Grundlagen und Anwendungsgebiete von Chipkarten

Überblick

Einleitung und Überblick

Kartenarten

Karten-Terminals

Chipkarten-Fertigung und Design von Anwendungen

Zusammenfassung

Ausblick

Kartenformate und Arten

Übliches Format: ID-1

+Telefonkarte

+Krankenversichertenkarte

Anderes Format: ID-000

+SIM im Mobiltelefon

Hochgeprägte Karten

+Abdruck der Daten ohne elektrische Energie möglich.
+Position bei Kreditkarten in ISO 7811 nachzulesen.
+in der Praxis nicht mehr üblich ohne zusätzliche Komponenten

Magnetstreifenkarten I

+Bekannteste Anwendung: Kreditkarte.
+Magnetstreifen enthält Daten.
+Magnetstreifen teilt sich in 3 Spuren.
+Spur 1 und 2 für den Lesebetrieb.
+Spur 3 für den Schreibbetrieb

Magnetstreifenkarten II

+Magnetstreifen kann ca. 1000 Bit speichern.
+Kein Schutz vor Manipulation.
+Zusätzliche Sicherheitssysteme für Praxis nötig.

Optische Speicherkarten

+Mit der CD zu vergleichen.
+Speicherung von großen Datenmengen möglich.
(4-10 MB)
+Auf die Schicht können auch Informationen aufgebracht werden, die für Menschen lesbar sind.
+Beispielanwendung: Amerikanische Einwanderungsbehörde.

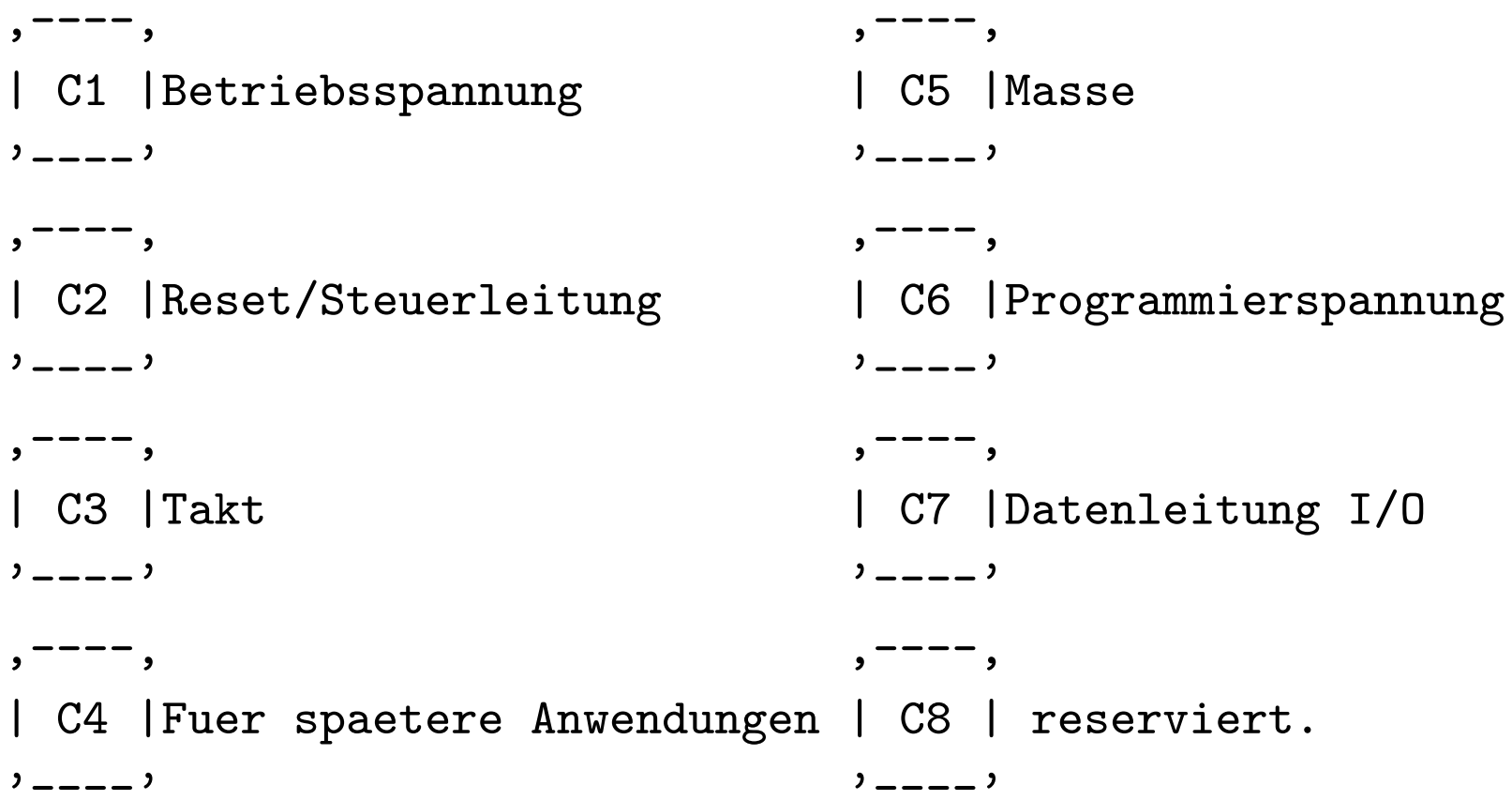
Chipkarten

+Speicherkarten
+Speicherkarten mit Sicherheitslogik
+Mikroprozessorkarten

Chipkartenvorteile

+Daten oder Algorithmen können geschützt eingesetzt werden.
+Ein kleiner Computer.

Kontakteinrichtungen der Chipkarte



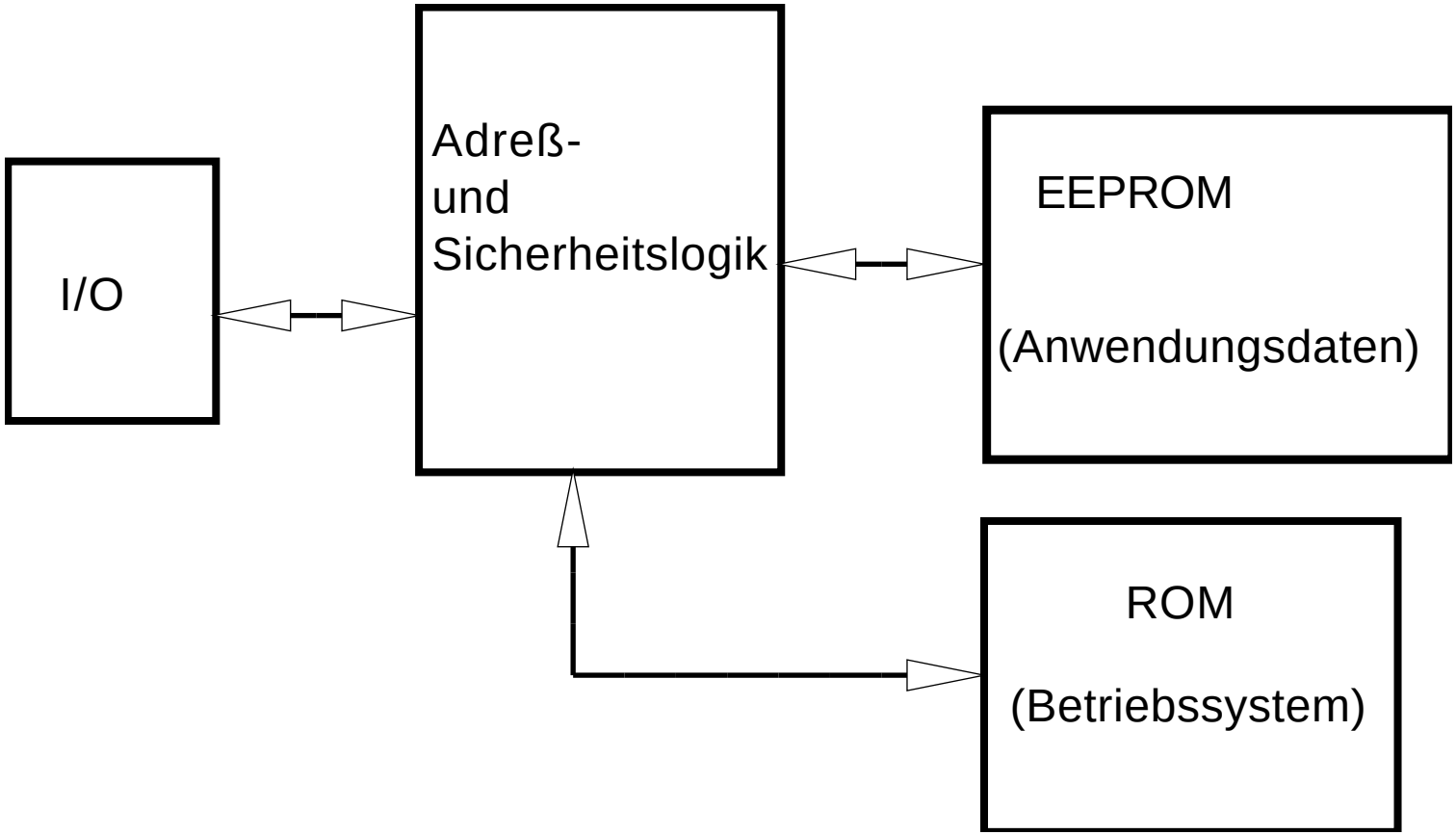
Kontaktlose Karten

+Werden extern mit Energie versorgt.
+Können teilweise auf weite Entfernung ausgelesen werden.
+Vorteile bei Handhabung.

Speicherkarte

+Krankenversichertenkarte
+Keine Sicherheitslogik
+Arbeitet im Bereich von 3-5 Volt

Speicherkarte: Aufbau



Speicherkarte: Daten auslesen

+Daten liegen in einem EF.
+Adresszähler
+Position und Länge von einem Bereich.

Telefonkarte

+Aufgabe
+Enthaltene Daten
+Eurochip SLE4436

Telefonkarte

1. Telefonzelle schickt Reset.
2. Karte schickt ATR.
3. Telefonzelle fragt alle Daten ab.
4. Telefonzelle generiert Zufallszahl und schickt diese an die Karte.
5. Telefonzelle und Karte führen einen geheimen Algorithmus aus. Eingabe sind dabei die Daten der Karte und die Zufallszahl.
6. Die Karte schickt das Ergebnis an die Telefonzelle.
7. Wenn die das Ergebnis von der Karte mit dem der Telefonzelle übereinstimmt, gibt die Telefonzelle die Leitung frei.
8. Bei einem Gebührenimpuls wird der betreffende Speicherbereich auf der Karte gelösch und die Prozedur beginnt wieder bei Punkt 3 (wobei die Telefonzelle das zu erwartende Guthaben der Karte berechnet).

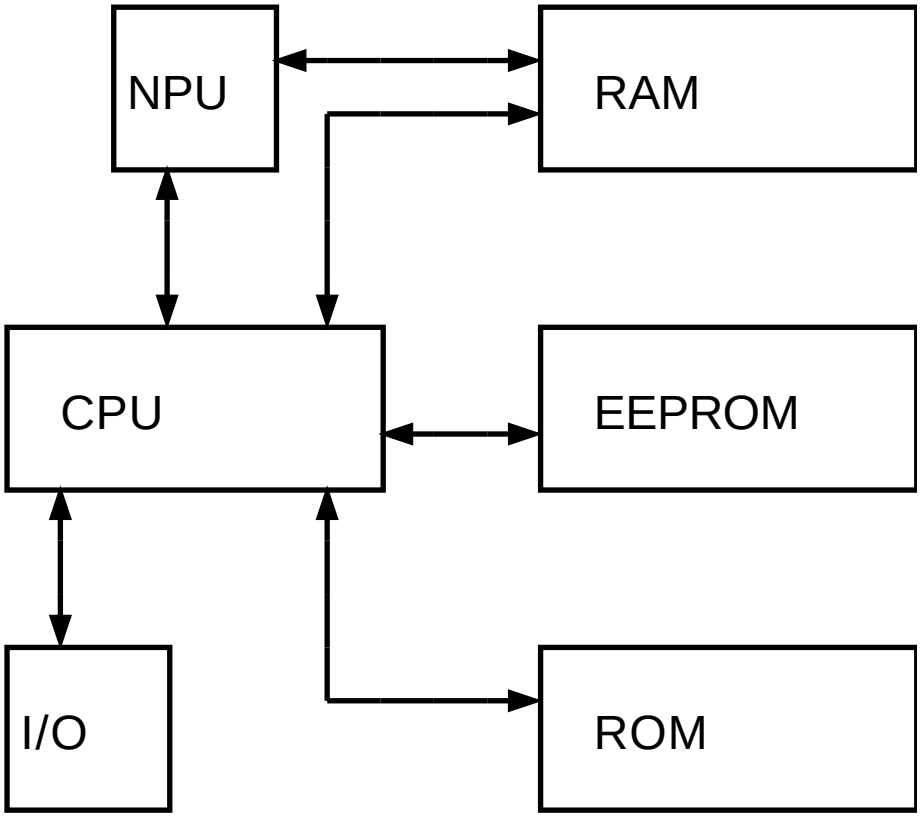
Telefonkarte

+Seriennummer nicht immer einzigartig gewesen.
+Manipulation war möglich.
+Neue Sicherheitssysteme in Telefonzellen.

Mikroprozessorkarte

+Daten können auf der Karte verarbeitet werden.
+Die verwendenten Algorithmen können geheimgehalten werden.
+Anwendungen: Geldkarte, SIM-Karte im GSM-Mobiltelefon

Aufbau der Mikroprozessorkarte



Sicherheitstechnik der Mikroprozessorkarte

+Identifizierung
+Authentisierung
+Sicherheit auf Anwendungsebene
+Sicherheit in der Hardware

Betriebssysteme für Mikroprozessorkarten

+Chipcard Operating System (COS)
+Nachladbarer Programmcode
+SmallOS (Basic)
+JavaCard (Java)

Betriebssysteme für Mikroprozessorkarten

+Kommunikation zwischen Terminal und Karte wird geregelt.
+Ablauf von Kommandos wird gesteuert.
+Verwaltung von Dateien und Zugriffsrechten.
+Verwaltung und Ausführung von kryptografischen Algorithmen.

Betriebssysteme für Mikroprozessorkarten

+I/O-Manager: Fehlerkorrektur
+Secure-Messaging-Manager: Kryptografie
+Kommandointerpreter: Befehle und Parameter aus Daten
+Logical-Channel-Manager: schaltet Zustände von Kanal
+Zustandsautomat: Prüft ob Vorgang erlaubt
+Anwendungsbefehl Modul: Befehl wird ausgeführt
+Returncode-Manager: Fehlerbehandlung
+Codeinterpreter Modul: Nachladbare Programme

Dateisystem

+Master File (MF)
+Dedicated File (DF)
+Elementary File (EF)

Datenübertragung

+Speicherkarte: synchrone Übertragung
+Mikroprozessorkarte: asynchrone Übertragung
+Protokolle in ISO 7816
+Schichtenmodel

Kommandos

+Challenge Response
+Application Protokol Data Unit (APDU)
+Beispiel: Lesen/Schreiben von Dateien

Digitale Signatur

+Auf der Karte wird der geheime Schlüssel gespeichert.
+Chipkarte signiert nur eine Prüfsumme.
+Stärkster Teil des Sicherheitskonzepts.
+Angriffsfläche kann verkleinert werden.

Terminals

+Spezialterminals
+Kontaktlose Terminals
+„Normale“ Terminals

Terminals

+Shutter
+Stromverbrauch
+Wärmeentwicklung
+Masse
+Stresstest
+Hintergrundsystem
+Problem: Toleranz für Fehler ist zwingend

Lebenszyklus einer Chipkarte

1. Herstellung von Chip und Karte
2. Kartenvorbereitung
3. Anwendungsvorbereitung
4. Kartenbenutzung
5. Ende der Kartenbenutzung

+Sicherung durch Transportcodes

Überlegungen bei einem Chipkartenprojekt

+Welche Sicherheitstechnik setze ich ein?
+Habe ich andere Sicherheitsprobleme?
+Wer haftet bei Missbrauch?
+Kann die Karte die Anwendung in annehmbarer Zeit durchführen?
+Wirtschaftlich bessere Alternativen.

Zusammenfassung

+Normale Speicherkarten sterben aus.
+„Moore's Law“

Ausblick

+Anonymität
+voll dokumentierte Chipkarte
+kommende Anwendungen