CHIPKARTENTECHIK

VP Wissenschaftliche Arbeitstechniken und Präsentation
[WS 2001/2002]

- Geierspichler Andrea
- Ruhs Gunnar
- Gross Roman
- Heimlich Martin
- Eisenprobst Florian

Geschichtlicher Hintergrund

- 50er Jahre: Diners Club ermöglichte erstmalig bargeldlose Bezahlung durch **Karten mit Hochprägung**
- Wirtschaft forderte zusätzlichen Speicherplatz $\longrightarrow$ **Magnetstreifenkarte** eingeführt
- 1974: **Chipkarte** patentiert
- 1984: 1. Telefonwertkarte
- Elektronisches Bargeld eingeführt
- Mobiltelefone

Arten von Karten

Karten mit Hochprägung:

- Älteste Technik
- ISO 7811
- Einfache Verwendung
- Papierflut
- Heute: Kreditkarten

Arten von Karten

Magnetstreifenkarten:

- ISO 7810 - 7813
- Geringe Speicherkapazität
- Geringe Sicherheit
- Weltweit standardisiert und weit verbreitet
- Durch zusätzliches Aufbringen von Fotos, Namen und Unterschrift für den Menschen überprüfbar
- Heute: Geldautomaten (PIN)

Arten von Karten

Chipkarten:

- Jüngste Entwicklung
- Hohe Speicherkapazität: bis 32kB
- Schutz vor unerlaubten Zugriffen
- Zusätzlicher Magnetstreifen möglich
- Anwendungsbereiche: Mobiltelefone, Krankenversicherungskarten, Pre-Paid-Karten,...

Grundlagen und Technik

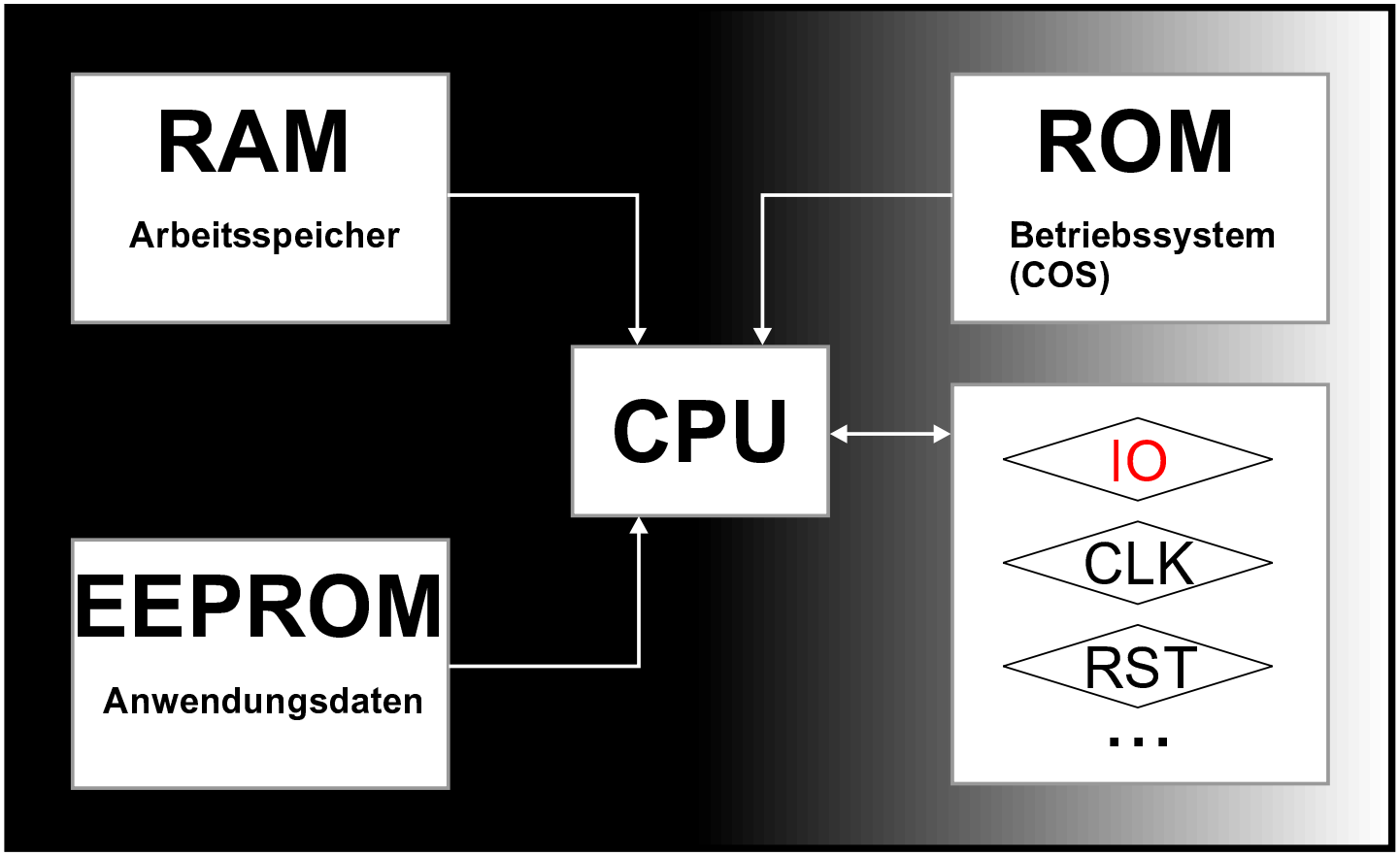
Unterschiedliche Chipkarten:

- **Speicherchipkarten:** Enthalten nur elektronischen Speicher, auf den direkt zugegriffen werden kann
- **Intelligente Speicherchipkarten:** Speicher ist nur über eine festverdrahtete Sicherheitslogik zugänglich
- **Prozessorchipkarten (Smartcards):** Enthalten einen kompletten Rechner (Prozessor, ROM, RAM)

Verbindung zur Außenwelt:

- **Chipkarten mit Kontakten**
- **Kontaktlose Chipkarten**

Aufbau von Smartcards



Herstellung und Personalisierung einer ICC (Intergrated Circuit Card)

- **Erstellung des Halbleiters**
- **Einbetten des Halbleiters**
- **Bedrucken der Karte**
- **Personalisierung**
- **Ausgabe der Karte**

Wichtige Normen

- **ISO 7816-1**: Physikalische Eigenschaften für Identifikatonskarten
- **ISO 7816-2**: Abmessungen und Lage der Kontakte
- **ISO 7816-3**: Elektrische Eigenschaften der Kontakte, Kommunikationsprotokolle
- **ISO 7816-4**: Kommunikationsinhalte, Datenstruktur der ICC, Sicherheitsarchitektur, Zugriffsmechanismen
- **ISO 7816-5**: Aufbau von Applikationen, Wahl und Ausführung

Das COS (Chipcard Operating System)

Stellt das Interface zwischen Hardware und Software zur Verfügung.

- Datenaustausch mit der Chipkarte
- Dateiverwaltung
- Kryptographische Funktionen
- Zugriffskontrolle und Sicherheit

Das COS ist maximal 16 KByte groß
und kann bei neueren Chipkarten auch nach der Herstellung noch upgedated werden.

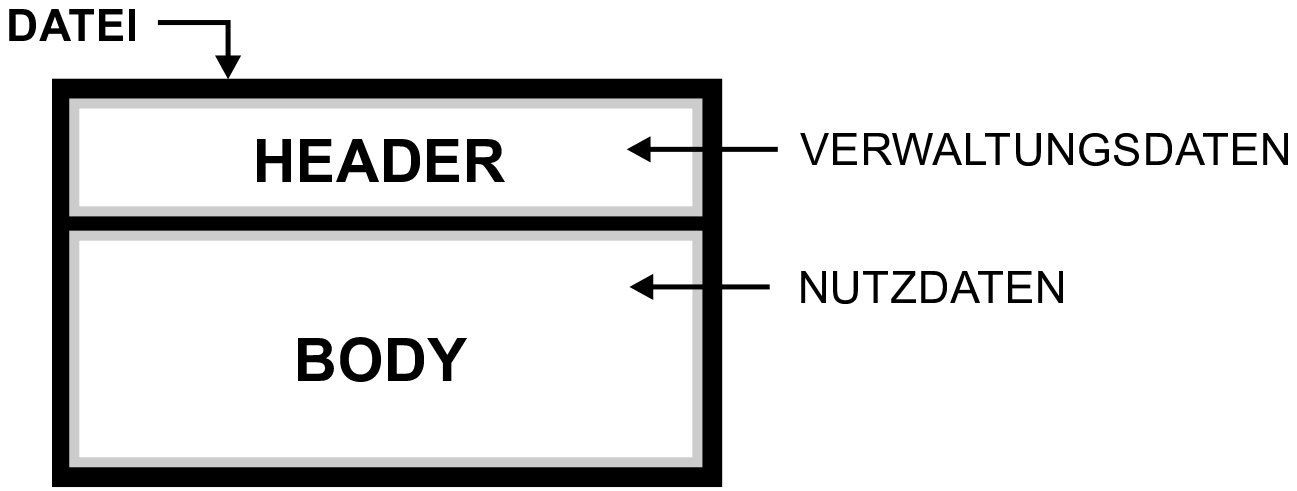
Die Arbeit des Betriebsystems

- Befehle erreichen den IO-Manager über die serielle Schnittstelle
- Ggf. Entschlüsselung durch den Security Manager
- Analyse duch den Kommandointerpreter
- Ausführung

Dateiverwaltung und Dateizugriff

Die Dateiverwaltung erfolgt in einer Baumstruktur, das Wurzelverzeichniss wird durch das Masterfile (MF) repräsentiert. Wenn eine Chipkarte über mehr als eine Anwendung verfügt, werden dafür Dedicated Files (DF) angelegt, unter denen die verschiedenen Anwendungen Platz finden.

Die eigentlichen Daten sind in den Elementary Files (EF) abgelegt (Im MF oder in den DF).



Dateiverwaltung und Dateizugriff

Dateizugriff:

- Selektieren der Anwendung (AID Applicationidentifier), in welcher dich die Datei befindet
- Selektieren der Datei (FID Fileidentifier, 2 Byte, z.B: Masterfile= 3F00)

Kommunikation zwischen Chipkarte und Terminal

- Master/Slave Prinzip, Terminal ist Master, Karte ist Slave
- Daten werden halbduplex übertragen, Vollduplexverfahren noch nicht implementiert
- ATR (Answer to Reset) wird bei jedem Reset einer Chipkarte übertragen, um dem Terminal das verwendete Protokoll mitzuteilen

Funktion des Übertragungsprotokolls bei Chipkarten:

- Synchronisation
- Erkennen von Datenverlusten auf der Übertragungsstrecke
- Erkennen von Datenverfälschungen

Verschiedene Übertragungsprotokolle

Es sind 15 Übertragungsprotokolle in der ISO-Norm 7816-3 vorgesehen. Die Bezeichnung setzt sich aus dem Ausdruck 'T=' und einer nachfolgenden Zahl zusammen:

Übertragungsproto-koll	**Beschreibung**	**Bemerkung**
T=0	asynchron, halbduplex	byteorientiert
T=1	asynchron, halbduplex	blockorientiert, fort-schrittlichstes Übertra-gungssprotokoll
T=2,3	reserviert für zukünftige vollduplex Anwendung	-
T=4	asynchron, halbduplex	byteorientiert, Erweite-rung von T=0
Rest	reserviert für zukünftige Anwendung	-

Befehlssatz des COS

Der Befehlssatz ist nicht einheitlich, aber man kann von einem Basisbefehlssatz ausgehen, der von den Firmen un spezielle Befehle erweitert wird.

Es existieren im Groben folgende Befehlsgruppen:

- Selektieren von Verzeichnissen und Dateien
- Lesen und Schreiben von Dateien
- Identifizierungsbefehle
- Authentisierungsbefehle
- Kryptographische Befehle
- Systemkonfigurationsbefehle

Löschen einer Speicherzelle

- Schlüsseldaten befinden sich im EEPROM
- Relativ hohe Spannung nötig, Unterbrechung der Spannung während dem Programmieren führt dazu, dass der Speicher nicht gelöscht wird
- Früher kam die notwendige Programmierspannung vom Host Angriffsziel von Hackern z.B. bei PayTV Karten
- Heute generiert die Karte die benötigte Programmierspannung (12V) aus den 5V der Versorgungsspannung, mit Hilfe von Oszillatoren und einem Dioden-Kondensatorennetzwerk
- Erschwert den Angriff, Zugriff nur mehr mit speziellen Geräten (Laser, Ultraschall, gebündelter Ionenstrahl) möglich

Non-invasive Attacken

- EEPROM reagiert empfindlich auf ungewöhnliche Temperaturen und Spannungen während des Beschreibens
- Es ist so möglich, dass Sicherheitsbit zurückzusetzen, ohne die Daten zu löschen (z.B. beim Sicherheitsprozessor DS5000)
- Gegenmaßnahmen: Sensoren, die ein Reset auslösen, sobald irgendeine Umgebungseinstellung einen unültigen Zustand aufweist
- Führt aber zu Rückgang der Robustheit, da z.B. schnelle Spannungsschwankungen beim Ein- und Ausschalten
- Neuere Sensoren lassen schnelle Spannungsveränderungen zu, aber viele Geräte können auch diese Eigenschaft nutzen

Befehle decodieren

- Spannungs und Taktänderungen können dazu verwendet werden, Befehle zu decodieren
- Jeder Transistor und seine Anschlüsse erscheinen nach aussen wie ein RC Element mit einer charakteristischen Zeitverzögerung
- Eine sich sehr schnell ändernde Eingangsspannung oder ein viel kürzerer Taktpuls betrifft nur die Transistoren innerhalb des Prozessors
- Eine Vielzahl von verschiedenen, unterschiedlichen Befehlen wird ausgeführt, die nicht unbedingt vom Mikroprogramm unterstützt werden müssen

Ausgabeschleifen

- Ausgeben des begrenzten Inhalts eines Speichers auf den seriellen Port
- Man sucht nach einer Eingangsstellung, wobei man in der Lage sein soll, diese exakt wiederholen zu können
- Alle Signale die gesendet und empfangen werden, müssen zeitlich exakt nach dem Reset eines Tests ausgeführt werden
- Es wird so lange getestet, bis ein Byte ausgegeben wird
- Vorgang mit der selben Einstellung wiederholen; gesamter Speicher wird dadurch ausgelesen

Physikalische Attacken

- Für aktuelle Smartcards gibt es nur einen leichten Schutz (kapazitiver- oder optischer Sensor) um direkten Zugriff auf das Silizium zu verhindern. Sensoren können leicht übergangen werden

- **Freilegen des Chips mit Säure:**

  1. Die hintere Chipabdeckung mit einem scharfen Messer entfernen, bis Epoxyd-Harz sichtbar wird
  2. Salpetersäure auf das Harz auftragen und warten, bis sich das Harz auflöst (mit Infrarotstrahl erhitzen)
  3. Ein Azetonbad entfernt Harzreste und Salpetersäure
  4. Prozedur fünf bis zehn mal wiederholen, bis die Siliziumschicht freigelegt ist

- Nun kann man den Chip mit verschiedenen Geräten bearbeiten z.B. microprobing needles, laser cutter, electron beam tester usw.

Advanced Attack Techniques: Reverse Engineering

- Schutzschicht entfernen und eine dünne schicht aus Gold oder Palladium aufbringen; Dieser Film bildet mit dem Silizium an gewissen Stellen Dioden (Schottkyeffekt)
- Der Electron Beam Tester erkennt die Dioden und die verschiedenen Schichten des Siliziums können nach und nach ausgelesen werden. Liefert Abbild des Chips
- Wenn das Layout eines Chips einmal bekannt ist, gibt es verschiedene Methoden, den Chip während der Ausführung zu beobachten

Chipkarten in der mobilen Telefonie

Chipkarten sind in der modernen mobilen Kommunikation nicht mehr wegzudenken. Das GSM (Global System for Mobile Communications) ist die weltweit größte Anwendung von Chipkarten

- Bezeichnung: SIM (Subscriber Identification Module)
- Zwei verschiedene Formate: ID-1 (Checkkarte), ID-000 (ca. 2x1 cm)
- Dient zur Identifikation der Benutzer
- Vom Standard abweichender Verschlüsselungsmechanismus (COMP128)
- Ermöglicht ein sicheres Abrechnungsverfahren

Details

- Ein SIM ist gekennzeichnet durch die im gesamten GSM Netz eindeutige IMSI (International Mobile Subscriber Identity)
- Um Anonymität zu gewährleisten wird meistens eine TMSI (Temporary Mobile Subscriber Identity) zur Identifizierung verwendet
- Aus IMSI und TSMI lassen sich die kartenindividuellen Schlüssel für die Authentisierungen und Verschlüsselung der Daten auf der Luftschnittstelle ableiten
- Die Verschlüsselung der übertragenen Sprachdaten wird nicht direkt von dem SIM ausgeführt, sondern vom Mobiltelefon übernommen (noch keine ausreichende Rechenleistung vorhanden)
- Kommunikation zwischen Mobiltelefon und SIM läuft mittels Übertragungsprotokoll T=0

Funktionsweise

- Aufbau einer Verbindung

1. Mobiltelefon schickt die IMSI/TSMI an die best-empfangbare Basisstation (Sendemast)
2. Der Netzbetreiber überprüft ob der Netzteilnehmer bei ihm registriert ist
3. Wenn ja wird eine Zufallszahl, mit deren Hilfe die Verschlüsselung erfolgt, zurückgeschickt, wenn nein wird der Anmeldevorgang abgebrochen
4. SIM errechnet und schickt den aus IMSI und der Zufallszahl mittels COMP128 gebildeten Schlüsselblock an die Basisstation
5. Die Basisstation führt die selben Berechnungen durch und vergleicht das Ergebnis mit dem des Mobiltelefons
6. Bei Übereinstimmung ist der Teilnehmer erfolgreich authentifiziert

Gespeicherte Daten

- Das SIM hat neben der Authenifizierung auch noch die Aufgabe einige für den Benutzer und das Mobiltelefon wichtige Daten zu speichern

- Das Dateisystem des SIM besteht aus einem MF und zwei DF in denen sich insgesamt 30 EF befinden

MF	
ICCID (10 Byte Identifikationsnummer der Chipkarte)	
DF enutzer	**DF Netzbetreiber**
Kurzrufnummern	Schlüssel Kc(Ciphering Key)
Festrufnummern	Service Provider Name
Gruppen	Bevorzugte Netze
zuletzt gewählte Rufnummer	IMSI
Kurzmitteilungen (SMS)	TMSI + Ortsinformationen
...	...

Die Telefonwertkarte

Der folgende Kartentyp nach ISO 7816-2 wird typischerweise in europäischen Wertkartentelefonen verwendet. In einigen Staaten, wie z.B. in der Tschechischen Republik werden Chipkarten eingesetzt, die sich nicht nach dem ISO Standard richten. Sie besitzen 256 Bit (32 Byte) Speicher und eine andere Pinbelegung bei gleicher Chipposition.

In Österreich wird nach wie vor eine einfache Variante der Telefonkarte eingesetzt, auf der sich ein Streifen befindet, der je nach Guthaben länger oder kürzer ist.

Die Telefonwertkarte

Kartentyp:

- Speicherchipkarte (synchrone Karte)

Merkmale:

- Verwenden in Deutschland den ISO 7816-2 Standard
- Intelligentes EEPROM (104 Bit = 13 Byte)
- Drei Speicherbereiche mit speziellen Eigenschaften (ROM, PROM, EEPROM)
- Bis zu 20.480 Zählereinheiten
- Integrierte Sicherheitsfunktionen
- Mindestens 10^4 Schreib-/Löschzyklen
- Datenerhalt länger als 10 Jahre

Die Telefonwertkarte

Speicherbelegung:

Speicherbaustein	Byte	Funktion
ROM	Byte 1, nibble 1	Funktion unbekannt
	Byte 1, nibble 2	Chip Hersteller
	Byte 2	Gültigkeitsland
	Byte 3	Funktion unbekannt
PROM	Byte 4, nibble 1	Kartenhersteller 1. Stelle der Seriennummer
	Byte 4, nibble 2	evtl. Gültigkeitsbereich
	Byte 5, nibble 1	Originalbetrag
	Byte 5, nibble 2	letzte Stelle des Herausgabejahres 2. Stelle der Seriennummer
	Byte 6, nibble 1	Herausgabemonat 3., 4. Stelle der Seriennummer
	Byte 6, nibble 2	9. Stelle der Seriennummer
	Byte 7, nibble 1	8. Stelle der Seriennummer
	Byte 7, nibble 2	7. Stelle der Seriennummer
	Byte 8, nibble 1	6. Stelle der Seriennummer
	Byte 8, nibble 2	5. Stelle der Seriennummer
EEPROM	Bit 65	”write enable bit”
	Byte 9	Betragsfeld $x * 8^4$
	Byte 10	Betragsfeld $x * 8^3$
	Byte 11	Betragsfeld $x * 8^2$
	Byte 12	Betragsfeld $x * 8^1$
	Byte 13	Betragsfeld $x * 8^0$

Die Telefonwertkarte

Anbindung des Kartenterminals:

- Das Terminal ist über eine Standleitung ständig mit der EDV der Post verbunden, beim Einschub einer Karte werden Werte wie Takt, Übertragungsprotokolle usw. eingestellt.
- Pro Einheit wird der zugehörige Preis mittels eines Löschbefehls vom Chip der Karte abgezogen und der Prozessor im Telefon (normalerweise 8031-er mit 10 MHz Taktrate) liest den Gebührenstand der Karte erneut und unterbricht bei Ablauf die Verbindung.
- Von den Karten wird üblicherweise Geld abgezogen, keine Einheiten.
- Telefon misst ständig den Gebührenstand und warnt den Benutzer rechtzeitig. Per Tastendruck kann die restliche Gebühr ins Telefon übertragen werden, um eine neue Karte einzuschieben.

Die Telefonwertkarte

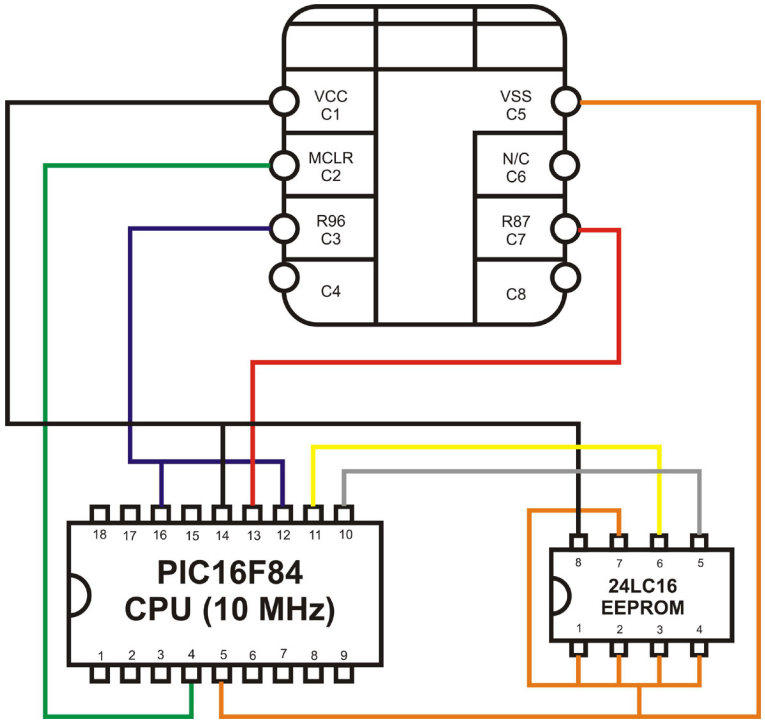
Sicherheit:

- Es ist nicht möglich, Guthaben zu addieren, es kann nur abgezogen werden.
- Das Terminal überprüft, ob der Betrag auf der Karte den Originalbetrag übersteigt.
- Alle unterschiedlichen Konfigurationsmöglichkeiten von Telefonkarten sind bekannt und werden überprüft.
- Die einzelnen Speicherbereiche werden getestet, genauso wie die überschreibung des ROMs.
- Gibt einer dieser Tests einen Fehler zurück, wird die Karte nicht angenommen.

Die Krankenschein-Karte

In Österreich soll 2003 der Krankenschein gegen eine Chipkarte ausgetauscht werden, auf dem sich Daten zu Krankenversicherten befinden werden.

In Deutschland gibt es schon seit Ende 1994 die Krankenversicherten Card nach ISO Standard 7816-2. Auf ihr befinden sich Name, Anschrift, Geburtstag und Angaben zur Versicherung des Versicherten.



Die Krankenschein-Karte

Kartentyp:

- Speicherchipkarte (synchrone Karte)

Merkmale:

- EEPROM mit 256 Byte
- Byteweise adressierbar
- Irreversibler, für die ersten 32 Byte einzeln aktivierbarer Schreibschutz
- mindestens 10^4 Schreibzyklen
- Datenerhalt länger als 10 Jahre

Die Krankenschein-Karte

Datenbereich (020h-0FFh):

Feldtag	Länge	Feldname	Optional
0x80	2-28	Krankenkassenname	nein
0x81	7	Krankenkassennummer	nein
0x8F	5	Versichertenkarten-Nr	ja
0x82	6-12	Versichertennummer	nein
0x83	1/4	Versichertenstatus	nein
0x90	1-3	Statusergänzung	ja
0x84	3-15	Titel	ja
0x85	2-28	Vorname	ja
0x86	1-15	Namenszusatz	ja
0x87	2-28	Familienname	nein
0x88	8	Geburtsdatum	nein
0x89	1-28	Straßenname	ja
0x8A	1-3	Wohnsitzländercode	ja
0x8B	4-7	Postleitzahl	nein
0x8C	2-23	Ortsname	nein
0x8D	4	Gültigkeitsdatum	ja
0x8E	1	Prüfsumme	nein

Die Krankenschein-Karte

Kartentyp:

- Speicherchipkarte (synchrone Karte)

Merkmale:

- EEPROM mit 256 Byte
- Byteweise adressierbar
- Irreversibler, für die ersten 32 Byte einzeln aktivierbarer Schreibschutz
- mindestens 10^4 Schreibzyklen
- Datenerhalt länger als 10 Jahre

Die Krankenschein-Karte

Sicherheit:

- Es werden keine medizinischen Daten auf der Karte gespeichert - sie ist nur mit Daten zu der Person bespeichert.
- Die Daten werden nur ausgegeben, wenn der Benutzer (Arzt) eine Schlüsselkarte besitzt.
- Bei Verlust der Karte kann diese sofort gesperrt werden und bei keinem Terminal mehr zum Einsatz kommen.

Zukunft:

- Schlüsselfunktion für Zugang zu zentral gespeicherten Gesundheitsdaten.
- Integration von Apotheken (Rezepte).

Weitere Verwendungsmöglichkeiten

- Geldkarte (EC-Card, Kreditkarte)
- Türpasskarte
- Pay-TV Karte
- Student Card (ersetzt Studentenausweis)
- Chipkarte statt Schlüssel (Mercedes Benz)
- noch viele weitere ...