

Aufbau, Funktion und Anwendung von Chipkarten

H. Kubin, Dresden

Nicht nur im privaten Bereich wird der Elektrotechniker zunehmend mit Chipkarten konfrontiert, sei es die Telefonkarte, die Krankenversichertenkarte, die EC-Karte ... In der Gebäudetechnik sind es vor allem die vielen Möglichkeiten von Zutritts- und Zugangskontrollen mit Chipkarten, die auch sein Ressort als Errichter berühren. Der Beitrag zeigt einen Blick in das Innenleben von Chipkarten und ihre Einsatzmöglichkeiten im Rahmen busorientierter Gebäudesystemtechnik.

1 Überblick

Chipkarten sind Informationsspeicher, die in jeder Brieftasche Platz finden. In einem flexiblen Trägermaterial sind elektronische Schaltkreise (Speicher, Mikroprozessoren) untergebracht. Trotz der Flexibilität ist die Funktion der Karte gewährleistet. Derzeit werden Speicherschaltkreise mit einer Kapazität von etwa 16 kByte eingesetzt.

Chipkarten mit Mikroprozessoren garantieren durch entsprechende Maßnahmen ein hohes Sicherheitsniveau, als Beispiel sei die EC-Sparkassenkarte mit Geldbörsenfunktion genannt.

Eine wesentliche Voraussetzung für die Einführung von Chipkarten ist die Vernetzung informationsverarbeitender Teilsysteme auf der Basis standardisierter Protokolle.

Zu den vielfältigen Einsatzgebieten von Chipkarten gehören u. a.:

- Zutrittsüberwachung für Gebäude, Räume, Anlagen, Parkplätze usw.
- Identitätsnachweis (Authentifikation) als Dienst- oder Berechtigungsausweis unter Verwendung einer persönlichen Identifikationsnummer (PIN) – der „Geheimnummer“
- elektronische Geldbörse mit Kleingeldfunktion, z. B. für Telefon, öffentlichen Personennahverkehr, Automaten (Getränke, Kopierer usw.), Warenanbieter, Kaufhäuser (Rabattsysteme), Müllentsorgung, Energieabrechnung, Dienstleistungen jeglicher Art,
- Leserausweis für Bibliotheken u. ä. mit Leihbestands- und Gebührenerfassung
- Servicefunktionen
- Krankenversichertenkarte.

Autor

Dr.-Ing. Hellmuth Kubin ist Mitarbeiter am Institut für Informationssysteme der TU Dresden, Fakultät Informatik.

Allerdings gibt es beim Chipkarteneinsatz auch Gefahren. Je nach Anwendungsfall können auf der Karte personenbezogene Informationen gespeichert sein, die bei Verlust oder Mißbrauch zu erheblichem Schaden für den Eigentümer führen können. Der Karteneigentümer kennt i. allg. den aktuellen Umfang der gespeicherten Informationen nicht oder nicht mehr und kann kaum nachvollziehen, wer wann welche Informationen gespeichert hat. Der Verlust wäre einem Gedächtnisverlust vergleichbar.

Mißbrauchsmöglichkeiten bestehen auch bei der Geldbörsenfunktion, bei der der im Speicher geführte Geldbetrag ohne jeden zusätzlichen Nachweis vollständig abgebucht werden kann.

Ein neuer Aspekt tritt durch die Vernetzung der Rechnersysteme auf, die im Hintergrund ein Chipkartensystem stützen. Durch das „Belauschen“ der Netzverbindung besteht die Möglichkeit festzustellen, ob, wann, wo und wie oft die Nutzung des Systems erfolgt, woraus Rückschlüsse auf das Verhalten des Eigentümers gezogen werden können.

Gegen den Zugriff auf die Informationen auf der Karte und das Belauschen der Netzverbindung werden entsprechende technische Maßnahmen eingesetzt.

2 Anwendungsbeispiel Zutrittssteuerung

Eine Einsatzmöglichkeit von Chipkarten, mit der der Elektrotechniker nicht nur passiv, sondern auch aktiv konfrontiert werden kann, wird hier etwas ausführlicher erläutert. Anschließend wird auf das Innenleben der Chipkarten eingegangen.

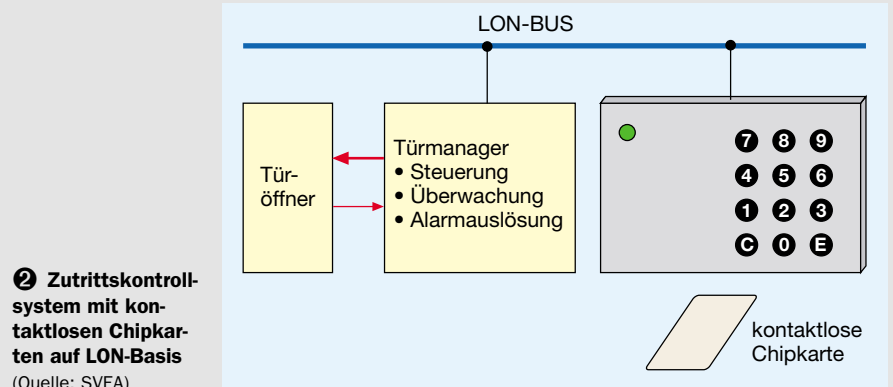
Das Errichten einer Zutrittssteuerung fällt durchaus in das Ressort des Elektrotechnikers. Am Beispiel einer Zutrittskontrolle der Fa. SVEA, Hamburg, wird die Funktionsweise erklärt. Die Chipkarte (oder Schlüsselanhänger) ist hier ein kontaktlos les- und beschreibbarer Datenträger. Im einfachsten Fall besteht das Zutrittskontrollsystem aus dem Terminal (Schreib-/Lesestation, Bild 1) und einer im gesicherten Bereich installierten Türüberwachungs- und -steuereinheit, dem Türmanager.

Der Türmanager ist mit dem Terminal über das LON-Bussystem [1] verbunden und steuert das Öffnungssystem der Tür (Bild 2). Er entscheidet über die Freigabe der Tür. Entsprechende Bestätigungen oder Fehlermeldungen werden über den LON-Bus an das Terminal oder ein entsprechendes Display übertragen.

Durch den modularen Aufbau auf LON-Basis kann das System zu einem komplexen



1 Kartenterminal mit Tastatur für PIN-Abfrage für kontaktlose Chipkarten (oder Schlüsselanhänger)
(Quelle: SVEA)



2 Zutrittskontrollsystem mit kontaktlosen Chipkarten auf LON-Basis
(Quelle: SVEA)

Zutrittskontrollsystem ausgebaut werden. Die Daten werden hier dezentral verwaltet. Die Chipkarte enthält sämtliche Informationen für die Zutrittsberechtigung. Darüber hinaus kann sie aber auch Daten für andere Anwendungen, wie Zeit- und Betriebsdatenerfassung, Voreinstellungen für Regelungssysteme u. ä., verwalten.

Die Programmierung der Chipkarten mit den Berechtigungsprofilen erfolgt mit einer PC-gekoppelten Programmierstation.

Ein derartiges Zutrittskontrollsystem erfüllt Funktionen wie zeit- und raumzonenbezogene Zutritte für jeden Mitarbeiter, Umschalten zwischen verschiedenen Betriebsarten (Dauerfreigabe, Dauersperren, Einzelfreigabe und Einzelfreigabe mit PIN-Abfrage), Erkennen und Überwachen des Türstatus, Signalisieren von Einbrüchen oder das Löschen von verlorengegangenen Datenträgern (erfolgt automatisch durch den Ersatzdatenträger). Durch die Einbindung in das LON-Bussystem können sämtliche Informationen der Zutrittskontrolle anderen Gewerken, wie Licht-, Sonnenschutz- und Heizungssteuerung oder Brand- und Einbruchmeldeanlagen, zur Verfügung gestellt werden und umgekehrt. Dadurch lassen sich für den Anwender neue integrale Funktionalitäten moderner und nutzerorientierter Gebäudetechnik realisieren.

Eine wichtige und unbedingt zu bedenkende Frage ist das Verhalten bei Strom- oder Systemausfall.

Chipkarten bieten auch die Möglichkeit, die Berechtigung für Arbeiten an bestimmten Anlagen der Gebäudetechnik sicherzustellen. So können Arbeiten an Heizungs- und/oder Warmwasseranlagen in Abhängigkeit von der Herstellerzulassung geregelt werden (Bild 3). Einstellparameter für eine Anlage können dabei ebenfalls von einer Chipkarte geladen werden. Eingabefehler wären damit vermeidbar. Auch hier ist die Einbindung in ein Gebäudegesamtkonzept über LON vorteilhaft.

3 Aufbau von Chipkarten

Chipkarten unterscheiden sich nach der Art des Datenaustauschs und der Energieversorgung der Karte (über Kontakte oder kontaktlos) und nach dem Kartentyp (Speicherchipkarte, Prozessorchipkarte).

3.1 Kontaktbehaftete Chipkarten

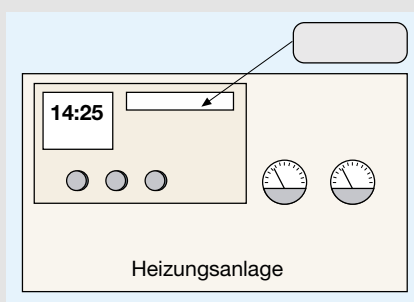
Bei diesen Chipkarten erfolgen Datenaustausch und Energieversorgung über mechanische Kontakte. Die Abmessungen der am weitesten verbreiteten ID-1-Karte und die Belegung der Kontakte zeigt Bild 4 a. Über C7 erfolgt der serielle Datenaustausch.

Als Material für die Karten werden z. B. Polyvinylchlorid, Polycarbonat oder Acrylnitril-Butadien-Styrol eingesetzt.

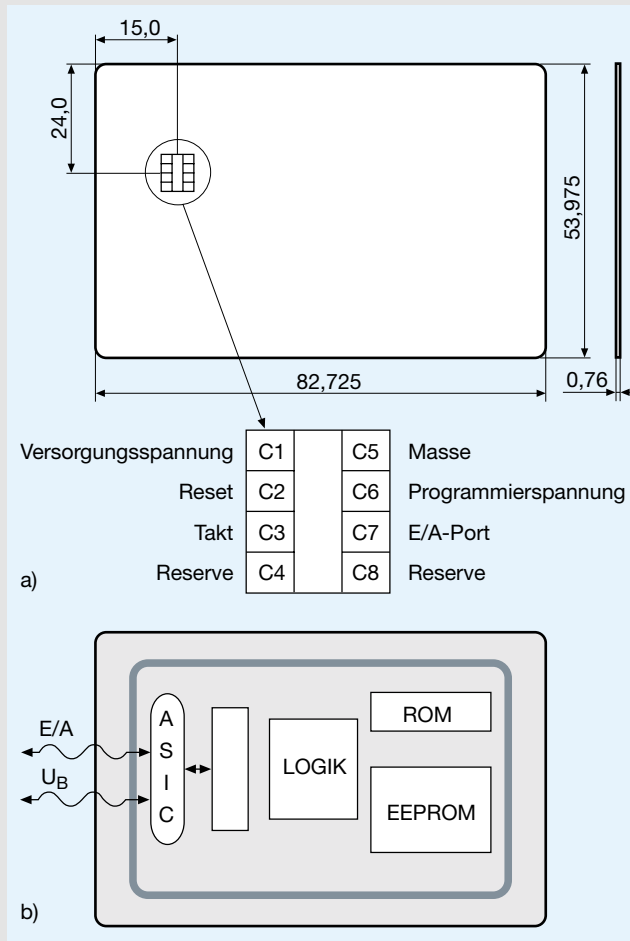
3.2 Kontaktlose Chipkarten

Bild 4 b zeigt den inneren Aufbau einer kontaktlosen Chipkarte. Über eine Leiter Schleife, die als Antenne wirkt, erfolgt der Informationsaustausch mit dem Kartenterminal. Ein zusätzlicher Chip auf der Karte wandelt das amplitudenmoduliert übertragene Signal in digitale Informationen für die Logikbaugruppe um und gewinnt gleichzeitig aus diesem Signal die Betriebsspannung für die Chipkarte. Aufgrund des zusätzlichen Flächenbedarfs werden vorwiegend Speicherchipkarten (vgl. Abschn. 3.3) kontaktlos realisiert.

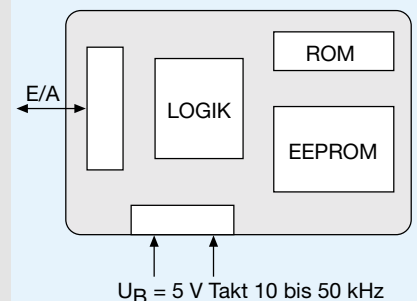
Kontaktlose Chipkarten werden für unter-



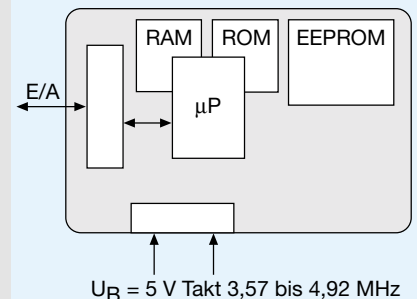
3 Chipkartennutzung an einer Heizungsanlage



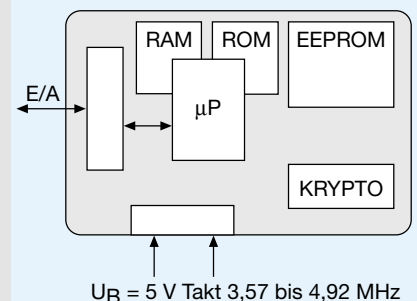
Speicherchipkarte



Prozessorchipkarte

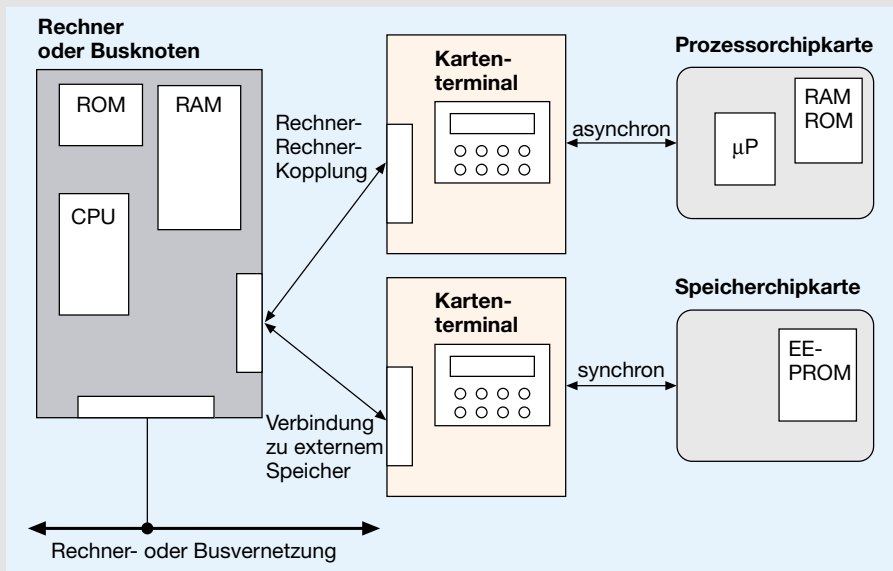


Krypto-Prozessorchipkarte



5 Interne Chipkartenstruktur

4 Aufbau von Chipkarten
a) kontaktbehaftete Karte im Format ID-1. Die Kontaktierung erfolgt im Terminal in der Reihenfolge: Masse – Versorgungsspannung – Resetsignal – Taktsignal. Programmierspannung wird nur bei Speicherung im EEPROM angelegt. Serieller Informationsaustausch über E/A-Port C7
b) kontaktlose Karte. Datenübertragung und Energieversorgung erfolgen kontaktlos über eine Antenne und einen zusätzlichen Chip



6 Verbindung des übergeordneten Rechners oder Busknotens mit der Speicher- bzw. Prozessorchipkarte

schiedliche maximal mögliche Sender-Empfänger-Abstände hergestellt:

- Nahbereich – Abstand < 10 cm
- Fernbereich – Abstand < 2 m.

Probleme können sich mit diesen Karten z. B. bei Türschließsystemen ergeben, wenn sich eine autorisierte Person in der Nähe des Systems aufhält.

Kontaktlose Chipkarten haben zwar eine höhere Lebensdauer als kontaktbehaftete, sind dafür aber 20 % bis 50 % teurer.

3.3 Chipkartentyp

Grundsätzlich wird zwischen Speicher- und Prozessorchipkarten unterschieden.

Speicherchipkarten (Bild 5 a) verfügen über eine Logikbaugruppe, die das Ansprechen der Speicherplätze (ROM oder EEPROM) und damit das Lesen bzw. Lesen und Schreiben von Speicherinhalten ermöglicht. Bei nichtladbaren Speicher-karten (z. B. Telefonkarten) erfolgt ein zerstörendes Entladen von vorbelegten Speicherpositionen (entsprechend der

Kartengebühr), um Mißbrauch zu unterbinden. Die Chipfläche beträgt etwa 2 mm².

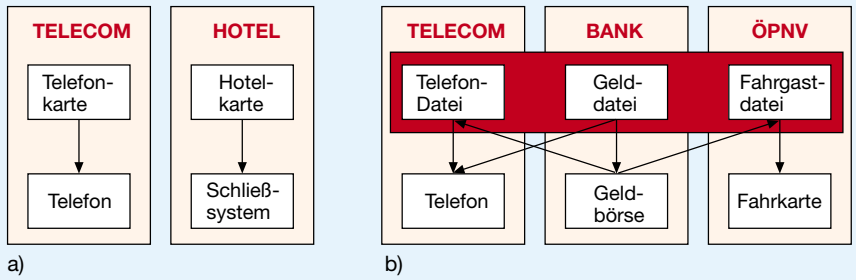
Prozessorchipkarten (Bild 5 b) enthalten einen kompletten Rechner ohne Bedieneinheit. Er besteht aus einem 8-Bit-Mikroprozessor, der mit den entsprechenden Speichern verbunden ist (Leistungsaufnahme etwa 200 mW). Im ROM (etwa 16 KByte) ist das aufgabenorientierte Betriebssystem fest eingetragen. Der RAM-Speicher (≤ 512 Byte) wird als Arbeitsspeicher für Zwischenergebnisse und der EEPROM (≤ 16 kByte) als eigentlicher Datenspeicher genutzt. Die Chip-Fläche beträgt hier etwa 20 mm².

Krypto-Prozessorchipkarten (Bild 5 c) realisieren gegenüber den Einfach-Prozessor-karten eine

- softwareunterstützte (rechenzeitaufwendige) oder
- hardwareunterstützte (schnelle) Informationsver- und -entschlüsselung.

Bei Hardwareunterstützung durch einen Kryptoprozessorchip wächst die Chipfläche auf bis zu 27 mm² an, woraus sich erhöhte Anforderungen an die mechanische Stabilität des Chipkartenmaterials ergeben.

Alle Chipkarten werden weltweit vom Hersteller mit einer eindeutigen Chipnummer versehen, die genutzt werden



7 Schema des Systemzuganges
a) geschlossenes System
b) offenes System

kann, um die Chipkarte vor Fälschungen zu sichern.

4 Chipkarte und umgebendes System

Die Zusammenarbeit der Chipkarte mit dem übergeordneten System erfolgt je nach Kartentyp in unterschiedlicher Weise:

Speicherchipkarten stellen einen externen Speicher für ein anderes Rechnersystem dar (Bild 6).

Prozessorchipkarten tauschen als Rechner ohne Bedienterminal über ihr serielles Interface mit einem anderen Rechner Informationen aus (Bild 6).

Kartenterminals dienen der Versorgung der Chipkarte mit Hilfsenergie und Informationen. Sie verfügen über die Elemente:

- Kartenleser, der die Kontaktiereinheit steuert, und
- Terminalcomputer, der den Kartenleser ansteuert und das Chipkarteninterface in beiden Richtungen (Rechner ↔ Chipkarte) bedient.

Reaktionszeit T_R . Als Zeit vom Einstecken ins Kartenterminal bis zur erwarteten Wirkung gilt bei

- steckbaren Chipkarte $T_R < 1$ s und
- kontaktlosen Chipkarte $T_R < 250$ ms.

Bei Informationsverschlüsselung wird zusätzlich Zeit benötigt, die je nach angewendetem Verfahren und gewählter Sicherheitsstufe bis zu 220 ms betragen kann.

5 Datenaustausch

Der Datenaustausch beginnt zwischen der Chipkarte und dem Kartenterminal. Das Terminal ist seinerseits mit einem Rechner oder einem Bussystem mit vielen Knoten verbunden und übernimmt die Protokollübersetzung zwischen Chipkarte und übergeordnetem System.

Start des Datenaustauschs. Das Kartenterminal bewirkt zunächst den definierten Start der Logik bei der Speicherchipkarte bzw. den definierten Anlauf des Betriebssystems der Prozessorchipkarte. Die Karte sendet daraufhin als Antwort Angaben zur Datenübertragungsart u. a. zum Kartenterminal. Da das Terminal das Übertragungsprotokoll nicht kennt, wird beim Verbin-

dungsaufbau das Protokoll solange gewechselt, bis der Protokolltyp erkannt ist.

Befehl-Antwort-Verkehr. Bei der **Speicher-karte** erfolgt der Signalaustausch über ein **serielles synchrones Interface**. Der Befehl vom Terminal an die Speicherkarte enthält ein Befehlsbyte (Speicher lesen/schreiben), ein Adreßbyte (woher oder wohin) und ein Datenbyte (Nutzinformation). Die Karte antwortet mit takt synchronen Datenbytes. Bei der **Prozessorchipkarte** handelt es sich um eine **Rechner-Rechner-Kopplung**. Aufgrund unterschiedlicher Rechengeschwindigkeiten erfolgt die Übertragung **asynchron** mit etwa 9600 Bit/s. Nach der Klärung des Protokolls gibt das Kartenterminal Befehle an das Kartenbetriebssystem. Der Befehlssatz der Karte ist viel leistungsfähiger und umfaßt derzeit 52 Befehle, z. B.:

- Eröffnen einer Datei
- Lesen/Schreiben aus/in eine/r Datei
- Aufladen einer Börse
- Bezahlen mit der Börse
- Ausführen eines Programms
- Überprüfen einer Signatur des Kartenherausgebers.

6 Datensicherheit

Sicherheit ist das Hauptproblem beim Einsatz von Chipkarten für eine allgemeine, öffentliche Nutzung. Jeder Nutzer hat das Bedürfnis, seine individuellen Daten vor fremdem Zugriff zu schützen oder diese nur mit seiner Zustimmung weiterzugeben.

Datenverschlüsselung. Durch Datenverschlüsselung kann die belauschbare Schnittstelle zwischen Chipkarteneingang und Kartenterminal gesichert werden. Der Verschlüsselungsalgorithmus bildet gewissermaßen das Schloß. Nur von der Schlüsselform (den ankommenden Daten) ist es abhängig, ob sich der Schlüssel drehen läßt und die Tür geöffnet werden kann (auf Daten zugegriffen werden kann). Auf dem EEPROM wird ein hierarchisches Dateisystem eingerichtet, in dem die Dateien durch Zugriffsschlüssel gegen unerlaubten Zugriff gesichert sind. Nur durch Hardwarerealisierung dieser Algorithmen in einem zusätzlichen Chip der Karte läßt sich ein ausreichendes Sicherheitsniveau bei hinreichend kleinen Reaktionszeiten erreichen.

Hardwareerschutz. Auch hardwaremäßige Vorkehrungen verhindern den Angriff auf die Chipkarte:

- Eine chaotische Speicherorganisation erschwert das Lesen von Datenstrukturen.
- Ein befehlsweises Abarbeiten des Programms wird verhindert.
- Eine Analyse des Speichers durch Elektronenstrahl ist nicht möglich, da der Speicher dabei gelöscht wird.

7 Einsatzfragen

Beim Einsatz eines Chipkartensystems ist zu klären, welche Informationsmenge auf der Chipkarte zu speichern ist. Da ein Chipkartensystem stets aus der Chipkarte, dem Kartenterminal und einem eventuell in ein größeres Informationssystem integrierten Rechner besteht, muß die Speicherung umfangreicher personenbezogener Daten nicht notwendigerweise auf der Chipkarte erfolgen. Je nach Umfang der auf der Chipkarte enthaltenen Informationsmenge werden unterschieden:

Passive Chipkarten. Auf der Karte ist nur eine minimale Informationsmenge gespeichert, z. B. die Mitarbeiternummer der Firma o. ä.

Aktive Chipkarten. Auf der Karte werden „große“ Informationsmengen gespeichert, z. B. wenn die Teilsysteme eines Informationssystems noch nicht vernetzt sind und die Chipkarte als Datenträger benutzt wird.

Persönliche Identifikationsnummern (PIN) sollte es auf jeder Chipkarte geben, damit sich der Chipkarteninhaber bei Bedarf identifizieren kann.

Ein weiterer Gesichtspunkt bei der Einführung von Chipkartensystemen ist die Art des Systemzuganges. Zu unterscheiden sind dabei:

Geschlossene Systeme (Bild 7 a). Jeder Dienstleister gibt seine eigene Chipkarte heraus. Der Nutzer ist gezwungen, für die sichere Aufbewahrung von vielen Chipkarten zu sorgen, was nicht unbedingt erstrebenswert ist.

Offene Systeme (Bild 7 b). Kartenherausgeber und eine (erweiterbare) Gruppe von Dienstleistern bilden eine Kooperation. Der Abstimmungsaufwand ist dabei nicht zu unterschätzen. Bei einem offenen Systemzugang liegen die Schwierigkeiten in der Entwicklungsphase. Der Nutzer hat hier den Vorteil, daß er nur wenige Chipkarten in der Tasche hat. Das ist für ihn zwar angenehmer, aber der Kartenverlust dafür gravierender.

In jedem Fall sind die Probleme bei defekten oder verlorenen Chipkarten zu lösen.

Literatur

- [1] Pohl, W.: LON in der Elektroinstallation – eine Alternative zum EIB? Elektropraktiker, Berlin 53(1999)3, S. 202-204.