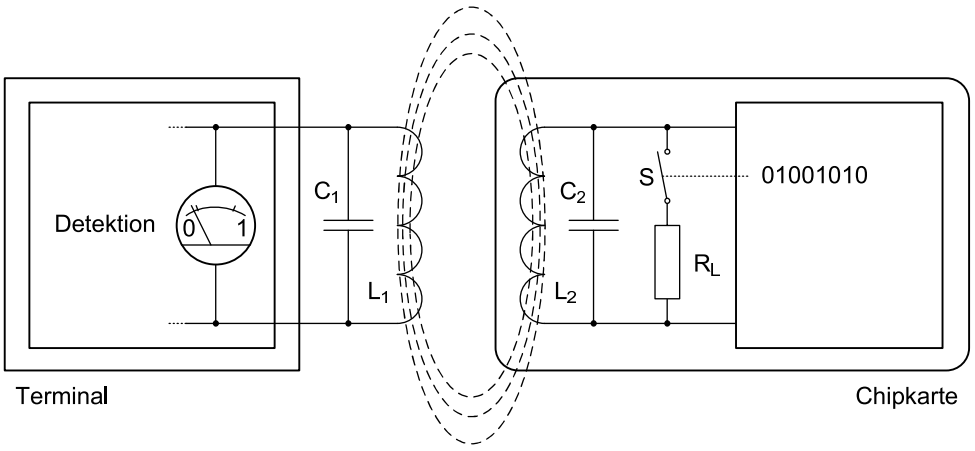

Abb. 2.11: Transformatorische Kopplung und Lastmodulation

Abbildung 2.11 zeigt das Prinzip dieser Datenübertragung: In Abhängigkeit der zu übertragenden Bits generiert die Chipkarte mittels Widerstand R_L eine höhere Last (Schalter S ist geschlossen) oder nicht (Schalter S ist offen). Auf das komplexe Zusammenspiel zwischen Amplitudentastung, Lastmodulation und Generierung der Versorgungsspannung für die Chipkarte soll hier nicht weiter eingegangen werden.

Eigenschaften kontaktloser Chipkarten

Tabelle 2.6 zeigt einige Eigenschaften der unterschiedlichen Ausprägungen von kontaktlosen Chipkarten, wie Schreib/Lesedistanz, verwendeter Frequenzbereich, Datenübertragungsrate und relevanter Standard.

Tab. 2.6: Eigenschaften kontaktloser Chipkarten

	Close Coupling	Proximity	Vicinity (Long Range)
Schreibdistanz	wenige mm	100 mm	> 20 mm
Lesedistanz	wenige mm	100 mm	1000 mm
Frequenz	4.91 MHz	13.56 MHz	135 kHz, 13.56 MHz und 2.45 GHz
Datenrate	> 100 kBit/s	100 kBit/s	wenige kBit/s
Datenübertragung	induktiv, kapazitiv	induktiv	induktiv
Standard	ISO/IEC 10536	ISO/IEC 14443	ISO/IEC 15693

2.5 Lebenszyklus

In diesem Kapitel wird der generische Lebenszyklus von Chipkarten beschrieben, der im weitesten Sinne dem ISO-Standard ISO 10202-1 entspricht. Abbildung 2.12 skizziert die unterschiedlichen Phasen im Leben einer Chipkarte.

Je nach Art der Anwendung sind unterschiedliche Phasen (vor allem Vorpersonalisierung und Personalisierung) unterschiedlich stark ausgeprägt. Werden keine kartenindividuellen (z.B. personenbezogenen) Daten auf die Chipkarte aufgebracht, so kann die Personalisierung sogar komplett entfallen.

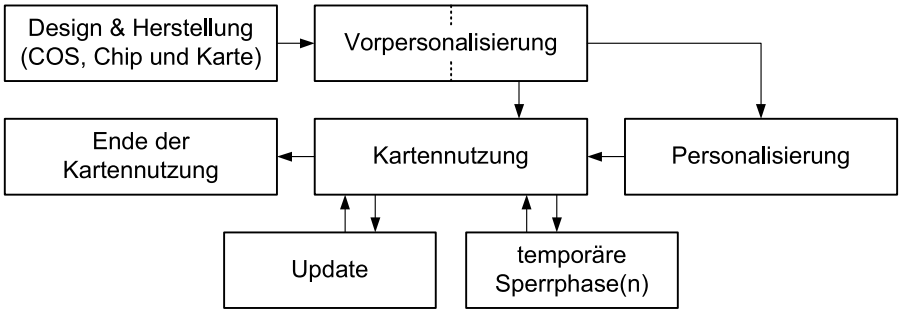

Abb. 2.12: Lebenszyklus einer Chipkarte

Lebenszyklus von Chipkarten

Es folgt nun eine Auflistung der in diesem Abschnitt beschriebenen Phasen im Leben einer Chipkarte, wobei in Klammern die involvierte(n) Instanz(en) angegeben werden:

1. Design und Herstellung (Chipkartenhersteller)
   - Erstellung des COS und der ROM-Maske, Design des Chips
   - Produktion und Zusammenführung von Kartenkörper, Chip und gegebenenfalls weiterer Module
2. Vorpersonalisierung (Chipkartenhersteller und Anwendungshersteller)
   - Elektrisches Testen der Chipkarte
   - Laden der noch fehlenden SW-Teile ("Komplettierung")
   - Initialisierung der Karte
   - Laden von Daten und Anwendungen
3. Personalisierung (Systembetreiber)
   - Individualisierung und Personalisierung
   - Ausgabe bzw. Kuvertieren und Versenden
4. Kartennutzung (Benutzer und Systembetreiber)
   - Kartennutzung in diversen Anwendungen
   - Temporäre Sperrphase
     - PIN wiederholt falsch eingegeben
     - Anwendung sperrt Karte
   - Update der Karte
     - Update von Daten und Schlüsseln
     - Nachladen von Applikationen
5. Ende der Kartennutzung (Systembetreiber)
   - Deaktivieren der Anwendungen
   - Deaktivierung, Rücknahme und Recycling der Karte

2.5.1 Design und Herstellung

Design

Die erste Phase im Leben einer Chipkarte umfasst das Design des Betriebssystems und des Mikroprozessors. Aus Abschnitt 2.2.3 wissen Sie, dass große Teile des Betriebssystems aus Platzgründen im ROM abgelegt werden. Daher ist es notwendig in dieser Phase auch die ROM-Masken (die Abbildung des Betriebssystem-Codes auf einen ROM-Speicher) zu erstellen. Zudem müssen auch die restlichen Speichermodule in den Chip integriert werden.

Produktion

Im Falle von Hybridkarten müssen eventuell noch Magnetstreifen und optische Speicherbereiche bedacht werden. Zudem muss der Chip bei kontaktlosen Chipkarten noch das Modul zur Spannungsversorgung und Kommunikation enthalten und der Kartenkörper die Antennenspule.

Test

Nach der Produktion von Kartenkörper, Chip und gegebenenfalls weiterer Module erfolgt bereits ein erster gründlicher Test des Chips und der zusätzlichen Module. Dadurch können fehlerhafte Komponenten so früh wie möglich ausgeschieden werden.

Zusammenführung

An den Test der Komponenten schließt sich deren Zusammenführung an. Abbildung 2.13 zeigt die Einbettung eines Chipmoduls in den Kartenkörper. Hier wird der Chip, der wiederum direkt auf der Kontaktfläche aufgebracht wurde, in eine Aussparung des Kartenkörpers geklebt. Die Verbindung des Chips mit den einzelnen Kontaktflächen wird mittels feiner Bonddrähte durchgeführt. Eine Schutzabdeckung verhindert die mechanische Beschädigung von Verbindungsdrähten und Chip und schützt sie zudem vor Umwelteinflüssen.

Abschließender Test

Nach der Zusammenführung der einzelnen Komponenten ist die Herstellungsphase beendet und es erfolgt ein abschließender Test der Funktionstüchtigkeit der Chipkarte.

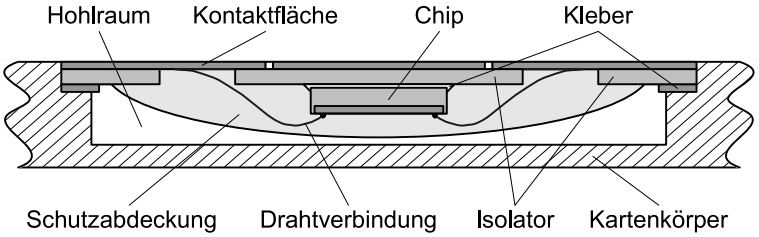

Abb. 2.13: Einbettung des Chipmoduls mittels Bonding

Eine neuere Technologie, die so genannte Flip-Chip-Technik verzichtet auf die Verwendung von Bonddrähten, indem der Chip umgedreht (engl. flip) und direkt mit dem Kontaktfeld verbunden wird (siehe Abbildung 2.14). Diese Art der Kontaktierung ist wesentlich stabiler als jene, die durch Bonding erzielt werden kann. Zudem kann die Schutzabdeckung entfallen, da nun nur mehr die Rückseite des Chips zugänglich ist und auch keine feinen Bonddrähte mehr geschützt werden müssen.

Design der Anwendung

Beachten Sie, dass im Prinzip im Herstellungsprozess auch das Design der Anwendungen enthalten ist. Allerdings ist der Entwickler der Anwendung (Anwendungshersteller) meist nicht identisch mit dem Chipkartenhersteller.

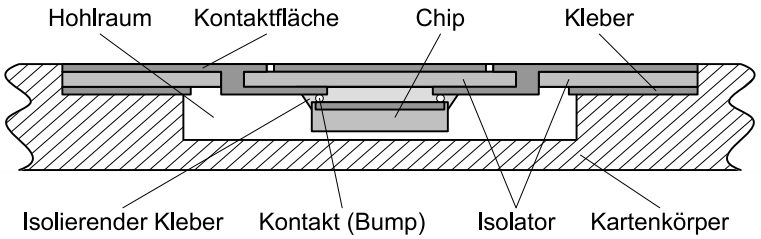

Abb. 2.14: Einbettung des Chipmoduls mittels Flip-Chip-Technik

Die Anwendungen werden vom Anwendungshersteller im Rahmen der Vorpersonalisierung (Komplettierung) auf die Chipkarte geladen.

Um die spätere Komplettierung (Nachladen von Komponenten des Betriebssystems und Anwendungen) der Chipkarte abzusichern, werden nun auch Transportschlüssel in die Karte geladen. In weiterer Folge kann nur dann auf die Chipkarte zugegriffen werden, wenn zuvor der Transportschlüssel erfolgreich verifiziert wurde.

2.5.2 Vorpersonalisierung

Zu Beginn dieser Phase wird erneut die korrekte Funktion der Chipkarte verifiziert. Danach erfolgt eine Authentifikation mittels Transportschlüssel. Danach werden unter anderem folgende Schritte abgearbeitet:

- Nachladen von Betriebssystemkomponenten (Komplettierung). Dies umfasst z.B. proprietäre kryptographische Mechanismen des Anwendungsherstellers, die er vor dem Chipkartenhersteller geheim halten möchte.
- Nachladen von anwendungsspezifischen Softwarekomponenten.
- Anlegen der Filestruktur inklusive der Zugriffsrechte.
- Laden von systemweit konstanten Daten (z.B. kryptographische Schlüssel der Anwendung).
- Laden von Personalisierungsschlüssel(n), die in weiterer Folge zur Entschlüsselung der verschlüsselt übertragenen Personalisierungsdaten verwendet werden.

2.5.3 Personalisierung

Vielfach ist eine Chipkarte an eine bestimmte Person (oder Anwendung) gebunden. Hierzu müssen die personen- oder anwendungsbezogenen Daten sowohl auf den Kartenkörper als auch in den Chip geschrieben werden. Diesen Prozess bezeichnet man als Personalisierung.

Im Rahmen der Personalisierung werden unter anderem folgende Daten auf den Kartenkörper gedruckt (bzw. gestanzt) und/oder im Chip (oder auf dem meist aus Gründen der Kompatibilität vorhandenen Magnetstreifen) gespeichert:

- Persönliche Daten, wie Name oder Anschrift des Karteninhabers
- Foto des Karteninhabers
- Sicherheitsrelevante Daten wie PINs und kryptographische Schlüssel des Karteninhabers
- Weitere anwendungsspezifische Daten

Das Bedrucken der Kartenoberfläche nennt man physikalische Personalisierung, das Speichern von Daten auf den Magnetstreifen oder im Chip wird logische Personalisierung genannt.

Sofern keine personenbezogenen oder anwendungsspezifischen Daten vorhanden sind, entfällt die Personalisierung und die Karte geht über die Ausgabe direkt in die nächste Phase (die Kartennutzung) über.

Die Ausgabe der Chipkarten kann unterschiedlich gestaltet sein. Sofern die Chipkarte mittels PIN geschützt ist, wird die (Initial-)PIN dem Benutzer meist in einem so genannten PIN-Brief (spezielle "blickdichte" Kuverts) übermittelt.

Beim Versenden von personalisierten Chipkarten (wie GSM-SIM-Karten oder Signaturkarten) kann der so genannte Postident-Dienst (der deutschen Post) hilfreich sein. Hier wird von Seiten der Post sichergestellt, dass nur die berechtigte Person Zugriff auf das Schriftstück und die darin enthaltene Chipkarte erhält. Andere Paketdienste wie UPS bieten ähnliche Dienstleistungen an, z.B. "Delivery Confirmation" (mit und ohne Empfangsbestätigung) und "Adult Signature Required").

2.5.4 Kartennutzung

Verwendung in Anwendungen

Die Phase der Kartennutzung beinhaltet logischerweise die Verwendung der Chipkarte in diversen Anwendungen. In vielen Fällen kann (muss) der Benutzer als ersten Schritt nach der ersten Aktivierung der Chipkarte die Initial-PIN ändern. Eine weitere Sicherheitsmaßnahme ist auch das Setzen eines Gültigkeitstages, so dass die Karte im vorgesehenen System erst nach diesem Datum verwendet werden kann.

Update

Im Laufe der Kartennutzung kann es auch zu Updates von Anwendungen und gespeicherten Daten (Anwendungsdaten, aber auch kryptographischen Schlüsseln) kommen. Dies kann z.B. erforderlich sein, wenn eine neue Version der Anwendungssoftware eingesetzt werden soll, oder gar neue Anwendungen auf die Chipkarte geladen werden. Das Update und Nachladen von Anwendungen ist natürlich durch entsprechende Schlüssel (bzw. PINs) abgesichert. Zudem können Anwendungen auch deaktiviert werden.

Werden Sicherheitsbedingungen (z.B. das Limit des Fehlbedienungszählers) verletzt, so tritt die Chipkarte meist selbständig (d.h. durch interne Abläufe gesteuert) in eine temporäre Sperrphase ein. Dies hat zur Folge, dass die Karte vorübergehend nicht mehr genutzt werden kann. Meist besteht aber

die Möglichkeit, die Karte mittels des Personal Unblocking Keys (PUK – auch PIN Unblocking Key) zu entsperren.

Sperrung

Zudem kann eine Sperrung auch von außen durch den Systembetreiber erfolgen. Ein typisches Szenario ist die Verwendung einer als gestohlen oder verloren gemeldeten Bankomatkarte. Nach der Online-Verifikation der Gültigkeit (Abgleich der Kartennummer mit einer so genannten Sperrliste – auch schwarze Liste oder Blacklist genannt) sperrt die Bankomat-Software die gerade bearbeitete Karte (zudem wird sie meist auch noch im Terminal einbehalten!). Diese Art der Sperrung kann der Benutzer i.Allg. nicht selbst aufheben. Ist die Sperrung irreversibel – man spricht auch von der Deaktivierung der Karte – d.h. auch der Systembetreiber kann die Sperrung nicht wieder aufheben, dann tritt die Chipkarte in die letzte Phase des Lebenszyklus ein.

2.5.5 Ende der Kartennutzung

Der letzte Abschnitt im Lebenszyklus einer Chipkarte beschäftigt sich mit deren Rücknahme (sofern die Karte noch vorhanden ist). Daran kann eine erneute Ausgabe der Karte oder deren Vernichtung folgen.

Ursachen

Es gibt verschiedene Ursachen für die Rücknahme einer Karte:

- Gültigkeitsdauer der Karte ist abgelaufen.
- Die Karte wurde gesperrt und kann nicht mehr entsperrt werden.
- Die Karte ist defekt, z.B. durch
  - Speicherfehler des EEPROMs,
  - starke Abnutzung des Kontaktfeldes oder
  - Beschädigung des Kartenkörpers.

Wird die Chipkarte erneut ausgegeben, so muss sichergestellt werden, dass zuvor zumindest die sensitiven Daten von der Karte und aus der PC-Anwendung gelöscht werden. Dient die Karte zum Beispiel nur dazu, einen bestimmten Benutzer mittels eines Identifiers zu identifizieren (und ist sie somit nicht personalisiert), so kann die erneute Ausgabe ohne Zusatzaufwand erfolgen.

In den meisten Fällen wird im Zuge der Ausgabe der Chipkarte deren Oberfläche personalisiert (z.B. Aufdrucken von Name oder Foto). Zudem enthalten die Chipkarten oft sensitive oder personenbezogene Informationen, die aus Sicherheitsgründen nicht wieder gelöscht (und neu beschrieben) werden können. In beiden Fällen ist eine Wiederverwendung der Chipkarte nicht möglich, und die Chipkarte muss vernichtet werden. Meist werden die Chipkarten in einem Schredder zerstört und anschließend verbrannt. Aus Gründen des Umweltschutzes wäre hier allerdings ein Recycling von Chip und Kartenkörper angebracht.

Zusammenfassung

In diesem Kapitel haben Sie zunächst die physikalischen und elektrischen Eigenschaften von Chipkarten kennen gelernt. Danach folgte eine Beschreibung der Kontaktierung, ihres inneren Aufbaus und der einzelnen Komponenten wie Mikrocontroller, Speicher (RAM, ROM, PROM und EEPROM) und diverser Zusatzmodule.
Nach dieser Beschreibung des Aufbaus folgte die Darstellung der Kommunikation mit der Außenwelt (genauer, der über das Terminal verbundenen Host-Anwendung). Hier haben Sie sowohl die Protokolle und Nachrichtenformate in der Anwendungsschicht (APDUs) als auch die Protokolle auf der Leitungsschicht kennen gelernt. Die unterste Schicht, die physikalische Schicht, wurde ebenfalls beschrieben.
Abschließend erfolgte eine allgemeine Beschreibung des Lebenslaufs einer Chipkarte, von ihrem Design über Produktion und Verwendung bis hin zur Rücknahme und Vernichtung (Recycling) der Chipkarte.

Übungsaufgaben

2.1 Wiederholen Sie die wesentlichen positiven und negativen Eigenschaften von Chipkarten und grenzen Sie Chipkarten gegenüber PCs ab.

2.2 In Chipkarten werden unterschiedliche Speicherarten verwendet. Beschreiben Sie diese Speicherarten und charakterisieren Sie ihre Eigenschaften. Geben Sie zudem Beispiele für Daten an, die in den jeweiligen Speicherarten abgelegt werden. Diskutieren Sie auch die Frage, welche Daten nicht in welchem Speichertyp abgelegt werden können (oder aus Sicherheitsgründen nicht dort abgelegt werden dürfen/sollen).

2.3 Kommunikation der Chipkarte mit der Außenwelt:
   a) Kann eine Chipkarte eigenständig mit der Kommunikation beginnen? Begründen Sie Ihre Antwort!
   b) Betrachtet man Command- und Response-APDUs, so gibt es bedingt durch die optionalen Felder vier verschiedene Kombinationen. Geben Sie für jede mögliche Kombination aus Command- und Response-APDU ein Beispiel an.
   c) Wozu können die Felder P1 und P2 einer Command-APDU genutzt werden? Geben Sie drei Verwendungsmöglichkeiten an.

2.4 Lebenszyklus von Chipkarten
   a) Wann kann auf eine optische Personalisierung verzichtet werden? Nennen Sie zwei Beispiele.
   b) Nennen Sie drei Ursachen, die zur Sperrung einer Chipkarte führen.