[redacted] LD2

Kiel, 12.02.2008
Tel.: 988 - 1205

Rechtlichen Bewertung des Vorschlags, im Rahmen der eGK-Testung auf die Verwendung der PIN bei den freiwilligen Anwendungen zu verzichten und stattdessen mit einer Default-PIN zu arbeiten

Im Rahmen der Testung der eGK in Flensburg hat sich gezeigt, dass eine erhebliche Zahl der multimorbiden Teilnehmerinnen und Teilnehmer nicht mit der Eingabe der PIN zurecht kommen. Im jetzigen Stadium der Testung betrifft dies nur das Schreiben der Notfalldaten. In Zukunft werden davon weitere Anwendungen betroffen sein, die gerade für die genannten Patientengruppen hilfreich sein können, namentlich die elektronischen Patientenakte.

Es stellt sich die Frage, ob es mit den Vorgaben den § 291a SGB V vereinbar ist, auf Veranlassung der Patienten eine Default-PIN zu setzen, was dazu führt, dass keine Abfrage der PIN und keine Eingabe derselben durch den Patienten zur Freischaltung der freiwilligen Anwendungen mehr erforderlich ist.

Maßstab ist hier die Regelung des § 291a Abs. 5 Satz 2 SGB V. Die Vorschrift lautet: „Durch technische Vorkehrungen ist zu gewährleisten, dass in den Fällen des Absatzes 3 Satz 1 Nr. 2 bis 6 der Zugriff nur durch Autorisierung der Versicherten möglich ist."

Es ergibt sich bereits ohne weiteres aus dem Wortlaut des Gesetzes, dass eine PIN-Eingabe nicht ausdrücklich verlangt wird. Erforderlich ist vielmehr eine Autorisierung des Zugriffs durch den Versicherten. Die Gesetzesbegründung enthält dazu den Hinweis: „Erstens muss der Karteninhaber mit Ausnahme der Rezept und Notfalldaten den Zugriff freigeben (z. B. durch einen PIN-Code)."[1] Demnach wurde die Freischaltung durch PIN als eine mögliche oder wahrscheinlich, nicht aber als die einzig zulässige Variante der Autorisierung gesehen.

Es stellt sich die Frage, welche Möglichkeiten der Autorisierung es noch gibt. Autorisierung ist „die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Dienste an Systemnutzer"[2]. Sie geschieht regelmäßig nach der Authentisierung, d.h. des Vorgangs des Nachweises der eigenen Identität[3]. Bei der eGK (wie bei anderen kartenbasierten Verfahren, z.B. Kreditkarte) fallen Authentisierung und Autorisierung zusammen: Ist jemand gegenüber der Kartenanwendung authentisiert, hat der die mit der rolle des Karteninhabers verbundenen Rechte.

Authentisierung (und damit hier auch Autorisierung) erfolgt regelmäßig mit einem von drei Elementen oder einer Kombination aus diesen: **Besitz** (Das Subjekt hat etwas, Beispiel: Schlüssel); **Wissen** (Das Subjekt weiß etwas, Beispiel: PIN); **Sein** (Das Subjekt ist etwas, Beispiel: biometri-

---

1 BT-Drucksache 15/1525 S. 145
2 http://de.wikipedia.org/wiki/Autorisierung
3 http://de.wikipedia.org/wiki/Authentifizierung

sches Merkmal). Es ist zuzugeben, dass eine Kombination der Elemente zu einer höheren Sicherheit führt. Daher enthält die Gesetzesbegründung als Standard die Kombination von Besitz und Wissen.

Allerdings schließt die gesetzliche Regelung nicht aus, dass nur ein Authentisierungselement angewandt wird. Im Fall des effektiven Verzichts auf die PIN durch Einsetzen einer Default-PIN bleibt noch das Authentisierungs- (und Autorisierungs-)element Besitz der Karte. Durch Benutzung des Besitzes (Vorlegen der Karte) erfolgt also die Autorisierung der Kartennutzung. Das Weglassen der PIN-Eingabe und die ausschließliche Nutzung der Karte als Token zur Authentisierung und gleichzeitigen Autorisierung ist also mit dem Gesetz konform.

Es kann übrigens bemerkt werden, dass dieses Verfahren keineswegs einmalig ist. Z.B. genügt es bei vielen Bezahlautomaten, wenn eine Kreditkarte eingeführt wird. Zusätzliches Wissen (PIN) wird oft nicht verlangt.

Gegen die hier gefundene Auslegung ließe sich ins Feld führen, dass sowohl die Formulierung des Gesetzes als auch der Text der Begründung zu unterstellen scheinen, dass die Absicherung, also die bei der Autorisierung nötigen Sicherheitselemente, bei den sog. freiwilligen Anwendungen höher sein sollte als beim eRezept und beim Zugriff auf Notfalldaten. Sollte ein solches Gefälle bei der Autorisierung tatsächlich eine Anforderung sein, so wäre sie nicht mehr realisiert.

Bei näherer Betrachtung zeigt sich freilich, dass zwar ein Gefälle besteht, aber in einem etwas anderen Sinn: Beim Lesen der Notfalldaten und beim Nutzen der Karte für die Übertragung des eRezepts ist gar keine Autorisierung erforderlich.

Im Hinblick auf die Notfalldaten lässt sich dies leicht nachvollziehen. Hier muss der Zugriff ohne jede Autorisierung möglich sein, also auch ohne *Benutzung* des Besitzes. Der Zugriff auf diese Daten soll und darf gerade nicht von der Autorisierung abhängen, sondern muss für jeden Arzt ohne Zutun des Karteninhabers möglich sein. Hier ist also immer noch ein klares Gefälle gegeben: Zugriff zum Schreiben der Notfalldaten nur mit aktiver Autorisierung (Vorlage der Karte), Zugriff beim Lesen im Notfall ohne jede patientenseitige Autorisierung.

Nichts anderes gilt letztlich für das e-Rezept. Anders als nach § 291a Abs. 5 Satz 1 SGB V bei der Nutzung der Karte für die freiwilligen Anwendungen ist nämlich die Nutzung zur Übertragung von eRezepten nicht vom Einverständnis des Versicherten abhängig. Auch hier kommt man also, genauso wie beim Lesen der Notfalldaten, ohne Autorisierung aus, jedoch nicht aus tatsächlichen Gründen, sondern aus Rechtsgründen. Das von der Vorschrift geforderte Gefälle besteht damit auch hier: *keine Autorisierung* beim eRezept gegenüber *irgendeiner Art der Autorisierung* bei den freiwilligen Anwendungen. Damit sind die Fälle, in denen es auf eine aktive Autorisierung durch den Patienten ankommt, zugleich die Fälle, in denen eine ausdrückliche Einverständniserklärung durch den Patienten vorliegen muss.

In § 291a SGB V wird jedoch keine Aussage darüber getroffen, welcher Art die Autorisierung auf technischer Ebene sein muss. Allerdings muss aus Gründen der Datensicherheit gefordert werden, dass die Verfahren bei einer Autorisierung nur mittels der Karte so sicher sind, dass erfolgreiche Angriffe praktisch ausgeschlossen sind.