Die Plastikkarte als Informationsträger für Geldersatz- und Ausweisapplikationen

DK: 351.755.62 336.777 336.736

J.-F. Moser

In den letzten 25 Jahren erlebten die hochentwickelten Industriestaaten einen steten Anstieg des Kreditkartengebrauchs im Zahlungsverkehr. „Cashless and Checkless Society" sind heute die Schlagworte der Wirtschaftssoziologen, die uns den unvermeidbaren Weg zum EFTS, d. h. dem „Elektronischen Funds Transfer System" weisen, dessen Zugang erst mit einer Identitätskarte ermöglicht wird. In nicht allzuferner Zukunft, so heisst es, ermögliche die rasante technische Innovation auf dem Elektronikbereich sogar einen beleglosen Zahlungsverkehr, in welchem die menschliche Stimme zur Identifizierung des Kontoinhabers genüge. Muss man demzufolge schon annehmen, dass die Karte als Identifikations- und Zahlungsmittel überholt ist?

1. Überblick über Kartenverwendungsarten

Um diese Frage zu beantworten, muss man dem Wesen, der Funktion und den Einsatzmöglichkeiten der Karte nachgehen. Ein grober Überblick über die heutigen Verwendungsmöglichkeiten der Karte und ihrer Systeme kann dabei als Referenz dienen. Die Zusammenstellung in *Bild 1* zeigt, wie mannigfaltig die Einsatzmöglichkeiten von Karten sind. Die Liste enthält nur einige offenkundige Anwendungen und könnte beliebig erweitert werden.

Man unterteilt mit Vorteil die Kartenverwendungsarten gemäss ihrer dominanten Funktion in vier Hauptsparten. Zur einzelnen Anwendung innerhalb einer Sparte gehören wohldefinierte Organisations- und Operationsziele, die gemeinsam mit der anlagemässigen Realisierung ein System darstellen. Die Karte erfüllt dabei als Komponente des Systems nur Teilfunktionen dieses Systems. Selbstverständlich ist die Systemkomplexität je nach Anwendungsart verschieden. So ist z. B. das System der visuell kontrollierten Badge-Karten inbezug auf Organisation und Operation besonders einfach, während ein Zutrittskontrollsystem mit maschinell gelesenen Karten äusserst komplex sein kann.

Erkundigt man sich nach den Anforderungen, die man an eine Karte stellt, so müssen diese aus der Sicht des ganzen Systems formuliert werden. Vor allem muss aus der Systemdefinition eindeutig hervorgehen, ob die Karte visuell und/oder maschinell geprüft werden soll. Diese Unterscheidung erlaubt uns, die Karten in zwei Klassen zu unterteilen, wobei uns besonders die maschinell geprüfte Karte beschäftigen wird.

Kartentypus mit dominanter Funktion

Check-Karte[1]	Kredit-Karte[2]	Identitäts-Karte	vorbezahlte Karte
Berechtigungskarte für bargeldlose Bezahlung oder Bezug von Bargeld durch Belastung des persönlichen Bankkontos	Berechtigungskarte für bargeldlose Bezahlung durch Kredit (z.B. Abzahlungskredit mit Kreditlimite)	Persönliche Ausweiskarte zur Personen-Identifikation	Gekaufte Karte, die bargeldlosen Bezug von Waren oder Dienstleistungen erlaubt. Die Karte ist übertragbar
Beispiele			
— EUROCHEQUE — BARCLAY CARD — LLOYDS CARD ⋮ — etc. für fast alle grossen Banken — MIGROS Check-Karte — BANCOMAT-Karte (Geldkarte)	— DINERS CLUB — AMERICAN EXPRESS — BANKAMERICARD — HERTZ — VISA — AVIS — Benzinkarten — Einkaufskarte (Warenhaus, z.B. Jelmoli)	— Fahrausweis — BADGE Karte — Pass — Identitätskarte — Computer Access Karte — Zutrittskontroll-Karte — Mitgliederausweis — Persönliche Abonnements	— PHONOCARD — Benzinkarte — EASIRIDER-Karte — Skiliftkarte — Parkhauskarte — Elektrizitätskarte — Karte mit Jeton- oder Token-Funktion

Weitere Typen

Karten zur innerbetrieblichen Vereinfachung

— Gästepass (zur Bestellung und Rechnungsstellung in Restaurationsbetrieben)
— Hotelzimmerkarte (als sichere Zimmerschlüssel)
— Steuerkarte (für den Betrieb von Maschinen, Automaten)
— Zeiterfassungskarte (Vereinfachung der Arbeitszeitkontrolle)

936482B

1) Auch DEBIT-Karte genannt für Verfügung über ein Kontoguthaben ohne Kreditberechtigung sowie sonstige Mischformen der Verfügungskarten über personenbezogenes Konto.
2) Karten für monatliche Abrechnung entweder mit Sofort-Fälligkeit oder mit längerfristiger Kreditlimite als «revolving credit». Ein Oberbegriff für Kreditkarten ist «TRANSACTION CARD».

Bild 1 Verwendungsarten von Karten in Anwendungssparten aufgeteilt

Bild 2 Verschiedene Plastikkarten als Informationsträger

2. Die visuell geprüften Karten

Wendet man sich jedoch zuerst dem nur visuell geprüften Untersuchungsgegenstand zu, stellt man fest, dass hier die Karte die Rolle eines Passes spielt, d. h. eines Dokumentes, das den rechtmässigen Besitzer zum Vollzug der mit der Karte gegebenen Ermächtigung berechtigt. Die Prüfprozedur beschränkt sich vor allem auf die Identifizierung des Kartenbenützers und die Kontrolle des Berechtigungsbereiches, wobei sich der Mensch als Prüfer so gut wie möglich von der Echtheit der Karte überzeugt. Man stellt folglich fest, dass sich die auf oder in der Karte befindliche Information auf drei Typen beschränkt:

- Information zur Identifizierung des Kartenbenützers,
- Information zur Sicherstellung der Echtheit der Karte,
- Information zur Definition der Autorisationsart mittels visuell lesbaren Daten, d. h. alphanumerischen Zeichen.

2.1 Beispiele

2.1.1 Die Kreditkarte

Die ausschliesslich visuell geprüfte Durchschnitts-Kreditkarte dürfte ein besonders einfaches Beispiel darstellen. Eine solche Karte enthält als Identifizierungsinformation eine Adresse in hochgeprägter Schrift sowie Unterschrift des Kartenbenützers. Die Dateninformation besteht in einer alpha-numerischen ebenfalls hochgeprägten Zeichenfolge, die etwa die Träger-, Besitzer- und Kartennummer darstellt. Die Reihenfolge dieser Ziffern wird in einer ISO-Norm vorgeschrieben. Die Transaktion wird mit Hilfe eines Imprinters dokumentiert, der die hochgeprägte Schrift auf ein Papierformular transferiert. Der Kartenbesitzer unterschreibt üblicherweise dieses Dokument vor dem Gläubiger. Ein Unterschriftsvergleich zwischen Karte und Formular bietet somit die einzige adhoc Identifizierung des Kartenbenützers. Eine Echtheitsinformation existiert praktisch nicht, sie besteht üblicherweise bei diesem Kartentyp in einer sehr einfachen graphischen und farblichen Gestaltung.

2.1.2 Die Bankkarte

Als zweites Beispiel einer visuell geprüften Karte soll eine Bankkarte, z. B. die bekannte Eurocheque Karte betrachtet werden. Sie unterscheidet sich von der Kreditkarte dadurch, dass sie nur im Zusammenhang mit dazugehörigen Checks gebraucht werden kann. Die Identifizierungsinformation ist durch den Namen des Kartenbesitzers in Hochprägung und durch seine Unterschrift gegeben. Die Echtheitsinformation ist in Form eines beidseitig mit Kunststoff verschweissten Papieres mit Wasserzeichen und Farbguillochen dargestellt. Eine hochgeprägte Ziffernfolge enthält als Dateninformation einen Code zur Trägerkennzeichnung, die Kontonummer des Kartenbenützers und die Kartennummer. Die Transaktion erfolgt durch Ausstellung eines dazugehörigen Checks. Unterschrift, Name der Bank und Kontonummer auf Check und Checkkarte müssen übereinstimmen. Der Check ist zusätzlich mit Hilfe einer alphanumerischen Zeichenfolge personalisiert zwecks automatischer Verarbeitung durch den Systemträger.

2.1.3. Die Zutrittskarte

Als letztes Beispiel einer visuell geprüften Karte sei hier die Zutrittskontrollkarte kurz analysiert. Die Identifizierung der zutrittsberechtigten Person ist hier von zentraler Wichtigkeit. Die diesbezügliche Information besteht aus Name, Unterschrift und Porträtfoto des Kartenbesitzers, die im Kartenmaterial unentfernbar eingebettet sein muss. Die Dateninformation enthält eine Kennzeichnung des Systemträgers und spezifiziert die Zonen (Ort, Zeit etc.), für die die Berechtigung gilt. Die graphische und farbliche Gestaltung der Karte beinhaltet die Echtheitsinformation.

2.2 Anforderungen an die Information auf der Karte

Mit diesen drei Beispielen sind selbstverständlich nicht alle visuell geprüften Kartentypen erfasst. Sie gestatten

Kartentyp	Informationstyp		
	Identifizierung	Echtheit	Daten
Kreditkarte	— Name — Adresse — Unterschrift (Vergleich)	Praktisch inexistent Graphische und farbliche Gestaltung	— Name des Trägers — Trägernummer in codierter Form — Nummer des Kartenbesitzers — Kartennummer
Eurochequekarte	— Name	Laminiertes Papier, das Wasserzeichen und Farbguillochen enthält	— Name der Bank — Kontonummer — Kartennummer
Zutrittskontrollkarte	— Name — Unterschrift — Foto	Graphische und farbliche Gestaltung	— Kennzeichnung des Trägers (z.B. Name) — Berechtigungszonen — Kartennummer

Bild 3 Die Karteninformationstypen

jedoch, eine zusammenfassende Liste der typischen Anforderungen an die Informationsstruktur der visuell gelesenen Karte aufzustellen *(Bild 3)*.

3. Die maschinell gelesene Karte

Welches ist nun der Sachverhalt bei einer ausschliesslich maschinell gelesenen Karte? Hier erfüllt die Karte die Funktion eines Informationsträgers zwischen Mensch und Maschine. Die Information wird maschinengerechten Charakter aufweisen müssen. Trotz dieser Auflage sind die in *Bild 3* genannten Informationskategorien festzustellen. Der Automat prüft die Echtheit der Karte, identifiziert den Kartenbenützer, indem er z. B. die der Identifizierung zugedachten Information mit einer vom Kartenbenützer gleichzeitig eingegebenen Information (*p*ersönliche *I*dentifikations*n*ummer PIN oder Körpermerkmal wie etwa Fingerabdruck) vergleicht und liest schliesslich die Daten, die er gegebenenfalls weiterleitet.

3.1 Maschinengerechte Codiermethoden

Damit man sich über die maschinengerechte Codierung für Karten im klaren ist, seien zunächst die wichtigsten Codierformen aufgezählt, ohne auf deren technische Details einzugehen:

- hochgeprägte Schrift (z. B. OCR)
- gestanzte Löcher
- magnetische Streifen
- Druck mit sog. magnetischer oder dotierter Tinte
- magnetische Löcher
- kapazitive Folien
- induktive Folien
- ferroelektrische Inserts
- radioaktive Tracers
- gedruckte Leiterbahnen
- optische Streifen (schwarz/weiss)
- Druck mit fluoreszierender Tinte
- Farbcodierung
- optische Reflektoren
- Watermark magnetics
- Drexon strip
- integrierte Schaltung
- holographische Codierung.

Eine Kombination der oben angegebenen Auswahl ist durchaus möglich. Selbstverständlich muss der Leser für die Erfassung dieser technischen Codierung ausgerüstet sein. Inwiefern die eine oder andere Methode gewählt wird, hängt, wie später gesehen werden kann, vom Sicherheit/Kosten-Verhältnis ab. Alle drei Informationskategorien, d. h. Identifizierung, Echtheit und Daten, sind in der einen oder anderen maschinengerechten Form auf die Karte zu bringen. Ein hoher Sicherheitsbedarf verlangt nach einer sophistizierten Codiermethode.

3.2. Karte und System anhand von Beispielen

Es kann nun anhand von Beispielen aus der Anwendungssparte «ID-Karte» und «vorbezahlte Karte» eine tentative Anforderungsliste für die Informationsstruktur auf der Karte zusammengestellt werden. Gerade in diesen Anwendungssparten sind klare Automationsvorteile zu erwarten.

3.2.1 Die Zutrittskontrolle

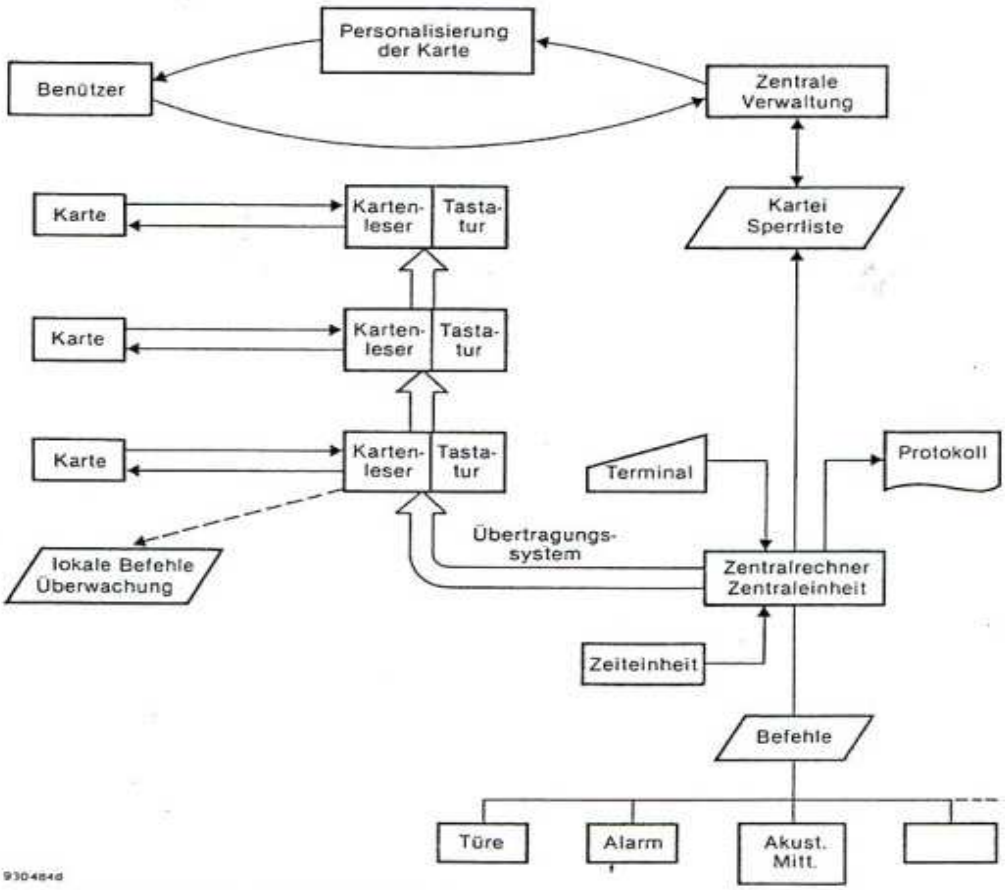
Es sei zunächst stellvertretend für Systeme mit grossem Anforderungskatalog die Zutrittskontrolle betrachtet, ohne in diesem Rahmen auf deren komplexe Problemaspekte einzugehen. Ein typischer Systemaufbau für eine zentral gesteuerte und überwachte Zutrittskontrolle ist in *Bild 4* grob skizziert.

Jede Tür ist mit einem Kartenleser versehen, der die Karteninformation prüft und liest. Diese wird on-line über eine Stern- oder Ringleitung dem Zentralcomputer zugeführt, der nach Überprüfung der Daten einen Befehl auslöst.

Das System kann so ausgelegt sein, dass die Kartenleser nur als rezeptive Peripherieelemente operieren, die die Information zur datenverarbeitenden Zentraleinheit weiterleiten, ohne selbst am Entscheidungsprozess teilzunehmen. Die Kartenleser sind sozusagen Terminals. Nachteilig für ein solches zentralisiertes System ist der Ausfall des Zentralcomputers, der zur Blockierung des ganzen Systems führt. In einem dezentralisierten System übernehmen periphere Elemente gewisse Entscheidungsfunktionen. Hiermit erreicht man eine Entlastung des Zentralcomputers und vor allem eine Überbrückung eines etwaigen Ausfalls der Zentraleinheit. Die Verlagerung der Intelligenz an die Peripherie gestattet somit off-line Betrieb des Systems.

Die Elemente des Systems sind über ein Kommunikationsnetz miteinander verbunden, das entweder mit Hilfe existierender Leitungen (z. B. Telefonleitungen) oder separaten Leitungen betrieben wird. Die Eingabe bzw. Entnahme der Information in bzw. aus dem Netz über sogenannte Modems, die die Information übertragungsgerecht modulieren bzw. demodulieren.

Die jeweils gewählten Charakteristiken des Systems, d. h. zentral/dezentral, off-line/on-line Modulationsart, Modems, beeinflussen die Informationsstruktur der Karte entscheidend, insbesondere z. B. dann, wenn die Karte nach jeder Operation mit neuer Information „beschriftet" werden soll. Als Beispiel sei hier die Möglichkeit



930484d

Bild 4 Systemstruktur eines Zutrittskontrollsystems

Identifizierung	Echtheit	Daten
Name (z.B. in OCR) ID-Nummer Körper-Merkmale, z.B. — Handgeometrie — Stimme PIN-Nummer	— Druck — Farbe — siehe Aufzählung der maschinengerechten technischen Codierformen unter 3.1	Beispiele: — Firmencode 16 Bit — Gültigkeitsdauer 4 Bit — Zeitzone 8 Bit — Ortszone 16 Bit — PIN-Ausgabe Nr. 4 Bit — ID-Nummer mit Ausgaben Nr. 20 Bit — Reserve 4 Bit Total 24 Bit 96 Bit

930+65a

Bild 5 Die Informationsstruktur der maschinengelesenen Karte

genannt, wonach nach jeder Operation der Zentralcomputer eine codierte Zufallsnummer erzeugt und über den Leser in die Karte „schreibt".

Es sollen nun die Anforderungen an die Informationsstruktur der Karte betrachtet werden. Die Identifizierungsinformation besteht aus dem Namen des Kartenbenützers, z. B. in OCR und einer ID-Nummer, die visuell und/oder maschinell gelesen werden kann. Die Dateninformation ist der Funktion der Karte entsprechend komplexer. Folgende Zusammenstellung gibt eine Reihe typischer Anforderungen mit Informationskapazität *(Bild 5)*.

Die Daten enthalten, wie aus der Bezeichnung ersichtlich ist, zusätzliche Informationen, die den Zutritt zeitlich wie örtlich festhalten. Die Identifizierung ist durch die zusätzliche Forderung an den Kartenbenützer, eine persönliche Identifikationsnummer (PIN) in die Tastatur des Lesers einzugeben, sehr sicher. Die PIN-Zahl kann eine über einen komplexen unknackbaren „Codierschlüssel" erhaltene Kombination sämtlicher Daten darstellen.

Die Echtheitsinformation spielt im Gegensatz zur ausschliesslich visuellen Karte hier eine wichtige Rolle. Die Maschinenprüfbarkeit der Echtheit kann sehr weit getrieben werden. Sie muss dabei in einem vertretbaren Sicherheit/Kosten-Verhältnis bleiben.

3.2.2 Die Benzinkarte

Als nächstes Beispiel sei nur kurz das Benzinkartensystem beleuchtet. Dieses System ist heute typischerweise ein dezentralisiertes, off-line System, dessen Peripherieelemente, d. h. der Kartenleser, mit einem kostenmässig vertretbaren Höchstmass an Intelligenz ausgerüstet werden muss. Ein Prinzipschema der Systemstruktur ist in *Bild 6* wiedergegeben.

Die Datenstruktur auf der Karte hat sehr grosse Ähnlichkeit mit derjenigen der Zutrittskarte. Karte und System müssen vor allem eine kostensparende Abrechnung gestatten. Auf eine weitere Diskussion der Systemstruktur und der Abwicklung der Prozesse muss hier verzichtet werden.

3.2.3 Die vorbezahlte Geldersatzkarte

Aus der Sparte „Vorbezahlte Karte" soll ein Beispiel der vorbezahlten Geldersatzkarte auf die Informationsstruktur der Karte hin untersucht werden. Betrachtet man das Phonocardsystem, das als Hauptfunktion das bargeldlose Telephonieren von öffentlichen Telephonstationen aus beinhaltet, ergibt sich folgendes:

Man stelle sich vor, dass die Postbetriebe z. B. am Schalter, Karten an Kunden verkaufen, die für einen bestimmten Betrag z. B. Fr. 20.— Werteinheiten enthalten. Der Kartenbenützer führt die Karte in den Leseschlitz des im Telephonautomaten integrierten Kartenlesers ein, wobei ihm der Wertstand der Karte angezeigt wird. Der Kartenleser entwertet nun ab Start der Gesprächsverbindung pro Taximpuls eine Werteinheit der Karte. Die Anforderungen an die Informationsstruktur lässt sich auch ohne Diskussion der technischen Details leicht erkennen. Die Identifizierungsinformation fällt weg, da die Karte anonymen Charakter besitzt. Die Karte muss jedoch eindeutig dem Systemträger zugeordnet werden können. Die Dateninformation enthält die Kennzeichnung des Systemträgers und den Wertstand. Der Echtheitsinformation kommt allerhöchste Bedeutung zu, da die Karte sozusagen Bargeldfunktionen erfüllt. Die Echtheitsinformation muss also weitmöglichst Kopien, Veränderungen, Falsifikate der Karte verhindern. Zudem muss die Karte als Wegwerfkarte kostengünstig sein.

Mit diesem letzten Beispiel ist die Sicherheit der Karte angesprochen, auf die im weiteren näher eingegangen wird.

4. Sicherheit von Karten und Kartensystemen

Die Sicherstellung einer betrugsfreien Operation von Kartensystemen bedingt die Ausarbeitung eines wohldurchdachten Sicherheitskonzeptes. Die Sicherheit des Kartensystems bestimmt das schwächste Glied in der Sicherheitskette. Anhand einer Aufstellung der Systematik der Delikte stellt man fest, dass sich eine Sicherheitsgefährdung auf verschiedenen Ebenen abspielen kann, nämlich in der Logistik des Kartenumlaufs ab Herstellung bis zur Vernichtung der Karte, in der Hardware- und Software-Manipulation des Systems inklusiv der Karte. Die Betriebssicherheit im Sinne der Betriebszuverlässigkeit sei hier nicht berücksichtigt.

4.1 Sicherheit im Kartenumlauf

Die Kartenumlaufslogistik ist in *Bild 7* festgehalten. Man unterscheidet fol-

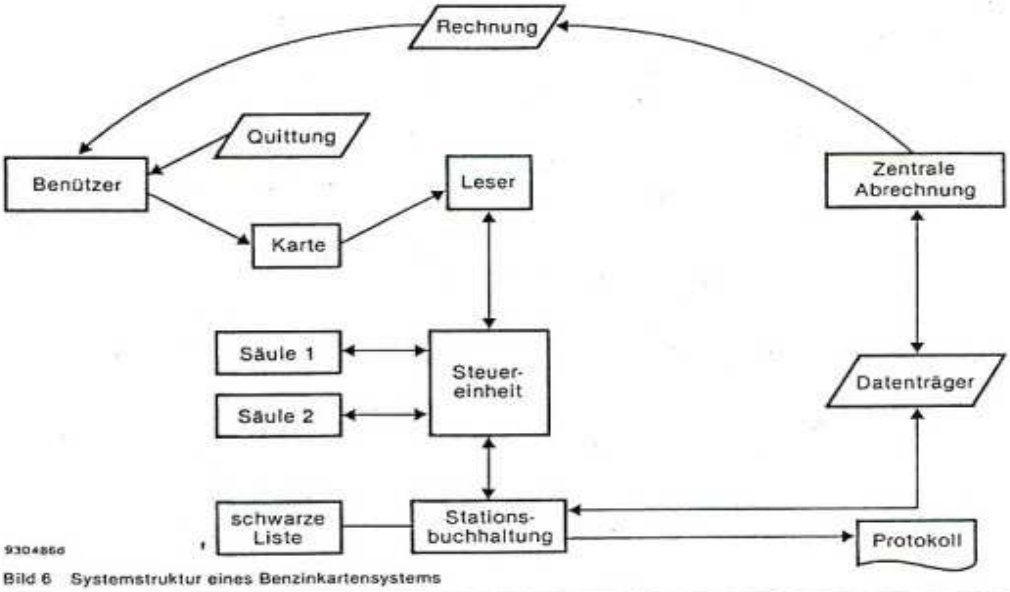


Bild 6 Systemstruktur eines Benzinkartensystems

gende wichtige Umlaufstellen: Hersteller, Träger des Kartensystems (oder Systembenützer), Händler zum Vertrieb oder Verkauf von Karten, der Kartenbenützer und die visuelle und/oder maschinelle Kontrolle der Karte und deren Vernichtung.

Die Sicherheit muss schon beim Kartenhersteller gewährleistet sein. Integrität und Sorgfaltspflicht sind gegenüber dem Systemträger wie dem Kartenbenützer unbedingte Erfordernisse. In der Sparte der Check-, Kredit- und Identitätskarte bedingt der Personalisierungsvorgang der Karte ähnliche Vorkehren wie bei der Herstellung von Banknoten und Wertpapieren. Der Zugang zu Blankokarten soll für unbefugte Personen unmöglich sein. Die Aufbewahrung dieser Karten muss sicher sein. Ähnliches gilt selbstverständlich für den Träger des Systems.

Auf der Händler- oder Vertriebsebene sind alle Kartentypen, Checkkarte, Kreditkarte, ID-Karte wie vorbezahlte Karte äusserst gefährdet. Hier müssen strenge Massnahmen zur Sicherung der Karte getroffen werden. Der Kartenbenützer kann die Rolle des Gefährdenden wie diejenige des Gefährdeten spielen. In der letzteren Rolle kann er Wesentliches zu seinem Schutz tun, z. B. die PIN-Nummer bei der Zutrittskarte nicht notieren (gar auf der Kartenrückseite) etc.

Die Kontrolle der Karte und deren Ausserkraftsetzung kann logistisch gesehen Probleme schaffen. Zieht man eine Karte nach ihrer Gültigkeit ein oder überlässt man sie dem Kartenbenützer? Soll man z. B. die Rückgabe mit einem Pfand „ermutigen" oder gar erzwingen (keine neue Karte, bevor die alte zurückgegeben ist!)? Dies sind wichtige Aspekte, die es für visuell und/oder maschinell kontrollierte Karten zu überlegen gibt.

4.2 Die Hardware-Sicherheit

Die Sicherheit auf der Hardware-Ebene betrifft vor allem die visuellen und maschinengerechten Echtheitsmerkmale und deren maschinelle, elektronische Prüfvorrichtungen sowie generell die apparativen, bautechnischen Elemente des ganzen Kartensystems. Die Karte muss eine hohe Sicherheit gegen Betrug aufweisen, d. h. sie muss schwer nachahmbar, schwer reproduzierbar (Herstellung von Doppeln) und schwer veränderbar sein. „Schwer" bedeutet im vorliegenden Fall, dass die zum Nachahmen, Reproduzieren und Verändern der Karte einzusetzenden Mittel erheblich sind. Die Sicherheit besteht in diesem Fall darin, dass die Anstrengungen für eine Fälschung in keinem Verhältnis zum erhaltenen Wert stehen würden.

Übergeordnete Grosssysteme, wie z. B. ausgedehnte Zutrittskontrollsysteme, bedürfen eines in allen Details wohldurchdachten Sicherheitskonzeptes. Die hauptsächlichen Gefahren sind hier in der Manipulation der Geräte und der Anlagen zu sehen. Eine z. B. vom Kartenbenützer durchgeführte technische Manipulation (Verhinderung, Veränderung) des Kartenlesers, so dass dieser z. B. auch ohne Karte ein gültiges elektronisches Signal weiterleitet, ist selbstverständlich unbedingt zu verunmöglichen. Ebenfalls ist eine Täuschung des Lesers durch Eingabe von maschinengerechten Falsifikaten zu verhindern.

Die Hardware-Sicherheit betrifft nicht nur den Kartenleser sondern ebenfalls sämtliche anderen maschinellen oder elektronischen Einrichtungen des Systems.

4.3 Die Software-Sicherheit

Eine zentrale Wichtigkeit kommt der Software-Sicherheit zu. Diese betrifft sämtliche informationsführende, -verarbeitende und -speichernde Medien des gesamten Systems. Das unbefugte Abrufen von Daten, Anzapfen von Informationsleitungen zwecks Injektion veränderter oder falscher Informationen oder zwecks Auffinden von Algorithmen sind Gefahrenmomente, mit denen sich die Computerfachleute mehr und mehr auseinandersetzen müssen. Mit steigender Komplexität der Systeme muss grösste Aufmerksamkeit der Absicherung der Daten und somit der Privatsphäre gewidmet werden.

Konzentriert man sich im besonderen auf die interessierende Sicherung der Information auf der Karte, so muss man die Widerstandsfähigkeit der einzelnen Informationstypen, d. h. Identifikation, Echtheit, Daten gegenüber Gefahrenmomenten analysieren. In *Bild 8* wird die Widerstandsfähigkeit der Informationstypen gegen allgemeine Gefahren und Verbrechen tabellarisch dargestellt.

Der Tabelle in *Bild 8* kann man folgendes entnehmen:

Man kann die Identifikationsinformation so weit steigern, bis sie einen guten Widerstand gegen generelle Gefahrenmomente aufweist. Dort, wo die Sicherung trotz bestmöglichen Massnahmen noch problematisch ist (z. B. Punkte 7 und 8 in *Bild 8*) ist eine weitere Absicherung durch eine adäquate Echtheitsinformation möglich. Die Dateninformation hingegen braucht keine hohe Widerstandsfähigkeit, dort wo sie ausnahmsweise vonnöten ist, kann diese durch Verflechtung mit der Echtheitsinformation erreicht werden.

Das oben Gesagte gilt besonders für die Check-, Kredit- und ID-Karten, wo die Identifikationsinformation prädominant ist. Anders verhält es sich mit vorbezahlten Karten. Da diese Karten anonym und übertragbar sind, entfällt die durch eine Identifikationsinformation gegebene Schutzwirkung. Die Echtheitsinformation bildet den einzig möglichen Widerstand und muss auf höchstmöglichem, jedoch kostenmäs-

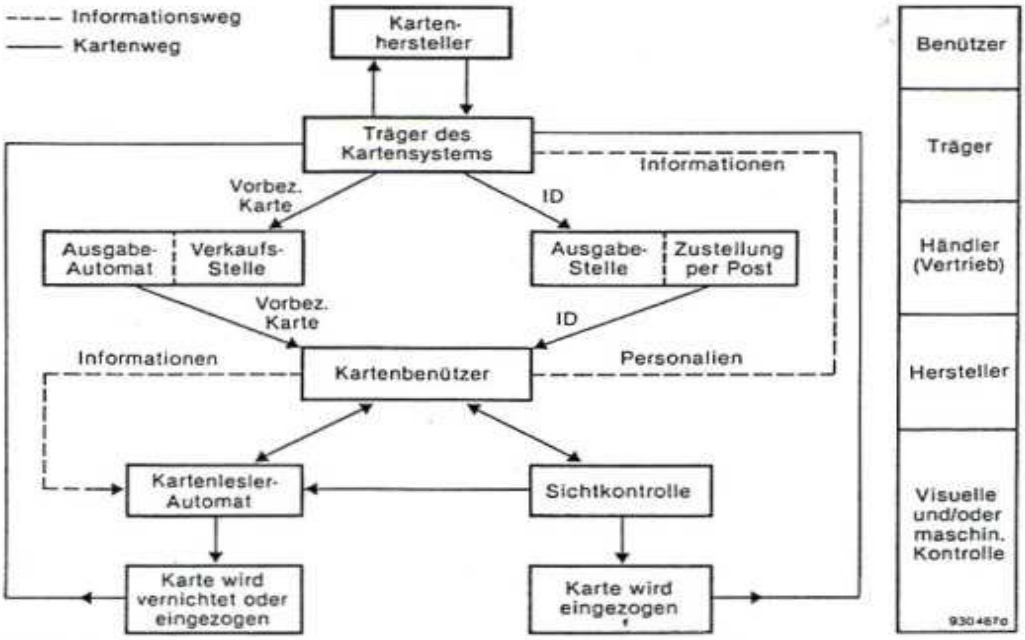


Bild 7 Struktur des Kartenumlaufs

sig vertretbarem Niveau gehalten werden. Die Karte besitzt Geldersatzfunktion und ist demzufolge ähnlichen Gefahren ausgesetzt wie die Banknote.

5. Kosten der Sicherheit

Abschliessend seien noch einige Gedanken zur Sicherheit und deren Kosten wiedergegeben. Eine absolute Sicherheit existiert nicht. Sicherheit ist teuer, aber sie ist ihren Preis wert. Die Sicherheit soll den Betrug kostspieliger machen, als den durch Betrug erwirkten Gewinn. Es lohnt sich also nicht, die Kosten der Antibetrugsmassnahmen über diejenigen der Betrugskonsequenzen wachsen zu lassen.

Letzten Endes gilt es, einen wirtschaftlichen Kompromiss zu suchen, dessen Gleichgewicht aber dynamischer Natur sein muss: Massnahmen rufen bekannterweise nach Gegenmassnahmen.

Autor: J.-F. Moser
LGZ Landis & Gyr Zug AG
CH-6301 Zug (Schweiz)

Gefahren, Fälschungen, Verbrechen und deren Folgemöglichkeiten	Identifikation	Echtheit	Daten
1. Verlust der Karte (in «falsche Hände» geraten)	gut (mit Körpermerkmal und PIN)	schlecht	schlecht
2. Diebstahl der Karte	gut (mit PIN)	schlecht	schlecht
3. Diebstahl der Information	gut aber nicht unschlagbar z.B. Fingerabdruck kann gestohlen werden, PIN durch Zusehen oder Zuhören	je nach Technologie	
4. Weitergabe an Unberechtigte	gut (mit Ausnahmen)	schlecht	schlecht
5. Erpressung der Information	gut (mit Ausnahme) der PIN-Nummer	schlecht (wegen 4.)	schlecht (wegen 4.)
6. Nötigung (Unberechtigter zwingt Berechtigten)	schlecht (ausg. Alarm PIN)	schlecht	schlecht
7. Fehlberechtigung oder Fehlverweigerung	problematisch weil sichere Körpermerkmale heute nicht mit erforderlicher Sicherheit maschinell identifiziert werden können)	gut	problematisch
8. Vervielfachung, Änderung, Falsifikat	gut, aber nicht ohne Problem	gut aber stark von Technologie abhängig gemäss Liste unter 3.1 in steigender Widerstandsfähigkeit: z.B. gestanzte Löcher: schwach; magnetischer Streifen: schwach; Hologramm: sehr gut.	schlecht kann aber durch Verflechtung mit Echtheit gehoben werden

Bild 8 Widerstandsfähigkeit der Infotypen gegen Gefahrenmomente