Elektronische Versichertenkarte

Grundlagen

Die hier gemachten Angaben basieren auf der Verordnung des Bundes über die Versichertenkarte (VVK, SR 832.105) vom 14. Februar 2007 und dem eCH Standard zur Versichertenkarte (eCH-0064 Spezifikation für das System Versichertenkarte).

Begriffe

Der Leistungserbringer ist eine Person, welche medizinische Dienste anbietet und verrechnet.

Der Versicherte ist die versicherte Person einer Krankenkasse gemäss dem Bundesgesetz über die Krankenversicherung (KVG, SR 832.10).

Prinzip

Zur Bearbeitung der elektronischen Versichertenkarte wird zusätzlich die Leistungserbringerkarte benötigt. Die Leistungserbringerkarte ermöglicht den Zugriff auf die Versichertenkarte und die darauf folgende Bearbeitung der Daten auf der Versichertenkarte. Leistungserbringerkarten werden die Leistungserbringer erhalten, welche in der Verordnung über die Versichertenkarte (VVK, SR 823.105) vom 14. Februar 2007 im Anhang aufgeführt sind.

Rechtevergabe

Grundsätzlich problematisch ist die Rechtevergabe (Autorisation) auf der Karte, s. Anhang VVK. Bedenklich ist unter anderem:

- Logopäden, Ernährungsberater, Physiotherapeuten haben das uneingeschränkte Recht, **den Hinweis auf eine Patientenverfügung** und die Kontaktadressen zu überarbeiten, d.h. lesen, schreiben und löschen!
- Ernährungsberater, Logopäden haben Einsicht (Lesezugriff) in alle höchst persönlichen Daten auf der Karte.
- Der Versicherte hat nicht die Möglichkeit, autonom, d.h. ohne einen Leistungserbringer, seine Personendaten einzusehen und diese zu kontrollieren. Für die Sicherheit wichtig ist meines Erachtens, dass der Versicherte seine Daten auf der Karte problemlos kontrollieren kann. Das schafft neben der Sicherheit auch Vertrauen in die Technologie von Seiten der Versicherten.

Eigentum an der Versichertenkarte bleibt beim Versicherer (Art. 11 Abs. 1 VVK). Die Karte muss nach Beendigung des Versichertenverhältnisses oder der Gültigkeit der Karte an den Versicherer zurückgegeben werden (Art. 10 Abs. 3 VVK). Nirgendwo wird aber festgelegt, dass der Versicherer bei der Ausstellung der Versichertenkarte diese an den Versicherten so auszuhändigen hat, dass der Versicherer nie wieder Zugriff auf die Karte haben werden kann.

Gesichert ist, dass gemäss technischer Spezifikation vom März 08 der Versicherer sogar die Möglichkeit hat, jederzeit die Karten PIN neu zu setzen, weil er das dazu notwenige Kartengeheimnis (engl. Personal Unblocking Key, kurz PUK) besitzt.

Der Versicherte selber kann die Daten auf der Karte nicht löschen, bevor er die Karte zurückgibt. Er muss dafür einen Leistungserbringer bemühen.

Backup der Daten auf der Versichertenkarte

Aus der VVK nicht ersichtlich, aber in der technischen Spezifikation auch nicht enthalten, ist ein Backup Konzept der Daten der Versichertenkarte. Geht eine Versichertenkarte also verloren, so können die Daten der verlorenen Karte nicht in einfacher Art und Weise auf die neue Karte geladen werden. Um die Konsistenz und Vollständigkeit der Daten nach Verlust muss der Versicherte (Leistungsbezüger) bemüht sein.

Wie der Aufwand, welcher bei den Leistungserbringern durch die Wiederherstellung der Daten verursacht wird, entgolten wird, ist nicht geregelt.

Wechselt der Versicherte die Krankenkasse und erhält deswegen eine neue Karte, dann kann er die Daten nicht auf die neue Karte kopieren.

Ungeklärte Kosten

Der Versicherte hat gemäss Art. 9 VVK das Recht, von irgendeinem Leistungserbringer zu erfahren, welche Daten auf seiner Karte enthalten sind. Gemäss Art 13 VVK kann der Versicherte in Erfahrung bringen, welcher Leistungserbringer welche Daten bearbeiten und einsehen kann und wie die Karte bezüglich PIN (Personal Identification Number) gesperrt werden kann.

Dies alles verursacht Beratungsaufwand auf Seiten der Leistungserbringer, insbesondere beim Erklären an technisch nicht versierte Patienten. Nicht geregelt ist, wie der Leistungserbringer dafür zu entgelten ist.

Das Setzen der PIN in der vom Versicherten gewünschten Form benötigt Zeit. In den meisten Fällen wird das Setzen der PIN, wenn überhaupt, beim Leistungserbringer erfolgen, was wiederum Beratungszeit beansprucht.

Aus Sicht der Leistungserbringer ist zusätzlich bedenklich, dass nicht geklärt ist, wer die zwei Lesegeräte für die Chip-Karten, die SW und die Installation der SW bezahlen muss.

Authentisierung der Karten

Grundsätzlich positiv ist, dass sich Leistungs- und Versichertenkarte gegenseitig authentisieren. Beim spezifizierten Authentisierungsverfahren nicht berücksichtigt worden ist:

Sperrung einer Versichertenkarte. Der Leistungserbringer kann alleine bei der Authentisierung der Karte nicht feststellen, ob die Versichertenkarte noch gültig ist oder ob er daran ist, eine alte oder verloren gegangene Karte zu überarbeiten. Er muss zusätzlich eine online Abfrage vornehmen.

Sperrung der Leistungserbringerkarte: Die Versichertenkarte kann nie feststellen, ob die Leistungserbringerkarte noch gültig oder inzwischen gesperrt worden ist. Angenommen, eine Leistungserbringerkarte eines Arztes wird mit dazu gehöriger PIN gestohlen, dann kann der neue Besitzer der Karte theoretisch alle Versichertenkarten auf Lebzeiten bearbeiten! Er benötigt lediglich noch die SW, welche beim Leistungserbringer zur Bearbeitung der Daten installiert werden muss. CD oder Laptop mit SW sind ausreichend. Nota bene: Bei den Daten auf der Versichertenkarte handelt es sich hier um besonders schützenswerte Daten nach Art. 3 lit. c des Datenschutzgesetzes (DSG, SR 235.1).

Die Verifikation der Zertifikatskette ist optional. Zudem wird die Zertifikatskette nicht von der Versichertenkarte, wie eigentlich für eine korrekte Authentisierung erforderlich, sondern vom Lesegerät (Terminal) oder von der Applikation geprüft. Weiter wird die Revokationsliste (Status) der Zertifikate nicht geprüft. Dies birgt weiter die Möglichkeit, dass sich nicht ein berechtigter Leistungserbringer bei der Versichertenkarte anmeldet.

Nicht authentisiertes Schreiben: Der Schreibvorgang selber wird von der Versichertenkarte nicht authentisiert, d.h. ein Leistungserbringer kann (theoretisch) im Namen eines

anderen Leistungserbringer Veränderungen auf der Karte vornehmen, wenn er dessen EAN Nr. kennt. Eine Sicherheitsvorkehrung gegen das soeben beschriebene Risiko ist in der technischen Spezifikation zur Versichertenkarte nicht aufgeführt.

Im Hinblick auf einen möglichen Verlust der Karte und der Unmöglichkeit, eine Karte zu sperren, stellt dies ein äusserst bedenkliches Sicherheitsmanko dar.

Schule machen

Es besteht die Gefahr, dass die hier vorgebrachten Sicherheitsmängel Schule machen, d.h., dass in anderen Bereichen ebenfalls nicht ausreichende Sicherheitsarchitekturen und –technologien konzipiert und realisiert werden.

Freiwilligkeit

Das Eintragen von Personendaten ist für den Versicherten freiwillig. Doch will er einen von der Bundesbehörden definierten und standardisierten Dienst nutzen, so darf er doch erwarten, dass das System der Versichertenkarte nicht solch gravierende Mängel aufweist. Es sollte keines Spezialisten bedürfen, um sich davon in Kenntnis zu setzen.

Online Dienst

Es besteht die Möglichkeit, dass der Leistungserbringer Informationen über den Versicherten in Erfahrung bringen kann, wie und ob dieser noch versichert ist. Gemäss eCH Standard muss die Verbindung per SSL v3.0 oder TLS1.0 geschützt werden. Dabei wird aber nicht festgelegt, wie die Verbindung verschlüsselt wird (DES oder AES).

Fazit

Die Vergütung der Mehraufwände, welche durch die Bearbeitung der Versichertenkarte verursacht werden, ist im Umfeld der Versichertenkarte nicht geregelt worden und somit unklar.

Die Rechtevergabe ist in der Verordnung zu wenig differenziert geregelt worden, insbesondere die Leserechte der höchst persönlichen Daten und die Bearbeitung der Notfalldaten und der Hinweis auf Patientenverfügungen.

Die Konsistenz (Vollständigkeit) der Daten kann nach Verlust der Karte unter Umständen nicht oder nur mühsam erreicht werden.

Zudem kann das Sperren einer Leistungserbringerkarte von der Versichertenkarte nicht festgestellt werden, was ein nicht zu übersehbares Sicherheitsrisiko in der Handhabung von besonders schützenswerten Daten darstellt.

Bemerkung

Der Autor war bei der Vernehmlassung des eCH Standards zur Versichertenkarte anwesend und hat dabei eine Vielzahl der hier aufgeführten Mängel vorgebracht. Diese wurden aber bei der Verabschiedung der Verordnung und des Standards nicht berücksichtigt.