# Smart Cards

Christian Koch
ckoch@et.htwk-leipzig.de

31. Mai 2000

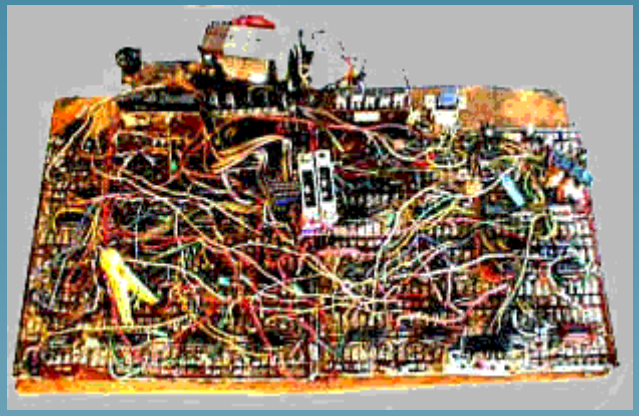
# Überblick

1. Historie
2. Einsatzgebiete
3. Aufbau
4. Protokolle
5. Angriffe
6. Vorteile – Nachteile
7. Literatur

# Historie

**1973** Roland Moreno, französischer Wissenschaftsjournalist und Autodidakt, gründet die Firma Innovatron

**Januar 1974** Moreno erhält Patent für ein „System zur Speicherung von Daten in einem unabhängigen, tragbaren Gegenstand“



**März 1974** Moreno führt französischen Bankiers Prototyp vor

**1978** erster Feldversuch mit Chipkarten bei französischen Banken

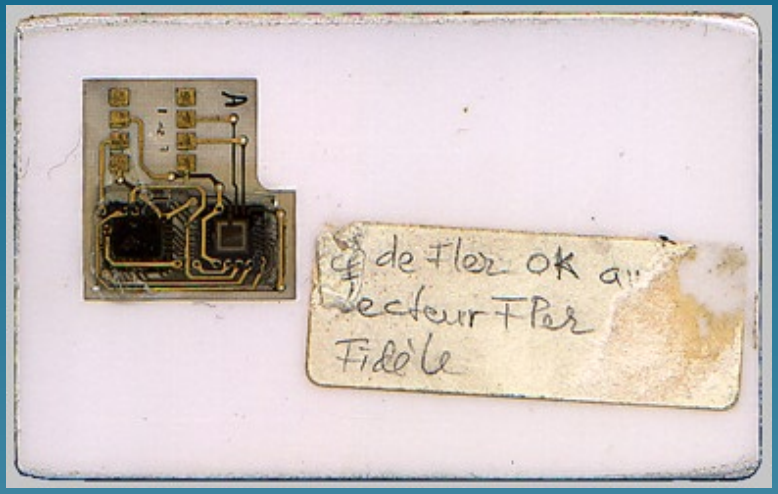
**1985** Standardisierung der physikalischen Eigenschaften von Identifikationskarten (ISO 7810), erste Prozessorchipkarte von Thomson/Bull

**1986** AT&T setzt kontaktlose Chipkarte für Kartentelefone ein

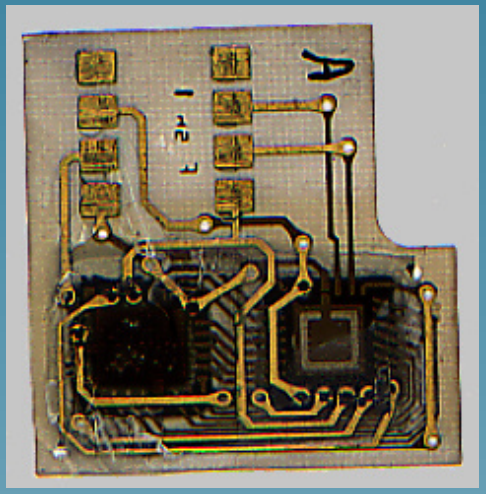
**1987** Standardisierung von Identifikationskarten mit integrierter Schaltung (ISO 7816)

**1991** erste Massenanwendung von Prozessorchipkarten im D-Netz der Deutschen Bundespost

**1993** Einführung der Krankenversichertenkarte in Deutschland




Testkarte der Firma Philips aus dem Jahr 1980



Detail der obigen Karte, Kontaktflächen oben, Mikroprozessor und Speicherschaltkreis im unteren Teil


eine der ersten einsetzbaren Speicherkarte im sog. ID-1-Format

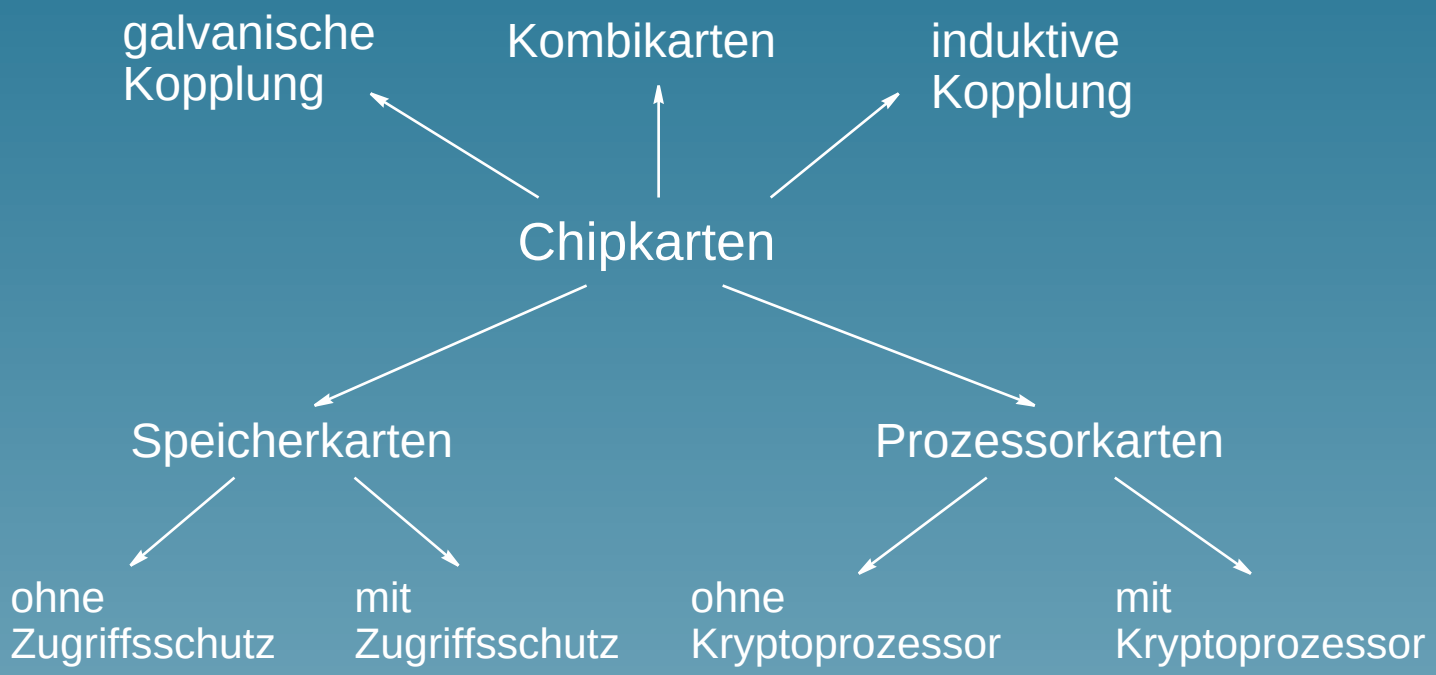

Smart Card zur Identifizierung Herzschrittmacher tragender Personen

# Einsatzgebiete

- Guthaben-Karten, z. B. Telefonkarte, GeldKarte, Ticket
- Authentifizierung, z. B. Internet-Banking, Mobiltelefonie, Zugangskontrolle, Stechkarte
- Informationsspeicher, z. B. Krankenversichertenkarte, Aufbewahrung kryptographischer Schlüssel (Signaturgesetz)
- Chiffrierung symmetrischer Schlüssel mit asymmetrischem Verfahren

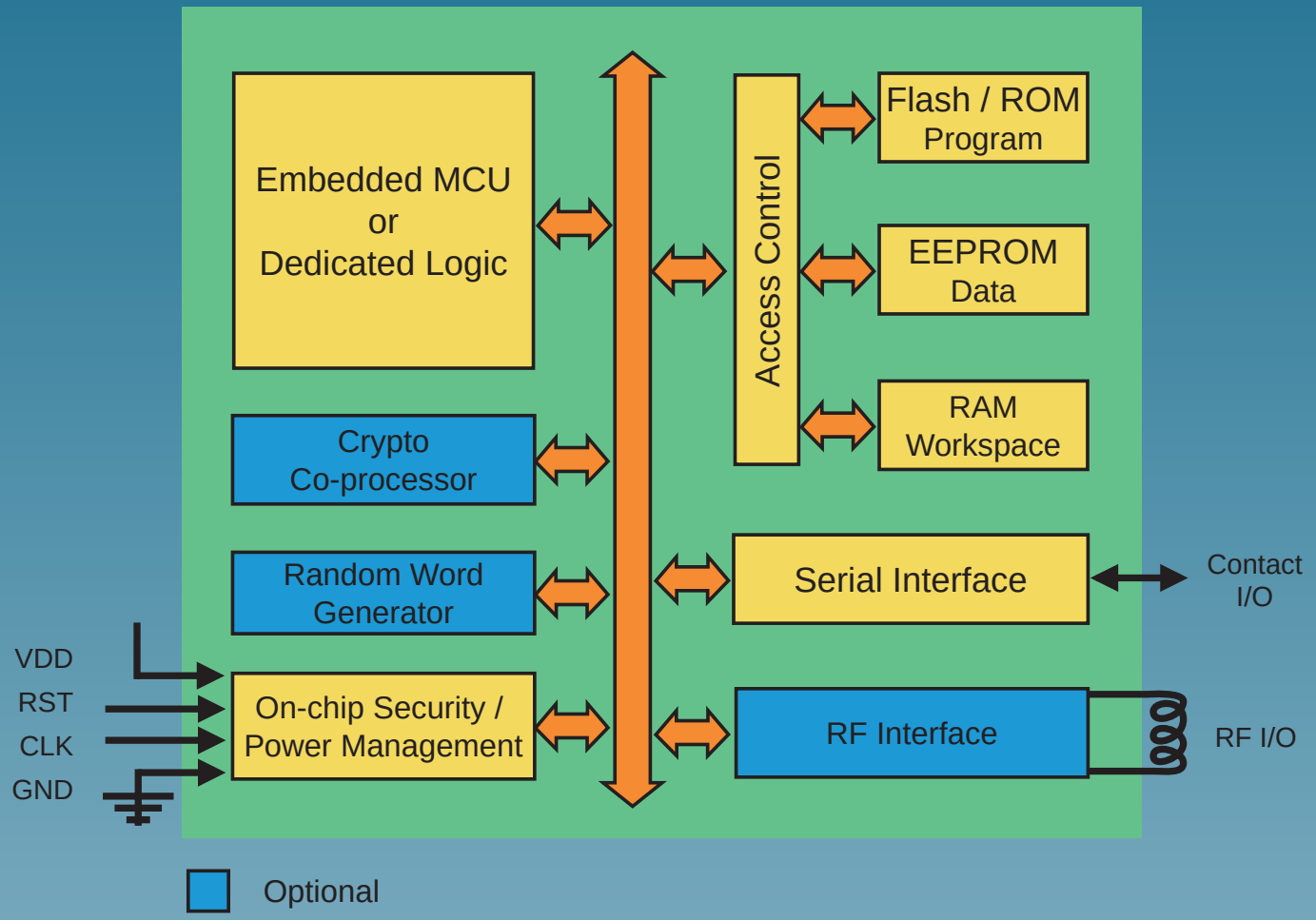
# Klassifikation

Die folgende Abbildung stellt eine mögliche Einteilung von Chipkarten dar.




Zu den Speicherkarten gehören die Telefonkarte und die Krankenversichertenkarte. Die GeldKarte ist eine Prozessorkarte.

# Schematischer Aufbau



Typische Eigenschaften einer Prozessorkarte sind

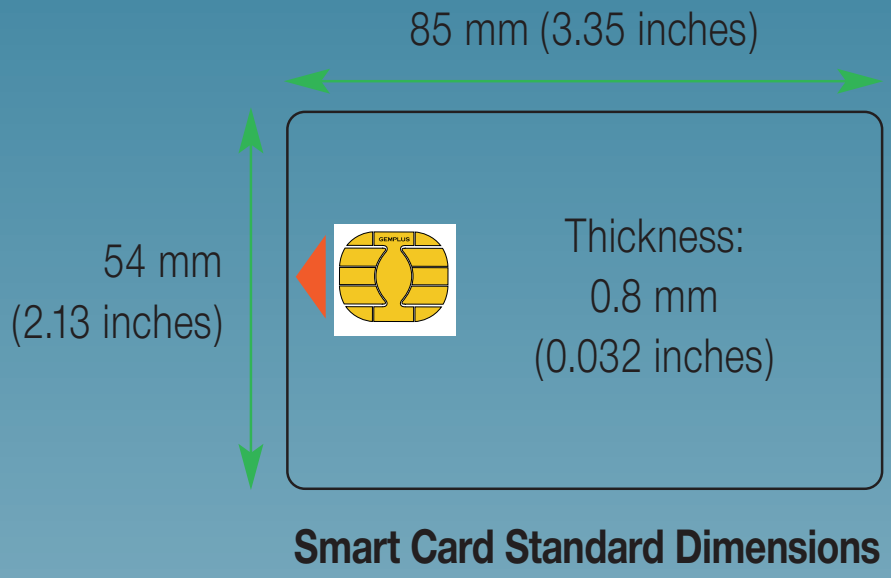
- 8 bit-CPU
- 16 kBytes ROM, 4 kBytes EEPROM, 256 bytes RAM
- Größenverhältnis der Speicherzellen:

  RAM = 4x EEPROM = 16x ROM
- Takt: 4 MHz
- Preis: 10 bis 50 DM, bei Karten mit Kryptoprozessor bis 100 DM

# ISO 7816-1

ISO 7816-1 beschreibt physikalische Eigenschaften von Chipkarten

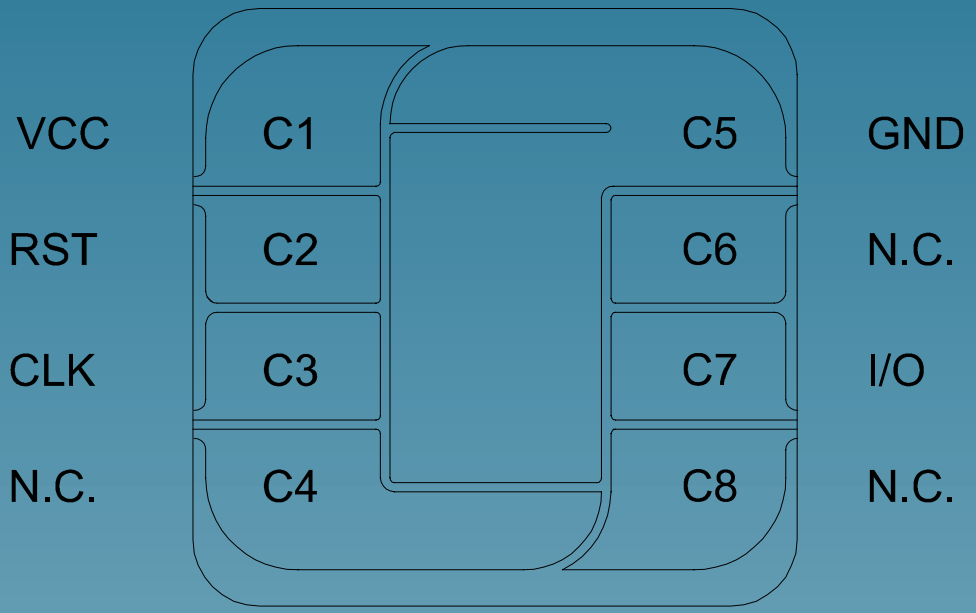
- Abmessungen und Lage evtl. vorhandener Prägezeichen und Magnetstreifen
- Material: Temperaturbeständigkeit, Biegefestigkeit (Chipfläche <30 $mm^2$)




**Smart Card Standard Dimensions**

# ISO 7816-2

ISO 7816-2 beschreibt Lage der elektrischen Kontakte



# ISO 7816-3

ISO 7816-3 beschreibt elektrische Signale an den Kontakten

**VCC** Betriebsspannungszufuhr, typ. 5 V, 10 mA, optionale Nutzung durch die Karte

**RST** Rücksetzeingang

**CLK** Takteingang, optionale Nutzung durch die Karte

**I/O** serieller Datenein- oder -ausgang (halbduplex, 9600 bps)

**GND** Bezugspotential Masse

Der Kontakt C6 diente bei älteren Karten der Zuführung der Programmierspannung VPP. Bei aktuellen Karten wird diese Spannung aus der Betriebsspannung mit Hilfe einer Ladungspumpe erzeugt.

ISO 7816-3 definiert außerdem die Übertragungsprotokolle der Bitübertragungs- und Sicherungsschicht.

1. Karte wird durch das Terminal getaktet

2. Karte meldet sich über I/O-Kontakt mit einer „answer to reset“ (ATR)

3. Terminal wertet die Antwort aus
   - snychrone oder asynchrone Übertragung
   - zeichen- oder blockorientiertes Protokoll
   - Taktzeiten des Protokolls
   - Programmierspannung und -strom (nur noch selten genutzt)

4. Daten sind je nach Protokoll durch Paritätsbit bzw. CRC gesichert

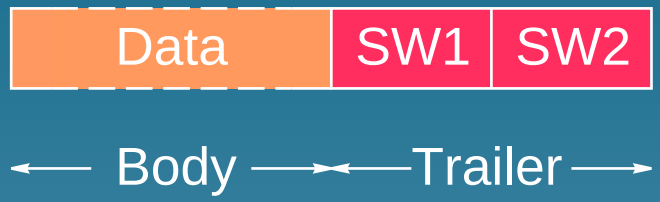
# ISO 7816-4

Aufbau einer Command Application Protocol Data Unit (C-APDU)


**Header:** zwingend; CLA – class byte; INS – instruction; P1, P2 – Parameter des Befehls

**Body:** Format bestimmt durch INS; Lc – Länge der Daten; Data – Daten variabler Länge; Le – erwartete Länge der Daten in Antwort

# Aufbau einer Response Application Protocol Data Unit (R-APDU)




**Body:** optional, je nach INS; Data – Daten variabler Länge

**Trailer:** zwingend; SW1, SW2 – Statusinformation

Bei fehlerfreier Abarbeitung des Befehls wird als Status 0x9000 zurückgegeben, anderenfalls ein standardisierter Fehlerkode.

- Daten in Dateisystem hierarchisch geordnet

  **MF** master file, Wurzel des Dateisystems, FID: 0x3F00
  **DF** dedicated file, Verzeichnis
  **EF** elementary file, Anwendungsdaten

- Dateibezeichner: 16 bit file identifier (FID), max. 16 bytes Dateiname, Anwendungsbezeichner (AID)

- AID setzt sich aus 5 bytes registered application provider ID (RID) und max. 11 bytes proprietary application identifier extension (PIX) zusammen

Eine evtl. nötige Authentifizierung für den Zugriff auf eine Datei erfolgt mittels einer PIN.

ISO 7816-7 sieht eine Verschlüsselung der Daten zwischen Karte und Terminal vor.

1. Select File

```
CLA INS P1 P2 Lc Path
00  A4  00 00 04 3F 00 A0 04

File Header                                          SW1 SW2
63 0C 00 20 A0 04 00 00 03 3F FF C3 01 00 90  00
```

2. Read Binary

```
CLA INS P1 P2 Le
00  B0  00 00 09

Data                          SW1 SW2
53 63 68 75 6C 7A 65 00 00 90 00
S  c  h  u  l  z  e
```

# Interoperabilität auf Anwendungsebene

Es existieren verschiedene Standardisierungsbemühungen, um mit den Karten auf Anwendungsebene zu kommunizieren. Dazu dienen APIs auf PC-Seite und Betriebssysteme auf der Kartenseite.

**APIs:** CT-API, PC/SC, OpenCard Framework, Cryptoki

**Betriebssyteme:** MULTOS, Card OS, JavaCard, MultiFunction Card, Starcos

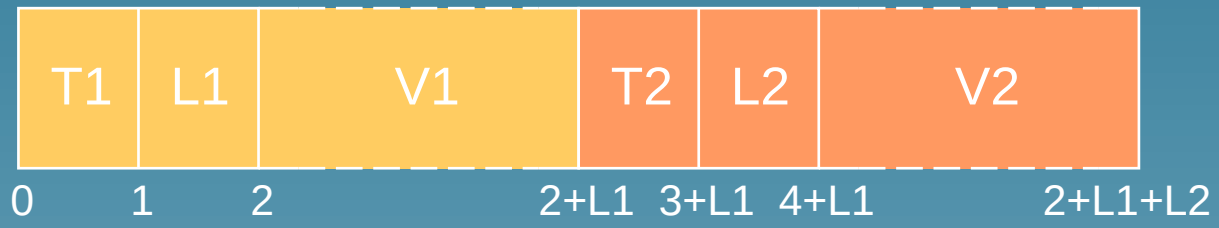
Die CT-API kann ISO-Befehle für Prozessorkarten auch in die Protokolle für Speicherkarten umsetzen. Ein Challenge-Response-Protokoll kann die Authentizität des Terminals und der Karte gewährleisten.

# Krankenversichertenkarte

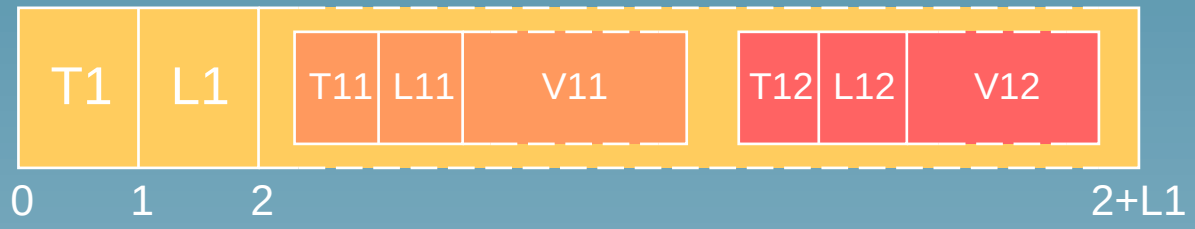
- Karte sollte billig sein → nur einfache Speicherkarte ohne Sicherheitslogik
- Speicherchip ST14C02 (2 kBit) der Firma SGS-Thomson
- Ansteuerung gemäß $I^2C$-Protokoll der Firma Philips
- Karte läßt sich über wahlfreien Zugriff beliebig lesen und beschreiben
- Datenstruktur gemäß Basic Encoding Rules (BER) für Abstract Syntax Notation One (ASN.1), ISO 8825

# Basic Encoding Rules

- dient der Kodierung von Daten mittels des Tag-Length-Value-Formats (TLV)
- T kennzeichnet Daten, L gibt Länge der Daten V an
- sechstes Bit von T1 = 0 → einfache Daten




- sechstes Bit von T1 = 1 → Datenstruktur



# Telefonkarte

- da Shutter an Kartentelefonen überlistet werden können, setzt Telekom den SLE4433 mit Authentifizierung ein
- proprietäres Übertragungsprotokoll
- zwei Authentifizierungsschlüssel der Länge 48 Bit
- Karte enthält fünfstelligen Oktalzähler, der nur abwärts zählt
- in höchster Stelle sechs Bits reserviert:

$$2 \cdot 8^4 + 8 \cdot 8^3 + 8 \cdot 8^2 + 8 \cdot 8^1 + 8 \cdot 8 = 12\,872 \text{ Zählereinheiten}$$

- 20 Pfennige pro Gebühreneinheit entsprechen 20 Zählereinheiten

# Global System for Mobile communications

- kurz: GSM, CEN prETS 300608
- Subscriber Identity Module (SIM) ist als Prozessorkarte ausgeführt
- enthält u. a. 128 bit-Schlüssel $K_\mathrm{i}$, der zusammen mit Algorithmus A3 der Authentifizierung gegenüber Basisstation und mit Algorithmus A8 der Berechnung des Schlüssels $K_\mathrm{c}$ dient
- 64 bit-Schlüssel $K_\mathrm{c}$ dient symmetrischer Chiffrierung
- Dateizugriffskontrolle über PINs: $K_\mathrm{i}$, Telefonbuch, Benutzerdaten
- Einsatz der SIM auch im Festnetz denkbar: Anwender jederzeit über eine einzige Telefonnummer erreichbar

# GeldKarte

- offener Standard vom Zentralen Kreditausschuß (ZKA)
- basiert auf der IBM Multifunction Card und einem speziellen Betriebssystem
- Geldbörse und elektronischer Scheck in einer Karte
- Geldbörse kann an Terminal geladen werden, keine PIN bei Benutzung der Geldbörse erforderlich
- Online-Transaktion anonym, Offline-Transaktion als gedeckter, elektronischer Scheck
- Händler muß 0.3% des Transaktionsbetrages, aber mind. 0.02 DM an Bank abführen

# Homebanking Computer Interface

- HBCI will zunehmender Kommerzialisierung des Internet Rechnung tragen und PIN/TAN-Verfahren auf Basis von BTX durch intelligentere Verfahren ablösen
- Authentifizierung und Verschlüsselung der Übertragung, TANs durch Sequenzzähler auf Chipkarte abgelöst
- bis jetzt: nur symmetrische kryptographische Verfahren auf Chipkarte, RSA als Computersoftware; Ziel: RSA in Hardware, so daß Schlüssel die Karte nie verlassen und HBCI multibankfähig wird
- Aufbewahrung der Schlüssel in GeldKarte möglich

# Angriffe auf Terminal

- Anzapfen der Verbindung zwischen Chipkarte und Terminal $\rightarrow$ Verschlüsselung
- Manipulation des Datenstromes $\rightarrow$ Signatur
- Man-in-the-middle-Angriff $\rightarrow$ Authentifizierung
- Replay-Attacke $\rightarrow$ Zeitstempel, TAN

# Angriffe auf Karte

- Fälschen (Kopieren) einer Chipkarte → Karte sollte nur nach Eingabe einer besonderen PIN beschrieben werden können
- Öffnen des Chips und Anbringen von Mikronadeln um Daten auszulesen → Sandwich-Struktur der Leiterbahnen
- geschickte Manipulation der Betriebsspannung → brown-out-Schutz in der Karte
- Terminal zeigt Betrag x an, bucht aber Betrag y ab → Superchipkarten mit eingebautem Display und Tastatur
- Terminal protokolliert PIN-Eingaben und speichert diese zusammen mit dem Namen des Karteninhabers ab, dann Mißbrauch der Karte möglich

# Vorteile

- handlich, hohe Informationsdichte
- lange Lebensdauer, keine Verbrauchsmaterialien
- kann viele Sicherheitsprobleme lösen
- standardisiert
- multifunktionale Nutzung möglich
- hohe Datensicherheit
- schnelle Identifikation durch PIN

# Nachteile

- Datenschutz, evtl. Speicherung unnötiger Daten
- Kartenterminal notwendig, kein direktes Lesen der Daten durch menschliche Sinne
- Abhängigkeit von der Karte, Reduzierung der Persönlichkeit auf Dateninhalt der Karte
- Anwender muß dem Betriebssystem der Karte und der Ausstellautorität vertrauen
- derzeit für jede Anwendung dedizierte Karte
- Realitätsverlust, Abstraktion von Transaktionen

# Ausblick

Kontaktlose Karten werden die galvanisch gekoppelten Karten verdrängen.

Die PIN wird durch biometrische Verfahren ersetzt werden.

Jede Person wird im Idealfall nur noch eine Karte besitzen, in die nach Bedarf neue Anwendungen hineingeladen werden. Auch eine Speicherung von Benutzerprofilen ist denkbar.

Das asymmetrische Schlüsselpaar sollte von jedem Anwender selber generiert und in die Karte geladen werden.

Was geschieht, wenn die Karte während eines Transaktionsvorgangs die Verbindung zum Terminal verliert?

# Literatur


- Beutelspacher: Chipkarten als Sicherheitswerkzeug. 1991, Springer-Verlag, Berlin.
- Mrkor: Kartenspiele. c't 08/2000, Heise-Verlag, Hannover.
- Schütt: Chipkarten. 1996, Oldenbourg-Verlag, München.
- Bo Lavare's Smartcard Security Page
- GMD Darmstadt - Smart Cards
- GSHO
- Identification cards and related devices

- LogoSec
- Smart Card Industry Association
- TOWITOKO

Rinaldo Di Giorgio: „As with any new technology, there are so many standards for smart cards that you find yourself discouraged and overwhelmed.“

Ich bedanke mich für die Aufmerksamkeit.