Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 76 (1985)

Heft: 7

Artikel: Kreditkarten : auf dem Weg zum bargeldlosen Verkehr

Autor: Eggenberger, H. P.

DOI: https://doi.org/10.5169/seals-904593

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 09.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Kreditkarten: auf dem Weg zum bargeldlosen Verkehr

1. Kreditkarten in Hülle und Fülle

Gegenüber Kreditkarten ist der Schweizer eher zurückhaltend. Bargeld liegt ihm gefühlsmässig näher. Seit einigen Jahren finden nun aber auch bei uns Kreditkarten vermehrt Verwendung.

Warenhäuser und Interessengemeinschaften des Detailhandels werben mit ihren Karten um Kundschaft, indem die Ware erst Wochen nach dem Bezug bezahlt werden muss. Mittels Kontokarten erleichtern die Banken ihren Kunden den Verkehr am Schalter. Mit der Bancomat- und der Postomatkarte - eigentlich nicht Kredit- sondern Debitkarten - kann vom eigenen Konto auch ausserhalb der Bürozeiten Geld bezogen werden. Wer viel im Ausland reist, besitzt ferner eine oder mehrere der internationalen Kreditkarten Visa, American Express, Eurocard usw. Dazu kommen noch vorbezahlte Wertkarten wie die Taxcard, mit der man ohne Kleingeld telefonieren kann (Fig. 1).

Neben dem Portemonnaie mit Münzen und Noten trägt man also heute ein Portefeuille mit Kreditkarten auf sich. Deshalb besteht bei vielen Leuten ein Bedürfnis nach einer vereinheitlichten, vielseitig verwendbaren Karte. Dabei spielt die Sicherheit gegen Missbrauch sowohl für den Kartenbesitzer wie für den Kreditgeber eine ausschlaggebende Rolle.

Der Artikel beruht auf Unterlagen von Bull, Autelca u.a.

Adresse des Autors

H.P. Eggenberger, Dr. sc. techn., Redaktor, Schweiz. Elektrotechnischer Verein, Postfach, 8034 Zürich.

Fig. 1 Vom Kartenspiel zur Einheitskarte

Erfreulich ist, dass das Format der Karten international genormt ist. Ebenso ist der Magnetstreifen vereinheitlicht, der bei verschiedenen Karten zur Identifizierung verwendet wird. Im übrigen aber herrscht grosse Mannigfaltigkeit.

2. Sicherheit als wichtigstes Anliegen

Voraussetzung für den Erfolg einer vielfältig verwendbaren Karte ist, dass diese gegen missbräuchliche Verwendung eine sehr hohe Sicherheit bietet.

Die Karte und das System müssen den Träger als rechtmässig «erkennen». Auch eine gestohlene oder gefundene Karte soll nicht missbraucht werden können. Die Identifizierung des Karteninhabers mittels Ausweis ist zu umständlich und bei Verwendung in Automaten gar nicht möglich. Bei verschiedenen Karten ist der Besitzer durch einen nur ihm bekannten Zahlencode vor fremdem Zugriff geschützt (PIN-Code). Er muss diesen Zahlencode am Endgerät eingeben, bevor er Bezüge tätigen kann. Der Schutz ist jedoch unvollständig, wenn mit einer entwendeten oder gefundenen Karte probiert werden kann, bis der Code geknackt ist.

In einem weiteren Schritt muss die Karte daraufhin überprüft werden, ob sie wirklich zum System gehört, ob sie eventuell gesperrt ist und ob die Kreditbezugsgrenzen noch nicht erreicht sind. Grosse Kartenorganisationen unterhalten diesbezüglich einen aufwendigen, weltweiten Autorisationsdienst mit Rückfragemöglichkeit.

Der dritte wichtige Aspekt ist die Sicherheit vor Fälschung und Manipulation. Professionelle Fälscherorganisationen interessieren sich beispielsweise für das Kohlepapier der Vertragsbelege, das beim Kauf mit Kreditkarte anfällt, um damit Duplikate echter Karten herzustellen. Die Karte darf also nicht nachgebaut und auch nicht verändert werden können. Sie muss deshalb Informationen enthalten, die unzugänglich sind.

3. Moderne Technologie führt weiter

Die genannten Sicherheitsbedingungen setzen voraus, dass die Karten selbsttätig gewisse Kontrollen vornehmen und sich gegen unbefugten Eingriff schützen. Dies ist bei den bisher üblichen Karten nicht der Fall, auch nicht bei solchen mit Magnetstreifen. Hier bietet sich aber der Mikroprozessor als aktiver Baustein an.

Die Chipkarte[1]) ist eine Erfindung des französischen Journalisten *R. Moréno*, der sie 1974 zum Patent anmeldete. Bis etwa 1979 fand die Idee kaum Interesse. Dann aber erkannten in Frankreich verschiedene Banken, grosse Herstellerfirmen und die PTT die Bedeutung und die potentiellen Anwendungsmöglichkeiten. Inzwischen sind Chipkarten und die entsprechenden Systeme von Bull, Philips und Schlumberger entwickelt worden. Bull und Philips haben sich bald zu einem gemeinsamen Vorgehen entschlossen. Bereits sind in Frankreich in mehreren Städten Grossversuche durchgeführt worden, mit denen die Zweckmässigkeit und Akzeptanz der Karten als einheitliches, bargeldloses Zahlungsmittel in zahlreichen Verkaufsläden und Warenhäusern sowie in öffentlichen Sprechstellen geprüft wurden. Nach bisherigen Ergebnissen wird sich die CP8-Chipkarte mit Mikroprozessor von Bull gegenüber derjenigen von Schlumberger mit Speicher und Logikschaltungen wegen den viel grösseren Möglichkeiten durchsetzen.

So einfach die Idee der Chipkarte erscheinen mag, die Realisierung einer marktgängigen Karte stellte hohe Anforderungen. Allein das Anbringen des Chips bot zahlreiche Probleme wegen der Flexibilität der Karte, wegen der vorgegebenen Dicke, den Anschlüssen, der Gefahr elektrostatischer Ladungen auf dem PVC und wegen schlechter Wärmeleitfähigkeit. In

[1]) französisch: carte à mémoire, besser auch carte vive; englisch: smart card.

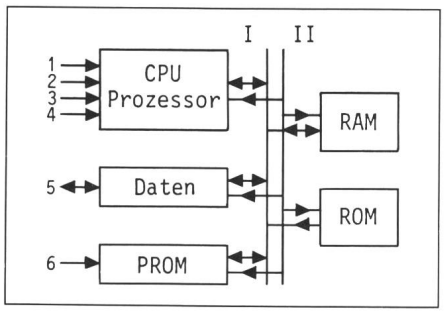


Fig. 2 Blockschema zum Aufbau der CP8-Karte

1 Speisung
2 Bezugsspannung (Masse)
3 Takt
4 Reset
5 Daten Ein-/Ausgang
6 Programmierspannung
I Datenbus
II Adressierbus

der Einführungsphase ist auch wichtig, dass die Chipkarte mit bisherigen Magnetstreifenkarten kompatibel ist.

4. Aufbau der CP8-Chipkarte

Auf der CP8-Karte ist eine integrierte Schaltung (IC) in Form eines 18 mm² grossen Monochips angeordnet, der auf dem Mikroprozessor 6805 von Motorola beruht und 8 Kbit Speicherkapazität aufweist. Die Architektur entspricht grundsätzlich der Standardstruktur (Fig. 2).

Die Karte enthält keine Energiequelle. Sie wird beim Einstecken vom jeweiligen Endgerät gespeist. Von den ursprünglich 23 Anschlüssen des IC wurden 15 entfernt, und nur 6 werden verwendet: Speisung, Bezugspotential 0 V, Programmierspannung (5...25 V, je nach Karte), Nullstellung (Reset, Initialisierung), Taktgeber (3,58 MHz), Datenausgang (wechselseitig mit 9600 bit/s). Der Datenaustausch erfolgt asynchron, Zyklus um Zyklus, wobei jeder Zyklus aus einem Anfangsbit, 8 Datenbits und einem Kontrollbit besteht.

Bei den üblichen integrierten Schaltungen wird absichtlich dafür gesorgt, dass zu möglichst vielen Stellen von aussen zugegriffen werden kann, sei es, um gewisse Funktionen zu kontrollieren, sei es, um Störungen zu untersuchen und Simulationen vorzunehmen. Dies darf bei der CP8 aus Geheimhaltungsgründen nicht sein. Dort ist der Mikroprozessor deshalb so ausgelegt, dass er den PROM-Speicher (Programmable Read-Only Memory) ohne äussere funktionale Einwirkung selbständig programmieren kann.

Im ROM (Read-Only Memory) sind das Anwendungsprogramm und der PIN-Algorithmus untergebracht. Das RAM (Random Access Memory) dient als Arbeitsspeicher und Statusbuffer.

Das PROM ist in drei Bereiche gegliedert: Der *Geheimbereich* enthält für jede Karte einmalige Daten, zu denen nur der karteninterne Prozessor Zugang hat (Herstellercode, Schlüsselcode des Herausgebers und des Karteninhabers). In der Statuszone wird zudem jeder Zugriff zur geschützten Zone registriert. Alle diese Daten können von aussen weder festgestellt noch verändert werden.

Der *geschützte Bereich* ist mittels richtiger PIN-Eingabe zugänglich; er enthält die Daten der Transaktionen und kann beschrieben und gelesen werden, wobei verschiedene Schutzmassnahmen möglich sind. Der *freie Zugriffbereich* enthält verschiedene sekundäre Informationen, die nicht schützenswert sind.

Der 8-bit-Prozessor kontrolliert die Speicherzugriffe, steuert und überprüft den Verkehr mit dem Kartenleser, führt Anwendungsprogramme durch und verschlüsselt und entschlüsselt Daten.

5. Sicherheitsaspekte der CP8-Karte

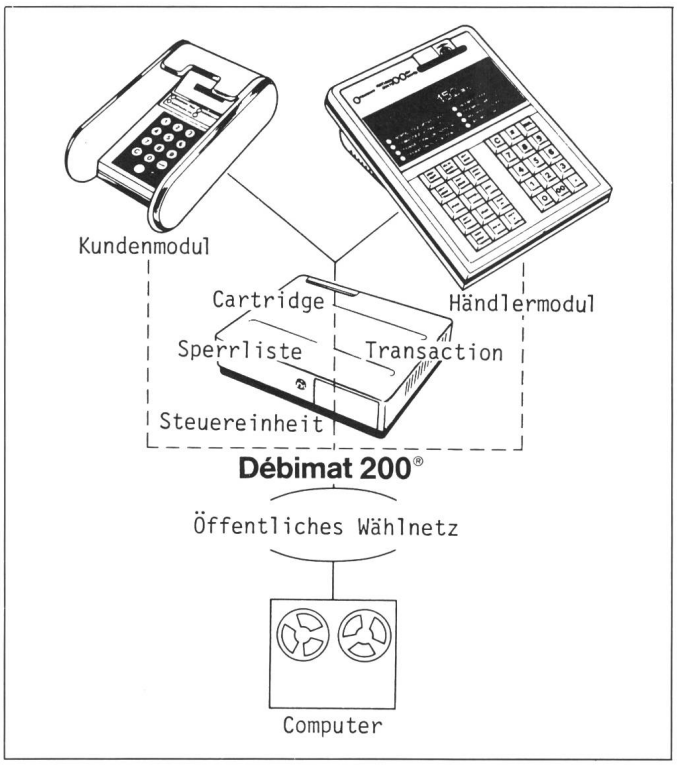
Für die geforderte hohe Sicherheit der Karte sorgen verschiedene Merkmale:

- *Identifizierung*: Der Benützer muss sich mit dem von ihm selbst gewählten PIN-Code zu Beginn jeder Kartenverwendung ausweisen. Verlorene und gestohlene Karten sind wertlos, sofern der rechtmässige Inhaber seinen Code nicht leichtfertig bekanntgibt. Falls dreimal hintereinander ein falscher Code eingegeben wird, blokkiert sich die Karte selbsttätig. Diese Blokkierung kann nur gemeinsam vom Herausgeber und dem Benützer aufgehoben werden.
- *Authentifizierung:* Die im Endgerät eingesteckte Karte wird durch Vergleich mit einer «Mutterkarte» im Zentralcomputer auf Echtheit und Systemzugehörigkeit geprüft und bezüglich Sperrliste, Bezugslimite und zeitliche Beschränkung kontrolliert.
- *Programmschutz:* Einen wesentlichen Beitrag zur Sicherheit vor Nachahmung und Manipulation bietet der als *Telepass* bezeichnete Vorgang: Aufgrund einer Zufallszahl und einer vertraulichen, internen Information errechnet der Kartenprozessor die Funktion Telepass. Sie wird einerseits zur Authentifizierung der Karte durch den Zentralcomputer des Systems (Host) verwendet, anderseits liefert sie den Chiffrierschlüssel für die Datenübermittlung.
- *Fehlerfreies Erfassen und Verrechnen:* Der Austausch von Informationen im Netz erfolgt codiert, wobei der Schlüssel laufend verändert wird. Eine Transaktion wird erst ausgeführt, wenn deren einwandfreie Übermittlung durch Rückmeldung feststeht. Die Transaktionen werden auch auf der Chipkarte aufgezeichnet und können vom Besitzer jederzeit eingesehen werden.
- *Datenschutz:* Zu diesem Zweck ist das PROM hierarchisch in verschiedene Zonen unterteilt. Wichtig dabei ist, dass die eingeschriebenen Daten ohne Zerstörung nicht löschbar sind. Die Grösse der Zonen hängt von der jeweiligen Anwendung ab. Die Codes und die Begrenzung der Zonen werden von einem Fachmann im «Personalisierungsgerät» festgelegt.

6. Anwendungen

In Blois, südlich von Paris, hat nach einem einjährigen Grossversuch die Betriebsphase des bargeldlosen Zahlungsverkehrs mittels CP8-Karte begonnen. Zahlreiche Verkaufsgeschäfte und Banken nehmen daran teil. Das Terminal in den Geschäften (Debimat 200) umfasst ein Kundenmodul, ein Händlermodul, eine Steuereinheit sowie einen Drucker (Fig. 3). Das Kunden-

Fig. 3 Das System der CP8-Karte



modul wird an einem geschützten Ort nahe der Kasse aufgestellt, damit der Kunde seinen PIN-Code unbeobachtet eingeben kann. Der vom Verkäufer auf seinem Modul eingetippte Betrag ist am Kundengerät ersichtlich, wo auch die Verbuchung freigegeben werden muss. Die Steuereinheit dient zur Speisung der übrigen Geräte sowie als Interface zum Netz und zum Systemcomputer. Eine CP8-Karte reicht für 200 Transaktionen. Der Karteninhaber kann an einem speziellen Kartenlesegerät jederzeit eine Aufstellung der bisherigen Transaktionen mit Datum, Uhrzeit und Betrag erhalten.

Zur Begleichung von Kleinbezügen an Automaten (z.B. Telefongespräche) kann der CP8-Inhaber von seinem Bankkredit bestimmte Beträge in «Börsenbereiche» der Karte transferieren. Diese Beträge werden dann bei Gebrauch off-line abgebucht, analog zu den Wertkarten (z.B. Taxcard).

Von besonderer Bedeutung ist die sichere Identifizierung bei Fernbezügen. Die CP8-Karte bietet deshalb im Rahmen des Videotex-Systems vielversprechende Möglichkeiten. Die Identifizierung ist aber nicht nur im bargeldlosen Verkehr wichtig. Die Karte ist auch als elektronischer Ausweis für den Zutritt zu geschützten Räumen und Gebieten geeignet.

In ganz anderer Richtung liegt die Verwendung der Karte als vertraulicher Datenträger, z.B. für Medizinaldaten. Bereits werden an einer Pariser Universität die Personalien und Studiendaten der Studenten versuchsweise auf diese Art erfasst.

Die vielseitigen Anwendungsmöglichkeiten haben bei der CP8-Karte zur Bezeichnung als Multifunktionskarte geführt. Diese Vielfalt ist möglich, weil die Anwenderprogramme im ROM mit der entsprechenden Maske erst als letzte Schicht der integrierten Schaltung festgelegt werden.

7. Ausblick

Die Versuche mit der CP8-Karte in Frankreich werden eindeutig positiv beurteilt. Im Bankwesen ist die allgemeine Einführung dieser Karte vorgesehen (Carte bancaire). Von grosser Bedeutung ist dabei die Kompatibilität der CP8-Karte mit den bisherigen Magnetstreifenkarten, was einen reibungslosen Übergang gestattet.

Derzeit sind in Frankreich mehr als eine halbe Million CP8-Karten im Umlauf. Die PTT haben über 10 000 Telefonautomaten (publiphones) und entsprechendes Kartenmaterial bestellt. Bull hat sich denn auch für die automatische Herstellung der CP8-Karte in grossen Serien eingerichtet.

In Frankreich sind wohl heute die Vorbereitungen zur Einführung des bargeldlosen Verkehrs am weitesten fortgeschritten. Pilotversuche sind aber auch in Deutschland, Norwegen und anderen Ländern geplant oder bereits in Betrieb. Anlässlich der Skiweltmeisterschaften in Bormio diente die CP8-Karte als Zahlungsmittel. Von ganz besonderer Bedeutung ist aber, dass sich kürzlich MasterCard, die grösste Kartenorganisation der USA, für die Technologie von Bull entschieden hat: Für einmal triumphiert europäischer Erfindergeist über den amerikanischen und japanischen.

In der Schweiz hat es die Autelca AG als Vertretung von Bull übernommen, die CP8-Karte für den bargeldlosen Zahlungsverkehr einzuführen. Vorbereitungen für Pilotprojekte in Zusammenarbeit mit Banken, Detailhandel und PTT sind im Gang. Im Rahmen der Videotex-Versuche finden ferner Untersuchungen statt, wie die Karte zur Autorisierung und vor allem für die sichere, codierte Übertragung eingesetzt werden kann.

Von grosser Bedeutung für die weltweite Verbreitung einer einzigen Karte ist deren internationale Normung. Bull hat bereits intensive Vorstösse unternommen, um neben den Dimensionen der Karten auch die Anordnung des Chips, die Zahl, Dimension und Funktion der Kontakte sowie sogar den Informationsaustausch zwischen Karte und System zu vereinheitlichen.

Bis zur allgemeinen Einführung und Verbreitung einer einheitlichen Karte werden noch Jahre vergehen. In der Zwischenzeit schreitet auch die Technik voran. So ist anzunehmen, dass die Speicherkapazität auf der Karte in wenigen Jahren vergrössert werden kann, was auch wünschbar erscheint. Das Konzept der Karte und des Systems sind davon aber nicht betroffen. Aus heutiger Sicht sind sie ausgesprochen zukunftsgerichtet, so dass sie technisch nicht so bald überholt sein werden.