Chipkarten im praktischen Einsatz:
Einführung, Auswahl und Sicherheit

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.

Chipkartentypen - 'Intelligenz'

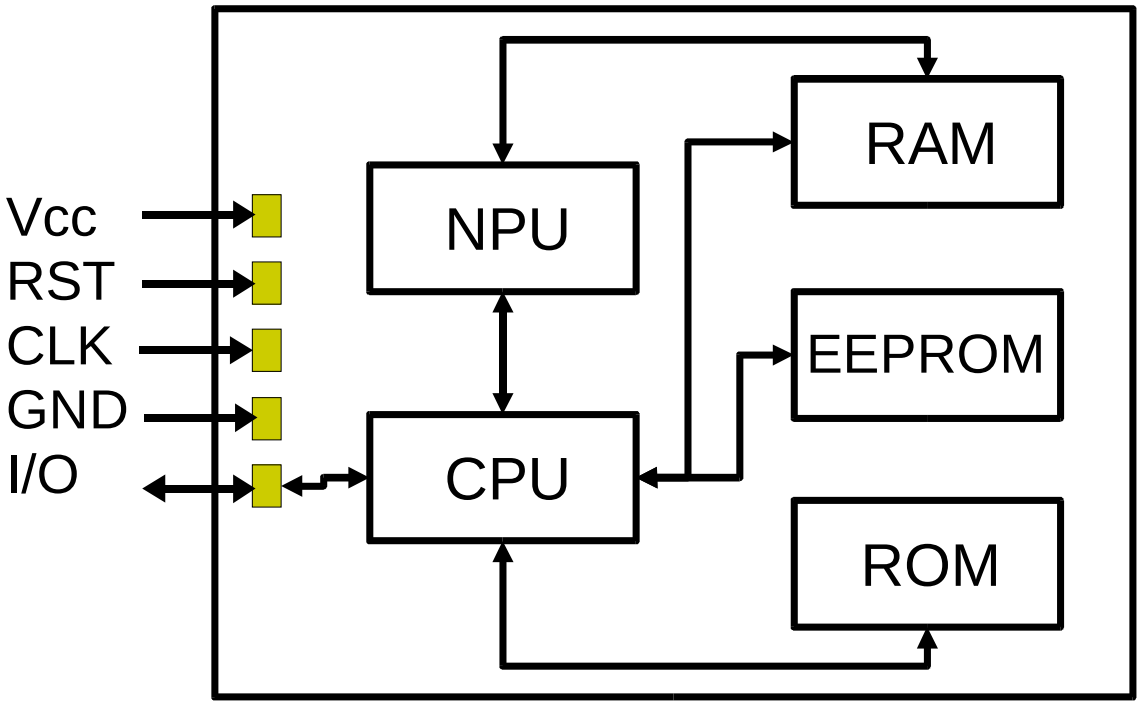
- Seriennummer (immer)
- Speicherkarte (ein paar Bits bis 16kB EEPROM)
- Speicherkarte mit Sicherheitslogik (Zähler, PIN)
- Mikroprozessorkarte

Chipkartentypen - Interface

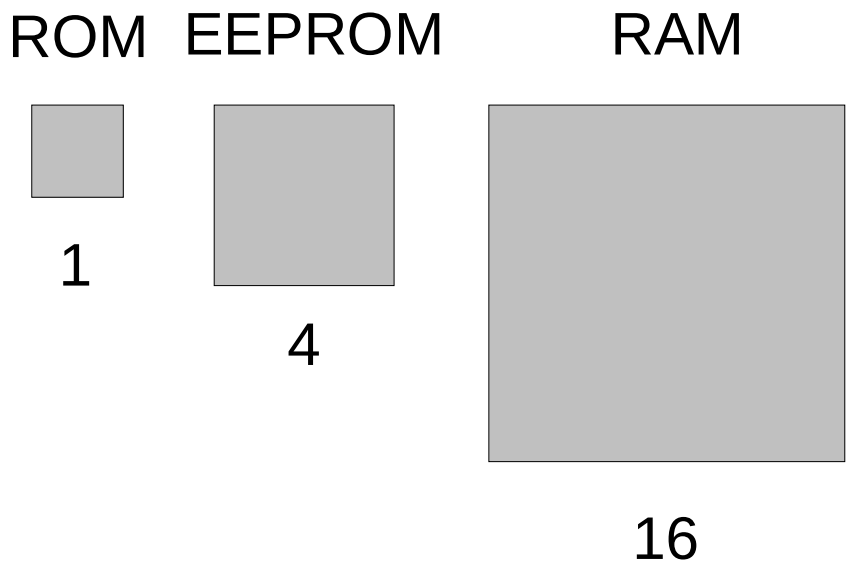
- Kontakte
  - Speicherkarten: I^2C, 2-Wire, 3-Wire, ...
  - Prozessorkarten: T=0, T=1 (ISO/IEC 7816-3), USB
- Funk (contactless)
  - Kapazitiv
  - Niederfrequenz (z.B. 115kHz, älteste Technik)
    - ISO-Standards, Legic, ...
  - Hochfrequenz (z.B. 13.5MHz)
    - ISO/IEC 14443 (Prozessork.), MIFARE, ...

Technik - Prozessorkarten

Chiparchitektur



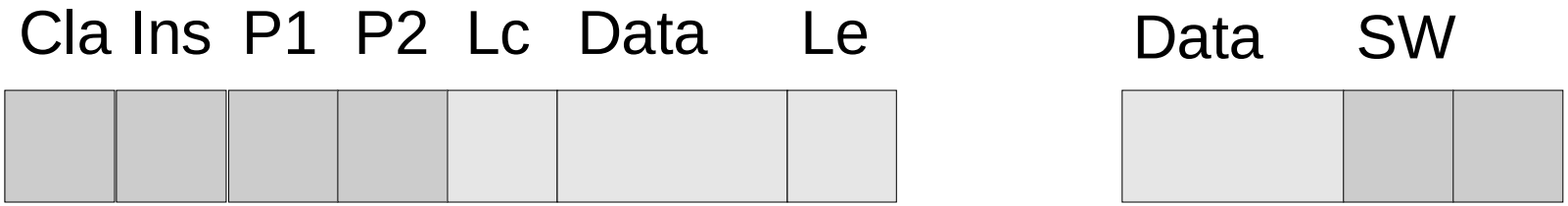
Platzbedarf des Speichers



ungefähres Größenverhältnis

Typische Größen: ROM 16k-256k Bytes, EEPROM 4k-72k Bytes, RAM 256-8192 Bytes

Befehlsaufbau



C-APDU R-APDU

Cla: Class, Ins: Instruction, P1/P2: Parameter,
Lc/Le: Length, SW: Status Word

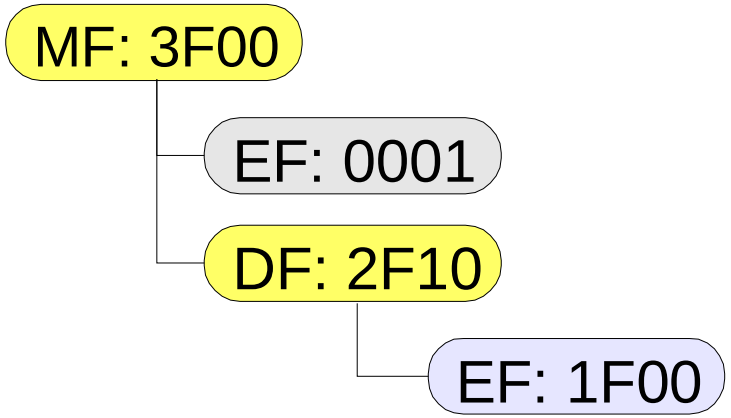
Case 1: Keine Daten
Case 2: Daten empfangen
Case 3: Daten senden
Case 4: Daten senden und empfangen

Karte nach ISO/IEC 7816 Teil 4-9

Karte mit Dateisystem und Kommandos für:

- Dateien anwählen, löschen, lesen, schreiben
- PIN verifizieren, ändern
- Administrationsschlüssel kryptographisch verifizieren
- Kryptographische Operationen durchführen
- zusätzlich Zähler (CEN 726), etc.
- Verschlüsselung und Sicherung der Befehle

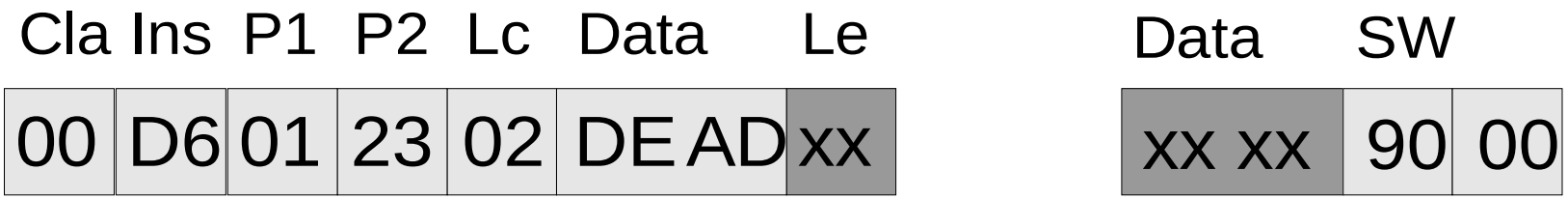
Dateisystem



MF: Master File
DF: Dedicated File
EF: Elementary File

- Verzeichnisbäume möglich (Verzeichnis: Dedicated File)
- Dateinamen (FID) bestehen aus zwei Bytes
- Wurzelverzeichnis hat immer die FID 0x3F00

Beispiel eines Befehls: Update Binary



C-APDU

R-APDU

Ins: Kommando ist Update Binary
P1/P2: Enthält die Schreibposition 0x0123
Lc: 2 Datenbytes folgen
SW: Befehl erfolgreich durchgeführt

ISO/IEC 7816 - Probleme

- Nicht alle Befehle implementiert
- Nicht alle Optionen implementiert
- Befehle nicht standardkonform implementiert (besonders alte Systeme)
- Befehle, die nicht im Standard implementiert sind
- Standard lückenhaft, z.B. Zugriffsrechte

'PKI'-Karte

- Koprozessor für die Verarbeitung von langen Zahlen (Big Integers)
- Ermöglicht Berechnung von Public Key Algorithmen (RSA/DSA) in kurzer Zeit
- 1024bit-RSA-Signatur inkl. Overhead ca. 1 Sekunde
- ECC-Koprozessoren im Kommen

Beispiel: Telesec TCOS 2

- Hält sich an ISO7816-4
- Kommandos können sowohl mit einem MAC gesichert als auch verschlüsselt zur Karte übertragen werden
- Daten sind TLV-kodiert (Tag/Length/Value)
- kryptographische Algorithmen: RSA (mit Koprozessor), DES, 3DES, IDEA, MD5, SHA-1
- erste SigG-konforme Karte

JavaCard

- kleinste JavaVM speziell entwickelt für Chipkarten
- Ziele:
  - Erweiterbar durch Kartenherausgeber (issuer)
  - Erweiterbar auch noch beim Kartenhalter (cardholder)
  - Erweiterungen können sich auch absichtlich nicht stören

JavaCard - Nachteile

- Langsamere Ausführungsgeschwindigkeit (32bit-Prozessoren auf Chipkarten, z.B. ARM, MIPS)
- Java-Untermenge (keine Gleitkommazahlen und Threads, selten dynamische Speicherverwaltung)
- Teuer (Java-Lizenzen, Hardware, EEPROM-Bedaf)
- Keine Grundfunktionalität (kein Dateisystem)

Beispiel: IBM JCOP

- schnellste JavaCard
- Entsprechend JavaCard 2.1 keine ISO7816-4/8/9-Befehle
- Verschlüsselte und/oder signierte Installation von Applets (GlobalPlatform)
- Unterstützt kryptographische Algorithmen (RSA, DES, 3DES, SHA-1)

Anwendungen

Loyalty

- 'Der Beck-Karte', Payback
- billige Karten (Barcode, Magnetstreifen, Speicherkarten) oder als Zusatzfunktion auf Prozessorkarten (z.B. GeldKarte)
- Ziel:
  - Kunde kauft weniger bei der Konkurenz ein
  - Sammeln von verkaufbaren Kundendaten

Transport und Verkehr

- kontaktlose Chipkarten für den öffentlichen Nahverkehr
  - Schaden durch gefälschte Papiertickets mit Magnetstreifen in Pariser Metro
  - Verbreitung bisher hauptsächlich in Asien
- kontaktlose Chipkarten (und Uhren, Handschuhe, etc.) für Skilifte
- Ziel: billiges Papierticket mit Chip (momentan iCode-Ticket für 0.20 EUR)

spezielle Bezahlfunktionen

- Telefonkarte (Speicherkarte mit Zähler)
- Kantinen und Automaten
  - FAU-Mensa: MIFARE
  - Solarium
  - Parkautomaten (Paris)
  - CineCard (Schweiz)
  - Kopierer

MIFARE

- kontaktlose Speicherkarte mit zusätzlicher fester Sicherheitsfunktionalität und Zähler
- Frequenz: 13.56 MHz
- Reichweite: 10 cm
- Speicher: bis 4 kB in Sektoren unterteilt
- 48bit-Schlüssel mit geheimem Algorithmus
- Preis: etwa 0.50 EUR für Chip

allgemeine Bezahlfunktionen

- GeldKarte
  - Strategische Kriminalitätsanalyse im BKA
- EMV
  - Kreditkarte (MasterCard, Visa) mit Chip
  - Karte erstellt Beleg für die Bank
  - Authentifizierung der Karte -> Terminal: SDA (statisches Zertifikat), DDA (Signatur)
  - Zusätzlich nach Regeln Online-Authorisierung

GSM (UMTS)

- Größte Chipkartenanwendung
- GSM ist für Chipkarten, was Spiele für PC sind, d.h. treibt technologische Entwicklung
- Enthält Schlüssel für Nutzungsberechtigung
- Viele Zusätze: SMS, Telefonbuch, JavaCard, SIM-Toolkit, fernsteuerbar Over the air (OTA)

Einsatz am PC

- Zugangsschutz für Webinhalte
  - Britney Spears
- Signatur und Verschlüsselung von Dokumenten/e-Mails
  - S/MIME
  - OpenPGP
  - Signaturgesetz (Notarverträge)
- Unverlässige PC-Software (PC/SC)

Ausweis

- Krankenversichertenkarte (KVK)
- Zutrittskontrolle und Zeitabrechnung
- Ausweis in der US-Armee
- International Civial Aviation Organization:
  - Machine Readable Travel Document, d.h. Reisepaß, Visum
  - kontaktloser Chip im Papierdokument integriert
  - Speicherung von u.a. Name, Foto, Fingerabdrücken, Iris möglich
  - Sicherheit durch Signatur der abgelegten Daten

Sicherheit

Große Sicherheitsbandbreite

- Frei veränderbare Daten bis hin zu
- Authentifizierung mit unlesbaren Schlüsseln
- Sicherheit durch zusätzliche Vorkehrungen verbesserbar, z.B.
  - Online-Vorgänge
  - Signatur der abgelegten Daten
  - Limitierung des möglichen Schadens oder Gewinns bei Betrug

Sicherheit - Prozessorkarte

- Prozessorkarte ist Sicherheitsplatform, aber trotzdem möglichst billiges Massenprodukt
  $\Rightarrow$ Chipkarten sind nicht 100%ig sicher!
- Eine Chipkarte ist aber sehr teuer, wenn keine Fehler gemacht wurden
- Bei der Entwicklung auf Kosten/Nutzen-Verhältnis des Angreifers und auf Schadensbegrenzung achten

Angriffe

- Zerlegen der Chipkarte und Analyse mit Microskopen und ähnlichem (Uni, Chiplabor)
- Messen des Stromverbrauchs (SPA, DPA) und elektromagnetischer Abstrahlung (EMA)
- Angriffe auf das Kommunikationsprotokoll
- Beeinflussung der Karte (DFA, Fehler beim Fehlbedienungszähler)
- Angriff auf Infrastruktur (Viren auf PC)
- Angriff auf Mensch (Social Engineering)

Common Criteria (ITSEC)

- Externe Evaluierung
- Versuch Vertrauen in ein Produkt zu schaffen
- Verschiedene Sicherheitsstufen
  - EAL 1: Durchsehen der Doku
  - EAL 4 bzw. 5: Höchste verbreitete Stufe
  - EAL 7: Beweisbar sicher

Literatur

- Rankl, W.; Effing, W. *Handbuch der Chipkarten*, 4. Aufl.; Hanser, 2003.

Mahlzeit

Matthias Brüstle
<m@mbsks.franken.de>

Kommunikationsnetz Franken e.V.