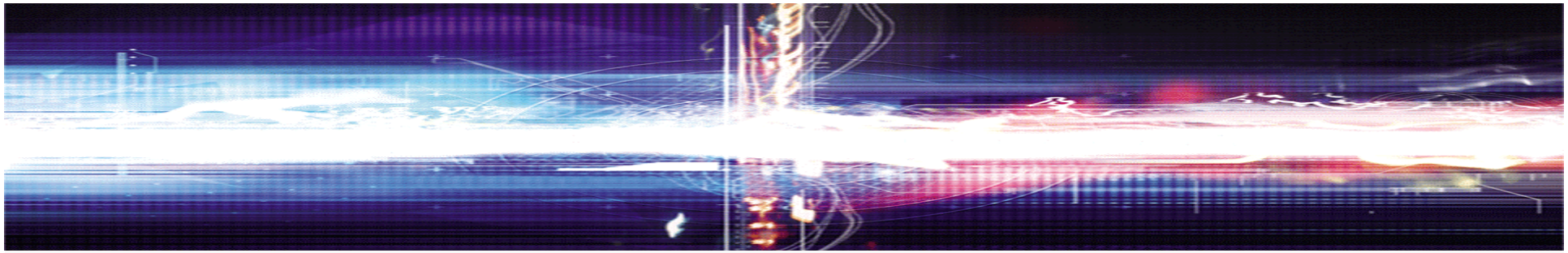


Sicherheits(technische) Aspekte der „neuen“ (Sozial)Versichertenkarte

Datenschutz-Forum Schweiz

Daniel Muster
Dipl. Physiker UNI Bern, NDS ETHZ
daniel.muster@it-rm.ch
www.it-rm.ch
20. Nov. 2014

Einleitung

Vorbemerkung:

Bei der Stellungnahme zum technischen Standard im 2007 anwesend. Die meisten der nun vorgestellten Mängel bereits damals vorgebracht.

Einleitung

Inhalt des Vortrags

- Allgemeine Infos
- Zweck der Versichertenkarte und die PIN
- Zugriff und Sperrung
- Hinweis auf die Patientenverfügung und Kontrolle
- Sicherheit des Aufbewahrungsmediums (Chip)
- Backup
- Eigentum
- Kosten (Aufwand)
- Fazit
- Fragen

Allgemeine Infos

Die hier vorgestellten Angaben basieren auf:

- Der Verordnung des Bundes über die Versichertenkarte (VVK, SR 832.105) vom 14. Februar 2007
- eCH Standard Spezifikation für das System Versichertenkarte (eCH-0064) und Authentisierung (eCH-0106)

Allgemeine Infos

Patientendaten

- haben zuverlässig oder verlässlich (d.h. zutreffend und möglichst aktuell) zu sein
- sind bezüglich Vertraulichkeit meistens besonders schützenswert

Zweck der Versichertenkarte

Der Chip der Versichertenkarte ist ein Speicherort für:

- Allgemeine Daten (kein Schutz) wie
  Personalien des Versicherten
  Hinweis auf eine Patientenverfügung
- Medizinaldaten (Zugriffsschutz + optional PIN-Eingabe durch den Versicherten)

Motivation, Patientendaten zu speichern:

- Zugriff auf Patientendaten im Notfall des Patienten

Zugriff und Sperrung

Datei Dateiname	Lesen	Schreiben/Löschen
Blutgruppen- und Transfusionsdaten	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Immunisierungsdaten	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Transplantationsdaten	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Allergien	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Krankheiten und Unfallfolgen	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Zusätzliche Einträge	Alle Leist. + PIN des Vers.	Ärzte und Chirop. + PIN des Vers.
Medikation	Alle Leist. + PIN des Vers.	Ärzte, Chirop. + PIN. oder Apotheker + PIN des Vers
Kontaktadressen	Alle Leist.	Alle Leist.
Patientenverfügungen	Alle Leist.	Alle Leist.

Zugriff und Sperrung

Kein Schutz bei den allgemeinen Daten bedeutet:

- Lese und Schreiberechte für alle Leistungserbringer im Gesundheitswesen, wie Ernährungsberater und Logopäden
- **Keine Leserechte** des Versicherten

Zugriffschutz bei Medizinaldaten bedeutet:

- Leserechte für alle Leistungserbringer
- Schreibrechte nur für gewisse Berufsgruppen auf die entsprechenden Daten
- **Keine Leserechte** des Versicherten

Zugriff und Sperrung

Keine Leserechte des Versicherten =>

- Es fehlt an einer wichtigen Kontrollmöglichkeit!
- Selbstbestimmung des Patienten leidet!

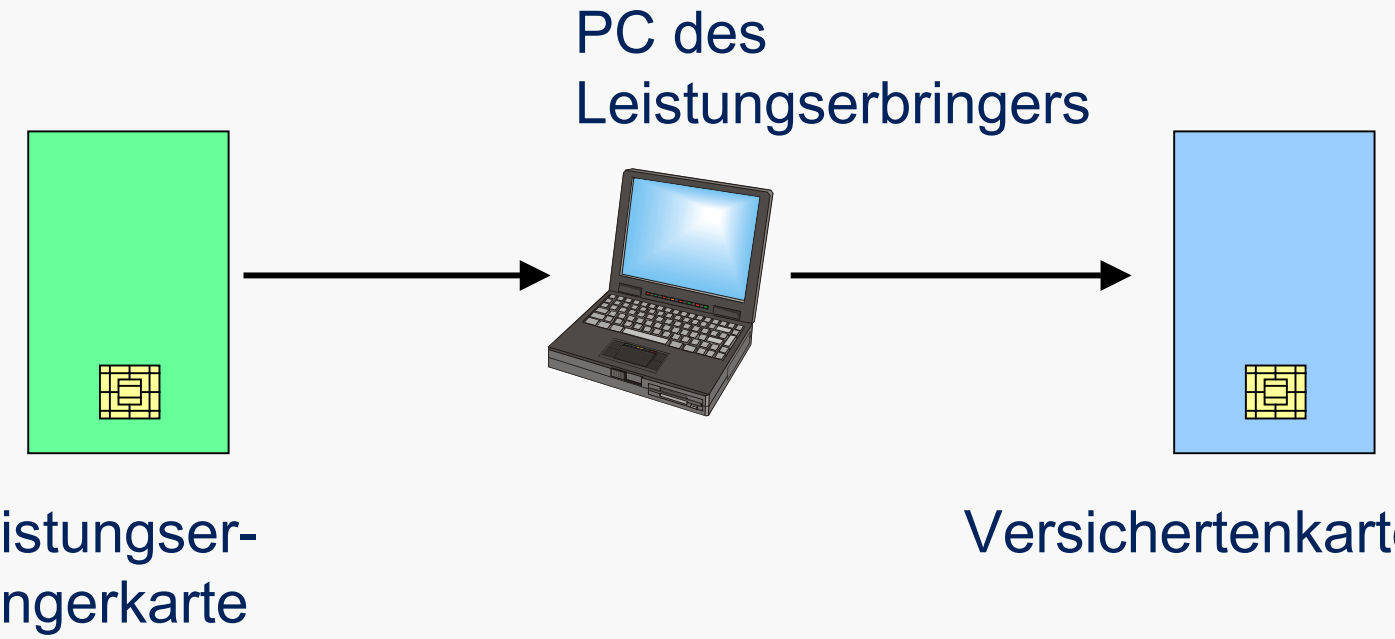
Motivation, Patientendaten zu speichern: Zugriff darauf bei einem Notfall des Patienten!
Das beutet jedoch, um wirksam zu sein: Kein PIN-Schutz, sonst kein Zugriff z.B. bei Nichtansprechbarkeit des Patienten möglich!

Quintessenz:

- PIN-Schutz ist ein **untaugliches** Mittel zum Schutz von Patientendaten im Notfall!
- Kein PIN-Schutz => jeder Leistungserbringer kann alles lesen!

Zugriff und Sperrung

Prinzip: Auf Zertifikat basierende Authentisierung!



Zugriff und Sperrung

Die eingesetzten Verfahren bei der „sicheren“ Authentisierung sind nicht mehr aktuell oder weisen erhebliche Sicherheitsmängel auf! Z.B.:

- Der Schreibprozess auf die Karte ist nicht ausreichend authentisiert!
- Die Authentisierung findet nicht vollständig zwischen den Karten statt.
- Die Zertifikate der Leistungserbringer werden nicht auf ihre Gültigkeit geprüft!

=> Eine Leistungserbringerkarte kann nicht gesperrt werden, z.B. bei Diebstahl oder Ungültigkeit im Laufe der Zeit! Konsequenz:

- Mit der entwendeten Leistungserbringerkarte und dazu gehöriger PIN kann auf die Patientendaten jede Versichertenkarte ohne PIN Schutz auf **ewig** zugegriffen werden!

Hinweis auf Patientenverfügung

Der Hinweis auf eine Patientenverfügung kann von jedem Leistungserbringer gelöscht werden!

Nicht vorgesehen: Der Patient kann grundsätzlich nichts kontrollieren und dies gegebenenfalls korrigieren lassen!

Nationalrat wollte 2013 bei der Transplantation von Organen einen Systemwechsel vollziehen, doch der Ständerat lehnte dies ab. Das hätte bedeutet, dass man in Zukunft neu aktiv erklären müsste, dass man keine Organe spenden will.

Sicherheit des Chip

An die Systemsicherheit des Chips werden für die Speicherung der Patientendaten keine Anforderung gestellt.

Für die Aufbewahrung der privaten Schlüssel für das Leisten einer der Hand gleichgestellten elektronischen Signatur jedoch schon!

Backup

Keine Möglichkeit für ein Backup =>

Bei Verlust der Karte müsste der Versicherte alle Leistungserbringer aufsuchen, welche jemals etwas auf die Karte geschrieben haben.
Problem, gegebenenfalls sich zu erinnern, bei welchem Leistungserbringer was auf die Karte geschrieben wurde!
=> Aufwand kann für Behinderte erheblich sein!

Eigentum

Eigentümer der Karte bleibt der Versicherer

Bei Wechsel der Versicherung kann die Versicherung darauf bestehen, dass ihnen die Karte zurückgegeben wird.
=> der Versicherer könnte dann theoretisch auf die Medizindaten des Versicherten zugreifen!
Infolge mangelnder Zugriffsrechte keine Anleitung an den Versicherten möglich, wie dieser selber seine Daten effizient löschen kann, (ohne dabei den Chip zu zerstören)!

Kosten

Neue Aufwände:

- Der Versicherte hat das Recht, vom Leistungserbringer zu erfahren, welche Daten auf seiner Karte enthalten sind (Art. 9 VVK).
- Der Versicherte kann dabei in Erfahrung bringen, welcher Leistungserbringer welche Daten bearbeiten und einsehen kann und wie die Karte bezüglich PIN (Personal Identification Number) gesperrt werden kann (Art 13 VVK).
- => Aufwand für den Arzt! Aber wie sieht die Verrechnung aus?

Fazit

- Die Versichertenkarte weist gravierende Sicherheitsmängel sowohl in der technischen wie auch in der administrativen Konzeption auf.
- Gefahr: Schule machen für weitere Sicherheitsimplementierungen => Ein grosses „?“ im Hinblick auf das elektronische Patientendossier
- Verlassen auf eine Scheinsicherheit!
- M.E. nicht Otto-Normalverbraucher tauglich, aber sicher nicht behindertengerecht.
- Durch die schlechte Implementierung kann die folgende Meinung entstehen: Auf Zertifikat basierende Authentisierung ist per se auch unsicher

Lösungsansätze

Zuerst einmal studieren, welche Lösungen bereits andere Länder im Einsatz haben und warum.
Die Prozesse im Gesundheitswesen besser verstehen, bevor technische Standards entworfen werden.
In Anbetracht der Sensitivität der Daten, angemessene Sicherheitslösungen vorschlagen.

Fragen