine Gefahr. Ärzte, die bereits jetzt ihren Heilberufsausweis einsetzen, sollten daher die Bedienungsanleitung bezüglich des sicheren Modus bei der PIN-Eingabe am Kartenterminal genau beachten: Die Anzeige für den sicheren PIN-Modus besitzen alle eHealth-BCS-Terminals, in der Regel in der Form einer LED oder eines Schloss-Symbols im Display. Befindet sich das Kartenterminal in einem sicheren PIN-Modus, ist der Schutz der eingegebenen Daten gewährleistet, da die Signalisierung auch durch Schadsoftware nicht beeinflusst werden kann. Sicherheits-Update der Kartenterminalsoftware nicht notwendig.

### **Ein Sicherheits-Update der Kartenterminalsoftware wird bei korrekter Nutzung der eHealth-BCS-Kartenterminals und Karten im „sicheren PIN-Modus“ nicht benötigt.**

Um zusätzlich auszuschließen, dass bei Fehlbedienung ein Angriff durch eine Schadsoftware erfolgen kann, wird derzeit eine Vorgabe für die Kartenterminalhersteller entwickelt, die die Grundlage künftiger Zulassungen darstellt. Diese Vorgabe wird die Eingabemöglichkeit über die ungesicherte Eingabeschnittstelle zukünftig auch technisch unterbinden. Für bereits im Feld befindliche Kartenterminals wird die Vorgabe mit einem der nächsten Updates, spätestens aber zum sogenannten Online-Rollout umgesetzt, da hier die Kartenterminals für das Lesen der geschützten Versichertenstammdaten planmäßig „aufgerüstet“ werden.

### **Auslieferung der Kartenterminals wird wie geplant fortgesetzt**

Die Auslieferung der eGK-Kartenterminals wird wie geplant fortgesetzt. Der Refinanzierungszeitraum für die Ausstattung der Praxen mit Kartenlesegeräten im Rahmen des Basis-Rollout der elektronischen Gesundheitskarte läuft noch bis zum 30. September 2011. Ab 1. Oktober werden die Krankenkassen dann bundesweit mit der Ausgabe der eGK beginnen.

Aktuelle Übersicht über zugelassene Kartenterminals unter:  
[www.kv-telematik.de](http://www.kv-telematik.de)

Für Rückfragen steht Ihnen unser Service-Team unter der Telefonnummer 31003 – 999 zur Verfügung.

**Festgestellte Schwachstelle der Software birgt kein Sicherheitsrisiko für PIN des elektronischen Heilberufsausweises sowie der eGK**

**Kein Sicherheitsrisiko bei korrekter Nutzung der eHealth-BCS-Kartenterminals und Karten im sog. „sicheren Pin-Modus“**

**Kein Sicherheits-Update bei korrekter Nutzung nötig**

**Auslieferung der eGK-Kartenterminals weiterhin wie geplant**