DuD
Datenschutz und Datensicherheit

Krankenversichertenkarte

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Die Krankenversichertenkarte (KVK) ist bis heute (abgesehen von der Telefonkarte) die Chipkartenanwendung mit der größten Verbreitung. Sie ersetzte nach einer Pilotphase zum 1. Januar 1995 bundesweit den Krankenschein der gesetzlichen Krankenversicherungen.

Für die Krankenversichertenkarte kommen ausschließlich Chipkarten mit einfachen Speicherchips, d.h. ohne eigenen Prozessor, zur Anwendung. Sie unterscheiden sich hinsichtlich der Datenspeicherung nicht wesentlich von Magnetstreifenkarten – abgesehen von deren Fehleranfälligkeit, verursacht durch Verschmutzungen des Magnetstreifens, und der dort auf 223 Zeichen beschränkten Speicherkapazität.

Eine KVK muß der „Technischen Spezifikation Versichertenkarte" genügen, die von der kassenärztlichen Bundesvereinigung herausgegeben wird. Die Chipkarten-Lesegeräte für Krankenversichertenkarten sollten ein Produktzertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besitzen – eine Anforderung, die dem BSI 1994 einen Anstieg der Zertifizierungsprojekte um einige hundert Prozent bescherte.

Die Krankenversichertenkarten besitzen einen auf 256 byte beschränkten Speicher. Die Versichertendaten werden in einem applikation data file (ADF) auf der Karte gespeichert. Sie umfassen im wesentlichen die Angaben auf dem früheren Krankenschein (siehe Tabelle); eine Speicherung weiterer Daten ohne Einwilligung des Patienten ist unzulässig (siehe SGB V § 291 Abs. 2; [Kuhl_93]).

Dem ADF geht ein 32 byte langer ISO-Header voraus, der Daten des Kartenherstellers und Informationen über die Anwendung enthält [ISO_89, ISO_95]. Die Versichertendaten sind in einem ASN.1 (abstract syntax notation one) ähnlichen Format, d.h. einer Typ-Länge-Wert-Darstellung, auf der Karte gespeichert: Das erste Byte eines jeden Datums gibt den Datentyp des Datenelements an (tag oder Kennziffer, siehe Tabelle), gefolgt von einem zweiten Byte, das die Länge des Datenelements in byte bezeichnet. Werden nicht alle 256 Bytes genutzt, folgt hinter den Daten ein Füller-Eintrag (tag 0xC0, Länge, Füll-Bytes).

Auf die auf der KVK gespeicherten Daten kann frei zugegriffen werden; es gibt keinen Schutzmechanismus, wie z.B. eine PIN-Abfrage, der vor unberechtigtem Auslesen schützt. Sogar auf einen Schreibschutzmechanismus, der ein erneutes Beschreiben oder Ändern der Krankenversichertendaten nach der Personalisierung durch den Versicherer verhindert, wurde verzichtet.

tag	Datenelement	Länge
0x80	Krankenkasse	2-28
0x81	Krankenkassennr.	7
0x82	Versichertennr.	6-12
0x83	Versichertenstatus	4
0x84	Titel	0-15
0x85	Vorname	0-28
0x86	Namenszusatz	0-15
0x87	Familienname	2-28
0x88	Geburtsdatum	8
0x89	Straße, Nr.	0-28
0x8A	Wohnsitz (Land)	0-3
0x8B	Postleitzahl	4-7
0x8C	Ort	2-22
0x8D	Gültigkeitsdatum	4
0x8F	VKNR	5
0x90	Status-Ergänzung	0-3
0x8E	Prüfsumme	1

Tabelle: Daten der Krankenversichertenkarte

Da die KV-Chipkarten ISO-konform sind, lassen sie sich leicht mit jedem handelsüblichen Chipkartenleser auslesen – und verändern. Der einzige „Integritätsmechanismus" ist die Prüfsumme, die durch eine Exklusiv-Oder-Verknüpfung aller Bytes des Datenbereichs bestimmt wird; ein leicht nachzubildender Mechanismus.

Auch ein BSI-Zertifikat bestätigt lediglich einen minimalen „Schutz": KVK-geeignete Lesegeräte dürfen, sofern sie in einer Arztpraxis eingesetzt werden, keine Schreiboperationen zulassen.

Der Selbstbau eines einfachen Kartenlesers, der sich an die serielle Schnittstelle eines PC anschließen läßt, wurde Ende 1994 in der Zeitschrift c't vorgestellt [Meye_94]. Materialkosten: unter 20 DM. Damit wird die Manipulation der Krankenversichertenkarte technisch und finanziell zu einem Kinderspiel.

Eine manipulationssichere Lösung wäre leicht durch die üblichen Hardware-Schreibschutz-Mechanismen oder, wenn ein erneutes Beschreiben der Karte zulässig sein soll, durch Verwendung einer kryptographischen Einweg-Funktion als Prüfsumme möglich gewesen, z.B. eines verschlüsselten CRC (cyclic redundancy check) oder eines MAC (message authentication code). Dies wäre nicht einmal mit zusätzlichen Kosten für das Chipkarten-Lesegerät verbunden.

Die Versichertendaten ließen sich technisch vor unberechtigter Kenntnisnahme durch einen PIN-Mechanismus schützen. Eine solche datenschutzfreundlichere technische Lösung würde jedoch spürbare Mehrkosten auf der Seite des Lesegeräts (zusätzliche PIN-Tastatur) und bei der Personalisierung (PIN-Vergabe, Neuausstellung von Karten bei PIN-Verlust) verursachen; sie ließe sich möglicherweise nicht einmal bei den Versicherten durchsetzen.

Literatur

[ISO_89] ISO/IEC 7816-3 (IS): Information technology – Identification cards – Integrated circuit card(s) with contacts – Part 3: *Electronic signals and transmission protocols*, 1989 (Revision of ISO 7816-3: 1989, DIS, 1997).

[ISO_95] ISO/IEC 7816-4 (IS): Information technology – Identification cards – Integrated circuit card(s) with contacts – Part 4: *Interindustry commands for interchange*, 1995.

[Kuhl_93] Kuhlmann, Jan: *Die Verarbeitung von Patientendaten nach dem SGB V und das Recht auf selbstbestimmte medizinische Behandlung*. Datenschutz und Datensicherung (DuD), 4/1993, S. 198-208.

[Meye_94] Meyer, Carsten: *Chipkarten-Terminal mit seriellem Anschluß*. c't 12/94, S. 319 ff.